

School of Design and Informatics

BSc Ethical Hacking, 2022/23

**An Evaluation of Modular Incident Response Plans for Efficient Cyber Incident Mitigation in Businesses**

**NotPetya Analysis**

**Author:** Martin Georgiev **Supervisor**: Natalie Coull

Head of Division of Cybersecurity Abertay

Contents

[1 Introduction 2](#_Toc134539697)

[**1.1** **Background** 2](#_Toc134539698)

[**1.2** **Aims** 2](#_Toc134539699)

[2 Procedure 3](#_Toc134539700)

[**2.1** **Overview** 3](#_Toc134539701)

[**2.2** **Static Analysis** 3](#_Toc134539702)

[**2.2.1** **File Hashes Discovery** 3](#_Toc134539703)

[**2.2.2** **String Extraction** 4](#_Toc134539704)

[**2.2.3** **In-depth Inspection** 6](#_Toc134539705)

[**2.2.4** **Dropped Files** 8](#_Toc134539706)

[**2.3** **Dynamic Analysis** 10](#_Toc134539707)

[**2.3.1** **Detonation Symptoms** 10](#_Toc134539708)

[**2.3.2** **Network Symptoms** 12](#_Toc134539709)

[**2.3.3** **Host Symptoms** 13](#_Toc134539710)

[**2.3.4** **Memory Analysis** 15](#_Toc134539711)

[**2.4** **Yara Rule** 16](#_Toc134539712)

[3 Results 18](#_Toc134539713)

[**3.1** **Static Analysis** 18](#_Toc134539714)

[**3.2** **Dynamic Analysis** 18](#_Toc134539715)

[4 Discussion 19](#_Toc134539716)

[**4.1** **General Discussions** 19](#_Toc134539717)

[**4.2** **Countermeasures** 19](#_Toc134539718)

[**4.2.1** **Pre-infection Countermeasures** 19](#_Toc134539719)

[**4.2.1.1** **Frequent Security Updates** 19](#_Toc134539720)

[**4.2.1.2** **Distinguishing Spam** 19](#_Toc134539721)

[**4.2.1.3** **Blacklisting Unknown Applications and Anti-Virus Software** 19](#_Toc134539722)

[**4.2.1.4** **File Scanners and IDS** 20](#_Toc134539723)

[**4.2.1.5** **Webserver Methods** 20](#_Toc134539724)

[**4.2.2** **Post-infection Countermeasures** 20](#_Toc134539725)

[**4.2.2.1** **Data Backups** 20](#_Toc134539726)

[**4.2.2.2** **Refuse Ransom Payments** 20](#_Toc134539727)

[5 Conclusion 21](#_Toc134539728)

[**5.1** **Conclusion** 21](#_Toc134539729)

[**5.2** **Future Work** 21](#_Toc134539730)

[6 References 22](#_Toc134539731)

[7 Appendices 24](#_Toc134539732)

[**Appendix A – Strings** 24](#_Toc134539733)

[**Appendix B – Memory Forensics** 24](#_Toc134539734)

[**Appendix B1 – Command Line** 24](#_Toc134539735)

[**Appendix B2 – Environmental Variables** 28](#_Toc134539736)

[**Appendix B3 – Malfind** 31](#_Toc134539737)

[**Appendix B4 – Privileges** 31](#_Toc134539738)

[**Appendix B5 – Processes** 34](#_Toc134539739)

[**Appendix C – Network Data in CSV Format** 34](#_Toc134539740)

[**Appendix D – Yara Rule** 46](#_Toc134539741)

The report was adapted from the CMP320 Mini Project **Analysis and comparison of WannaCry and NotPetya** (Georgiev, 2022)with multiple changes. Advanced analysis techniques such as debugging and reverse engineering were omitted, while Memory Analysis and Packer Identification were included in the report.

# **Introduction**

## **Background**

NotPetya (or ExPetr) surfaced in 2017, about a month after the infamous WannaCry attack. Despite infecting fewer machines than WannaCry, NotPetya caused much more damage. The malicious software was distributed through a backdoor in an update for the Ukrainian accounting software called M.E.Doc. Unlike its predecessor, Petya, NotPetya used a modified version of Mimikatz to steal passwords before encrypting the Master Boot Record (MBR) of the drive. Some experts believe that NotPetya was not ransomware, but a wiper disguised as one. Researchers claim this because the installation ID of NotPetya contained randomly generated data encoded in BASE58 format, which made it impossible to extract a decryption key, rendering the encryption irreversible. (Ivanov and Mamedov, 2017)

NotPetya could spread like a worm by leveraging the EternalBlue vulnerability. The exploit was originally discovered by the NSA then later leaked by the Shadow Brokers hacker group. This exploit took advantage of a critical vulnerability in SMBv1, which allowed attackes to execute arbitrary code remotely (RCE). To implant a backdoor on the targeted machines and gain access, the exploit was combined with DoublePulsar. (Hurley and Sood, 2017)

## **Aims**

The report aims to provide the reader with an analysis of a NotPetya sample with the simplified Malware Analysis and Digital Forensics Framework and how it can show them information about its capabilities. The information can be used to take precautions until a professional team starts handling the case. It can also be given to the team handling the incident as this could greatly decrease the time to respond to the attack. The report will be split into three major sections to efficiently achieve the goal:

* **Procedure** – Analysis of the sample using the methodology and creation of a Yara rule to detect its signature
* **Results** – Overview and summary of the procedure and its subsections
* **Discussion** – General discussion and appropriate countermeasures

# **Procedure**

## **Overview**

As the developed methodology is aimed at small and medium-sized businesses that may not have a specialised response team due to budget constraints, the procedure will attempt to obtain as much intel as possible with simple techniques and tools. This will ensure that even users without significant technological knowledge can seamlessly follow it without significant difficulties. Considering the beforementioned requirements, an advanced static and dynamic analysis will not be performed on the sample as they require extensive knowledge of how computers operate, as well as high and low-level programming languages (JavaScript, C++, Assembly, etc.)

The hybrid analysis will be conducted on the sample in a safe testing environment. The static analysis will be achieved with a multitude of techniques and tools – obtaining file hashes, inspecting any human-readable strings within the binary (**Strings** (Russinovich, 2021) and **Floss** (Ballenthin, 2016)), analysing the executable’s library imports, functions and file entropy (**PEStudio** (Fox, 2021), and checking whether any known file packers have been used (**Exeinfo PE** (ALS, 2023)).

The Dynamic and Digital Forensic analysis will be combined as both can be done simultaneously. This section will cover the post-execution behaviour of the malicious sample – inspection of system modification (deleted/created/altered files, registries; PowerShell cmdlets execution, detection evasion and persistence mechanisms) with **Procmon**, possible network propagation or attempted communication with a **C&C** (**TCPView** (Russinovich, 2022), **Inetsim** (Hungenberg and Eckert, 2007)and **Wireshark** (Wireshark, 1997 – Present Day)). Additionally, analysing the system’s memory could display hidden processes, stolen data stored in the clipboard, possibly recover encryption keys and many more (**Volatility** (Volatility Foundation, 2020) and **WinPMem** (Cohen, et al., 2019)).

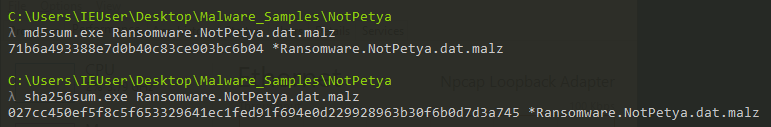
In the end, the obtained intel will be used to create a **Yara** (VirusTotal, 2013) rule for signature scanning that can then be incorporated with a scanner such as Strelka for passive file metadata scanning.

## **Static Analysis**

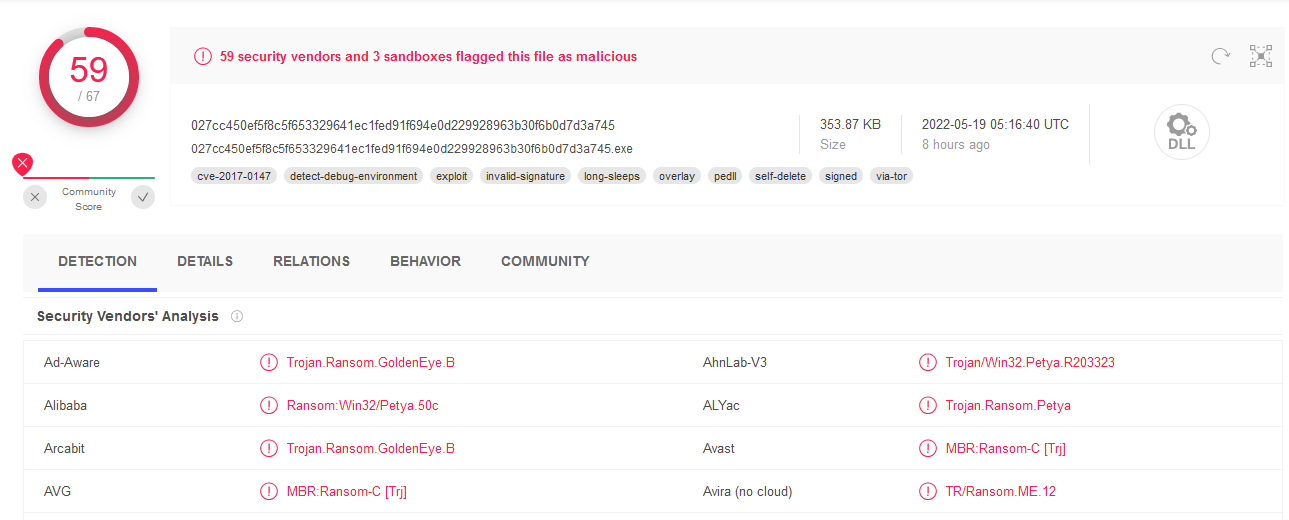
As mentioned in the previous section, the analysis will start with the static analysis of the sample. The basic static analysis provides limited information about the malware’s functionality. This, however, is often enough in introducing analysts with a base overview of the malicious software’s capabilities.

### **File Hashes Discovery**

To obtain the hashes of the malware, tools such as **md5sum.exe** and **sha256sum.exe** can be used from the command prompt. They will display the MD5 and SHA256 hashes of the sample respectively. The user can then copy them and check them in VirusTotal (VirusTotal, 2004 – Present Day). This will check the databases of multiple antivirus vendors and display any matching results. (**Figure 2.2.1** and **Figure 2.2.2**)



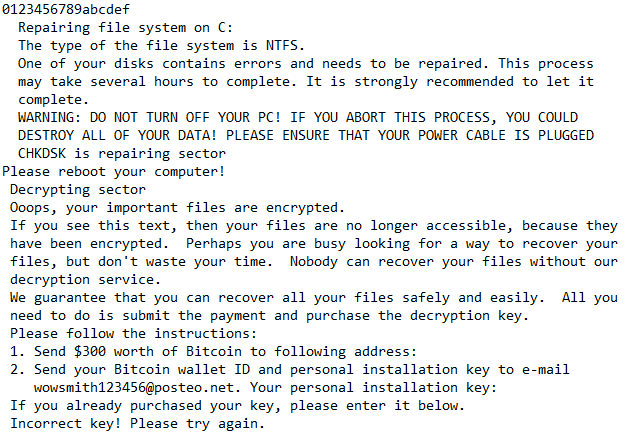
***Figure 2.2.1*** *– Obtaining MD5 and SHA256 hashes.*



***Figure 2.2.2*** *– VirusTotal indicating the sample is malicious.*

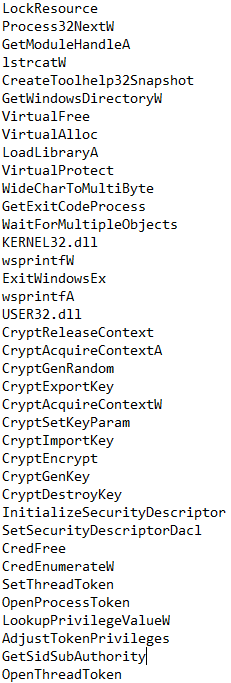
### **String Extraction**

Human-readable strings can be extracted from files with a variety of tools. Some of the most common ones are **strings** (Russinovich, 2021) and **floss** (Ballenthin, 2016). In some cases, **floss** may be a better alternative to the former tool as it attempts to de-obfuscate and decode any strings which were intentionally made hard to read. The tool also has a multitude of flags for data filtering. In this case, **-n** was used as this puts a minimum character length of the extracted strings. The analyst set the length to **8** as they were interested in possible sentences, links and/or imported functions/libraries. The output was piped onto a text file (with **>**) to allow easier analysis and further filtering. After utilising floss once more, the tester successfully extracted the strings from the binary. The output file ([**Appendix A**](#_Appendix_A_–)) revealed two key pieces of information: a ransom message and an email address (wowsmith123456@posteo.net) that could be used by the victim to reach out to the attacker if necessary. (**Figure 2.2.3**)



***Figure 2.2.3*** *– Ransom message and email address.*

NotPetya seemed to utilise various ransomware-related APIs for encryption, service and file manipulation, and internet connectivity. Additionally, the malware called upon several other functions that shed light on its overall functionality. These included privilege lookup and adjustment, window exiting, resource locking, and DHCP-related functions (**Figure 2.2.4**). The functions will be further discussed in section [**2.2.3 In-Depth Inspection**](#_In-depth_inspection).



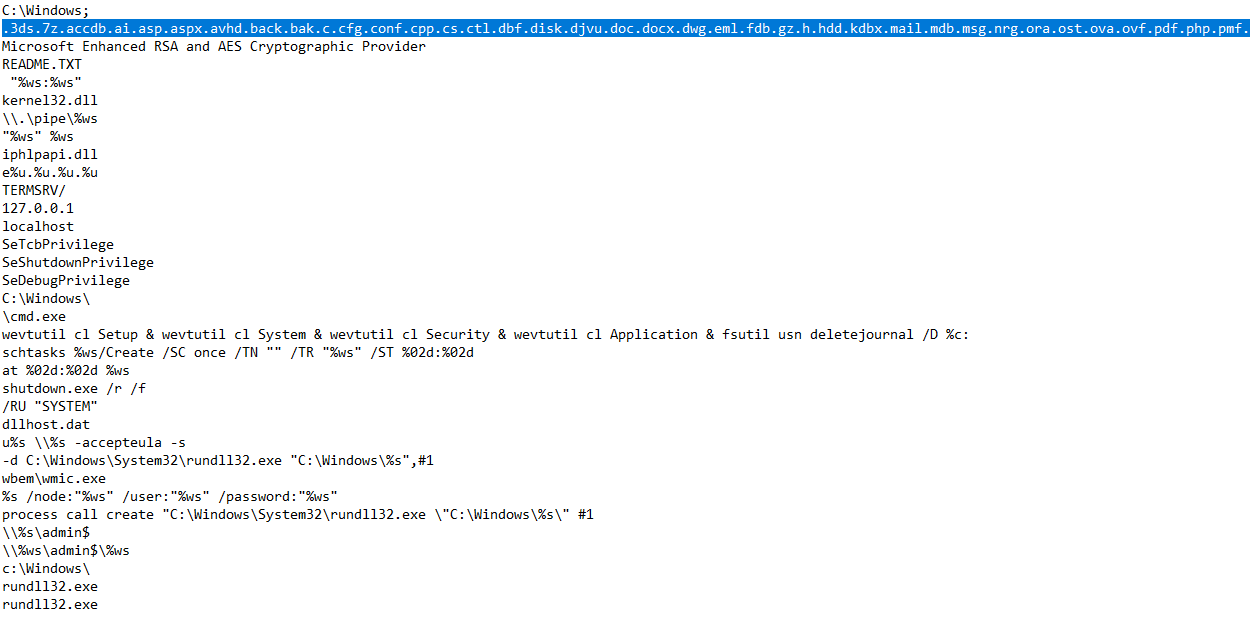
***Figure 2.2.4*** *– Part of the employed libraries and functions.*

Upon further examination of the extracted strings, the analyst identified all file extensions that were potentially targeted by the malware. These included executables, configuration files, virtual machine files, backups, emails, and virtual disks created by virtualisation software. Notably, the malware did not affect executables or system files, likely to avoid corrupting the operating system and ensuring persistence while allowing it to propagate through the network.

Several commands were listed below the extensions, with the first calling two dynamic-link libraries - kernel32.dll and iphlpapi.dll. Subsequently, **wbem/wmic.exe** (Windows Management Instrumentation) was called, followed by obtaining the node, username, and password. This suggests that the ransomware had credential dumping capabilities, with "TERMSRV/" also present in the strings, indicating the potential for the malware to propagate itself through RDP accounts.

The sample then used SeTcbPrivilege, SeShutDownPrivilege, and SeDebugPrivilege, providing access to resources based on the infected account's authorisations, shutdown and debugging privileges, and retrieving system logs from Setup, System, Security, and Application before clearing them with "**wevtutil cl**" and deleting the USN Journal with "**fsutil usn deletejournal /D %c:**". This would remove all logs and information regarding changes in files on that specific volume.

Finally, NotPetya scheduled a shutdown and ran a few commands as a system user, including one to automatically run the malware after propagation through the network **- u%s \\%s -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\%s",#1**. Ultimately, the malware appeared to create a rundll32.exe process call within the Windows directory. Rundll32.exe is a Windows executable that runs 32-bit DLL files. (**Figure 2.2.5**)

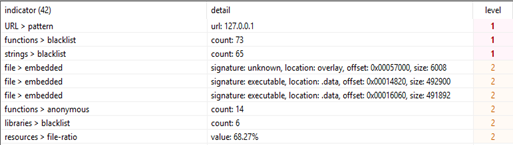


***Figure 2.2.5*** – Affected file extensions and executed commands.

During the analysis, the analyst also came across a file name - perfc.dat. Further research revealed a connection between the ransomware, its killswitch, and this file. (Symantec, 2017) As a result, the tester renamed the file from its SHA256 hash to perfc.dll.

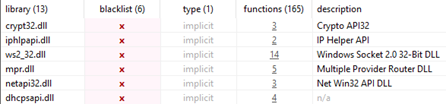
### **In-depth Inspection**

After analysing the string, the tester proceeded to load the sample into PEStudio. The researcher inspected the indicators and discovered three critical and six medium issues. The more dangerous markers included a URL (127.0.0.1), suspicious strings and functions. The medium ones revealed additional potentially dangerous libraries, three embedded files (two of which were executables), and one file with an unknown signature. Additionally, the resources compared to the file size were 68.27% (**Figure 2.2.6**).



***Figure 2.2.6*** *– NotPetya malicious indicators.*

In the previous section, the researcher mentioned that NotPetya utilised dangerous libraries related to ".dll" loading and the Windows IP Helper – specifically, ws2\_32.dll and iphlpapi.dll. However, the binary also employed four other libraries – crypt32.dll, mpr.dll, netapi32.dll, and dhcpsapi.dll (**Figure 2.2.7**). Crypt32.dll contains numerous functions from CryptoAPI (Certificate and Cryptographic Messaging), while mpr.dll (Multiple Provider Router) facilitates communication between Windows and the network providers installed on the system. Additionally, netapi32.dll enabled the ransomware to access a Microsoft network, and dhcpsapi.dll provided a list of the DHCP servers in the directory service. These libraries suggested that the malware was designed for network propagation within the victim's network.



***Figure 2.2.7*** *– Blacklisted libraries.*

The malware employed seventy blacklisted functions (out of one hundred and sixty-five). These functions granted it capabilities similar to the infamous ransomware WannaCry, such as file manipulation, execution, service and synchronisation, and socket functions sourced from non-blacklisted libraries (kernel32.dll and advapi32.dll), as well as the same libraries utilised by some ransomware samples. The remaining four libraries conferred the following abilities on the malware, according to Windows documentation from 2020-2022:

• **crypt32.dll** – string conversion and decoding (**Figure 2.2.8**)

• **mpr.dll** – network/connection enumeration, connection manipulation (**Figure 2.2.9**)

• **netapi32.dll** – NetAPIBuffer manipulation and server enumeration (**Figure 2.2.9**)

• **dhcpsapi.dll** – subnet/subnet client enumeration, and RPC memory manipulation (**Figure 2.2.10**)



***Figure 2.2.8*** *– crypt32.dll functions.*

**

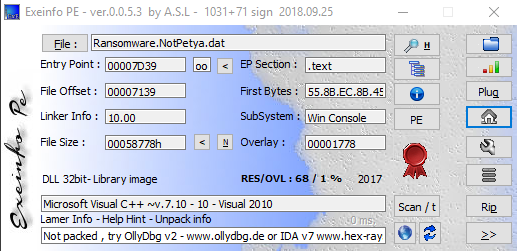
***Figure 2.2.9*** *– netapi32.dll and mpr.dll employed functions.*

**

***Figure 2.2.10*** *– dhcpsaip.dll utilised functions.*

PEStudio did not blacklist the functions from the final dynamic-link library, dhcpsapi.dll, possibly because they were not recognised as malicious. However, the researcher identified one suspicious function from kernel32.dll - DeviceIoControl (Microsoft, 2022). This Windows function permits direct access to a physical drive without interacting with the operating system. It enables the application to unmount volumes, determine drive geometry (such as the number of sectors and bytes per sector), and identify the number of disks/partitions. The malware took advantage of this access to corrupt crucial data and then replaced the bootloader with the corrupted data - this contributed to classifying NotPetya as a wiper masquerading as ransomware.

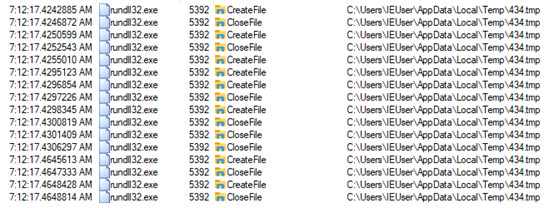
Opening the file in ExeInfoPE revealed that the EP Section was in **.text**, indicating that the malware did not use any type of file packer for compression. (**Figure 2.2.11**)



***Figure 2.2.11*** *– ExeInfoPE results.*

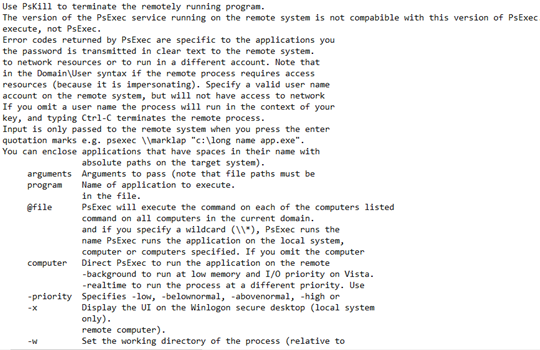
### **Dropped Files**

The wiper also generated two additional files - **434.tmp** in the Temp directory and **dllhost.dat** in the Windows directory. Further investigation by the tester revealed the purpose and functionalities of these files. The former file, 434.tmp (**Figure 2.2.12**), was a temporary file that shared similar code with **Mimikatz**, a credential dumping tool. This file was created and deleted multiple times from the directory, and its name changed with each execution of the malware. Unfortunately, the analyst could not obtain the file because all logs, including file recovery, were deleted by the malware. ([**Section 2.2.2 String Extraction**](#_String_Extraction))



***Figure 2.2.12*** *– Dropped 434.tmp file attempting credential theft.*

The latter file, **dllhost.dat**, was analysed by extracting the strings. It appeared to be a disguised version of **PSExec** - a tool that permits remote execution of processes and console applications, as well as launching interactive command prompts and displaying information about remote hosts, such as IP configurations. The analyst concluded that the malware might have used this file, given its location and disguise, to execute the copied binary on other hosts after scanning the **admin$** shares of the network. (**Figure 2.2.13**)



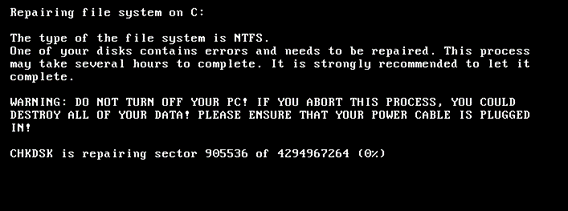
***Figure 2.2.13*** *– PSExec capabilities in dllhost.dat.*

## **Dynamic Analysis**

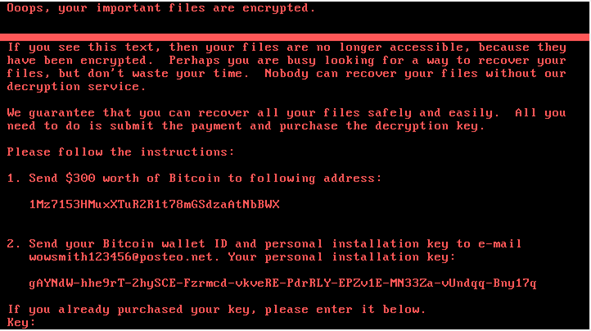
Dynamic analysis of malware is achieved by detonating the sample in a safe environment (or surveying an already compromised environment) to see how it behaves on a local and network level. This may be dangerous if the safe environment is not properly set up as it may allow the malicious software to propagate to the physical machine, the user’s network, and possibly even other connected networks.

### **Detonation Symptoms**

In [**Section 2.2.2 String Extraction**](#_String_Extraction), the researcher identified that a different approach was needed to execute the wiper. The analyst used the command found during the strings analysis to launch the binary, specifically: "**rundll32 Ransomware.NotPetya.dll, #1**". This command utilised the rundll32.dll (Microsoft, 2021) to execute the malware with an entry point of 1. While there were no visible signs of infection after the malicious file removed itself upon detonation, the tester decided to reboot the machine. However, the boot process was unsuccessful, and a fake error message appeared on the disk (**Figure 2.3.1**). Despite attempting to repair the device, the process was unsuccessful, and in the end, the ransom message was displayed (**Figure 2.3.2**). The fake repair message and the ransom message had the same fonts, and the repair message showed unrealistic sector numbers – over 4 billion for an 80GB drive. An 80GB drive should have around 167,772,160 sectors, approximately 4.1 billion less than what was displayed. Furthermore, during the fake repair process, the malware caused additional damage to the system.

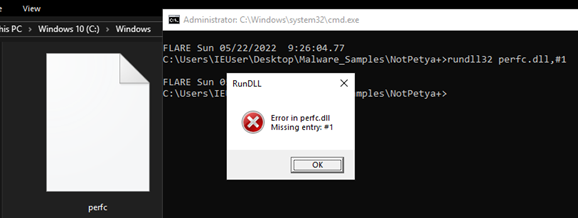


***Figure 2.3.1*** *– Fake disk repair message.*

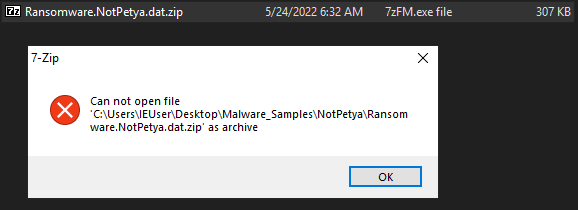
**

***Figure 2.3.2*** *– Ransom message after unsuccessful “repair”.*

To prevent the malware from executing fully, the analyst created a file named "**perfc**" in the "C:\Windows" directory. A similar file name was found in the Floss output, but the file had a .dat extension. Several analysts discovered this local killswitch and provided different files for the vaccine, including **perfc**, **perfc.dll**, and **perfc.dat**. While all three files were successful, the first two produced an error indicating that the .dll file had no such entry point (**Figure 2.3.3**). The killswitch files successfully prevented the ransomware from executing. However, the system was infected if the malware was run again after the researcher deleted the previously noted files. Notably, running NotPetya as a regular user encrypted the files (**Figure 2.3.4**) without damaging the Master Boot Record, meaning that victims could still access their machine while losing the affected files.



***Figure 2.3.3*** *– Killswitch results.*

**

***Figure 2.3.4*** *– Encrypted file.*

### **Network Symptoms**

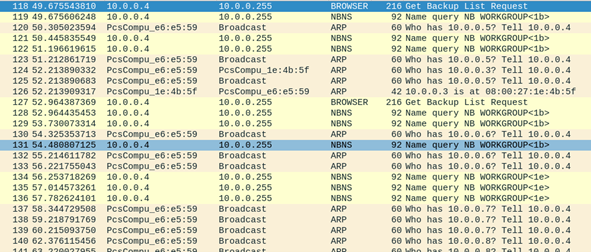
The static analysis on NotPetya identified its additional propagation features in the following four blacklisted libraries – **crypt32.dll**, **mpr.dll**, **netapi32.dll**, and **dhcpsapi.dll**. These libraries enabled NotPetya to interrogate entire networks and communicate with them.

To monitor the packets sent by NotPetya to the custom network, the analyst used **TCPView** and **Wireshark/Inetsim**. The researcher inspected TCP connections opened by the malware with **TCPView**. NotPetya did not open multiple connections in different subnets; instead, it attempted to connect to **APIPA** (169. addresses) and addresses within the same subnet as the infected machine (10.0.0.0/24). The malware targeted two SMB ports on each IP address (**139** and **445**) while iterating the last octet of the address by one (**Figure 2.3.5**), revealing its movement after impersonating the infected machine. The process was named rundll32.exe due to the execution of the wiper with that binary.



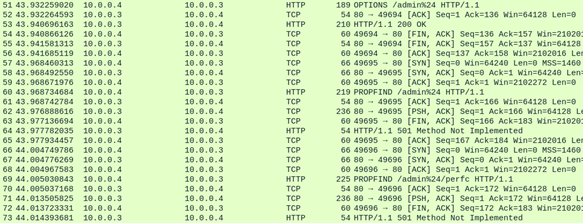
***Figure 2.3.5*** *– TCPView results.*

Using Wireshark, the same behaviour observed with TCPView was inspected. ([**Appendix C**](#_Appendix_C_–)) NotPetya initially requested a backup list from the network's broadcast address using the Browser protocol, which maintains an up-to-date list of hosts on the local network and provides it to the requesting application. Additionally, the malware attempted to query the workgroups on the system using the **NBNS** (NetBIOS Name Service) protocol. NotPetya then used the **ARP** (Address Resolution Protocol) protocol to interrogate each IP, sending three packets for each (**Figure 2.3.6**). The ARP requests stopped after reaching the final address of the subnet (10.0.0.254) without iterating the third octet of the IP address or moving to a different subnet.



***Figure 2.3.6*** *– Broadcast address interrogation.*

The analyst also observed a different propagation method - through a web server. Using INetSim to simulate a web server, NotPetya sent a decoy page upon request. The tester examined the malware's actions, including an **OPTIONS** request to the root and admin directories. These requests provided the malware with information on available methods - **GET**, **HEAD**, **POST**, and **OPTIONS**. Despite this, NotPetya attempted to use the **WebDAV PROPFIND** method to browse the web directories and discover hidden files. The malware made two PROPFIND requests - one for the entire directory and one for a specific file named "perfc." The first PROPFIND request resulted in an error (501 Method Not Implemented) because it was not among the available methods, which suggested that the malware might have more brute forcing capabilities. The second PROPFIND request indicated that the wiper checked whether the webserver was infected. (**Figure 2.3.7**)

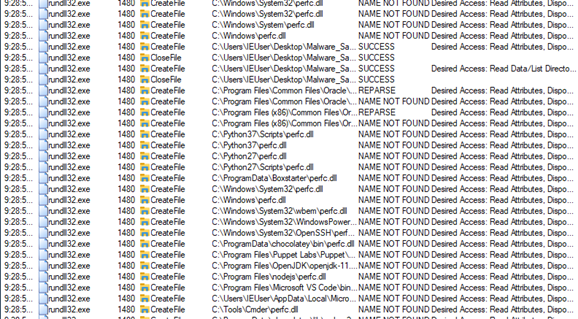


***Figure 2.3.7*** *– Server interrogation.*

NotPetya repeated this process five times (three for the directory and two for the file) before switching to interrogating the network. A CSV version of the packet capture is available in Appendix C. The server could not be infected because it was running a Linux operating system, which does not natively support .dll files.

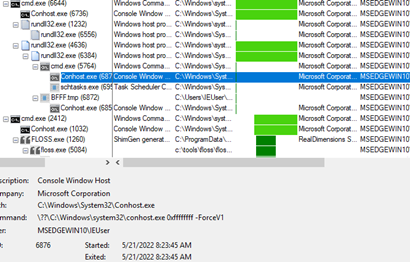
### **Host Symptoms**

The disguised ransomware created perfc.dll in multiple directories, all containing files targeted during the encryption process. These files were then deleted using a **CloseFile** operation, which suggests that they might have been used to encrypt files and then deleted to hide any malicious activity. Notably, this behaviour differed from other ransomware, which leave artefacts in all affected folders (**Figure 2.3.8**). Finally, the process created a file named "perfc" without deleting it. This file served as an indicator of whether the system was already infected.



***Figure 2.3.8*** *– Perfc creation in multiple directories.*

Upon inspecting the process tree, the researcher identified that the **434.tmp** file and a scheduled shutdown (set for one hour after the malware's activation) were both accompanied by an executable called conhost.exe, which ran the command "**conhost.exe 0xffffffff -ForceV1**" (**Figure 2.3.9**). **Conhost** is a service that allows the command prompt to work with Windows Explorer. The "-ForceV1" attribute of the command directly obtains information from the Kernel space connected to the console application (Gonzales, 2020). The malware used the command to perform a check; if no active sessions were attached to the console, the instruction would return 0xffffffff (equivalent to -1) (DarkMatter, 2019). It allowed the malware to be notified if an error occurred, possibly leading to the restart of the processes.

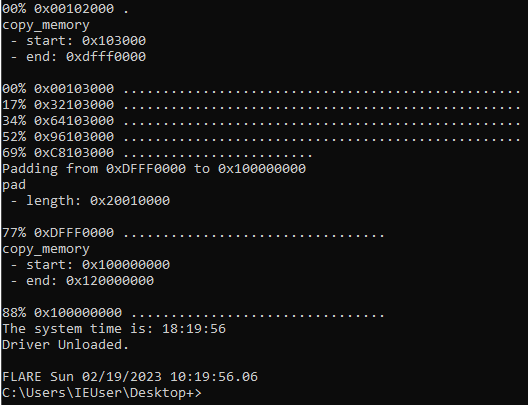


***Figure 2.3.9*** *– Process tree.*

### **Memory Analysis**

Memory analysis can be a tedious task, but simple checks may reveal malicious behaviour in different processes. To analyse the memory of the infected virtual machine, the analyst used **Volatility 3.0** and **WinPMem** to dump the memory.

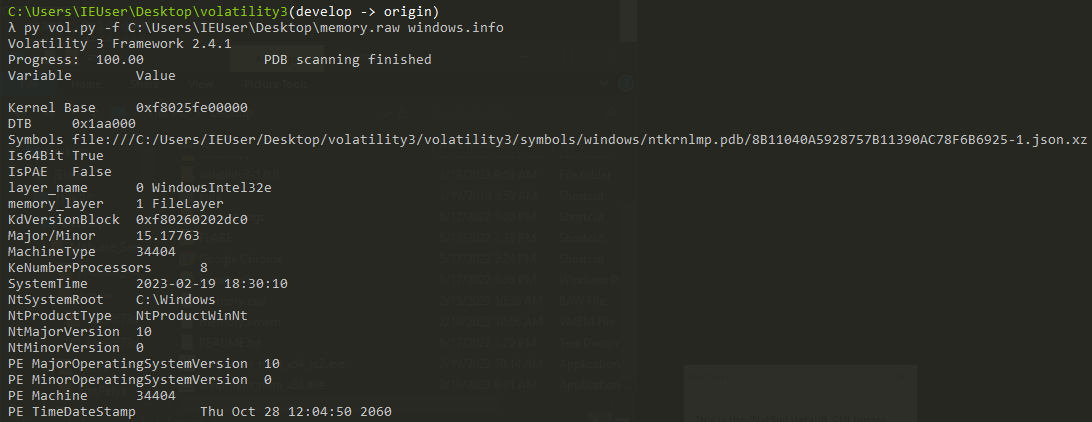
Dumping the memory could be easily achieved with the beforementioned tool. The analyst ran the following command in a **CMD** window to acquire the memory data in raw format: **winpmem\_mini\_x64\_rc2.exe memory.raw**. This command wrote the contents of the RAM in a file called **memory.raw**. (**Figure 2.3.10**)

****

***Figure 2.3.10*** *– Dumping the memory using WinPMem.*

Afterwards, the researcher analysed different data from the raw memory dump. (**Figure 2.3.11**) This was achieved with various plugins, in this case specifically:

* windows.info – basic information about the windows machine
* windows.cmdline – executed cmd commands
* windows.envars – list of environmental variables
* windows.malfind – looking for applications/services with injected malicious code
* windows.privileges – display the privileges for all dumped processes
* windows.pslist – lists the visible processes
* windows.certificates – lists the user certificates on the machine



***Figure 2.3.11*** *– Running the windows.info plugin on the memory dump.*

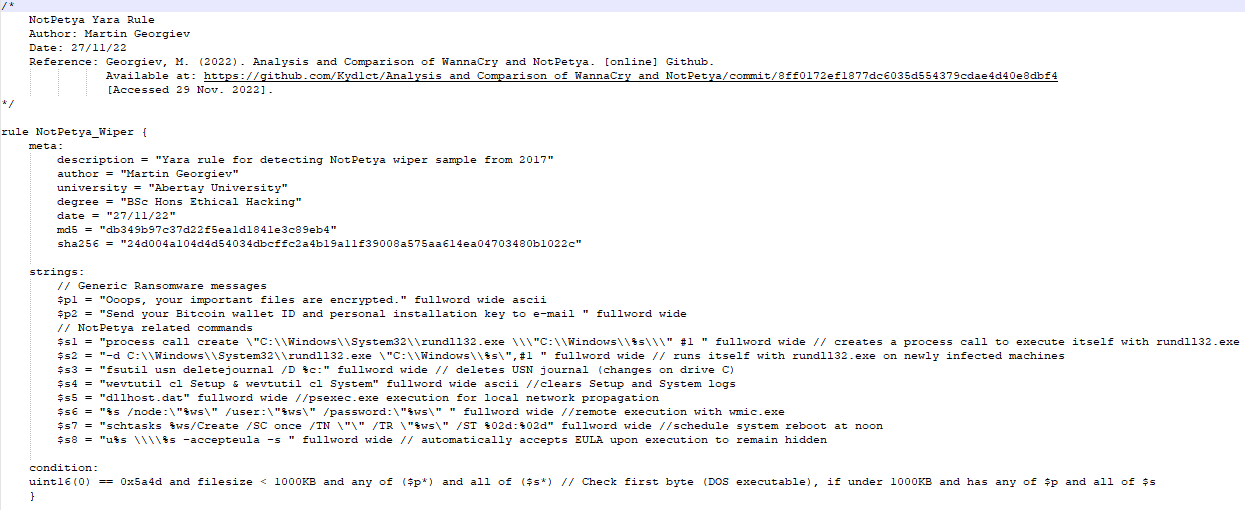
The tool could not reveal any additional information about the malware, any hidden connections/processes, nor injected malicious code. The privileges assigned to the processes were identical to other analysed malware and provided the following authorisations:

* System shutdown
* Program debugging
* Load/unload device drivers
* Change system time
* Manage security logs
* Act as a part of the OS
* Process-level tokens
* Lock pages in memory
* Manage files on volumes
* Obtain an impersonation token for another user in the same session
* Client impersonation after authentication
* Memory allocation for user—space applications

The dumps can be found in [**Appendix B**](#_Appendix_B_–).

## **Yara Rule**

The Yara rule was created with notable data from the analysed strings. This is the easiest method to create simple Yara rules which can detect the malware – file names, specific commands and other strings related to this specific malware. (**Figure 2.4.1**) The Yara rule can be found in [**Appendix D**](#_Appendix_D_–).



***Figure 2.4.1*** *– NotPetya Yara Rule.*

# **Results**

## **Static Analysis**

The Static Analysis allowed the tester to acquire detailed intel regarding the functionality of the malware. The multitude of tools made procedure faster, yet efficient. The analyst successfully obtained the hashes for the main executable and identified the various functions and libraries used to provide it with the malicious capabilities. Combining this with PEStudio, they identified a lot of information about how it accessed the MBR of the connected drives and encrypted the data.

## **Dynamic Analysis**

Unlike other ransomware samples (such as Jigsaw), NotPetya did not exhibit any visible signs of infection. Instead, it created two files in the C:\Windows directory without changing the extensions of any files. The malware also utilised password-dumping executables disguised as temporary files to obtain credentials used to traverse the network. NotPetya's propagation method was unique as it targeted machines on the local network while attempting to exploit and take control of web servers through HTTP requests, leveraging its additional capabilities.

# **Discussion**

## **General Discussions**

The 2017 NotPetya attacks revealed the extent of the malware's destructive power and its rapid spread across networks. NotPetya could encrypt the entire system of a victim and move effortlessly through networks to infect other hosts, including regular computers and servers. This traversal was possible because of the thorough interrogation of the networks and hosts. The malware also exploited the EternalBlue vulnerability, which at the time affected a large portion of Windows systems.

Today, the vulnerability has been patched, and a killswitch prevents in-the-wild samples from executing and propagating as easily. However, an adversary could still infect the machines if NotPetya was locally executed, and the killswitch was bypassed. The analyst successfully achieved their goals of analysing the sample at both a surface and in-depth level, identifying its capabilities and weaknesses.

## **Countermeasures**

The best defence against malicious software, such as ransomware/wipers, is evading infection. Once a system is infected, it can be difficult, if not impossible, to recover files or regain control of the system. Therefore, it is crucial to take proactive safety measures to protect systems and prevent infections from occurring in the first place.

### **Pre-infection Countermeasures**

The most effective way to protect a system from infection would be before it becomes infected. As some of the modules contain cryptography functions, a fully working sample could encrypt the victim’s files. This, in most cases, would not allow them to retrieve their files.

#### **Frequent Security Updates**

One of the reasons why malware is successful is the lack of security patches or users refusing to apply the newest updates to their operating systems and/or anti-virus applications. Additionally, using pirated versions may lack the newer patches and/or contain other vulnerabilities – or even malware as can be seen from the analysis of FileTour. Keeping your system and anti-virus software up to date would ensure that publicly known vulnerabilities could not be exploited, and the AV may have updated signature databases to detect the sample.

#### **Distinguishing Spam**

As the malware is primarily distributed through social engineering, users must be able to distinguish spam emails from real ones. This also applies to legitimate and fake websites and/or files. Users should not open any links or execute files unless they know the sender and the nature of the link or file. Additionally, users should look for bad grammar, fearmongering, rushed actions or similar addresses to legitimate ones.

#### **Blacklisting Unknown Applications and Anti-Virus Software**

System administrators could put restrictions on users by blacklisting unknown software. This way they would not be able to execute suspicious applications and provide the system/network with damage control to prevent any harm. It could be achieved with Anti-Virus software and integrated browser protection.

An updated Anti-Virus software could be used to perform system scans or simply scan newly generated files. Some may even prevent the malicious software from executing itself if they recognise specific code patterns or behaviours.

#### **File Scanners and IDS**

Intrusion Detection Systems will alert security analysts if they detect any suspicious behaviour – phishing emails, specific signatures, etc. Some of them can also be combined with file scanners such as Strelka for greater detection accuracy. This way the internal SOC team could notice the threat before it causes any harm to the system.

#### **Webserver Methods**

As seen in [**Section 2.3.2 Network Symptoms**](#_Network_Symptoms), NotPetya interrogated the webserver with the **OPTIONS** method. It then used the **PROPFIND**, attempting to find a specific file name within the **admin** directory. A negative response would mean that the system was not infected and the wiper would attempt to infect it. Webservers should be configured to only use generic methods such as **OPTIONS**, **GET**, **HEAD**, and **POST** unless others are specifically required for the proper functionality of the server.

### **Post-infection Countermeasures**

#### **Data Backups**

As some of the payloads contained cryptography-related libraries and functions, it would be beneficial to keep data backups. With such, the company could wipe the infected drive and simply replace it with the information they have stored elsewhere. It is also advised to keep such data in physical storage if possible or in locations which are not directly connected to the network of the infected machine as some malware could propagate to it and destroy the backups.

#### **Refuse Ransom Payments**

Ransom payments should **NOT** be considered even in dire situations. In the case of encrypted files, the adversary may attempt to fearmonger the victim by threatening them to publicly post their data or delete it. Paying the ransom does not guarantee that the data can be recovered as the attacker may send a fake decryption key or they may not send one at all.

# **Conclusion**

## **Conclusion**

NotPetya is a dangerous and destructive malware that can infect an entire system within seconds, leaving the victim with little to no chance of recovery. Its advanced propagation capabilities enable it to easily traverse through networks and servers, exploiting vulnerabilities such as EternalBlue. The malware employs various techniques to obfuscate its activities and slow down analysis, including embedding multiple resources and executables within the initial executable and using false messages. NotPetya disguises itself as ransomware, but its true intention is to corrupt both files and the hard drive's MFT and MBR. The MBR is then modified with a custom code that displays a fake disk repair message before switching to the ransom message, which can be seen after the system restarts or if the user restarts the system before the scheduled restart by the wiper.

## **Future Work**

Given more time, the tester could conduct a more thorough analysis of NotPetya's propagation component, which appears to be more sophisticated than other malware samples. This more in-depth understanding of its propagation techniques could be useful for detecting and defending against similar malware strains in the future. Additionally, the analysis could lead to the development of more effective countermeasures against advanced malware attacks.

# **References**

VirusTotal (2004 – Present Day). VirusTotal. [online] Available at: https://www.virustotal.com/gui/home/upload [Accessed 15 Nov. 2022].

Ballenthin, W. (2016). Floss. [online] Available at: https://github.com/mandiant/flare-floss. [Accessed 20 Nov. 2022].

Russinovich, M. (2021). Strings v2.54. [online] Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/strings [Accessed 20 Nov. 2022].

ASL (2023). ExeInfoPE. [online] Available at: http://www.exeinfo.byethost18.com/?i=1 [Accessed 24 Nov. 2022].

Hungenberg, T and Eckert, M. (2007). INetSim. [online] Available at: https://www.inetsim.org/. [Accessed 27 Nov. 2022].

Russinovich, M. (2022). TCPView v4.17. [online] Available at: https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview. [Accessed 27 Nov. 2022].

Wireshark. (1997 - Present Day). Wireshark Documentation. [online] Available at: https://www.wireshark.org/docs/. [Accessed 27 Nov. 2022].

Russinovich, M. (2022). Process Monitor v3.89. [online] Available at: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon. [Accessed 28 Nov. 2022].

Fox, N. (2021). PeStudio Overview: Setup, Tutorial and Tips. [online] Available at: https://www.varonis.com/blog/pestudio. [Accessed 28 Nov. 2022].

Volatility Foundation (2020). Volatility 3.0. [online] Available at: https://www.volatilityfoundation.org/3 [Accessed 15 Dec. 2022].

Cohen, M., et al. (2019). WinPmem. [online] Available at: https://github.com/Velocidex/WinPmem [Accessed 15 Dec. 2022].

Georgiev, M. (2022). Analysis and comparison of WannaCry and NotPetya. [online] Available at: https://github.com/Kyd1ct/Analysis\_and\_Comparison\_of\_WannaCry\_and\_NotPetya/blob/main/Analysis\_and\_Comparison\_of\_WannaCry\_and\_NotPetya.pdf [Accessed 16 Feb. 2023].

AbuseCH (2020). MalwareBazaar. [online] Available at: https://bazaar.abuse.ch/ [Accessed 24 Mar. 2023].

Hurley, S. and Sood, K. (2017). NotPetya Technical Analysis Part II: Further Findings and Potential for MBR Recovery. [online] Available at: https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/ [Accessed 15 Mar. 2023].

Microsoft. (2021). PsExec v2.34. [online] Available at: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec/ [Accessed 25 Mar. 2023].

DarkMatter. (2019). What is the effect of the arguments in the following: conhost.exe 0xffffffff -ForceV1. [online] Available at: https://security.stackexchange.com/questions/198816/what-is-the-effect-of-the-arguments-in-the-following-conhost-exe-0xffffffff-fo/ [Accessed 28 Mar. 2023].

Microsoft. (2022). DeviceIoControl function (ioapiset.h). [online] Available at: https://docs.microsoft.com/en-us/windows/win32/api/ioapiset/nf-ioapiset-deviceiocontrol/ [Accessed 29 Mar. 2023].

VirusTotal (2013). Yara - The pattern matching Swiss knife for malware researchers (and everyone else). [online] Available at: https://virustotal.github.io/yara/ [Accessed 29 Mar. 2023].

Microsoft. (2021). rundll32. [online] Available at: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/rundll32/ [Accessed 29 Mar. 2023].

Microsoft. (2015). PROPFIND Method. [online] Available at: https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2003/aa142960(v=exchg.65) [Accessed 12 Apr. 2023].

Gonzales, R. (2020). Covid-19 Cyber Infection. [online] Available at: https://cybercryptosec.medium.com/covid-19-cyber-infection-c615ead7c29/ [Accessed 14 Apr. 2023].

Sool, K and Hurley, S. (2017). NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft. [online] Available at: https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ [Accessed 23 Apr. 2023].

Eschweiler, S. (2017). Decrypting NotPetya/Petya: Tools for Recovering Your MFT After an Attack. [online] Available at: https://www.crowdstrike.com/blog/decrypting-notpetya-tools-for-recovering-your-mft-after-an-attack/ [Accessed 24 Apr. 2023].

Asher-Dotan, L. (2017). NotPetya Vaccine Discovered by Cybereason. [online] Available at: https://www.cybereason.com/blog/cybereason-discovers-notpetya-kill-switch/ [Accessed 25 Apr. 2023].

# **Appendices**

## **Appendix A – Strings**

***Note: The output was truncated to remove a lot of illegible data.***

As the size of the strings remained substantial, they were not included in the report. They can be found in the folders of each binary in .txt files.

## **Appendix B – Memory Forensics**

### **Appendix B1 – Command Line**

Volatility 3 Framework 2.4.1

PID Process Args

4 System Required memory at 0x20 is not valid (process exited?)

136 Registry Required memory at 0x20 is not valid (process exited?)

360 smss.exe \SystemRoot\System32\smss.exe

452 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

528 wininit.exe wininit.exe

544 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

628 winlogon.exe winlogon.exe

672 services.exe C:\Windows\system32\services.exe

680 lsass.exe C:\Windows\system32\lsass.exe

816 svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p -s PlugPlay

840 fontdrvhost.ex "fontdrvhost.exe"

848 fontdrvhost.ex "fontdrvhost.exe"

856 svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p

956 svchost.exe C:\Windows\system32\svchost.exe -k RPCSS -p

1008 svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM

408 dwm.exe "dwm.exe"

836 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts

1048 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService

1056 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc

1164 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p

1204 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule

1288 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog

1376 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc

1468 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s nsi

1496 VBoxService.ex C:\Windows\System32\VBoxService.exe

1532 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager

1540 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

1664 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain

1680 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes

1696 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem

1780 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc

1808 MemCompression Required memory at 0x20 is not valid (process exited?)

1896 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS

1960 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder

1968 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache

1976 svchost.exe C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm

1636 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p

2072 svchost.exe C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache

2088 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p

2096 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p

2164 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection

2228 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc

2360 spoolsv.exe C:\Windows\System32\spoolsv.exe

2408 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p

2444 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p -s LanmanWorkstation

2532 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s IKEEXT

2540 svchost.exe C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted -p -s PolicyAgent

2676 ruby.exe "C:\Program Files\Puppet Labs\Puppet\sys\ruby\bin\ruby.exe" -rubygems "C:\Program Files\Puppet Labs\Puppet\service\daemon.rb"

2684 svchost.exe C:\Windows\system32\svchost.exe -k NetworkService -p -s CryptSvc

2692 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p -s DPS

2700 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TrkWks

2708 wlms.exe C:\Windows\system32\wlms\wlms.exe

2716 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s SstpSvc

2724 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt

2732 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s WpnService

2784 OfficeClickToR "C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service

2896 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s LanmanServer

2928 svchost.exe C:\Windows\System32\svchost.exe -k NetSvcs -p -s iphlpsvc

3016 svchost.exe C:\Windows\System32\svchost.exe -k LocalService -p -s WdiServiceHost

3056 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs

4000 sihost.exe sihost.exe

4028 svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc

4068 svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService

3684 taskhostw.exe taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}

1036 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s TokenBroker

2188 svchost.exe C:\Windows\system32\svchost.exe -k appmodel -p -s StateRepository

4168 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s CDPSvc

4292 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService

4336 ctfmon.exe "ctfmon.exe"

4652 userinit.exe Required memory at 0x422e23b020 is not valid (process exited?)

4688 explorer.exe C:\Windows\Explorer.EXE

4848 svchost.exe C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc

5056 SearchIndexer. C:\Windows\system32\SearchIndexer.exe /Embedding

4284 ShellExperienc "C:\Windows\SystemApps\ShellExperienceHost\_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca

5148 SearchUI.exe "C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca

5328 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

5364 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

5756 dllhost.exe C:\Windows\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}

6064 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

3680 dllhost.exe C:\Windows\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}

6336 VBoxTray.exe "C:\Windows\System32\VBoxTray.exe"

6544 Teams.exe Required memory at 0x7852d0a020 is not valid (process exited?)

7012 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo

6300 cmd.exe cmd.exe C:\Windows\system32\MusNotification.exe LogonUpdateResults

3672 conhost.exe \??\C:\Windows\system32\conhost.exe 0x4

6796 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc

916 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s SSDPSRV

5464 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p -s DoSvc

760 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc

4908 SgrmBroker.exe C:\Windows\system32\SgrmBroker.exe

1092 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc

4176 cmd.exe cmd.exe C:\Windows\system32\MusNotification.exe

6548 conhost.exe \??\C:\Windows\system32\conhost.exe 0x4

2812 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p -s WinRM

6016 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc

4304 svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvcGroup

5068 svchost.exe Required memory at 0x5be1799020 is not valid (process exited?)

2960 WindowsInterna "C:\Windows\SystemApps\InputApp\_cw5n1h2txyewy\WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe" -ServerName:App.AppXagta193n5rpf7mheremt3yyfa1g555vc.mca

5516 SecurityHealth C:\Windows\system32\SecurityHealthService.exe

4608 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s fdPHost

2424 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s FDResPub

1524 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s Netman

1528 dllhost.exe C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

6532 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost

2428 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -s W32Time

3928 ApplicationFra C:\Windows\system32\ApplicationFrameHost.exe -Embedding

640 MicrosoftEdge. Required memory at 0x28af2f6020 is not valid (process exited?)

5680 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s BthAvctpSvc

3036 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc

3528 dllhost.exe C:\Windows\system32\DllHost.exe /Processid:{3AD05575-8857-4850-9277-11B85BDB8E09}

5696 chrome.exe Required memory at 0x2a2bf68020 is not valid (process exited?)

4016 upfc.exe C:\Windows\System32\Upfc.exe /launchtype periodic /cv bf60kCZOlE2vEfcnNA1BUw.0

720 GoogleUpdate.e "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /c

1820 OneDriveStanda "C:\Program Files (x86)\Microsoft OneDrive\OneDriveStandaloneUpdater.exe"

4448 OneDriveStanda "C:\Program Files (x86)\Microsoft OneDrive\OneDriveStandaloneUpdater.exe" /reporting

6168 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s wuauserv

5044 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS

880 smartscreen.ex Required memory at 0x29e598f2588 is not valid (process exited?)

656 cmd.exe "cmd.exe" /s /k pushd "C:\Users\IEUser\Desktop\Malware\_Samples\NotPetya"

3904 conhost.exe \??\C:\Windows\system32\conhost.exe 0x4

2556 rundll32.exe rundll32 Ransomware.NotPetya.dat, #1

6608 rundll32.exe rundll32 Ransomware.NotPetya.dat, #1

704 cmd.exe Required memory at 0x2c92020 is not valid (process exited?)

2008 EAE7.tmp Required memory at 0x345020 is not valid (process exited?)

1096 cmd.exe "cmd.exe" /s /k pushd "C:\Users\IEUser\Desktop"

116 conhost.exe \??\C:\Windows\system32\conhost.exe 0x4

2672 winpmem\_mini\_x winpmem\_mini\_x64\_rc2.exe memory.raw

6592 Taskmgr.exe "C:\Windows\system32\taskmgr.exe" /4

### **Appendix B2 – Environmental Variables**

2556 rundll32.exe 0x2e9e1fe2600 ALLUSERSPROFILE C:\ProgramData

2556 rundll32.exe 0x2e9e1fe2600 APPDATA C:\Users\IEUser\AppData\Roaming

2556 rundll32.exe 0x2e9e1fe2600 ChocolateyInstall C:\ProgramData\chocolatey

2556 rundll32.exe 0x2e9e1fe2600 ChocolateyLastPathUpdate 132973136170645366

2556 rundll32.exe 0x2e9e1fe2600 ChocolateyToolsLocation C:\Tools

2556 rundll32.exe 0x2e9e1fe2600 CommonProgramFiles C:\Program Files\Common Files

2556 rundll32.exe 0x2e9e1fe2600 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files

2556 rundll32.exe 0x2e9e1fe2600 CommonProgramW6432 C:\Program Files\Common Files

2556 rundll32.exe 0x2e9e1fe2600 COMPUTERNAME MSEDGEWIN10

2556 rundll32.exe 0x2e9e1fe2600 ComSpec C:\Windows\system32\cmd.exe

2556 rundll32.exe 0x2e9e1fe2600 DriverData C:\Windows\System32\Drivers\DriverData

2556 rundll32.exe 0x2e9e1fe2600 HOMEDRIVE C:

2556 rundll32.exe 0x2e9e1fe2600 HOMEPATH \Users\IEUser

2556 rundll32.exe 0x2e9e1fe2600 JAVA\_HOME C:\Program Files\OpenJDK\openjdk-11.0.15\_10

2556 rundll32.exe 0x2e9e1fe2600 LOCALAPPDATA C:\Users\IEUser\AppData\Local

2556 rundll32.exe 0x2e9e1fe2600 LOGONSERVER \\MSEDGEWIN10

2556 rundll32.exe 0x2e9e1fe2600 NUMBER\_OF\_PROCESSORS 8

2556 rundll32.exe 0x2e9e1fe2600 OneDrive C:\Users\IEUser\OneDrive

2556 rundll32.exe 0x2e9e1fe2600 OS Windows\_NT

2556 rundll32.exe 0x2e9e1fe2600 Path C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Python37\Scripts\;C:\Python37\;C:\Python27\;C:\Python27\Scripts;C:\ProgramData\Boxstarter;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Program Files\Puppet Labs\Puppet\bin;C:\Program Files\OpenJDK\openjdk-11.0.15\_10\bin;C:\Program Files\nodejs\;C:\Program Files\Microsoft VS Code\bin;C:\Users\IEUser\AppData\Local\Microsoft\WindowsApps;C:\Tools\Cmder;C:\ProgramData\chocolatey\lib\radare2.flare\tools\radare2\bin;C:\Tools\java-deobfuscator-gui;C:\Tools\Bytecode-Viewer;C:\Program Files (x86)\Nmap;C:\ProgramData\chocolatey\lib\rawcap\tools\rawcap;C:\Tools\pyinstxtractor;C:\Tools\oledump;C:\Tools\rtfdump;C:\Tools\msoffcrypto-crack;C:\Program Files (x86)\pdfid;C:\Program Files (x86)\pdfparser;C:\pdfstreamdumper;C:\iDefense\SysAnalyzer;C:\Users\IEUser\AppData\Local\Programs\Fiddler;C:\Users\IEUser\AppData\Roaming\npm

2556 rundll32.exe 0x2e9e1fe2600 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

2556 rundll32.exe 0x2e9e1fe2600 PROCESSOR\_ARCHITECTURE AMD64

2556 rundll32.exe 0x2e9e1fe2600 PROCESSOR\_IDENTIFIER AMD64 Family 23 Model 113 Stepping 0, AuthenticAMD

2556 rundll32.exe 0x2e9e1fe2600 PROCESSOR\_LEVEL 23

2556 rundll32.exe 0x2e9e1fe2600 PROCESSOR\_REVISION 7100

2556 rundll32.exe 0x2e9e1fe2600 ProgramData C:\ProgramData

2556 rundll32.exe 0x2e9e1fe2600 ProgramFiles C:\Program Files

2556 rundll32.exe 0x2e9e1fe2600 ProgramFiles(x86) C:\Program Files (x86)

2556 rundll32.exe 0x2e9e1fe2600 ProgramW6432 C:\Program Files

2556 rundll32.exe 0x2e9e1fe2600 PROMPT FLARE$S$d$s$t$\_$p$+$g

2556 rundll32.exe 0x2e9e1fe2600 PSModulePath C:\Users\IEUser\Documents\WindowsPowerShell\Modules

2556 rundll32.exe 0x2e9e1fe2600 PUBLIC C:\Users\Public

2556 rundll32.exe 0x2e9e1fe2600 RAW\_TOOLS\_DIR C:\Tools

2556 rundll32.exe 0x2e9e1fe2600 SystemDrive C:

2556 rundll32.exe 0x2e9e1fe2600 SystemRoot C:\Windows

2556 rundll32.exe 0x2e9e1fe2600 TEMP C:\Users\IEUser\AppData\Local\Temp

2556 rundll32.exe 0x2e9e1fe2600 TMP C:\Users\IEUser\AppData\Local\Temp

2556 rundll32.exe 0x2e9e1fe2600 TOOL\_LIST\_DIR C:\ProgramData\Microsoft\Windows\Start Menu\Programs\FLARE

2556 rundll32.exe 0x2e9e1fe2600 TOOL\_LIST\_SHORTCUT C:\Users\IEUser\Desktop\FLARE.lnk

2556 rundll32.exe 0x2e9e1fe2600 USERDOMAIN MSEDGEWIN10

2556 rundll32.exe 0x2e9e1fe2600 USERDOMAIN\_ROAMINGPROFILE MSEDGEWIN10

2556 rundll32.exe 0x2e9e1fe2600 USERNAME IEUser

2556 rundll32.exe 0x2e9e1fe2600 USERPROFILE C:\Users\IEUser

2556 rundll32.exe 0x2e9e1fe2600 VM\_COMMON\_DIR C:\ProgramData\FEVM

2556 rundll32.exe 0x2e9e1fe2600 windir C:\Windows

2556 rundll32.exe 0x2e9e1fe2600 \_NT\_SYMBOL\_PATH symsrv\*symsrv.dll\*C:\symbols\*http://msdl.microsoft.com/download/symbols

6608 rundll32.exe 0xf82600 ALLUSERSPROFILE C:\ProgramData

6608 rundll32.exe 0xf82600 APPDATA C:\Users\IEUser\AppData\Roaming

6608 rundll32.exe 0xf82600 ChocolateyInstall C:\ProgramData\chocolatey

6608 rundll32.exe 0xf82600 ChocolateyLastPathUpdate 132973136170645366

6608 rundll32.exe 0xf82600 ChocolateyToolsLocation C:\Tools

6608 rundll32.exe 0xf82600 CommonProgramFiles C:\Program Files\Common Files

6608 rundll32.exe 0xf82600 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files

6608 rundll32.exe 0xf82600 CommonProgramW6432 C:\Program Files\Common Files

6608 rundll32.exe 0xf82600 COMPUTERNAME MSEDGEWIN10

6608 rundll32.exe 0xf82600 ComSpec C:\Windows\system32\cmd.exe

6608 rundll32.exe 0xf82600 DriverData C:\Windows\System32\Drivers\DriverData

6608 rundll32.exe 0xf82600 HOMEDRIVE C:

6608 rundll32.exe 0xf82600 HOMEPATH \Users\IEUser

6608 rundll32.exe 0xf82600 JAVA\_HOME C:\Program Files\OpenJDK\openjdk-11.0.15\_10

6608 rundll32.exe 0xf82600 LOCALAPPDATA C:\Users\IEUser\AppData\Local

6608 rundll32.exe 0xf82600 LOGONSERVER \\MSEDGEWIN10

6608 rundll32.exe 0xf82600 NUMBER\_OF\_PROCESSORS 8

6608 rundll32.exe 0xf82600 OneDrive C:\Users\IEUser\OneDrive

6608 rundll32.exe 0xf82600 OS Windows\_NT

6608 rundll32.exe 0xf82600 Path C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Python37\Scripts\;C:\Python37\;C:\Python27\;C:\Python27\Scripts;C:\ProgramData\Boxstarter;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Program Files\Puppet Labs\Puppet\bin;C:\Program Files\OpenJDK\openjdk-11.0.15\_10\bin;C:\Program Files\nodejs\;C:\Program Files\Microsoft VS Code\bin;C:\Users\IEUser\AppData\Local\Microsoft\WindowsApps;C:\Tools\Cmder;C:\ProgramData\chocolatey\lib\radare2.flare\tools\radare2\bin;C:\Tools\java-deobfuscator-gui;C:\Tools\Bytecode-Viewer;C:\Program Files (x86)\Nmap;C:\ProgramData\chocolatey\lib\rawcap\tools\rawcap;C:\Tools\pyinstxtractor;C:\Tools\oledump;C:\Tools\rtfdump;C:\Tools\msoffcrypto-crack;C:\Program Files (x86)\pdfid;C:\Program Files (x86)\pdfparser;C:\pdfstreamdumper;C:\iDefense\SysAnalyzer;C:\Users\IEUser\AppData\Local\Programs\Fiddler;C:\Users\IEUser\AppData\Roaming\npm

6608 rundll32.exe 0xf82600 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

6608 rundll32.exe 0xf82600 PROCESSOR\_ARCHITECTURE AMD64

6608 rundll32.exe 0xf82600 PROCESSOR\_IDENTIFIER AMD64 Family 23 Model 113 Stepping 0, AuthenticAMD

6608 rundll32.exe 0xf82600 PROCESSOR\_LEVEL 23

6608 rundll32.exe 0xf82600 PROCESSOR\_REVISION 7100

6608 rundll32.exe 0xf82600 ProgramData C:\ProgramData

6608 rundll32.exe 0xf82600 ProgramFiles C:\Program Files

6608 rundll32.exe 0xf82600 ProgramFiles(x86) C:\Program Files (x86)

6608 rundll32.exe 0xf82600 ProgramW6432 C:\Program Files

6608 rundll32.exe 0xf82600 PROMPT FLARE$S$d$s$t$\_$p$+$g

6608 rundll32.exe 0xf82600 PSModulePath C:\Users\IEUser\Documents\WindowsPowerShell\Modules

6608 rundll32.exe 0xf82600 PUBLIC C:\Users\Public

6608 rundll32.exe 0xf82600 RAW\_TOOLS\_DIR C:\Tools

6608 rundll32.exe 0xf82600 SystemDrive C:

6608 rundll32.exe 0xf82600 SystemRoot C:\Windows

6608 rundll32.exe 0xf82600 TEMP C:\Users\IEUser\AppData\Local\Temp

6608 rundll32.exe 0xf82600 TMP C:\Users\IEUser\AppData\Local\Temp

6608 rundll32.exe 0xf82600 TOOL\_LIST\_DIR C:\ProgramData\Microsoft\Windows\Start Menu\Programs\FLARE

6608 rundll32.exe 0xf82600 TOOL\_LIST\_SHORTCUT C:\Users\IEUser\Desktop\FLARE.lnk

6608 rundll32.exe 0xf82600 USERDOMAIN MSEDGEWIN10

6608 rundll32.exe 0xf82600 USERDOMAIN\_ROAMINGPROFILE MSEDGEWIN10

6608 rundll32.exe 0xf82600 USERNAME IEUser

6608 rundll32.exe 0xf82600 USERPROFILE C:\Users\IEUser

6608 rundll32.exe 0xf82600 VM\_COMMON\_DIR C:\ProgramData\FEVM

6608 rundll32.exe 0xf82600 windir C:\Windows

6608 rundll32.exe 0xf82600 \_NT\_SYMBOL\_PATH symsrv\*symsrv.dll\*C:

### **Appendix B3 – Malfind**

Volatility 3 Framework 2.4.1

PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Hexdump Disasm

5148 SearchUI.exe 0x1a0eb850000 0x1a0eb86ffff VadS PAGE\_EXECUTE\_READWRITE 6 1 Disabled

48 89 54 24 10 48 89 4c H.T$.H.L

24 08 4c 89 44 24 18 4c $.L.D$.L

89 4c 24 20 48 8b 41 28 .L$.H.A(

48 8b 48 08 48 8b 51 50 H.H.H.QP

48 83 e2 f8 48 8b ca 48 H...H..H

b8 60 00 85 eb a0 01 00 .`......

00 48 2b c8 48 81 f9 70 .H+.H..p

0f 00 00 76 09 48 c7 c1 ...v.H.. 48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c 89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 48 83 e2 f8 48 8b ca 48 b8 60 00 85 eb a0 01 00 00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1

5148 SearchUI.exe 0x1a0ec060000 0x1a0ec0c3fff VadS PAGE\_EXECUTE\_READWRITE 5 1 Disabled

e9 fb ff 08 00 00 00 00 ........

00 cc cc cc cc cc cc cc ........

e9 eb 0f 09 00 00 00 00 ........

00 cc cc cc cc cc cc cc ........

e9 db 01 09 00 00 00 00 ........

00 cc cc cc cc cc cc cc ........

e9 cb 1f 09 00 00 00 00 ........

00 cc cc cc cc cc cc cc ........ e9 fb ff 08 00 00 00 00 00 cc cc cc cc cc cc cc e9 eb 0f 09 00 00 00 00 00 cc cc cc cc cc cc cc e9 db 01 09 00 00 00 00 00 cc cc cc cc cc cc cc e9 cb 1f 09 00 00 00 00 00 cc cc cc cc cc cc cc

### **Appendix B4 – Privileges**

2556 rundll32.exe 2 SeCreateTokenPrivilege Create a token object

2556 rundll32.exe 3 SeAssignPrimaryTokenPrivilege Replace a process-level token

2556 rundll32.exe 4 SeLockMemoryPrivilege Lock pages in memory

2556 rundll32.exe 5 SeIncreaseQuotaPrivilege Present Increase quotas

2556 rundll32.exe 6 SeMachineAccountPrivilege Add workstations to the domain

2556 rundll32.exe 7 SeTcbPrivilege Act as part of the operating system

2556 rundll32.exe 8 SeSecurityPrivilege Present Manage auditing and security log

2556 rundll32.exe 9 SeTakeOwnershipPrivilege Present Take ownership of files/objects

2556 rundll32.exe 10 SeLoadDriverPrivilege Present Load and unload device drivers

2556 rundll32.exe 11 SeSystemProfilePrivilege Present Profile system performance

2556 rundll32.exe 12 SeSystemtimePrivilege Present Change the system time

2556 rundll32.exe 13 SeProfileSingleProcessPrivilege Present Profile a single process

2556 rundll32.exe 14 SeIncreaseBasePriorityPrivilege Present Increase scheduling priority

2556 rundll32.exe 15 SeCreatePagefilePrivilege Present Create a pagefile

2556 rundll32.exe 16 SeCreatePermanentPrivilege Create permanent shared objects

2556 rundll32.exe 17 SeBackupPrivilege Present Backup files and directories

2556 rundll32.exe 18 SeRestorePrivilege Present Restore files and directories

2556 rundll32.exe 19 SeShutdownPrivilege Present Shut down the system

2556 rundll32.exe 20 SeDebugPrivilege Present Debug programs

2556 rundll32.exe 21 SeAuditPrivilege Generate security audits

2556 rundll32.exe 22 SeSystemEnvironmentPrivilege Present Edit firmware environment values

2556 rundll32.exe 23 SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files or directories

2556 rundll32.exe 24 SeRemoteShutdownPrivilege Present Force shutdown from a remote system

2556 rundll32.exe 25 SeUndockPrivilege Present Remove computer from docking station

2556 rundll32.exe 26 SeSyncAgentPrivilege Synch directory service data

2556 rundll32.exe 27 SeEnableDelegationPrivilege Enable user accounts to be trusted for delegation

2556 rundll32.exe 28 SeManageVolumePrivilege Present Manage the files on a volume

2556 rundll32.exe 29 SeImpersonatePrivilege Present,Enabled,Default Impersonate a client after authentication

2556 rundll32.exe 30 SeCreateGlobalPrivilege Present,Enabled,Default Create global objects

2556 rundll32.exe 31 SeTrustedCredManAccessPrivilege Access Credential Manager as a trusted caller

2556 rundll32.exe 32 SeRelabelPrivilege Modify the mandatory integrity level of an object

2556 rundll32.exe 33 SeIncreaseWorkingSetPrivilege Present Allocate more memory for user applications

2556 rundll32.exe 34 SeTimeZonePrivilege Present Adjust the time zone of the computer's internal clock

2556 rundll32.exe 35 SeCreateSymbolicLinkPrivilege Present Required to create a symbolic link

2556 rundll32.exe 36 SeDelegateSessionUserImpersonatePrivilege Present Obtain an impersonation token for another user in the same session.

6608 rundll32.exe 2 SeCreateTokenPrivilege Create a token object

6608 rundll32.exe 3 SeAssignPrimaryTokenPrivilege Replace a process-level token

6608 rundll32.exe 4 SeLockMemoryPrivilege Lock pages in memory

6608 rundll32.exe 5 SeIncreaseQuotaPrivilege Present Increase quotas

6608 rundll32.exe 6 SeMachineAccountPrivilege Add workstations to the domain

6608 rundll32.exe 7 SeTcbPrivilege Act as part of the operating system

6608 rundll32.exe 8 SeSecurityPrivilege Present Manage auditing and security log

6608 rundll32.exe 9 SeTakeOwnershipPrivilege Present Take ownership of files/objects

6608 rundll32.exe 10 SeLoadDriverPrivilege Present Load and unload device drivers

6608 rundll32.exe 11 SeSystemProfilePrivilege Present Profile system performance

6608 rundll32.exe 12 SeSystemtimePrivilege Present Change the system time

6608 rundll32.exe 13 SeProfileSingleProcessPrivilege Present Profile a single process

6608 rundll32.exe 14 SeIncreaseBasePriorityPrivilege Present Increase scheduling priority

6608 rundll32.exe 15 SeCreatePagefilePrivilege Present Create a pagefile

6608 rundll32.exe 16 SeCreatePermanentPrivilege Create permanent shared objects

6608 rundll32.exe 17 SeBackupPrivilege Present Backup files and directories

6608 rundll32.exe 18 SeRestorePrivilege Present Restore files and directories

6608 rundll32.exe 19 SeShutdownPrivilege Present,Enabled Shut down the system

6608 rundll32.exe 20 SeDebugPrivilege Present,Enabled Debug programs

6608 rundll32.exe 21 SeAuditPrivilege Generate security audits

6608 rundll32.exe 22 SeSystemEnvironmentPrivilege Present Edit firmware environment values

6608 rundll32.exe 23 SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files or directories

6608 rundll32.exe 24 SeRemoteShutdownPrivilege Present Force shutdown from a remote system

6608 rundll32.exe 25 SeUndockPrivilege Present Remove computer from docking station

6608 rundll32.exe 26 SeSyncAgentPrivilege Synch directory service data

6608 rundll32.exe 27 SeEnableDelegationPrivilege Enable user accounts to be trusted for delegation

6608 rundll32.exe 28 SeManageVolumePrivilege Present Manage the files on a volume

6608 rundll32.exe 29 SeImpersonatePrivilege Present,Enabled,Default Impersonate a client after authentication

6608 rundll32.exe 30 SeCreateGlobalPrivilege Present,Enabled,Default Create global objects

6608 rundll32.exe 31 SeTrustedCredManAccessPrivilege Access Credential Manager as a trusted caller

6608 rundll32.exe 32 SeRelabelPrivilege Modify the mandatory integrity level of an object

6608 rundll32.exe 33 SeIncreaseWorkingSetPrivilege Present Allocate more memory for user applications

6608 rundll32.exe 34 SeTimeZonePrivilege Present Adjust the time zone of the computer's internal clock

6608 rundll32.exe 35 SeCreateSymbolicLinkPrivilege Present Required to create a symbolic link

6608 rundll32.exe 36 SeDelegateSessionUserImpersonatePrivilege Present Obtain an impersonation token for another user in the same session.

### **Appendix B5 – Processes**

2556 656 rundll32.exe 0xba87fdde3540 4 - 1 False 2023-04-27 11:14:27.000000 N/A Disabled

6608 2556 rundll32.exe 0xba87fee51540 15 - 1 True 2023-04-27 11:14:27.000000 N/A Disabled

## **Appendix C – Network Data in CSV Format**

***Note: The output was intentionally altered to remove IP checks after 10.0.0.41***

"No.","Time","Source","Destination","Protocol","Length","Info"

"1","0.000000000","10.0.0.3","10.0.0.2","DHCP","332","DHCP Request - Transaction ID 0x5f31c86f"

"2","0.004953983","10.0.0.2","10.0.0.3","DHCP","590","DHCP ACK - Transaction ID 0x5f31c86f"

"3","0.575619791","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"4","3.576844114","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"5","5.226803308","PcsCompu\_1e:4b:5f","PcsCompu\_ad:1c:cd","ARP","42","Who has 10.0.0.2? Tell 10.0.0.3"

"6","5.226899336","PcsCompu\_ad:1c:cd","PcsCompu\_1e:4b:5f","ARP","60","10.0.0.2 is at 08:00:27:ad:1c:cd"

"7","6.596326601","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"8","9.628908104","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"9","12.635865387","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"10","15.653220950","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"11","34.236568172","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.0? Tell 10.0.0.4"

"12","34.288986931","10.0.0.4","10.0.0.3","TCP","66","49675 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"13","34.289014456","10.0.0.3","10.0.0.4","TCP","54","445 > 49675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"14","34.799290630","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49675 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"15","34.799312362","10.0.0.3","10.0.0.4","TCP","54","445 > 49675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"16","35.206143778","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.0? Tell 10.0.0.4"

"17","35.299987678","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49675 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"18","35.300024295","10.0.0.3","10.0.0.4","TCP","54","445 > 49675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"19","35.301185828","10.0.0.4","10.0.0.3","TCP","66","49678 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"20","35.301191672","10.0.0.3","10.0.0.4","TCP","54","139 > 49678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"21","35.809166634","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49678 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"22","35.809188827","10.0.0.3","10.0.0.4","TCP","54","139 > 49678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"23","36.204486291","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.0? Tell 10.0.0.4"

"24","36.315792504","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49678 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"25","36.315824691","10.0.0.3","10.0.0.4","TCP","54","139 > 49678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"26","36.316830201","10.0.0.4","10.0.0.3","NBNS","92","Name query NBSTAT \*<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>"

"27","36.316864071","10.0.0.3","10.0.0.4","ICMP","120","Destination unreachable (Port unreachable)"

"28","37.832135092","10.0.0.4","10.0.0.3","NBNS","92","Name query NBSTAT \*<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>"

"29","37.832166155","10.0.0.3","10.0.0.4","ICMP","120","Destination unreachable (Port unreachable)"

"30","38.259366424","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.1? Tell 10.0.0.4"

"31","39.209305798","PcsCompu\_e6:e5:59","PcsCompu\_1e:4b:5f","ARP","60","Who has 10.0.0.3? Tell 10.0.0.4"

"32","39.209306069","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.1? Tell 10.0.0.4"

"33","39.209322598","PcsCompu\_1e:4b:5f","PcsCompu\_e6:e5:59","ARP","42","10.0.0.3 is at 08:00:27:1e:4b:5f"

"34","39.333474713","10.0.0.4","10.0.0.3","NBNS","92","Name query NBSTAT \*<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>"

"35","39.333502408","10.0.0.3","10.0.0.4","ICMP","120","Destination unreachable (Port unreachable)"

"36","39.530796981","PcsCompu\_1e:4b:5f","PcsCompu\_e6:e5:59","ARP","42","Who has 10.0.0.4? Tell 10.0.0.3"

"37","39.530948962","PcsCompu\_e6:e5:59","PcsCompu\_1e:4b:5f","ARP","60","10.0.0.4 is at 08:00:27:e6:e5:59"

"38","40.209122374","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.1? Tell 10.0.0.4"

"39","40.850692383","10.0.0.4","10.0.0.3","TCP","66","49691 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"40","40.850727637","10.0.0.3","10.0.0.4","TCP","66","80 > 49691 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"41","40.850989328","10.0.0.4","10.0.0.3","TCP","60","49691 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"42","40.851058993","10.0.0.4","10.0.0.3","HTTP","151","OPTIONS / HTTP/1.1 "

"43","40.851065137","10.0.0.3","10.0.0.4","TCP","54","80 > 49691 [ACK] Seq=1 Ack=98 Win=64256 Len=0"

"44","40.868967945","10.0.0.3","10.0.0.4","HTTP","210","HTTP/1.1 200 OK "

"45","40.869260651","10.0.0.4","10.0.0.3","TCP","60","49691 > 80 [FIN, ACK] Seq=98 Ack=157 Win=2102016 Len=0"

"46","40.869938510","10.0.0.3","10.0.0.4","TCP","54","80 > 49691 [FIN, ACK] Seq=157 Ack=99 Win=64256 Len=0"

"47","40.870132149","10.0.0.4","10.0.0.3","TCP","60","49691 > 80 [ACK] Seq=99 Ack=158 Win=2102016 Len=0"

"48","43.931965193","10.0.0.4","10.0.0.3","TCP","66","49694 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"49","43.931994452","10.0.0.3","10.0.0.4","TCP","66","80 > 49694 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"50","43.932192372","10.0.0.4","10.0.0.3","TCP","60","49694 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"51","43.932259020","10.0.0.4","10.0.0.3","HTTP","189","OPTIONS /admin%24 HTTP/1.1 "

"52","43.932264593","10.0.0.3","10.0.0.4","TCP","54","80 > 49694 [ACK] Seq=1 Ack=136 Win=64128 Len=0"

"53","43.940696163","10.0.0.3","10.0.0.4","HTTP","210","HTTP/1.1 200 OK "

"54","43.940866126","10.0.0.4","10.0.0.3","TCP","60","49694 > 80 [FIN, ACK] Seq=136 Ack=157 Win=2102016 Len=0"

"55","43.941581313","10.0.0.3","10.0.0.4","TCP","54","80 > 49694 [FIN, ACK] Seq=157 Ack=137 Win=64128 Len=0"

"56","43.941685119","10.0.0.4","10.0.0.3","TCP","60","49694 > 80 [ACK] Seq=137 Ack=158 Win=2102016 Len=0"

"57","43.968460313","10.0.0.4","10.0.0.3","TCP","66","49695 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"58","43.968492550","10.0.0.3","10.0.0.4","TCP","66","80 > 49695 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"59","43.968671976","10.0.0.4","10.0.0.3","TCP","60","49695 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"60","43.968734684","10.0.0.4","10.0.0.3","HTTP","219","PROPFIND /admin%24 HTTP/1.1 "

"61","43.968742784","10.0.0.3","10.0.0.4","TCP","54","80 > 49695 [ACK] Seq=1 Ack=166 Win=64128 Len=0"

"62","43.976888616","10.0.0.3","10.0.0.4","TCP","236","80 > 49695 [PSH, ACK] Seq=1 Ack=166 Win=64128 Len=182 [TCP segment of a reassembled PDU]"

"63","43.977136694","10.0.0.4","10.0.0.3","TCP","60","49695 > 80 [FIN, ACK] Seq=166 Ack=183 Win=2102016 Len=0"

"64","43.977782035","10.0.0.3","10.0.0.4","HTTP","54","HTTP/1.1 501 Method Not Implemented "

"65","43.977934457","10.0.0.4","10.0.0.3","TCP","60","49695 > 80 [ACK] Seq=167 Ack=184 Win=2102016 Len=0"

"66","44.004749786","10.0.0.4","10.0.0.3","TCP","66","49696 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"67","44.004776269","10.0.0.3","10.0.0.4","TCP","66","80 > 49696 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"68","44.004967583","10.0.0.4","10.0.0.3","TCP","60","49696 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"69","44.005030843","10.0.0.4","10.0.0.3","HTTP","225","PROPFIND /admin%24/perfc HTTP/1.1 "

"70","44.005037168","10.0.0.3","10.0.0.4","TCP","54","80 > 49696 [ACK] Seq=1 Ack=172 Win=64128 Len=0"

"71","44.013505825","10.0.0.3","10.0.0.4","TCP","236","80 > 49696 [PSH, ACK] Seq=1 Ack=172 Win=64128 Len=182 [TCP segment of a reassembled PDU]"

"72","44.013723331","10.0.0.4","10.0.0.3","TCP","60","49696 > 80 [FIN, ACK] Seq=172 Ack=183 Win=2102016 Len=0"

"73","44.014393681","10.0.0.3","10.0.0.4","HTTP","54","HTTP/1.1 501 Method Not Implemented "

"74","44.014509576","10.0.0.4","10.0.0.3","TCP","60","49696 > 80 [ACK] Seq=173 Ack=184 Win=2102016 Len=0"

"75","44.040393519","10.0.0.4","10.0.0.3","TCP","66","49697 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"76","44.040419360","10.0.0.3","10.0.0.4","TCP","66","80 > 49697 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"77","44.040602169","10.0.0.4","10.0.0.3","TCP","60","49697 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"78","44.040780492","10.0.0.4","10.0.0.3","HTTP","219","PROPFIND /admin%24 HTTP/1.1 "

"79","44.040791197","10.0.0.3","10.0.0.4","TCP","54","80 > 49697 [ACK] Seq=1 Ack=166 Win=64128 Len=0"

"80","44.049105228","10.0.0.3","10.0.0.4","TCP","236","80 > 49697 [PSH, ACK] Seq=1 Ack=166 Win=64128 Len=182 [TCP segment of a reassembled PDU]"

"81","44.049293435","10.0.0.4","10.0.0.3","TCP","60","49697 > 80 [FIN, ACK] Seq=166 Ack=183 Win=2102016 Len=0"

"82","44.049973007","10.0.0.3","10.0.0.4","HTTP","54","HTTP/1.1 501 Method Not Implemented "

"83","44.050072012","10.0.0.4","10.0.0.3","TCP","60","49697 > 80 [ACK] Seq=167 Ack=184 Win=2102016 Len=0"

"84","44.076343540","10.0.0.4","10.0.0.3","TCP","66","49698 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"85","44.076371586","10.0.0.3","10.0.0.4","TCP","66","80 > 49698 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"86","44.076544136","10.0.0.4","10.0.0.3","TCP","60","49698 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"87","44.076647180","10.0.0.4","10.0.0.3","HTTP","229","PROPFIND /admin%24/perfc.dll HTTP/1.1 "

"88","44.076653906","10.0.0.3","10.0.0.4","TCP","54","80 > 49698 [ACK] Seq=1 Ack=176 Win=64128 Len=0"

"89","44.085151510","10.0.0.3","10.0.0.4","TCP","236","80 > 49698 [PSH, ACK] Seq=1 Ack=176 Win=64128 Len=182 [TCP segment of a reassembled PDU]"

"90","44.085383891","10.0.0.4","10.0.0.3","TCP","60","49698 > 80 [FIN, ACK] Seq=176 Ack=183 Win=2102016 Len=0"

"91","44.086050592","10.0.0.3","10.0.0.4","HTTP","54","HTTP/1.1 501 Method Not Implemented "

"92","44.086153927","10.0.0.4","10.0.0.3","TCP","60","49698 > 80 [ACK] Seq=177 Ack=184 Win=2102016 Len=0"

"93","44.111893575","10.0.0.4","10.0.0.3","TCP","66","49699 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"94","44.111919697","10.0.0.3","10.0.0.4","TCP","66","80 > 49699 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"95","44.112088978","10.0.0.4","10.0.0.3","TCP","60","49699 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"96","44.112241650","10.0.0.4","10.0.0.3","HTTP","219","PROPFIND /admin%24 HTTP/1.1 "

"97","44.112249308","10.0.0.3","10.0.0.4","TCP","54","80 > 49699 [ACK] Seq=1 Ack=166 Win=64128 Len=0"

"98","44.120548894","10.0.0.3","10.0.0.4","TCP","236","80 > 49699 [PSH, ACK] Seq=1 Ack=166 Win=64128 Len=182 [TCP segment of a reassembled PDU]"

"99","44.120903696","10.0.0.4","10.0.0.3","TCP","60","49699 > 80 [FIN, ACK] Seq=166 Ack=183 Win=2102016 Len=0"

"100","44.121407110","10.0.0.3","10.0.0.4","HTTP","54","HTTP/1.1 501 Method Not Implemented "

"101","44.121536287","10.0.0.4","10.0.0.3","TCP","60","49699 > 80 [ACK] Seq=167 Ack=184 Win=2102016 Len=0"

"102","46.290672233","10.0.0.4","10.0.0.3","TCP","66","49703 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"103","46.290695278","10.0.0.3","10.0.0.4","TCP","54","445 > 49703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"104","46.362177824","10.0.0.4","10.0.0.255","BROWSER","216","Get Backup List Request"

"105","46.362289289","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"106","46.806737684","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49703 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"107","46.806762483","10.0.0.3","10.0.0.4","TCP","54","445 > 49703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"108","47.128064882","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"109","47.319003130","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49703 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"110","47.319024510","10.0.0.3","10.0.0.4","TCP","54","445 > 49703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"111","47.903636172","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"112","48.292136087","10.0.0.4","10.0.0.3","TCP","66","49705 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"113","48.292160635","10.0.0.3","10.0.0.4","TCP","54","139 > 49705 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"114","48.807211446","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49705 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"115","48.807235594","10.0.0.3","10.0.0.4","TCP","54","139 > 49705 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"116","49.317447347","10.0.0.4","10.0.0.3","TCP","66","[TCP Retransmission] 49705 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"117","49.317472376","10.0.0.3","10.0.0.4","TCP","54","139 > 49705 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"

"118","49.675543810","10.0.0.4","10.0.0.255","BROWSER","216","Get Backup List Request"

"119","49.675606248","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"120","50.305023594","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.5? Tell 10.0.0.4"

"121","50.445835549","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"122","51.196619615","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"123","51.212861719","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.5? Tell 10.0.0.4"

"124","52.213890332","PcsCompu\_e6:e5:59","PcsCompu\_1e:4b:5f","ARP","60","Who has 10.0.0.3? Tell 10.0.0.4"

"125","52.213890683","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.5? Tell 10.0.0.4"

"126","52.213909317","PcsCompu\_1e:4b:5f","PcsCompu\_e6:e5:59","ARP","42","10.0.0.3 is at 08:00:27:1e:4b:5f"

"127","52.964387369","10.0.0.4","10.0.0.255","BROWSER","216","Get Backup List Request"

"128","52.964435453","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"129","53.730073314","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"130","54.325353713","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.6? Tell 10.0.0.4"

"131","54.480807125","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1b>"

"132","55.214611782","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.6? Tell 10.0.0.4"

"133","56.221755043","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.6? Tell 10.0.0.4"

"134","56.253718269","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1e>"

"135","57.014573261","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1e>"

"136","57.782624101","10.0.0.4","10.0.0.255","NBNS","92","Name query NB WORKGROUP<1e>"

"137","58.344729508","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.7? Tell 10.0.0.4"

"138","59.218791769","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.7? Tell 10.0.0.4"

"139","60.215093750","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.7? Tell 10.0.0.4"

"140","62.376115456","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.8? Tell 10.0.0.4"

"141","63.220027955","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.8? Tell 10.0.0.4"

"142","64.215272826","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.8? Tell 10.0.0.4"

"143","66.385644295","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.9? Tell 10.0.0.4"

"144","67.222268415","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.9? Tell 10.0.0.4"

"145","68.213811387","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.9? Tell 10.0.0.4"

"146","70.410441991","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.10? Tell 10.0.0.4"

"147","71.224387931","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.10? Tell 10.0.0.4"

"148","72.222693980","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.10? Tell 10.0.0.4"

"149","74.460432138","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.11? Tell 10.0.0.4"

"150","75.240313479","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.11? Tell 10.0.0.4"

"151","76.227233172","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.11? Tell 10.0.0.4"

"152","78.503560433","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.12? Tell 10.0.0.4"

"153","79.228662500","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.12? Tell 10.0.0.4"

"154","80.225372338","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.12? Tell 10.0.0.4"

"155","82.528014966","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.13? Tell 10.0.0.4"

"156","83.245245479","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.13? Tell 10.0.0.4"

"157","84.246351455","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.13? Tell 10.0.0.4"

"158","86.433890388","10.0.0.4","10.0.0.255","BROWSER","243","Host Announcement MSEDGEWIN10, Workstation, Server, NT Workstation"

"159","86.590622891","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.14? Tell 10.0.0.4"

"160","87.246766863","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.14? Tell 10.0.0.4"

"161","88.228921968","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.14? Tell 10.0.0.4"

"162","90.624435139","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.15? Tell 10.0.0.4"

"163","91.242920618","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.15? Tell 10.0.0.4"

"164","92.248972113","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.15? Tell 10.0.0.4"

"165","94.642550464","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.16? Tell 10.0.0.4"

"166","95.246387529","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.16? Tell 10.0.0.4"

"167","96.236709451","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.16? Tell 10.0.0.4"

"168","98.703592792","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.17? Tell 10.0.0.4"

"169","99.253687816","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.17? Tell 10.0.0.4"

"170","100.253804375","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.17? Tell 10.0.0.4"

"171","102.723368563","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.18? Tell 10.0.0.4"

"172","103.251905603","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.18? Tell 10.0.0.4"

"173","104.256031939","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.18? Tell 10.0.0.4"

"174","106.757592819","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.19? Tell 10.0.0.4"

"175","107.758383117","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.19? Tell 10.0.0.4"

"176","108.742847488","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.19? Tell 10.0.0.4"

"177","110.801155350","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.20? Tell 10.0.0.4"

"178","111.743742254","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.20? Tell 10.0.0.4"

"179","112.744853845","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.20? Tell 10.0.0.4"

"180","114.822672110","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.21? Tell 10.0.0.4"

"181","115.761774922","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.21? Tell 10.0.0.4"

"182","116.757099601","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.21? Tell 10.0.0.4"

"183","118.855428024","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.22? Tell 10.0.0.4"

"184","119.752616997","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.22? Tell 10.0.0.4"

"185","120.748849723","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.22? Tell 10.0.0.4"

"186","122.901878237","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.23? Tell 10.0.0.4"

"187","123.757206617","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.23? Tell 10.0.0.4"

"188","124.766550006","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.23? Tell 10.0.0.4"

"189","126.954041788","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.24? Tell 10.0.0.4"

"190","127.748467487","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.24? Tell 10.0.0.4"

"191","128.753459813","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.24? Tell 10.0.0.4"

"192","130.988676726","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.25? Tell 10.0.0.4"

"193","131.769975843","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.25? Tell 10.0.0.4"

"194","132.768202062","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.25? Tell 10.0.0.4"

"195","135.020100859","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.26? Tell 10.0.0.4"

"196","135.766638019","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.26? Tell 10.0.0.4"

"197","136.766850859","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.26? Tell 10.0.0.4"

"198","139.071020927","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.27? Tell 10.0.0.4"

"199","139.770631204","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.27? Tell 10.0.0.4"

"200","140.774690300","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.27? Tell 10.0.0.4"

"201","141.710345680","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"202","143.087661345","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.28? Tell 10.0.0.4"

"203","143.770658817","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.28? Tell 10.0.0.4"

"204","144.725883179","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"205","144.758022441","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.28? Tell 10.0.0.4"

"206","147.134405148","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.29? Tell 10.0.0.4"

"207","147.746563718","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"208","147.778614932","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.29? Tell 10.0.0.4"

"209","148.774715988","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.29? Tell 10.0.0.4"

"210","150.778963794","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"211","151.155001732","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.30? Tell 10.0.0.4"

"212","151.776916348","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.30? Tell 10.0.0.4"

"213","152.777043045","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.30? Tell 10.0.0.4"

"214","153.810485914","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"215","155.202982983","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.31? Tell 10.0.0.4"

"216","155.760286243","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.31? Tell 10.0.0.4"

"217","156.779026443","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.31? Tell 10.0.0.4"

"218","156.843626487","10.0.0.4","239.255.255.250","SSDP","179","M-SEARCH \* HTTP/1.1 "

"219","159.231256338","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.32? Tell 10.0.0.4"

"220","159.761761714","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.32? Tell 10.0.0.4"

"221","160.778544456","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.32? Tell 10.0.0.4"

"222","163.270565647","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.33? Tell 10.0.0.4"

"223","164.265400296","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.33? Tell 10.0.0.4"

"224","165.268027267","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.33? Tell 10.0.0.4"

"225","167.331715301","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.34? Tell 10.0.0.4"

"226","168.272828734","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.34? Tell 10.0.0.4"

"227","169.288608677","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.34? Tell 10.0.0.4"

"228","171.364994239","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.35? Tell 10.0.0.4"

"229","172.287289322","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.35? Tell 10.0.0.4"

"230","173.281249287","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.35? Tell 10.0.0.4"

"231","174.372818768","10.0.0.4","10.0.0.3","DNS","72","Standard query 0x968a A www.bing.com"

"232","174.372819029","10.0.0.4","10.0.0.3","DNS","84","Standard query 0x7aa0 A onecs-live.azureedge.net"

"233","174.405540206","10.0.0.3","10.0.0.4","DNS","88","Standard query response 0x968a A www.bing.com A 10.0.0.3"

"234","174.408293252","10.0.0.4","10.0.0.3","TCP","66","49833 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"235","174.408316056","10.0.0.3","10.0.0.4","TCP","66","443 > 49833 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"236","174.408546242","10.0.0.4","10.0.0.3","TCP","60","49833 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0"

"237","174.410400862","10.0.0.3","10.0.0.4","DNS","100","Standard query response 0x7aa0 A onecs-live.azureedge.net A 10.0.0.3"

"238","174.410523132","10.0.0.4","10.0.0.3","TLSv1.2","245","Client Hello"

"239","174.410533878","10.0.0.3","10.0.0.4","TCP","54","443 > 49833 [ACK] Seq=1 Ack=192 Win=64128 Len=0"

"240","174.411049391","10.0.0.4","10.0.0.3","TCP","66","49834 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"241","174.411057640","10.0.0.3","10.0.0.4","TCP","66","443 > 49834 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"242","174.411178026","10.0.0.4","10.0.0.3","TCP","60","49834 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0"

"243","174.411422185","10.0.0.4","10.0.0.3","TLSv1.2","257","Client Hello"

"244","174.411426846","10.0.0.3","10.0.0.4","TCP","54","443 > 49834 [ACK] Seq=1 Ack=204 Win=64128 Len=0"

"245","174.470425302","10.0.0.4","10.0.0.3","DNS","91","Standard query 0x2613 A settings-win.data.microsoft.com"

"246","174.474590953","10.0.0.3","10.0.0.4","DNS","107","Standard query response 0x2613 A settings-win.data.microsoft.com A 10.0.0.3"

"247","174.476449151","10.0.0.4","10.0.0.3","TCP","66","49835 > 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"248","174.476484355","10.0.0.3","10.0.0.4","TCP","66","443 > 49835 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"249","174.476639313","10.0.0.4","10.0.0.3","TCP","60","49835 > 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"250","174.479521450","10.0.0.4","10.0.0.3","TLSv1.2","250","Client Hello"

"251","174.479542139","10.0.0.3","10.0.0.4","TCP","54","443 > 49835 [ACK] Seq=1 Ack=197 Win=64128 Len=0"

"252","174.492286007","10.0.0.3","10.0.0.4","TLSv1.2","1352","Server Hello, Certificate, Server Key Exchange, Server Hello Done"

"253","174.492483476","10.0.0.4","10.0.0.3","TCP","60","49833 > 443 [ACK] Seq=192 Ack=1299 Win=260608 Len=0"

"254","174.493365458","10.0.0.3","10.0.0.4","TLSv1.2","1352","Server Hello, Certificate, Server Key Exchange, Server Hello Done"

"255","174.493486566","10.0.0.4","10.0.0.3","TCP","60","49834 > 443 [ACK] Seq=204 Ack=1299 Win=260608 Len=0"

"256","174.494465237","10.0.0.3","10.0.0.4","TLSv1.2","1352","Server Hello, Certificate, Server Key Exchange, Server Hello Done"

"257","174.502684418","10.0.0.4","10.0.0.3","TLSv1.2","147","Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message"

"258","174.502703743","10.0.0.3","10.0.0.4","TCP","54","443 > 49835 [ACK] Seq=1299 Ack=290 Win=64128 Len=0"

"259","174.502970236","10.0.0.3","10.0.0.4","TLSv1.2","280","New Session Ticket, Change Cipher Spec, Encrypted Handshake Message"

"260","174.512101068","10.0.0.4","10.0.0.3","TCP","66","49836 > 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"261","174.512134457","10.0.0.3","10.0.0.4","TCP","66","443 > 49836 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"262","174.512318579","10.0.0.4","10.0.0.3","TCP","60","49836 > 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"263","174.512497303","10.0.0.4","10.0.0.3","TLSv1.2","250","Client Hello"

"264","174.512507898","10.0.0.3","10.0.0.4","TCP","54","443 > 49836 [ACK] Seq=1 Ack=197 Win=64128 Len=0"

"265","174.515053227","10.0.0.4","10.0.0.3","TCP","60","49835 > 443 [FIN, ACK] Seq=290 Ack=1525 Win=2102272 Len=0"

"266","174.516296586","10.0.0.3","10.0.0.4","TLSv1.2","85","Encrypted Alert"

"267","174.516409394","10.0.0.3","10.0.0.4","TCP","54","443 > 49835 [FIN, ACK] Seq=1556 Ack=291 Win=64128 Len=0"

"268","174.516448527","10.0.0.4","10.0.0.3","TCP","60","49835 > 443 [RST, ACK] Seq=291 Ack=1556 Win=0 Len=0"

"269","174.516514253","10.0.0.4","10.0.0.3","TCP","60","49835 > 443 [RST] Seq=291 Win=0 Len=0"

"270","174.520004468","10.0.0.4","10.0.0.3","DNS","83","Standard query 0x5bd2 A ctldl.windowsupdate.com"

"271","174.524433124","10.0.0.3","10.0.0.4","DNS","99","Standard query response 0x5bd2 A ctldl.windowsupdate.com A 10.0.0.3"

"272","174.525001583","10.0.0.4","10.0.0.3","TCP","66","49837 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"273","174.525015135","10.0.0.3","10.0.0.4","TCP","66","80 > 49837 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"274","174.525048915","10.0.0.4","10.0.0.3","TCP","66","49838 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"275","174.525052293","10.0.0.3","10.0.0.4","TCP","66","80 > 49838 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"276","174.525136302","10.0.0.4","10.0.0.3","TCP","60","49837 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"277","174.525185158","10.0.0.4","10.0.0.3","TCP","60","49838 > 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"278","174.525223920","10.0.0.4","10.0.0.3","HTTP","256","GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e4ee65c3692f1e8b HTTP/1.1 "

"279","174.525223950","10.0.0.4","10.0.0.3","HTTP","256","GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?adccf1aab51974c6 HTTP/1.1 "

"280","174.525231007","10.0.0.3","10.0.0.4","TCP","54","80 > 49837 [ACK] Seq=1 Ack=203 Win=64128 Len=0"

"281","174.525236981","10.0.0.3","10.0.0.4","TCP","54","80 > 49838 [ACK] Seq=1 Ack=203 Win=64128 Len=0"

"282","174.531360329","10.0.0.3","10.0.0.4","TLSv1.2","1352","Server Hello, Certificate, Server Key Exchange, Server Hello Done"

"283","174.532358116","10.0.0.4","10.0.0.3","TLSv1.2","147","Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message"

"284","174.532372801","10.0.0.3","10.0.0.4","TCP","54","443 > 49836 [ACK] Seq=1299 Ack=290 Win=64128 Len=0"

"285","174.532584062","10.0.0.3","10.0.0.4","TLSv1.2","280","New Session Ticket, Change Cipher Spec, Encrypted Handshake Message"

"286","174.533106401","10.0.0.4","10.0.0.3","TCP","60","49836 > 443 [FIN, ACK] Seq=290 Ack=1525 Win=2102272 Len=0"

"287","174.545778253","10.0.0.3","10.0.0.4","TLSv1.2","85","Encrypted Alert"

"288","174.545922656","10.0.0.3","10.0.0.4","TCP","54","443 > 49836 [FIN, ACK] Seq=1556 Ack=291 Win=64128 Len=0"

"289","174.545966119","10.0.0.4","10.0.0.3","TCP","60","49836 > 443 [RST, ACK] Seq=291 Ack=1556 Win=0 Len=0"

"290","174.546180307","10.0.0.4","10.0.0.3","TCP","60","49836 > 443 [RST] Seq=291 Win=0 Len=0"

"291","174.569444798","10.0.0.3","10.0.0.4","TCP","204","80 > 49838 [PSH, ACK] Seq=1 Ack=203 Win=64128 Len=150 [TCP segment of a reassembled PDU]"

"292","174.570335290","10.0.0.3","10.0.0.4","TCP","204","80 > 49837 [PSH, ACK] Seq=1 Ack=203 Win=64128 Len=150 [TCP segment of a reassembled PDU]"

"293","174.571703806","10.0.0.3","10.0.0.4","HTTP","312","HTTP/1.1 200 OK (text/html)"

"294","174.571951193","10.0.0.4","10.0.0.3","TCP","60","49837 > 80 [ACK] Seq=203 Ack=410 Win=2101760 Len=0"

"295","174.572527701","10.0.0.4","10.0.0.3","TCP","60","49837 > 80 [FIN, ACK] Seq=203 Ack=410 Win=2101760 Len=0"

"296","174.572539980","10.0.0.3","10.0.0.4","TCP","54","80 > 49837 [ACK] Seq=410 Ack=204 Win=64128 Len=0"

"297","174.575056800","10.0.0.3","10.0.0.4","HTTP","312","HTTP/1.1 200 OK (text/html)"

"298","174.575806879","10.0.0.4","10.0.0.3","TCP","60","49838 > 80 [ACK] Seq=203 Ack=410 Win=2101760 Len=0"

"299","174.576437335","10.0.0.4","10.0.0.3","TCP","60","49838 > 80 [FIN, ACK] Seq=203 Ack=410 Win=2101760 Len=0"

"300","174.576447820","10.0.0.3","10.0.0.4","TCP","54","80 > 49838 [ACK] Seq=410 Ack=204 Win=64128 Len=0"

"301","174.576851948","10.0.0.4","10.0.0.3","TCP","60","49833 > 443 [FIN, ACK] Seq=192 Ack=1299 Win=260608 Len=0"

"302","174.577253892","10.0.0.4","10.0.0.3","TCP","60","49834 > 443 [FIN, ACK] Seq=204 Ack=1299 Win=260608 Len=0"

"303","174.580527278","10.0.0.3","10.0.0.4","TCP","54","443 > 49834 [FIN, ACK] Seq=1299 Ack=205 Win=64128 Len=0"

"304","174.580675229","10.0.0.4","10.0.0.3","TCP","60","49834 > 443 [ACK] Seq=205 Ack=1300 Win=260608 Len=0"

"305","174.583189774","10.0.0.3","10.0.0.4","TCP","54","443 > 49833 [FIN, ACK] Seq=1299 Ack=193 Win=64128 Len=0"

"306","174.583342136","10.0.0.4","10.0.0.3","TCP","60","49833 > 443 [ACK] Seq=193 Ack=1300 Win=260608 Len=0"

"307","175.419649321","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.36? Tell 10.0.0.4"

"308","175.509121257","10.0.0.4","10.0.0.3","TCP","66","49841 > 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1"

"309","175.509154305","10.0.0.3","10.0.0.4","TCP","66","443 > 49841 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM=1 WS=128"

"310","175.509339945","10.0.0.4","10.0.0.3","TCP","60","49841 > 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0"

"311","175.509546505","10.0.0.4","10.0.0.3","TLSv1.2","250","Client Hello"

"312","175.509553382","10.0.0.3","10.0.0.4","TCP","54","443 > 49841 [ACK] Seq=1 Ack=197 Win=64128 Len=0"

"313","175.512784277","10.0.0.3","10.0.0.4","TLSv1.2","1352","Server Hello, Certificate, Server Key Exchange, Server Hello Done"

"314","175.513710309","10.0.0.4","10.0.0.3","TLSv1.2","147","Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message"

"315","175.513753010","10.0.0.3","10.0.0.4","TCP","54","443 > 49841 [ACK] Seq=1299 Ack=290 Win=64128 Len=0"

"316","175.514017908","10.0.0.3","10.0.0.4","TLSv1.2","280","New Session Ticket, Change Cipher Spec, Encrypted Handshake Message"

"317","175.514520671","10.0.0.4","10.0.0.3","TCP","60","49841 > 443 [FIN, ACK] Seq=290 Ack=1525 Win=2102272 Len=0"

"318","175.516888118","10.0.0.3","10.0.0.4","TLSv1.2","85","Encrypted Alert"

"319","175.517023218","10.0.0.3","10.0.0.4","TCP","54","443 > 49841 [FIN, ACK] Seq=1556 Ack=291 Win=64128 Len=0"

"320","175.517171089","10.0.0.4","10.0.0.3","TCP","60","49841 > 443 [RST, ACK] Seq=291 Ack=1556 Win=0 Len=0"

"321","175.517171450","10.0.0.4","10.0.0.3","TCP","60","49841 > 443 [RST] Seq=291 Win=0 Len=0"

"322","176.269869636","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.36? Tell 10.0.0.4"

"323","177.292536563","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.36? Tell 10.0.0.4"

"324","179.457706259","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.37? Tell 10.0.0.4"

"325","180.292989307","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.37? Tell 10.0.0.4"

"326","181.279180095","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.37? Tell 10.0.0.4"

"327","183.467772619","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.38? Tell 10.0.0.4"

"328","184.292556633","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.38? Tell 10.0.0.4"

"329","185.280959034","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.38? Tell 10.0.0.4"

"330","187.516251857","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.39? Tell 10.0.0.4"

"331","188.284581517","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.39? Tell 10.0.0.4"

"332","189.276968238","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.39? Tell 10.0.0.4"

"333","191.543428666","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.40? Tell 10.0.0.4"

"334","192.278893623","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.40? Tell 10.0.0.4"

"335","193.281017732","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.40? Tell 10.0.0.4"

"336","195.581539147","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.41? Tell 10.0.0.4"

"337","196.280382867","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.41? Tell 10.0.0.4"

"338","197.301120811","PcsCompu\_e6:e5:59","Broadcast","ARP","60","Who has 10.0.0.41? Tell 10.0.0.4"

## **Appendix D – Yara Rule**

