

# Projekt - część 3

## Analiza Dynamiczna

Julia Sadecka, Marcel Trzaskawka

Cyberbezpieczeństwo

<b>KeyPass.....</b>	<b>3</b>
Wstępna Analiza Dynamiczna.....	3
Przygotowanie.....	3
Początkowe obserwacje.....	4
Sieć.....	5
Procexp.....	5
RegShot.....	6
Procmon.....	7
Eksperymentowanie.....	12
Podsumowanie Wstępnej Analizy.....	13
Zaawansowana Analiza Dynamiczna.....	14
<b>NotPetya.....</b>	<b>27</b>
Uruchomienie wirusa.....	27
Wstępna Analiza Dynamiczna.....	30
Process Explorer.....	30
RegShot.....	30
Process Monitor.....	32
Sieć.....	35
Podsumowanie Wstępnej Analizy Dynamicznej.....	37
Zaawansowana Analiza Dynamiczna.....	38
Biblioteka i funkcje UI.....	38
Antywirus.....	40
Informacje o sieci.....	41
Odczytywanie rejestrów.....	42
Okienko OllyDbg.....	42
Szyfrowanie.....	43
Podsumowanie Analizy Dynamicznej.....	44

Wirus	MD5	SHA-256
NotPetya	71b6a493388e7d0b40c83ce903bc6b04	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
KeyPass Ransomware	6999c944d1c98b2739d015448c99a291	35b067642173874bd2766da0d108401b4cf45d6e2a8b3971d95bf474be4f6282

# KeyPass

## Wstępna Analiza Dynamiczna

### **Przygotowanie**

Aby zebrać jak najwięcej informacji przy podstawowej analizie użyłem narzędzi:

- FakeNet-ng - stworzenie sztucznego serwera i połączenia sieciowego
- Procmon - przechwytywanie zdarzeń
- Procexp - Analiza aktywnych i usuniętych procesów
- Regshot - Porównanie kluczy rejestrów przed i po

Zacząłem od utworzenia zrzutu kluczy rejestru, następnie uruchomiłem przechwytywanie zdarzeń w Procmon. Uruchomiłem program.

## Początkowe obserwacje

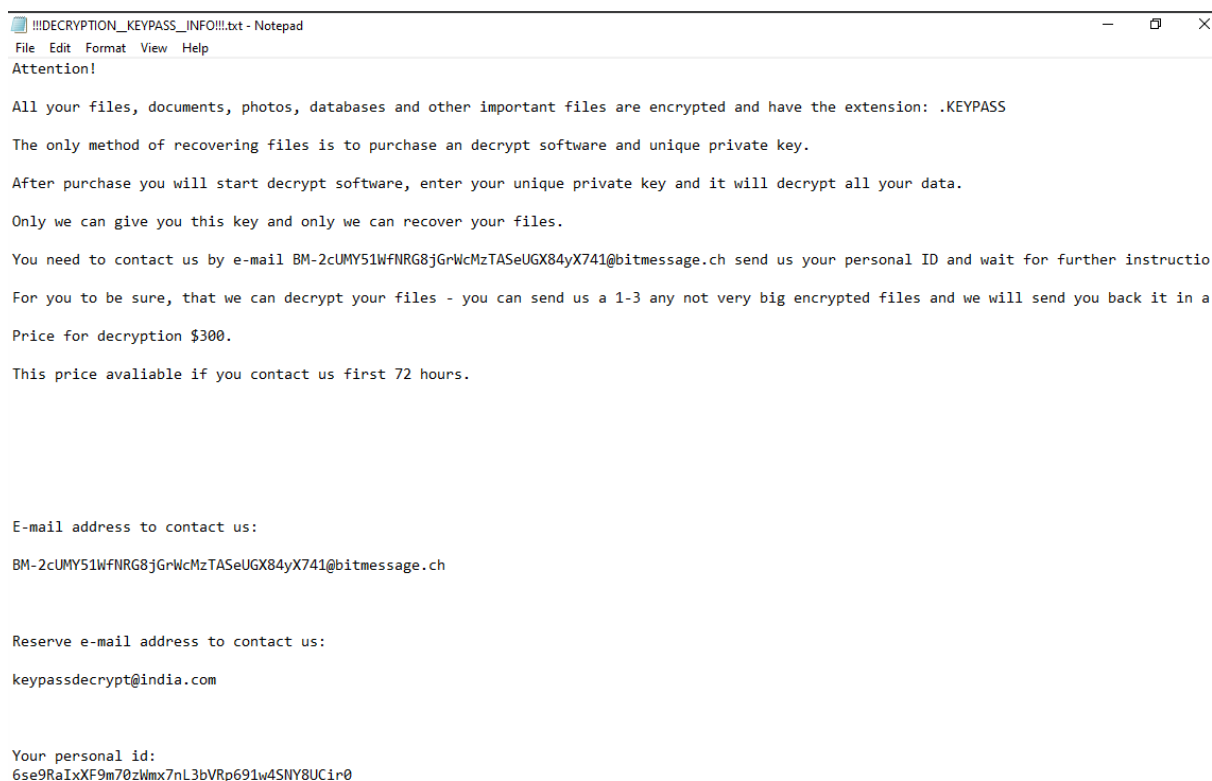
Malware wymaga uprawnień administratora do uruchomienia.

Program silnie wykorzystuje dysk twardy, CPU używa od 2% do nawet 15%.

Ogólne działanie systemu bardzo zwolniło.

Po zakończeniu pracy wszystkie moje pliki zostały zaszyfrowane, z wyjątkiem katalogu systemowego Windows. Skróty do aplikacji systemowych zostały zaszyfrowane, ale mogę je uruchomić za pomocą Win + R (run menu) lub skrótów dla poszczególnych aplikacji: Win + E (Eksplorator plików), Ctrl + Shift + Esc (Menadżer zadań) itd.

Została dodana wiadomość z żądaniem okupu 300\$:



```
!!!DECRYPTION_KEYPASS_INFO!!!.txt - Notepad
File Edit Format View Help
Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .KEYPASS

The only method of recovering files is to purchase an decrypt software and unique private key.

After purchase you will start decrypt software, enter your unique private key and it will decrypt all your data.

Only we can give you this key and only we can recover your files.

You need to contact us by e-mail BM-2cUMY51WfN8G8jGrWcMzTASeUGX84yX741@bitmessage.ch send us your personal ID and wait for further instructio

For you to be sure, that we can decrypt your files - you can send us a 1-3 any not very big encrypted files and we will send you back it in a

Price for decryption $300.

This price avaiable if you contact us first 72 hours.


E-mail address to contact us:

BM-2cUMY51WfN8G8jGrWcMzTASeUGX84yX741@bitmessage.ch


Reserve e-mail address to contact us:

keypassdecrypt@india.com


Your personal id:
6se9RaIxXF9m70zWmx7nL3bVRp691w45NY8UCir0
```

## Sieć

Zauważyłem również, że program bez przerwy próbuje nawiązać połączenie ze stroną *kronus.pp.ua*. Po kilkunastu minutach nie zauważyłem więcej takich prób. Możliwe, że po określonym czasie lub ilości prób, program przestaje.

```
DNS Server] Received A request for domain 'kronus.pp.ua'.  
Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101  
Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
```

Próbowałem połączyć się ze stroną, lecz strona nie istnieje.

Wayback Machine nie ma rekordu z przeszłości tej strony.

## Procexp

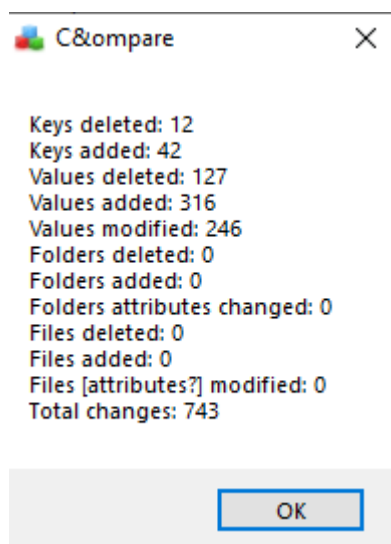
Zauważyłem, że po kilku minutach malware zduplikował swój proces, a po krótkiej chwili je usunął

[-] [img alt="yellow circle icon"] KeypassRansomware.exe	10.94	27,016 K	37,840 K	4112
[-] [img alt="yellow circle icon"] KeypassRansomware.exe	< 0.01	2,788 K	13,400 K	3232
[img alt="yellow circle icon"] KeypassRansomware.exe	< 0.01	2,240 K	10,104 K	1952
[img alt="yellow circle icon"] KeypassRansomware.exe	< 0.01	2,232 K	9,948 K	456
[img alt="yellow circle icon"] KeypassRansomware.exe	1.28	35,304 K	46,068 K	4112
[img alt="yellow circle icon"] KeypassRansomware.exe	< 0.01	2,232 K	9,948 K	456

W szczegółach procesu nie znalazłem nic ciekawego poza stringami, które, były omówione w części analizy statycznej

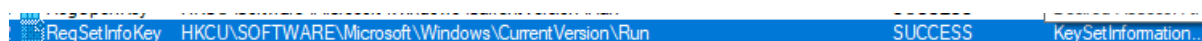
## RegShot

Tak prezentują się różnice w kluczach rejestrów



Dużo zmian rejestrów należy do Procexp. Nie potrafię zidentyfikować rejestrów zmienianych przez KeypassRansomware.

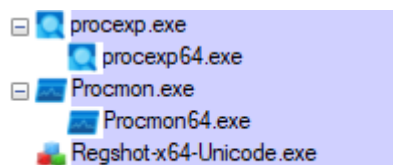
Sprawdziłem natomiast, czy program dodaje się do autostartu za pomocą klucza rejestru.



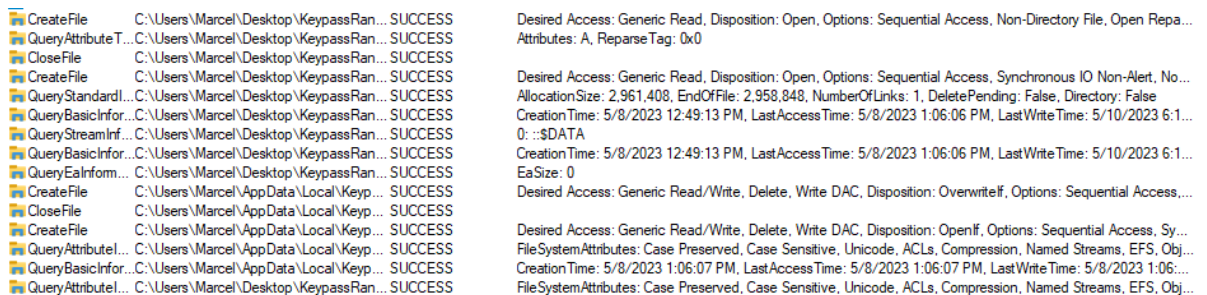
Jest tutaj klucz odpowiadający za autostart, ale nie widzę na jaką wartość został zmieniony. Prawdopodobnie dodał się do autostartu.

## Procmon

Tutaj dzieje się najwięcej rzeczy. Procmon zebrał ponad 1,5 miliona zdarzeń i nie zbiera więcej. Proces zniknął również z widoku procesów. KeypassRansomware skończył swoją pracę.



Program kopiuje siebie z lokalizacji w której został włączony do katalogu %appdata%\Local\ zachowując swoje parametry takie jak czas utworzenia, czas modyfikacji itp.



936	ReadFile	C:\Users\Marcel\Desktop\KeypassRan...	SUCCESS	Offset: 0, Length: 524,288, Priority: Norm
936	WriteFile	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	Offset: 0, Length: 524,288, Priority: Norm
936	ReadFile	C:\Users\Marcel\Desktop\KeypassRan...	SUCCESS	Offset: 524,288, Length: 524,288
936	WriteFile	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	Offset: 524,288, Length: 524,288
936	ReadFile	C:\Users\Marcel\Desktop\KeypassRan...	SUCCESS	Offset: 1,048,576, Length: 524,288
936	WriteFile	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	Offset: 1,048,576, Length: 524,288
936	ReadFile	C:\Users\Marcel\Desktop\KeypassRan...	SUCCESS	Offset: 1,572,864, Length: 524,288
936	WriteFile	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	Offset: 1,572,864, Length: 524,288
936	ReadFile	C:\Users\Marcel\Desktop\KeypassRan...	SUCCESS	Offset: 2,097,152, Length: 524,288
936	WriteFile	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	Offset: 2,097,152, Length: 524,288
936	ReadFile	C:\Users\Marcel\Desktop\KeypassRan...	SUCCESS	Offset: 2,621,440, Length: 337,408
936	WriteFile	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	Offset: 2,621,440, Length: 337,408
936	SetBasicInfo	C:\Users\Marcel\AppData\Local\Keyp...	SUCCESS	CreationTime: 1/1/2023 1:06:00 AM, L...

Program odczytuje bardzo dużo rejestrów, oraz zmienia niektóre z nich

RegQueryKey	HKCR\AllFileSystemObjects	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCR\AllFileSystemObjects\ShellEx\Co...	NAME NOT FOUND	Desired Access: Query Value
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: Name
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCR\Directory	SUCCESS	Desired Access: Maximum Allowed, Granted Access: Read
RegSetInfoKey	HKCR\Directory	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryValue	HKCU\Software\Classes\Directory\Doc...	NAME NOT FOUND	Length: 12
RegQueryValue	HKCR\Directory\DocObject	NAME NOT FOUND	Length: 12
RegCloseKey	HKCR\Directory	SUCCESS	
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: Name
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCU\Software\Classes\Directory\Doc...	NAME NOT FOUND	Desired Access: Query Value
RegOpenKey	HKCR\Directory\DocObject	NAME NOT FOUND	Desired Access: Query Value
RegQueryKey	HKCR\Folder	SUCCESS	Query: Name
RegQueryKey	HKCR\Folder	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCU\Software\Classes\Folder	NAME NOT FOUND	Desired Access: Maximum Allowed
RegQueryValue	HKCR\Folder\DocObject	NAME NOT FOUND	Length: 12
RegQueryKey	HKCR\Folder	SUCCESS	Query: Name
RegQueryKey	HKCR\Folder	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCU\Software\Classes\Folder\DocOb...	NAME NOT FOUND	Desired Access: Query Value
RegQueryKey	HKCR\Folder	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCR\Folder\DocObject	NAME NOT FOUND	Desired Access: Query Value
RegQueryKey	HKCR\AllFileSystemObjects	SUCCESS	Query: Name
RegQueryKey	HKCR\AllFileSystemObjects	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCU\Software\Classes\AllFileSystemO...	NAME NOT FOUND	Desired Access: Maximum Allowed
RegQueryValue	HKCR\AllFileSystemObjects\DocObject	NAME NOT FOUND	Length: 12
RegQueryKey	HKCR\AllFileSystemObjects	SUCCESS	Query: Name
RegQueryKey	HKCR\AllFileSystemObjects	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCU\Software\Classes\AllFileSystemO...	NAME NOT FOUND	Desired Access: Query Value
RegQueryKey	HKCR\AllFileSystemObjects	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCR\AllFileSystemObjects\DocObject	NAME NOT FOUND	Desired Access: Query Value
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: Name
RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCR\Directory	SUCCESS	Desired Access: Maximum Allowed, Granted Access: Read
RegSetInfoKey	HKCR\Directory	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryValue	HKCU\Software\Classes\Directory\Bro...	NAME NOT FOUND	Length: 12
RegQueryValue	HKCR\Directory\BrowseInPlace	NAME NOT FOUND	Length: 12

Odczytuje pliki desktop.ini z folderów katalogu użytkownika. Następnie zmienia/tworzy rejestry  
 HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions. Możliwe, że operacje są ze sobą powiązane, ponieważ w plikach desktop.ini znajdują się informacje na temat folderów oraz tego jak mają się wyświetlać. Podejrzewam, że program odczytuje te pliki i zapisuje je w kluczach rejestru.

CreateFile	C:\Users\Marcel\OneDrive\desktop.ini	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequential Access, Synchronous IO Non-Alert, No...
QueryStandard...	C:\Users\Marcel\OneDrive\desktop.ini	SUCCESS	AllocationSize: 104, EndOfFile: 97, NumberOfLinks: 1, DeletePending: False, Directory: False
ReadFile	C:\Users\Marcel\OneDrive\desktop.ini	SUCCESS	Offset: 0, Length: 97, Priority: Normal
QueryBasicInfor...	C:\Users\Marcel\OneDrive\desktop.ini	SUCCESS	CreationTime: 3/9/2023 7:12:18 PM, LastAccessTime: 5/8/2023 1:06:07 PM, LastWriteTime: 3/9/2023 7:12:...
CloseFile	C:\Users\Marcel\OneDrive\desktop.ini	SUCCESS	
RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
RegQueryKey	HKLM	SUCCESS	Query: Name
RegOpenKey	HKLM\Software\WOW6432Node\Micr...	REPARSE	Desired Access: Read
RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: Read
RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0



Każdy z tych rejestrów jest potem odczytywany. Kiedy wszystkie zostaną odczytane, tworzy się nowy wątek.

Thread Create		SUCCESS	Thread ID: 5180
RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
RegOpenKey	HKCU\Software\Classes\exe	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKCR\exe	SUCCESS	Desired Access: Read
RegSetInfoKey	HKCR\exe	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryKey	HKCR\exe	SUCCESS	Query: Name
RegQueryKey	HKCR\exe	SUCCESS	Query: HandleTags, HandleTags: 0x401
RegOpenKey	HKCU\Software\Classes\exe	NAME NOT FOUND	Desired Access: Maximum Allowed
RegQueryValue	HKCR\exe\Default	SUCCESS	Type: REG_SZ, Length: 16, Data: exefile

W tym miejscu utworzył się podproces.

936 Process Create	C:\Users\Marcel\AppData\Local\Key...	SUCCESS	PID: 5404, Command line: "C:\Users\Marcel\AppData\Local\KeypassRansomware.exe"
5404 Process Start		SUCCESS	Parent PID: 936, Command line: "C:\Users\Marcel\AppData\Local\KeypassRansomware.exe", Current direct...
5404 Thread Create		SUCCESS	Thread ID: 1156

Program załadował bibliotekę bcrypt.dll. Znajdują się w niej algorytmy kryptograficzne.

Utworzony został plik delfself.bat.

CreateFile	C:\Users\Marcel\AppData\Local\Temp\delfself.bat
CreateFile	C:\Users\Marcel\AppData\Local\Temp\delfself.bat
WriteFile	C:\Users\Marcel\AppData\Local\Temp\delfself.bat
FlushBuffersFile	C:\Users\Marcel\AppData\Local\Temp\delfself.bat
WriteFile	C:\Users\Marcel\AppData\Local\Temp\delfself.bat

Załadowanie bcryptprimitives.dll i odczytanie polityk FIPS dotyczących szyfrowania systemów plików.

Load Image	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Image Base: 0x75aa0000, Image Size: 0x5f000
CreateFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a
QuerySecurityFile	C:\Windows\SysWOW64\bcryptprimitives.dll	BUFFER OVERFL...	Information: Owner
QuerySecurityFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Information: Owner
CloseFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	
RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Se...	NAME NOT FOUND	Length: 528
QueryNameInfo...	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Name: \Windows\SysWOW64\bcryptprimitives.dll
RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	REPARSE	Desired Access: Query Value
RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	Desired Access: Query Value
RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryValue	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	NAME NOT FOUND	Length: 20
RegCloseKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	
RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	REPARSE	Desired Access: Query Value
RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	Desired Access: Query Value
RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryValue	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa	REPARSE	Desired Access: Query Value
RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	Desired Access: Query Value
RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryValue	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	NAME NOT FOUND	Length: 20
RegQueryValue	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	NAME NOT FOUND	Length: 20
RegCloseKey	HKLM\System\CurrentControlSet\Control\Lsa\Fips...	SUCCESS	
RegCloseKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	
RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Policies\Micro...	REPARSE	Desired Access: Query Value

Próba połączenia z siecią.

TCP Reconnect	DESKTOP-DVMRCP1:49753 -> 192.0.2.123:80	SUCCESS	Length: 0, seqnum: 0, connid: 0
TCP Reconnect	DESKTOP-DVMRCP1:49753 -> 192.0.2.123:80	SUCCESS	Length: 0, seqnum: 0, connid: 0
TCP Reconnect	DESKTOP-DVMRCP1:49753 -> 192.0.2.123:80	SUCCESS	Length: 0, seqnum: 0, connid: 0
TCP Reconnect	DESKTOP-DVMRCP1:49753 -> 192.0.2.123:80	SUCCESS	Length: 0, seqnum: 0, connid: 0
TCP Disconnect	DESKTOP-DVMRCP1:49753 -> 192.0.2.123:80	SUCCESS	Length: 0, seqnum: 0, connid: 0

Po około 2 minutach po zakończeniu enumeracji wielu rejestrów, program zaczyna tworzyć w każdym folderze plik z informacją o szyfrowaniu. Teoretycznie szyfrowanie jeszcze się nie rozpoczęło, więc możliwe jest przerwanie procesu.

CreateFile	C:\!!!DECRYPTION__KEYPASS__INFO!!!.txt	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share...
CreateFile	C:\!!!DECRYPTION__KEYPASS__INFO!!!.txt	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-A...
ReadFile	C:\\$Secure:\$SDH:\$INDEX_ALLOCATION	SUCCESS	Offset: 69,632, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchron...
Load Image	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Image Base: 0x74670000, Image Size: 0xf000
CloseFile	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	
WriteFile	C:\!!!DECRYPTION__KEYPASS__INFO!!!.txt	SUCCESS	Offset: 0, Length: 999, Priority: Normal
CreateFile	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a
QuerySecurityFile	C:\Windows\SysWOW64\kernel.appcore.dll	BUFFER OVERFL...	Information: Owner
WriteFile	C:\!!!DECRYPTION__KEYPASS__INFO!!!.txt	SUCCESS	Offset: 999, Length: 42
CloseFile	C:\!!!DECRYPTION__KEYPASS__INFO!!!.txt	SUCCESS	
QuerySecurityFile	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Information: Owner
CloseFile	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	
CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchron...
QueryDirectory	C:\	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: !!!DECRYPTION__KEYPASS__INFO!!!.txt
RegQueryKey	HKLM	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
RegQueryKey	HKLM	SUCCESS	Query: Name
RegOpenKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\C...	NAME NOT FOUND	Desired Access: Read
RegQueryKey	HKLM	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
RegQueryKey	HKLM	SUCCESS	Query: Name
RegOpenKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\...	SUCCESS	Desired Access: Query Value
RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\...	NAME NOT FOUND	Length: 16
RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\...	SUCCESS	
QueryDirectory	C:\	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: \$Recycle.Bin, 2: Documents and Settings, 3: Dump...
CreateFile	C:\\$Recycle.Bin\!!!DECRYPTION__KEYPASS__I...	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share...
CreateFile	C:\\$Recycle.Bin\!!!DECRYPTION__KEYPASS__I...	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-A...
WriteFile	C:\\$Recycle.Bin\!!!DECRYPTION__KEYPASS__I...	SUCCESS	Offset: 0, Length: 999, Priority: Normal
WriteFile	C:\\$Recycle.Bin\!!!DECRYPTION__KEYPASS__I...	SUCCESS	Offset: 999, Length: 42
CloseFile	C:\\$Recycle.Bin\!!!DECRYPTION__KEYPASS__I...	SUCCESS	
CreateFile	C:\\$Recycle.Bin	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchron...
QueryDirectory	C:\\$Recycle.Bin\*	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: !!!DECRYPTION__KEYPASS__INFO!!!.txt, 3: S...
QueryDirectory	C:\\$Recycle.Bin	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: ..., 2: !!!DECRYPTION__KEYPASS__INFO!!!.txt, 3: S...

Pierwszym miejscem, w którym pojawił się plik jest miejsce, w którym program został uruchomiony. Potem plik dodawany jest w każdym folderze na dysku zaczynając od kosza, kończąc na folderze użytkownika.

Od pojawienia się pierwszego pliku w koszu do ostatniego pliku w C:\Users\Public\Videos minęło około 2,5 min

CreateFile	C:\Users\Public\Videos\!!!DECRYPTION__KEYP...	SUCCESS
QueryBasicInfor...	C:\Users\Public\Videos\!!!DECRYPTION__KEYP...	SUCCESS
CloseFile	C:\Users\Public\Videos\!!!DECRYPTION__KEYP...	SUCCESS
CreateFile	C:\Users\Public\Videos	SUCCESS
QueryDirectory	C:\Users\Public\Videos\*	SUCCESS
QueryDirectory	C:\Users\Public\Videos	SUCCESS
QueryDirectory	C:\Users\Public\Videos	NO MORE FILES
QueryDirectory	C:\Users\Public	NO MORE FILES
QueryDirectory	C:\Users	NO MORE FILES
QueryDirectory	C:\	NO MORE FILES

Od razu po tym zaczyna się szyfrowanie wszystkich plików.

QueryDirectory	C:\	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
CreateFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	Desired Access: Generic Read/Write, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Direct
QueryStandardI...	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	AllocationSize: 136, EndOfFile: 129, NumberOfLinks: 1, DeletePending: False, Directory: False
ReadFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	Offset: 0, Length: 129, Priority: Normal
ReadFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	Offset: 0, Length: 129, I/O Flags: Non-cached, Paging I/O, Priority: Normal
WriteFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	Offset: 0, Length: 129, Priority: Normal
CloseFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	
CreateFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Options: Synchronous IO Non-
QueryAttributeT...	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	Attributes: HSA, Reparse Tag: 0x0
QueryBasicInfor...	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	CreationTime: 3/9/2023 7:51:32 PM, LastAccessTime: 5/8/2023 1:09:23 PM, LastWriteTime: 5/8/2023
CreateFile	C:\\$Recycle.Bin\S-1-5-18	SUCCESS	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, Options: , Attributes: n/a, ShareMc
SetRenameInfo...	C:\\$Recycle.Bin\S-1-5-18\desktop.ini	SUCCESS	ReplaceIfExists: False, FileName: C:\\$Recycle.Bin\S-1-5-18\desktop.ini.KEYPASS
CloseFile	C:\\$Recycle.Bin\S-1-5-18	SUCCESS	
CloseFile	C:\\$Recycle.Bin\S-1-5-18\desktop.ini.KEYPASS	SUCCESS	

Szyfrowanie zajmuje średnio 13 odwołań do funkcji systemowych. Nie licząc katalogu Windows (który wykluczony jest z szyfrowania w celu poprawnego działania systemu), system plików posiada około 100 tysięcy plików co daje ponad 1.3 miliona zdarzeń.

Co ciekawe, wirus szyfruje tylko pierwsze 5 MB każdego pliku (o ile jest na tyle duży). Możliwe, że robi to po to, aby działanie było o wiele sprawniejsze, bo i tak wszystkie programy wykonywalne będą niezdadne do uruchomienia, a dokumenty rzadko przekraczają 5MB.

ReadFile	C:\Program Files\010 Editor\010Editor.qch	SUCCESS	Offset: 0, Length: 5,242,880, Priority: Normal
ReadFile	C:\Program Files\010 Editor\010Editor.qch	SUCCESS	Offset: 0, Length: 2,097,152, I/O Flags: Non-c
ReadFile	C:\Program Files\010 Editor\010Editor.qch	SUCCESS	Offset: 2,097,152, Length: 2,097,152, I/O Flag
ReadFile	C:\Program Files\010 Editor\010Editor.qch	SUCCESS	Offset: 4,194,304, Length: 1,048,576, I/O Flag
WriteFile	C:\Program Files\010 Editor\010Editor.qch	SUCCESS	Offset: 0, Length: 5,242,880, Priority: Normal
CloseFile	C:\Program Files\010 Editor\010Editor.qch	SUCCESS	

Zauważyłem też, że Keypass nie zaszyfrował siebie.

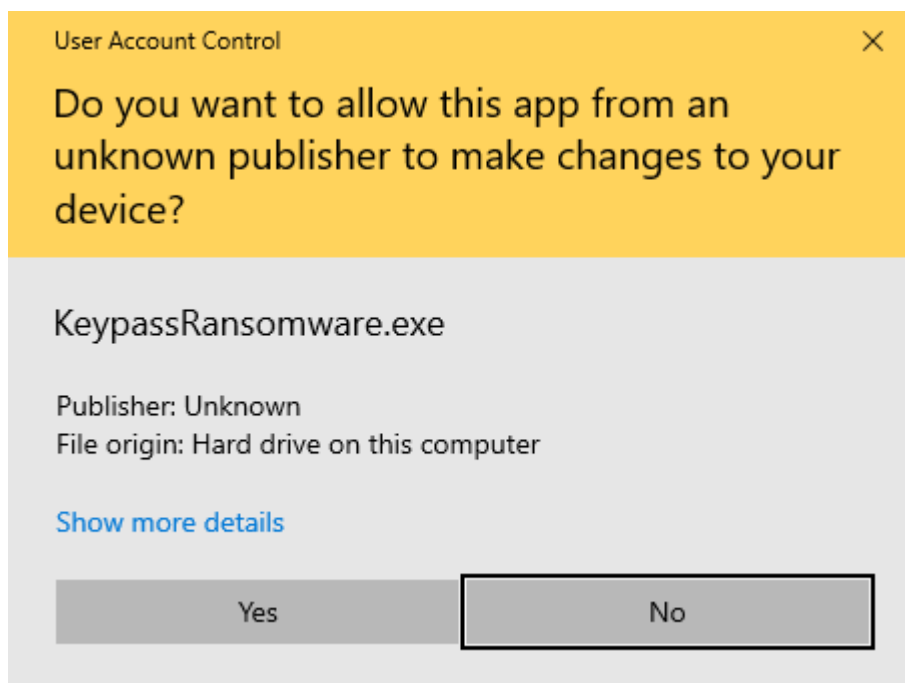
CreateFile	C:\Users\Marcel\AppData\Local\KeypassRansomware.exe	SHARING VIOLAT.
------------	---	-----------------

Na sam koniec program zamyka kilka rejestrów, które mogły być ważne dla działania programu. Potem zamyka wszystkie handle do plików. Oznacza to, że wszystkie operacje, które nie są szyfrowaniem wykonują się na początku programu. Ta informacja ułatwi mi analizę programu w OllyDbg.

Od początku wykonywania programu do końca zajęło lekko ponad 30 min.

## Eksperymentowanie

Z ciekawości chciałem sprawdzić czy da się powstrzymać wirusa zaraz po uruchomieniu



Po ponownym uruchomieniu wyświetliło mi się okienko uprawnień administratora. Po odmówieniu program nadal działał i używał 100% dysku. Nawet po odmówieniu praw administratora program nadal szyfruje wszystkie pliki na dysku.

Jeżeli zabijemy program zanim zdążył utworzyć pliki (pierwszy jest w miejscu, w którym został uruchomiony) to program nie dodał się jeszcze do autostartu i nie jest w stanie wyrządzić więcej szkód. W przypadku kiedy plik się pojawił, zabicie procesu i restart nie powstrzymał wirusa.

Kiedy cały system plików jest zaszyfrowany i wyłączę komputer - nadal jestem w stanie go uruchomić. I tak jak przy każdym uruchomieniu wyświetla się informacja z żądaniem okupu

## Podsumowanie Wstępnej Analizy

Wstępna analiza pozwoliła mi wywnioskować bardzo dużo o tym jak działa wirus.

Wirus usuwa się z katalogu, w którym został uruchomiony i kopiuje się do lokalizacji %appdata%\Local\KeypassRansomware.exe.

Odczytuje on różne pliki oraz bardzo dużą ilość rejestrów, przy okazji dodając aplikację do autostartu.

Do każdego folderu z wyjątkiem katalogu systemowego Windows dodaje plik z żądaniem okupu. Po zakończeniu tej operacji rozpoczyna on szyfrowanie pierwszych 5 MB wszystkich plików poza plikami systemowymi.

Wirus kończy swoje działanie.

Po ponownym uruchomieniu komputera wyświetla się plik z żądaniem okupu.

# Zaawansowana Analiza Dynamiczna

Zaawansowaną analizę zacząłem od załadowania programu do IDA. Wczytałem również plik FLIRT vc32rtf, aby IDA rozpoznała standardowe funkcje np. biblioteki C.

Rozpoznałem funkcję wWinMain. Według dokumentacji Microsoft hPrevInstance wynosi zawsze 0 co było wskazówką do rozpoznania. Nie mogła być to funkcja main ponieważ kod wygenerowany przez kompilator wygląda inaczej niż typowo dla main. Dodatkowo ta funkcja przyjmuje 4 argumenty, a nie 3 jak main. Wcześniej wykonują się funkcje z prefiksem "w" co oznacza, że jest to wersja funkcji dla Unicode, a nie ANSI.

```
.text:0056219A  
.text:0056219A      loc_56219A:  
.text:0056219A 038 call      __wWinMain  
.text:0056219F 038 push     esi           ; nShowCmd  
.text:005621A0 03C push     eax           ; lpCmdLine  
.text:005621A1 040 push     0             ; hPrevInstance  
.text:005621A3 044 push     offset __ImageBase ; hInstance  
.text:005621A8 048 call     wWinMain
```

Nazwałem też kilka funkcji typu FilePathFind, aby móc sprawniej poruszać się w Olly.

Utworzyłem Migawkę w VirtualBoxie.

W IDA niestety nie da się rozpoznać wszystkich funkcji ponieważ adresy tych funkcji są zapisywane na stacku. Jest to forma zaciemnienia programu. Na szczęście w Olly udało mi się rozpoznać te funkcje.

W funkcji main jest widoczna taka funkcja

```
loc_949709:  
010 mov     eax, [esi]  
010 mov     ecx, esi  
010 call    dword ptr [eax+50h] ; sub_7C72BA  
010 test    eax, eax  
010 jnz     short loc_949729
```

Zaglądając do środka rozpoznałem kolejną funkcję za pomocą Olly. Funkcja to jedynie wywołanie kolejnej funkcji, która już w IDA jest widoczna

```

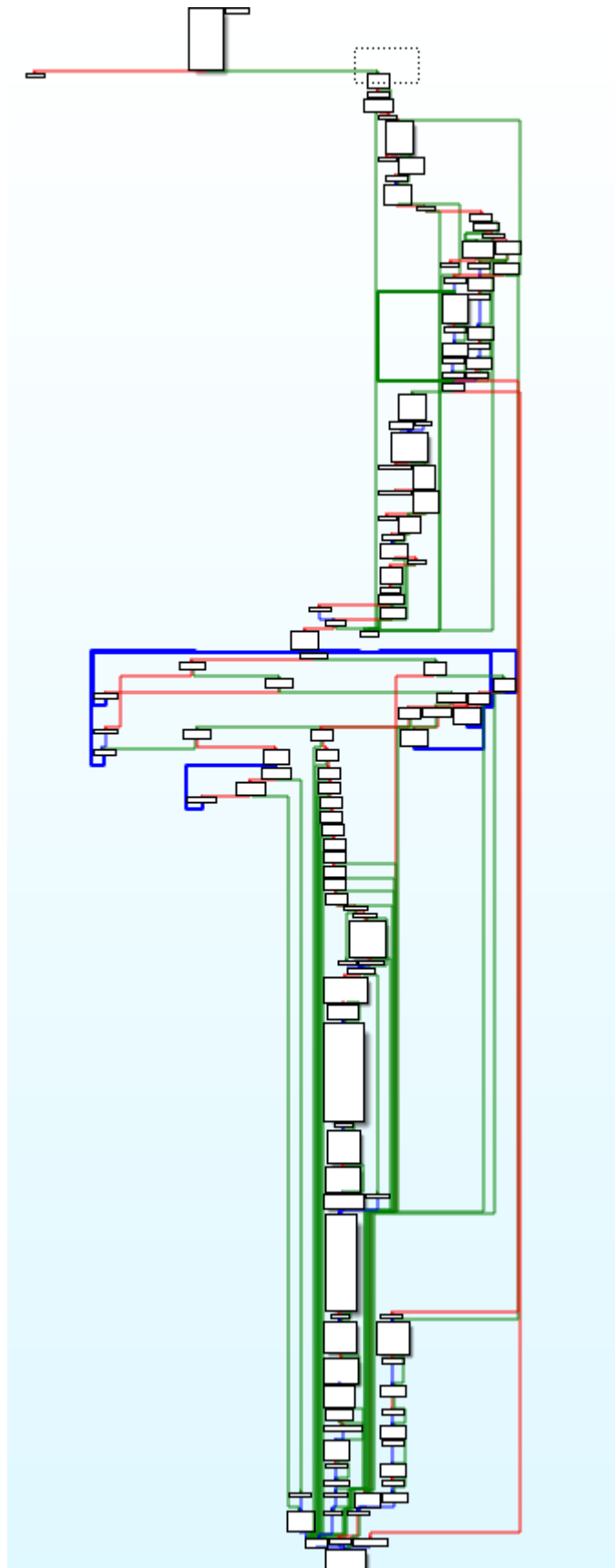
loc_7C72EB:
004 mov     eax, [esi]
004 mov     ecx, esi
004 call    dword ptr [eax+10Ch] ; sub_7C73FC
004 xor     eax, eax
004 inc     eax
004 pop     esi
000 retn

sub_7C73FC proc near
jmp     sub_7C7A51
sub_7C73FC endp

```

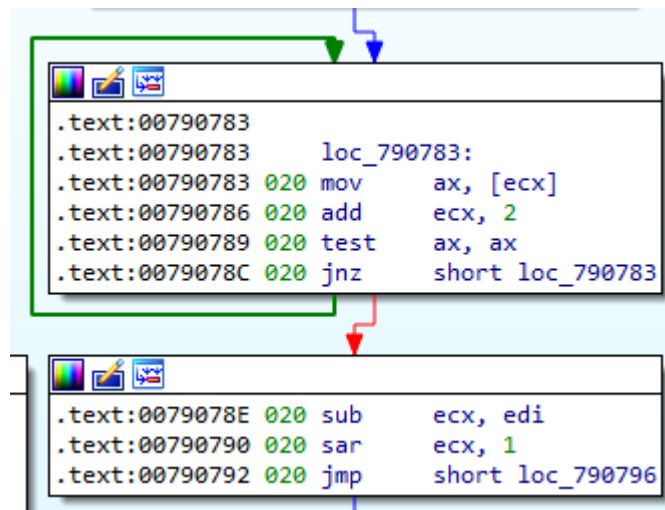
Ukazała się funkcja, która odczytuje rejestr  
 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies  
 Rejestr jest otwarty z opcją umożliwiającą jedynie odczyt wartości.

Następna funkcja również była zaciemniona i jest to prawdopodobnie najważniejsza funkcja tego programu, bo jest bardzo wielka i zawiera bardzo dużo innych funkcji wśród których znalazłem takie jak enumeracja procesów, kopiowanie i usuwanie plików.





Program w tej funkcji najpierw sprawdza gdzie znajduje się folder tymczasowy Temp. Pobiera następnie argumenty linii komend (czyli nazwę pliku, który wykonuje program) i porównuje obie ścieżki, przy okazji licząc jak długa jest ścieżka programu



Do rejestru Ecx jest dodawane 2, a nie 1 ponieważ program używa kodowania UTF-16. Na koniec przesuwą bitowo w prawo (dzieli liczbę na 2).

Funkcja została wywołana dwa razy: raz dla pełnej ścieżki i raz dla samej nazwy pliku.

Dalej wyszukuje folder Local Appdata za pomocą funkcji SHGetFolderPathW z argumentem [CSIDL](#) - 0x1C. Następnie łączy tę ścieżkę z nazwą pliku z poprzedniej funkcji w celu skopiowania programu do nowej lokalizacji.

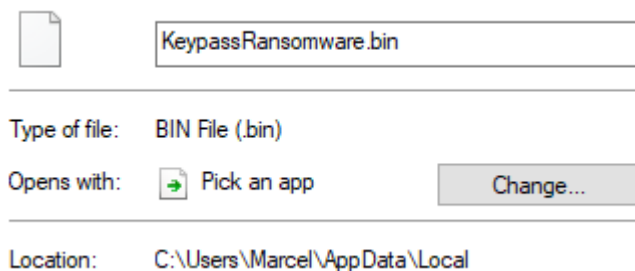
PUSH ESI	
PUSH 0	
PUSH 0	
PUSH 1C	
PUSH 0	
CALL DWORD PTR DS:[<&SHELL32.SHGetFolder	SHELL32.SHGetFolderPathW
PUSH DWORD PTR SS:[EBP-834]	None = "KeypassRansomware.bin"
PUSH ESI	Path
CALL DWORD PTR DS:[<&SHLWAPI.PathAppend	PathAppendW
PUSH DWORD PTR DS:[ESI-8]	Arg2
PUSH ESI	Arg1
CALL KeypassR.008E2CA6	KeypassR.008E2CA6

```

loc_793282:                ; lpFileName
push     esi
call     ds:DeleteFileW
push     0                ; bFailIfExists
push     esi              ; lpNewFileName
push     [ebp+pszPath]    ; lpExistingFileName
call     ds:CopyFileW

```

Warto zaznaczyć, że DeleteFileW usuwa plik z Local Appdata nawet jeżeli go tam nie ma.



Dalej dotarłem do funkcji ShellExecuteEx. Po wykonaniu jej program kończył swoje działanie, ponieważ utworzył się nowy podproces. Użyłem Olly aby się do niego “podpiąć”. Jest to dokładnie ten sam program, ale uruchomiony z innego miejsca (Local Appdata). Wcześniej opisałem, że program porównuje obie ścieżki, możliwe że to decyduje o dalszym przebiegu programu.

Program objął inną ścieżkę. Zamiast usunąć siebie i skopiować do Local Appdata (już się tam znajduje) obrał ścieżkę GlobalFree.

```
push    [ebp+hMem]      ; hMem
call    ds:GlobalFree
lea     edx, [esi-10h]
mov     byte ptr [ebp+var_4], 2
or      esi, 0FFFFFFFh
lea     ecx, [edx+0Ch]
mov     eax, esi
lock xadd [ecx], eax
dec     eax
test    eax, eax
jg      short loc_EA241E
```

Tutaj program próbował policzyć wszystkie procesy.

Następnie program wywołuje InitCommonControlsEx, które umożliwia tworzenie aplikacji GUI.

Odczytuje przy tym preferowany język, a następnie próbuje załadować bibliotekę odpowiednią danemu językowi (dla angielskiego en-US jest to KeypassRansomwareENU.dll, dla pl-PL jest to końcówka PLK.dll). Na koniec próbuje załadować bibliotekę z końcówką LOC.dll. Niestety nie posiadam takich bibliotek.

```

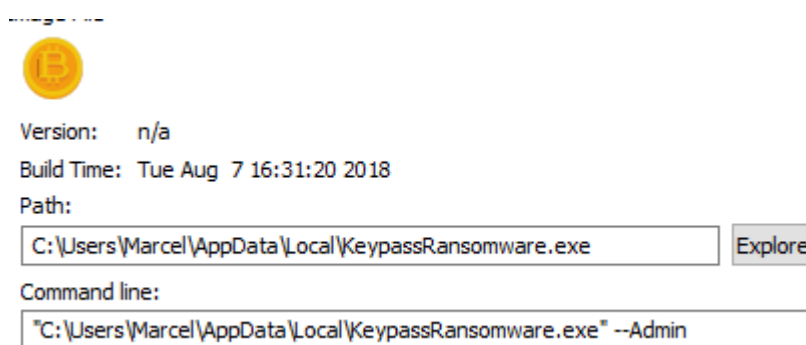
loc_7924AC:
DF8 mov     edx, offset aStart ; "start"
DF8 call    CopiedNewSus
DF8 push    eax
DFC call    sub_794020
DFC add     esp, 4
DF8 mov     [ebp+picce.dwSize], 8
DF8 lea     eax, [ebp+picce]
DF8 mov     [ebp+picce.dwICC], 0FFh
DF8 push    eax ; picce
DFC call    ds:InitCommonControlsEx
DF8 mov     ecx, ebx
DF8 call    sub_7C72FA
DF8 push    0
DFC call    sub_7C7C96
DFC push    0Ch
E00 call    sub_7BAB15
E00 add     esp, 8
DF8 mov     [ebp+var_DE0], eax
DF8 mov     [ebp+var_4], 7
DF8 test    eax, eax
DF8 jz      short loc_792520

```

Następna sekcja programu to bloki, które porównują czy program został uruchomiony z opcjami -Log, -Admin, -ForNetRes, -AutoStart. Jednak program nie został uruchomiony z tymi argumentami, więc obrał inną ścieżkę. W tej ścieżce program próbuje otworzyć podobne pliki, których nie ma u mnie na dysku.

CreateFile	C:\Windows\123.txtt	NAME NOT FO...
CreateFile	C:\Windows\123.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12344.txtt	NAME NOT FOUND
CreateFile	C:\Windows\123.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12344.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12355.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12366.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12377.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12388.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12399.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12300.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12____3.txtt	NAME NOT FOUND
CreateFile	C:\Windows\12_____3.txtt	NAME NOT FOUND
CreateFile	C:\Windows\123_____.txtt	NAME NOT FOUND

Następnie program uruchamia nowy proces z opcją –Admin



Nowy proces zaczął szyfrować pliki, więc to opcja –Admin odpowiada za szyfrowanie. Proces, który go uruchomił skończył swoją pracę.

Na początku proces Admin działa tak samo. Sprawdza, czy został uruchomiony z Local Appdata, enumeruje procesy oraz sprawdza czy istnieją pliki 123.txtt.

Dopiero tutaj zmienia się jego działanie. Program sprawdza, z którą opcją został uruchomiony. Działanie funkcji sprawdzającej zwraca uwagę jedynie na pierwszą podaną opcję, następne są ignorowane.

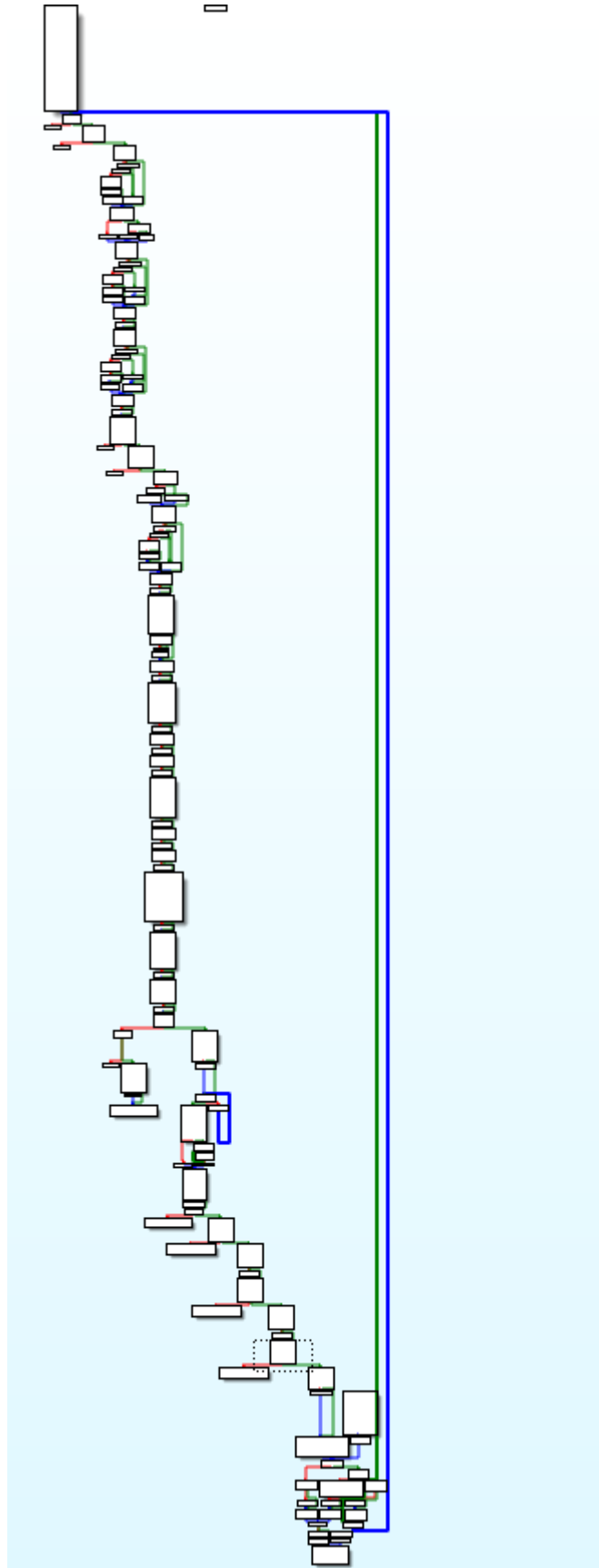
Program próbuje uruchomić Service Manager. W funkcji w której próbuje to zrobić widnieje też string *MYSQL*.

```
push    offset aMysql    ; "MYSQL"
lea     ecx, [esp+50h+lpServiceName]
mov     [esp+50h+var_28], 0
mov     word ptr [esp+50h+lpServiceName], ax
call    MYSQL
push    1                ; dwDesiredAccess
push    0                ; lpDatabaseName
push    0                ; lpMachineName
call    ds:OpenSCManagerW
```

W Procmon pojawiły się rejestry dotyczące [RPC](#) (Remote Procedure Call) umożliwiającą funkcjonalność Client-Server. Dzięki temu zainfekowana maszyna może przysyłać informacje przez połączenie zdalne.

RegOpenKey	HKLM\Software\WOW6432Node\Micr...
RegOpenKey	HKLM\SOFTWARE\Microsoft\Rpc
RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Rpc
RegQueryValue	HKLM\SOFTWARE\Microsoft\Rpc\Idle..
RegCloseKey	HKLM\SOFTWARE\Microsoft\Rpc

Program tworzy nowy wątek, który zaczyna się od funkcji sub\_D3ABC0 (ImageBase = 0xD10000, aby zgadzało się w Olly). Ta funkcja również jest ogromna.



Po szybkiej analizie statycznej zauważyłem tu dużo stringów sieciowych takich jak HTTP czy JSON. Moją uwagę przykuły dwie funkcje

```
call    ds:timeGetTime
push    eax                ; Seed
call    .srand
```

Program generuje losową wartość z seeda będącym obecnym czasem. Wartość jest podejrzana o bycie kluczem szyfrującym AES.

Funkcja jest wielką pętlą co wyjaśnia wiele zapytań we wstępnej analizie o stronę *kronus.pp.ua/* a konkretniej *kronus.pp.ua/upwinload/get.php*.

Funkcja nie odnosi sukcesu ponieważ host, z którym próbuje się połączyć nie odpowiada. Nie udało mi się odczytać konkretnych informacji na temat całego działania funkcji. Procmon pokazał jedynie odczyt pliku service w folderze ze sterownikami systemowymi. Może to być celowe działanie lub funkcjonalność systemu windows.

EAX=013F0D08, ASCII "A connection attempt failed because the connected party did not properly respond after a period of t  
Stack [03AFA190]=013F0D08, ASCII "A connection attempt failed because the connected party did not properly respond after  
Jump from 0D3B54E

ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,066, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,150, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,190, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,230, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,311, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,382, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,453, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,489, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,562, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,635, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,715, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,795, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,871, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,898, Length: 511
ReadFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	Offset: 1,925, Length: 511
CloseFile	C:\Windows\System32\drivers\etc\serv...SUCCESS	
Thread Exit	SUCCESS	Thread ID: 4268, User Time: 0.0156250, ..
Thread Exit	SUCCESS	Thread ID: 1432, User Time: 0.0312500, ..

Dalej w głównej w funkcji sprawdzana jest opcja -ForNetRes. Pojawiają też się takie stringi:

```
UNICODE "x5I74v4h003xJ0iyhUfH08W6o0RDSicmSfg72KUA"
UNICODE " 6se9RaIxXF9m70zWmx7nL3bURp691w4SNY8UCir0"
```

Powstaje z nich jedna długa opcja

```
UNICODE "--ForNetRes x5I74v4h003xJ0iyhUfHQSW6o0RDSicmSfg72KVA 6se9RaIxXF9m70zWmx7nL3bVRp691w4SNY8UCir0"
```

Może ona mieć wpływ na działanie programu

Tworzy się nowy proces

```
C:\Users\Marcel\AppData\Local\KeypassRansomware.exe --ForNetRes  
x5I74v4h003xJ0iyhUfHQSW6o0RDSicmSfg72KVA  
6se9RaIxXF9m70zWmx7nL3bVRp691w4SNY8UCir0
```

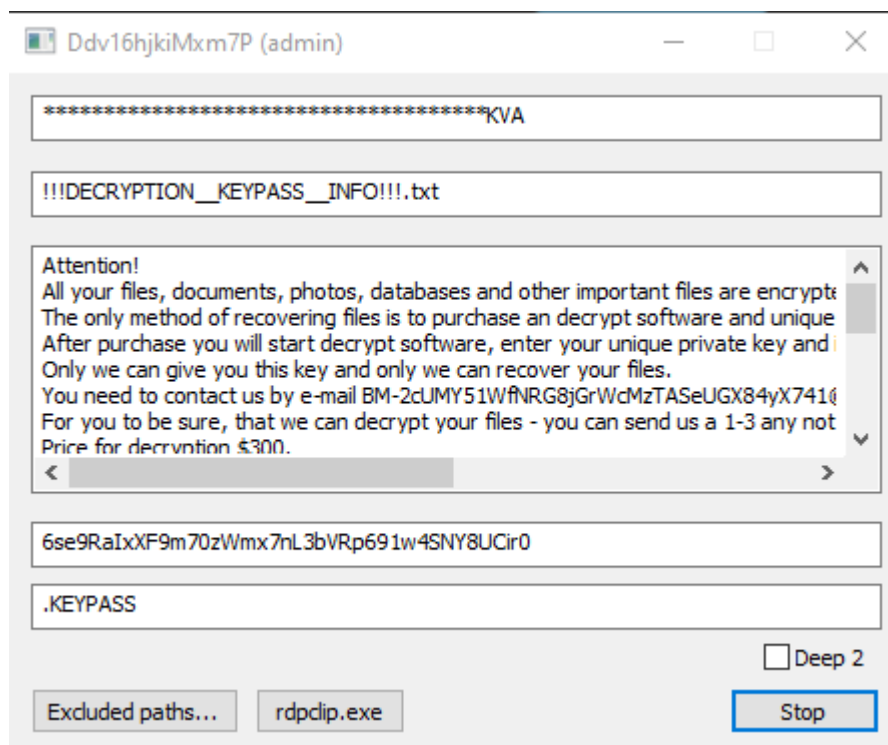
Obie wartości nie są zakodowane Base64. XOR też nie dał wartościowego wyniku.  
Oba stringi mają długość 40 znaków

Pojawił się również drugi proces:

```
C:\Users\Marcel\AppData\Local\KeypassRansomware.exe --Service <PPID>  
x5I74v4h003xJ0iyhUfHQSW6o0RDSicmSfg72KVA  
6se9RaIxXF9m70zWmx7nL3bVRp691w4SNY8UCir0
```

Nie wygląda na to, aby --Service wykonywał coś groźnego.

W międzyczasie kiedy zacząłem analizować nowopowstały wątek, główny proces  
(--Admin) rozpoczął dodawanie plików z okupem.



Zgodnie z treścią wiadomości losowy string jest naszym identyfikatorem, który należy przesłać przestępcom razem z 300\$ w celu odzyskania plików. Klucz który odsyłają jest zakodowany, lecz 3 ostatnie znaki są widoczne. Są one takie same jak przy pierwszym stringu podawanym do opcji –ForNetRes i –Service

Funkcja, która wykonuje kopiowanie pliku do każdego folderu oraz szyfrowanie to sub\_D542E1 wywoływana pod adresem 0xD2322D. Niestety kiedy pojawia się okienko, szyfrowanie włącza się mimo, że proces jest debugowany. Nie potrafię go zatrzymać w celu analizy. Jedyne co wiem na temat szyfrowania to klucz jakiego używa (nie udało mi się dowiedzieć w jakiej formie), oraz algorytm (po analizie statycznej za pomocą Binwalk jest to AES).



## Podsumowanie Analizy dynamicznej

Wirus jest bardzo dużym i skomplikowanym programem. Jest zaciemniony oraz utrudnia analizę.

Malware kopiuje siebie do Local Appdata, a następnie usuwa siebie z poprzedniego miejsca. Uruchamia proces z nowego miejsca oraz enumeruje procesy.

Sprawdza czy nie został uruchomiony, z którąś opcją spośród: –Admin, –Log, –Service <PPID>, –ForNetRes

Następnie uruchamia nowy proces z opcją –Admin jednocześnie kończąc stary. Proces Admin został dodany również do Autostartu

Proces Admin uruchamia dwa następne procesy z opcjami –ForNetRes <Klucz> <Personal ID> oraz –Service <PPID> <Klucz> <Personal ID>.

ForNetRes wysyła podane informacje w postaci pliku JSON (o ile uda mu się nawiązać połączenie) i na tym kończy swoją pracę.

Service nie robi nic złego, prawdopodobnie wysyła informacje procesowi Admin na temat klucza i personal ID.

Admin dodaje do każdego katalogu plik !!!DECRYPTION\_KEYPASS\_INFO!!!.txt.

Wyświetla się okno z tą samą informacją oraz 3 ostatnimi znakami klucza.

Po wyświetleniu okienka wirus przejmuje kontrolę i OllyDbg nie potrafił go zatrzymać, przez co rozpoczęło się szyfrowanie plików. Po przejęciu kontroli każda operacja Step Over trwała około 5 sekund co praktycznie uniemożliwiało dalsze debugowanie programu.

Do szyfrowania został użyty algorytm AES, lecz z powodu unikania debugera przy szyfrowaniu nie udało mi się stwierdzić w jakim trybie, ile bitów oraz jakie IV zostało użyte. Sam klucz składał się z 40 znaków, więc musiał przejść przez funkcję KDF, której też nie udało mi się namierzyć. Szyfrowane jest tylko pierwsze 5 MB Każdego pliku.

## Ochrona przed KeypassRansomware

Aby zapobiec zaszyfrowaniu dysku należy zabić proces KeypassRansomware, zanim pojawi się plik z żądaniem okupu. Wirus nie zdążył dodać siebie do autostartu, ani nie rozpoczął szyfrowania.

Kiedy plik się pojawił, ale nadal zabijemy program, trzeba będzie usunąć go z autostartu za pomocą rejestru SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Szyfrowanie plików zaczyna się od kosza oraz Program Files itd. Należy przejrzeć wszystkie katalogi i najwyżej pobrać zaszyfrowaną aplikację na nowo. Pliki w folderze Użytkownika są szyfrowane jako jedne z ostatnich więc mamy wystarczająco dużo czasu na wykonanie tej czynności.

W przypadku zaszyfrowania plików osobistych należy zobaczyć szczegóły procesu, który zużywa mniej zasobów i odczytanie z niego klucza oraz Personal ID. Kiedy znane są szczegóły szyfrowania możliwe jest napisanie programu, który odszyfruje pliki.

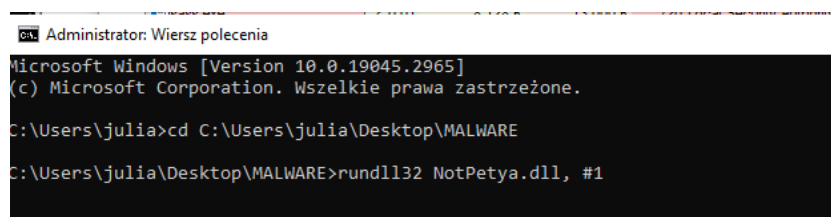
# NotPetya

## Uruchomienie wirusa

Aby odpalić wirusa należało zmienić jego rozszerzenie z .bin na .dll i w cmd (uruchamiając jako administrator) odpalić go poleceniem:

```
rundll32 NotPetya.dll, #1
```

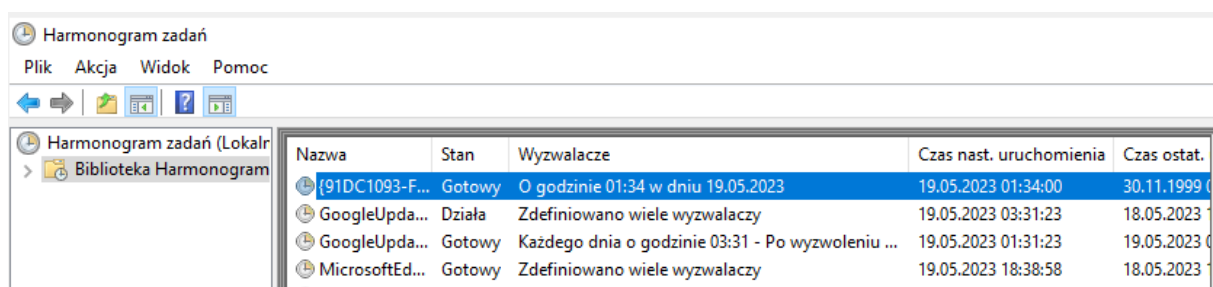
#1 -> oznacza punkt początkowy, który w tym przypadku to 1.



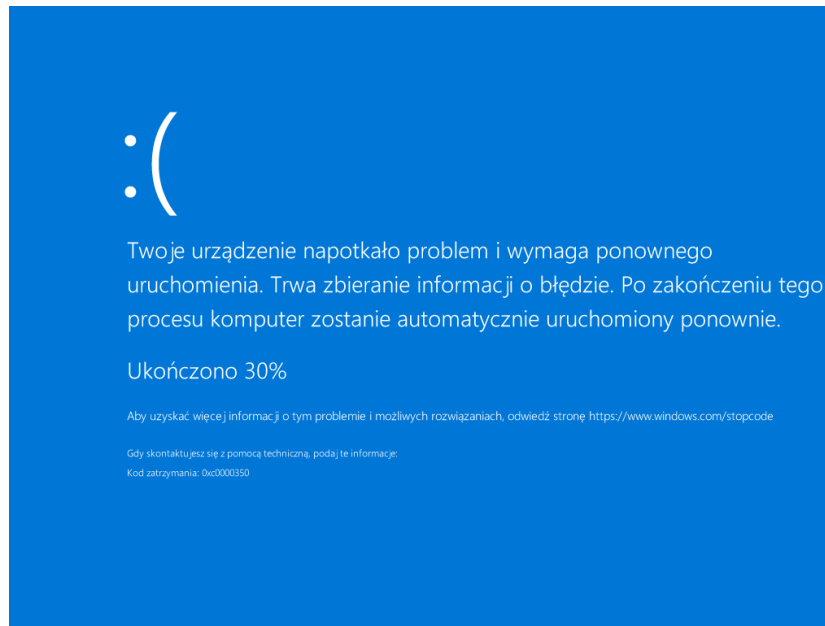
```
Administrator: Wiersz polecenia
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\julia>cd C:\Users\julia\Desktop\MALWARE
C:\Users\julia\Desktop\MALWARE>rundll32 NotPetya.dll, #1
```

Po włączeniu wirusa zwykły użytkownik nie widzi nic specjalnego.

W Harmonogramie zadań zostaje ustawione zadanie restartu komputera po około 1h od włączenia wirusa.



Po tym czasie użytkownik otrzymuje informację o ponownym uruchomieniu komputera. Gdy użytkownik samodzielnie zrestartuje komputer przed tym czasem będzie ten sam skutek.



Po ponownym włączeniu użytkownik dostaje informację o tym, że jego dysk został uszkodzony i partycja C jest naprawiana. Tak naprawdę rozpoczyna się mozolne szyfrowanie plików.

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 13568 of 4294967264 (0%)
```

Gdy proces szyfrowania się kończy dostajemy informację, że twoje ważne pliki zostały zaszyfrowane. Jest także informacja, że pliki zostaną odszyfrowane jeżeli przeleję się kwotę 300\$ w Bitcoinach na podany adres razem z teoretycznie personalnym mailem. Jednak email jest zawsze taki sam dla wszystkich zakażonych komputerów. Pod całą wiadomością znajduje się miejsce do wpisania klucza.

```
Ooops, your important files are encrypted.
```

```
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
```

```
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
```

```
Please follow the instructions:
```

```
1. Send $300 worth of Bitcoin to following address:
```

```
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx
```

```
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
```

```
r2EqKq-afZHq3-GEjpJr-XF1uJK-ntzZMR-JFqk1u-T2Y3Zn-mUJ6jZ-wxAYho-3VBBBw
```

```
If you already purchased your key, please enter it below.
```

```
Key: _
```

```
If you already purchased your key, please enter it below.
```

```
Key:
```

```
Incorrect key! Please try again.
```

```
Key: kjf
```

```
Incorrect key! Please try again.
```

```
Key: akjdfn
```

```
Incorrect key! Please try again.
```

```
Key:
```

```
Incorrect key! Please try again.
```

```
Key: key
```

```
Incorrect key! Please try again.
```

```
Key: _
```

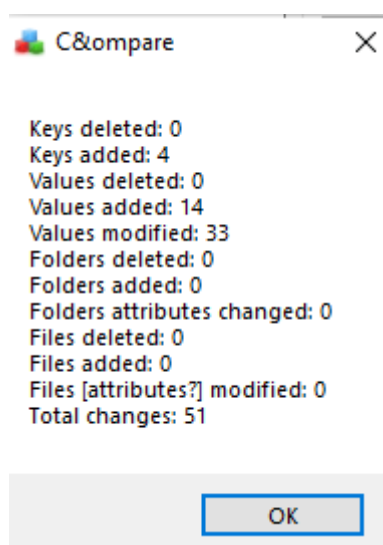
## Wstępna Analiza Dynamiczna

### Process Explorer





explorer.exe	0.76	91 916 K	138 056 K	3856	Eksplorator Windows	Microsoft Corporation
SecurityHealthSystray.exe		1 668 K	3 052 K	6876	Windows Security notificatio...	Microsoft Corporation
cmd.exe		3 456 K	4 728 K	3232	Windows Command Processor	Microsoft Corporation
conhost.exe	< 0.01	7 488 K	21 772 K	5548	Host okna konsoli	Microsoft Corporation
rundll32.exe		988 K	4 508 K	5876	Proces hosta systemu Windo...	Microsoft Corporation
rundll32.exe	2.78	7 764 K	13 620 K	3836	Windows host process (Run...	Microsoft Corporation
cmd.exe		2 260 K	4 540 K	2008	Windows Command Processor	Microsoft Corporation
conhost.exe		7 552 K	22 096 K	8864	Host okna konsoli	Microsoft Corporation
fakenet.exe		844 K	4 504 K	1876		
fakenet.exe	0.51	26 796 K	33 108 K	3040		

Pojawił się tylko jeden nowy proces - rundll32.exe, którym to był uruchomiony wirus. W procesie możemy odnaleźć stringi, które były już omawiane podczas analizy statycznej.

### RegShot



Według RegShot po uruchomieniu malware zostało dodanych 1 wartości rejestrów, a 33 zostały zmodyfikowane. 4 rejestry zostały dodane. Przy takich filtrach w Process Monitor:

Column	Relation	Value	Action
<input checked="" type="checkbox"/>  Process N...	is	rundll32.exe	Include
<input checked="" type="checkbox"/>  Operation	is	RegCreateKey	Include
<input checked="" type="checkbox"/>  Operation	is	RegSetValue	Include
<input checked="" type="checkbox"/>  Process N	is	Process.exe	Exclude

Zobaczmy takie wyniki:

Time ...	Process Name	PID	Operation	Path	Result
00:23:...	rundll32.exe	6444	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475	SUCCESS
00:23:...	rundll32.exe	6444	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3484787753-195693438-265454704-...	SUCCESS
00:37:...	rundll32.exe	3612	RegCreateKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS
00:37:...	rundll32.exe	3612	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS
00:44:...	rundll32.exe	3612	RegCreateKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS
00:44:...	rundll32.exe	3612	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS

#### Detail

Type: REG\_BINARY, Length: 368, Data: 71 03 00 00 00 00 00 00 04 00 04 00 01 02 03 00

Type: REG\_BINARY, Length: 24, Data: 53 98 A6 61 D7 89 D9 01 00 00 00 00 00 00 00

Desired Access: Query Value, Disposition: REG\_OPENED\_EXISTING\_KEY

Desired Access: Query Value, Disposition: REG\_OPENED\_EXISTING\_KEY

Desired Access: Query Value, Disposition: REG\_OPENED\_EXISTING\_KEY

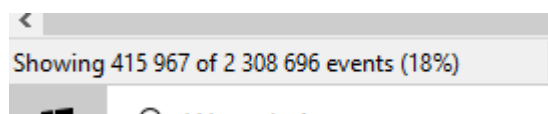
Desired Access: Query Value, Disposition: REG\_OPENED\_EXISTING\_KEY

W Process Monitor możemy zobaczyć stworzone dwa klucze rejestru:

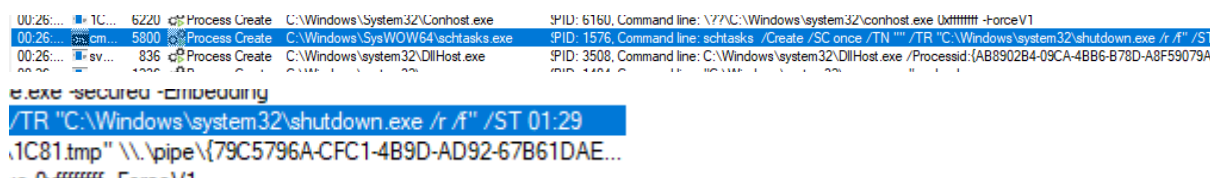
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connections:  
Ten klucz rejestru przechowuje globalne ustawienia połączenia internetowego dla wszystkich użytkowników komputera. Może zawierać konfigurację proxy, ustawienia sieci VPN lub inne ustawienia połączenia, które mają zastosowanie do wszystkich użytkowników systemu.
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections:  
Ten klucz rejestru za to przechowuje indywidualne ustawienia połączenia internetowego dla aktualnie zalogowanego użytkownika. Każdy użytkownik systemu Windows ma swój osobisty klucz rejestru HKCU, a w nim znajdują się jego własne ustawienia połączenia internetowego.

W dwóch zostały ustawione wartości

## Process Monitor



Wszystkich eventów, które zostały znalezione jest ponad 415 tysięcy.



Malware tworzy proces do czasowego restartu komputera.

00:23:...	rundll32.exe	6444	ReadFile	C:\Windows\System32\FirewallControlP...	SUCCESS	Offset: 360 448, Le...
00:23:...	rundll32.exe	6444	ReadFile	C:\Windows\System32\rundll32.exe	SUCCESS	Offset: 42 496, Len...
00:23:...	rundll32.exe	6444	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
00:23:...	rundll32.exe	6444	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: R...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Desired Access: R...
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: Name
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: Q...
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCR\CLSID\{00020424-0000-0000-C...	NAME NOT FOUND	Desired Access: Q...
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: Name
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: Name
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: M...
00:23:...	rundll32.exe	6444	RegQueryValue	HKCR\CLSID\{00020424-0000-0000-C...	NAME NOT FOUND	Length: 16
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: Name
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: M...
00:23:...	rundll32.exe	6444	RegQueryValue	HKCR\CLSID\{00020424-0000-0000-C...	BUFFER OVERFL...	Length: 12
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: Name
00:23:...	rundll32.exe	6444	RegQueryKey	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Query: HandleTag...
00:23:...	rundll32.exe	6444	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: M...
00:23:...	rundll32.exe	6444	RegQueryValue	HKCR\CLSID\{00020424-0000-0000-C...	SUCCESS	Type: REG_SZ, Le...

Malware odczytuje i wartości rejestrów m.in. HKCR, które są odpowiedzialne za przechowywanie informacji o zarejestrowanych typach plików, rozszerzeniach plików, programach, protokołach, rozszerzeniach powłoki i innych składnikach systemu.



00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\w...	REPARSE	Desired Access: Read
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Desired Access: Read
00:26:...	rundll32.exe	3068	RegEnumKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Index: 0, Name: wofis Instance
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Desired Access: Read
00:26:...	rundll32.exe	3068	RegQueryValue	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
00:26:...	rundll32.exe	3068	RegQueryValue	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Type: REG_SZ, Length: 14, Data: 189900
00:26:...	rundll32.exe	3068	RegCloseKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	
00:26:...	rundll32.exe	3068	RegEnumKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Index: 1, Name: wofis Outer Instance
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Desired Access: Read
00:26:...	rundll32.exe	3068	RegQueryValue	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
00:26:...	rundll32.exe	3068	RegQueryValue	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	Type: REG_SZ, Length: 14, Data: 189899
00:26:...	rundll32.exe	3068	RegCloseKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	
00:26:...	rundll32.exe	3068	RegEnumKey	HKLM\System\CurrentControlSet\Services\w...	NO MORE ENTRI...	Index: 2, Length: 80
00:26:...	rundll32.exe	3068	RegCloseKey	HKLM\System\CurrentControlSet\Services\w...	SUCCESS	
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\st...	REPARSE	Desired Access: Read
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	Desired Access: Read
00:26:...	rundll32.exe	3068	RegEnumKey	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	Index: 0, Name: storosft
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	Desired Access: Read
00:26:...	rundll32.exe	3068	RegQueryValue	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
00:26:...	rundll32.exe	3068	RegQueryValue	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	Type: REG_SZ, Length: 14, Data: 244000
00:26:...	rundll32.exe	3068	RegCloseKey	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	
00:26:...	rundll32.exe	3068	RegEnumKey	HKLM\System\CurrentControlSet\Services\st...	NO MORE ENTRI...	Index: 1, Length: 80
00:26:...	rundll32.exe	3068	RegCloseKey	HKLM\System\CurrentControlSet\Services\st...	SUCCESS	
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\p...	REPARSE	Desired Access: Read
00:26:...	rundll32.exe	3068	RegOpenKey	HKLM\System\CurrentControlSet\Services\p...	SUCCESS	Desired Access: Read

Odczytuje także klucz HKLM. Ten klucz zawiera informacje dotyczące konfiguracji systemu i oprogramowania na komputerze. Ścieżka HKLM/System/CurrentControlSet/ odnosi się do bieżącego zestawu sterowników i konfiguracji systemowych, które są używane podczas uruchamiania systemu. Procesy, które odczytują lub zmieniają wartości w tej ścieżce, mogą próbować uzyskać informacje na temat konfiguracji systemu lub dostosować ustawienia sterowników.

00:26:...	rundll32.exe	3068	WriteFile	C:\\$Secure:\$SDS:\$DATA	SUCCESS	Offset: 2 183 168, Length: 4 096, I/O Flags: Non-cached, Paging I/O, Synchron...
00:26:...	rundll32.exe	3068	WriteFile	C:\\$Secure:\$SDS:\$DATA	SUCCESS	Offset: 2 445 312, Length: 4 096, I/O Flags: Non-cached, Paging I/O, Synchron...
00:26:...	rundll32.exe	3068	WriteFile	C:\Users\Wlodek\AppData\Local\Microsoft\Edge...	SUCCESS	Offset: 0, Length: 8 192, I/O Flags: Non-cached, Paging I/O, Synchronous Pa...

Malware wykonuje zmiany w pliku \$Secure:\$SDS:\$DATA, który przechowuje informacje o zabezpieczeniach plików i folderów na dysku.

00:32:...	rundll32.exe	3068	CreateFileMap...	C:\Python39\Lib\site-packages\visgraph\__p...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_REA...
00:32:...	rundll32.exe	3068	QueryStandardl...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	AllocationSize: 8 192, EndOfFile: 6 243, NumberOfLinks: 1, DeletePending: Fal...
00:32:...	rundll32.exe	3068	SetEndOfFileInf...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	EndOfFile: 6 256
00:32:...	rundll32.exe	3068	CreateFileMap...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	SyncType: SyncTypeOther
00:32:...	rundll32.exe	3068	ReadFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	Offset: 0, Length: 6 256, I/O Flags: Non-cached, Paging I/O, Synchronous Pa...
00:32:...	rundll32.exe	3068	WriteFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	Offset: 0, Length: 8 192, I/O Flags: Non-cached, Paging I/O, Synchronous Pa...
00:32:...	rundll32.exe	3068	CloseFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	
00:32:...	rundll32.exe	3068	CreateFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	Desired Access: Generic Read/Write, Disposition: Open, Options: Synchronou...
00:32:...	rundll32.exe	3068	QueryStandardl...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	AllocationSize: 232, EndOfFile: 227, NumberOfLinks: 1, DeletePending: False...
00:32:...	rundll32.exe	3068	CreateFileMap...	C:\Python39\Lib\site-packages\visgraph\__p...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_REA...
00:32:...	rundll32.exe	3068	QueryStandardl...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	AllocationSize: 232, EndOfFile: 227, NumberOfLinks: 1, DeletePending: False...
00:32:...	rundll32.exe	3068	SetEndOfFileInf...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	EndOfFile: 240
00:32:...	rundll32.exe	3068	CreateFileMap...	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	SyncType: SyncTypeOther
00:32:...	rundll32.exe	3068	ReadFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	Offset: 0, Length: 240, I/O Flags: Non-cached, Paging I/O, Synchronous Pag...
00:32:...	rundll32.exe	3068	WriteFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	Offset: 0, Length: 4 096, I/O Flags: Non-cached, Paging I/O, Synchronous Pa...
00:32:...	rundll32.exe	3068	CloseFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	
00:32:...	rundll32.exe	3068	QueryDirectory	C:\Python39\Lib\site-packages\visgraph\__p...	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
00:32:...	rundll32.exe	3068	CloseFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	
00:32:...	rundll32.exe	3068	QueryDirectory	C:\Python39\Lib\site-packages\visgraph\__p...	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
00:32:...	rundll32.exe	3068	CloseFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	
00:32:...	rundll32.exe	3068	CreateFile	C:\Python39\Lib\site-packages\visgraph\__p...	SUCCESS	Desired Access: Read Data (Not Directory), Synchronous, Disposition: Create...

00:32:...	rundll32.exe	3068	SetEndOfFileInf...	C:\Tools\cygwin\usr\share\man\man1\chrt.1.gz	SUCCESS	EndOfFile: 1968
00:32:...	rundll32.exe	3068	CreateFileMapp...	C:\Tools\cygwin\usr\share\man\man1\chrt.1.gz	SUCCESS	SyncType: SyncTypeOther
00:32:...	rundll32.exe	3068	ReadFile	C:\Tools\cygwin\usr\share\man\man1\chrt.1.gz	SUCCESS	Offset: 0, Length: 1968, I/O Flags: Non-cached, Paging I/O, Sync
00:32:...	rundll32.exe	3068	WriteFile	C:\Tools\cygwin\usr\share\man\man1\chrt.1.gz	SUCCESS	Offset: 0, Length: 4 096, I/O Flags: Non-cached, Paging I/O, Sync
00:32:...	rundll32.exe	3068	CloseFile	C:\Tools\cygwin\usr\share\man\man1\chrt.1.gz	SUCCESS	
00:32:...	rundll32.exe	3068	CreateFile	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	Desired Access: Generic Read/Write, Disposition: Open, Options:
00:32:...	rundll32.exe	3068	QueryStandardI...	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	AllocationSize: 12 288, EndOfFile: 9 616, NumberOfLinks: 1, Delet
00:32:...	rundll32.exe	3068	CreateFileMapp...	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXE
00:32:...	rundll32.exe	3068	QueryStandardI...	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	AllocationSize: 12 288, EndOfFile: 9 616, NumberOfLinks: 1, Delet
00:32:...	rundll32.exe	3068	SetEndOfFileInf...	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	EndOfFile: 9 632
00:32:...	rundll32.exe	3068	CreateFileMapp...	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	SyncType: SyncTypeOther
00:32:...	rundll32.exe	3068	ReadFile	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	Offset: 0, Length: 9 632, I/O Flags: Non-cached, AllocationSize: 12 288, EndOfFile: 9 616, NumberOfLinks: 1, Delet
00:32:...	rundll32.exe	3068	WriteFile	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	Offset: 0, Length: 12 288, I/O Flags: Non-cached, EndOfFile: 9 616
00:32:...	rundll32.exe	3068	CloseFile	C:\Tools\cygwin\usr\share\man\man1\ciphers.1.gz	SUCCESS	DeletePending: F
00:32:...	rundll32.exe	3068	CreateFile	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	SUCCESS	Directory: False
00:32:...	rundll32.exe	3068	QueryStandardI...	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	SUCCESS	Desired Access: Generic Read/Write, Disposition: Open, Options:
00:32:...	rundll32.exe	3068	CreateFileMapp...	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXE
00:32:...	rundll32.exe	3068	QueryStandardI...	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	SUCCESS	AllocationSize: 4 096, EndOfFile: 1 427, NumberOfLinks: 1, Delet
00:32:...	rundll32.exe	3068	SetEndOfFileInf...	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	SUCCESS	EndOfFile: 1 440
00:32:...	rundll32.exe	3068	CreateFileMapp...	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	SUCCESS	SyncType: SyncTypeOther
00:32:...	rundll32.exe	3068	ReadFile	C:\Tools\cygwin\usr\share\man\man1\cksum.1.gz	SUCCESS	Offset: 0, Length: 1 440, I/O Flags: Non-cached, Paging I/O, Sync
00:33:...	rundll32.exe	3068	CloseFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\Vogs	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition:
00:33:...	rundll32.exe	3068	CreateFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: .
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: ..., 2: Personal, 3
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition:
00:33:...	rundll32.exe	3068	CreateFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: .
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: ..., 2: assertInfor
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
00:33:...	rundll32.exe	3068	CloseFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	FileInformationClass: FileBothDirectoryInformation
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
00:33:...	rundll32.exe	3068	CloseFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\settings	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition:
00:33:...	rundll32.exe	3068	CreateFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: .
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: ..., 2: ECSCConfig
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition:
00:33:...	rundll32.exe	3068	CreateFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: *, 2: .
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: ..., 2: DeviceHea
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: Install_2023-05-
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: Update_2023-05-
00:33:...	rundll32.exe	3068	QueryDirectory	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
00:33:...	rundll32.exe	3068	CloseFile	C:\Users\julia\AppData\Local\Microsoft\OneDrive\setup	SUCCESS	

NotPeya zmienia, a także wykorzystuje funkcję CreateFile, aby utworzyć plik. Szuka także ścieżki do takich folderów jak: C:\Python39, C:\Tools, C:\Users\julia. Znajduje się mnóstwo takich zdarzeń

00:42:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50879 -> 192.168.56.250:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:42:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50879 -> 192.168.56.250:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:42:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50880 -> 192.168.56.250:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:42:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50880 -> 192.168.56.250:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:42:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50881 -> 192.168.56.251:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:42:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50881 -> 192.168.56.251:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50882 -> 192.168.56.251:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50882 -> 192.168.56.251:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50883 -> 192.168.56.252:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50883 -> 192.168.56.252:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50884 -> 192.168.56.252:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50884 -> 192.168.56.252:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50885 -> 192.168.56.253:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50885 -> 192.168.56.253:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50886 -> 192.168.56.253:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50886 -> 192.168.56.253:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50887 -> 192.168.56.254:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50887 -> 192.168.56.254:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Reconnect	DESKTOP-KOF02SB-50888 -> 192.168.56.254:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50888 -> 192.168.56.254:netbios-ssn	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:43:...	rundll32.exe	3068	Thread Exit		SUCCESS	Thread ID: 7192, User Time: 0.0156250, Kernel Time: 0.1250000
00:43:...	rundll32.exe	3068	Thread Exit		SUCCESS	Thread ID: 8896, User Time: 0.0000000, Kernel Time: 0.0000000
00:46:...	rundll32.exe	3068	TCP Connect	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 262800
00:46:...	rundll32.exe	3068	TCP Send	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 137, starttime: 4518219, endtime: 4518220, seqnum: 0, conn
00:46:...	rundll32.exe	3068	TCP Receive	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 137, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Send	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 140, starttime: 4518222, endtime: 4518222, seqnum: 0, conn
00:46:...	rundll32.exe	3068	TCP Receive	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 140, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Send	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 43, starttime: 4518228, endtime: 4518229, seqnum: 0, connid
00:46:...	rundll32.exe	3068	TCP Receive	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 43, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50901 -> DESKTOP-URVJSB0:micro...	SUCCESS	Length: 0, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Connect	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 262800
00:46:...	rundll32.exe	3068	TCP Send	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 137, starttime: 4518235, endtime: 4518236, seqnum: 0, conn
00:46:...	rundll32.exe	3068	TCP Receive	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 137, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Send	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 140, starttime: 4518241, endtime: 4518241, seqnum: 0, conn
00:46:...	rundll32.exe	3068	TCP Receive	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 140, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Send	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 43, starttime: 4518246, endtime: 4518247, seqnum: 0, connid
00:46:...	rundll32.exe	3068	TCP Receive	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 43, seqnum: 0, connid: 0
00:46:...	rundll32.exe	3068	TCP Disconnect	DESKTOP-KOF02SB-50903 -> 192.168.56.100:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0

Malware próbuje się połączyć z Internetem.



## Sieć

Na samym początku komunikacji program próbuje wysłać informacje do sieci

```
05/19/23 12:32:00 AM [RawTCPListener] 0000: 20 4C 4D 20 30 2E 31 32 00 02 53 4D 42 20 32 2E LM 0.12..SMB 2.
05/19/23 12:32:00 AM [Diverter] rundll32.exe (3836) requested TCP 192.168.56.1:80 002..SMB 2.???
05/19/23 12:32:00 AM [Diverter] System (4) requested TCP 192.168.56.1:445
05/19/23 12:32:00 AM [RawTCPListener] Connection timeout
05/19/23 12:32:00 AM [RawTCPListener] 0000: 00 00 00 9B FF 53 4D 42 72 00 00 00 00 18 53 C8 .....SMB.....S.
05/19/23 12:32:00 AM [RawTCPListener] 0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE .....X..PC NETWO
05/19/23 12:32:00 AM [RawTCPListener] 0020: 00 00 00 00 00 78 00 02 50 43 20 4E 45 54 57 4F .....RK PROGRAM 1.0..
05/19/23 12:32:00 AM [RawTCPListener] 0030: 52 48 20 50 52 4F 47 52 41 40 20 31 2E 30 00 02 LANMAN1.0..Windo
05/19/23 12:32:00 AM [RawTCPListener] 0040: 4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F s 3.1a..LM1.2X00
05/19/23 12:32:00 AM [RawTCPListener] 0050: 77 73 20 66 6F 72 20 57 6F 72 68 67 72 6F 75 70 ws for Workgroup
05/19/23 12:32:00 AM [RawTCPListener] 0060: 73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30 s 3.1a..LM1.2X00
05/19/23 12:32:00 AM [RawTCPListener] 0070: 32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54 2..LANMAN2.1..NT
05/19/23 12:32:00 AM [RawTCPListener] 0080: 20 4C 4D 20 30 2E 31 32 00 02 53 4D 42 20 32 2E LM 0.12..SMB 2.
05/19/23 12:32:01 AM [RawTCPListener] 0090: 30 30 32 00 02 53 4D 42 20 32 2E 3F 3F 00 002..SMB 2.???
05/19/23 12:32:01 AM [RawTCPListener] 0000: 00 00 00 9B FF 53 4D 42 72 00 00 00 00 18 53 C8 .....SMB.....S.
05/19/23 12:32:01 AM [RawTCPListener] 0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE .....X..PC NETWO
05/19/23 12:32:01 AM [RawTCPListener] 0020: 00 00 00 00 00 78 00 02 50 43 20 4E 45 54 57 4F .....RK PROGRAM 1.0..
05/19/23 12:32:01 AM [RawTCPListener] 0030: 52 48 20 50 52 4F 47 52 41 40 20 31 2E 30 00 02 LANMAN1.0..Windo
05/19/23 12:32:01 AM [RawTCPListener] 0040: 4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F s 3.1a..LM1.2X00
05/19/23 12:32:01 AM [RawTCPListener] 0050: 77 73 20 66 6F 72 20 57 6F 72 68 67 72 6F 75 70 ws for Workgroup
05/19/23 12:32:01 AM [RawTCPListener] 0060: 73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30 s 3.1a..LM1.2X00
05/19/23 12:32:01 AM [RawTCPListener] 0070: 32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54 2..LANMAN2.1..NT
05/19/23 12:32:01 AM [RawTCPListener] 0080: 20 4C 4D 20 30 2E 31 32 00 02 53 4D 42 20 32 2E LM 0.12..SMB 2.
05/19/23 12:32:01 AM [RawTCPListener] 0090: 30 30 32 00 02 53 4D 42 20 32 2E 3F 3F 00 002..SMB 2.???
05/19/23 12:32:01 AM [RawTCPListener] Connection timeout
05/19/23 12:32:01 AM [RawTCPListener] 0000: 00 00 00 9B FF 53 4D 42 72 00 00 00 00 18 53 C8 .....SMB.....S.
05/19/23 12:32:01 AM [RawTCPListener] 0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE .....X..PC NETWO
05/19/23 12:32:01 AM [RawTCPListener] 0020: 00 00 00 00 00 78 00 02 50 43 20 4E 45 54 57 4F .....RK PROGRAM 1.0..
05/19/23 12:32:01 AM [RawTCPListener] 0030: 52 48 20 50 52 4F 47 52 41 40 20 31 2E 30 00 02 LANMAN1.0..Windo
05/19/23 12:32:01 AM [RawTCPListener] 0040: 4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F s 3.1a..LM1.2X00
05/19/23 12:32:01 AM [RawTCPListener] 0050: 77 73 20 66 6F 72 20 57 6F 72 68 67 72 6F 75 70 ws for Workgroup
05/19/23 12:32:01 AM [RawTCPListener] 0060: 73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30 s 3.1a..LM1.2X00
05/19/23 12:32:01 AM [RawTCPListener] 0070: 32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54 2..LANMAN2.1..NT
```

Następnie próbuje pingować domenę 43.56.168.192.in-addr.arpa, który jest rekordem PTR (Pointer) w systemie Domain Name System (DNS) odwracający standardową notację adresu IP na nazwę domenową. Jednak ta domena nie dostarcza informacji o konkretnym zasobie sieciowym ani nie prowadzi do konkretnej strony internetowej.

```
FakeNet-NG - "C:\Tools\FakeNet-NG\fakeNet1.4.11\fakeNet.exe"
05/19/23 12:34:34 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:34 AM [DNS Server] Received PTR request for domain '41.56.168.192.in-addr.arpa'.
05/19/23 12:34:36 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:36 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:37 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:38 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:38 AM [DNS Server] Received PTR request for domain '42.56.168.192.in-addr.arpa'.
05/19/23 12:34:39 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:40 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:41 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:42 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:42 AM [DNS Server] Received PTR request for domain '43.56.168.192.in-addr.arpa'.
05/19/23 12:34:44 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:44 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:45 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:46 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:46 AM [DNS Server] Received PTR request for domain '44.56.168.192.in-addr.arpa'.
05/19/23 12:34:46 AM [DNS Server] Received A request for domain 'activity.windows.com'.
05/19/23 12:34:48 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:49 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:49 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:50 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:50 AM [DNS Server] Received PTR request for domain '45.56.168.192.in-addr.arpa'.
05/19/23 12:34:52 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:52 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:53 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:54 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:54 AM [DNS Server] Received PTR request for domain '46.56.168.192.in-addr.arpa'.
05/19/23 12:34:54 AM [DNS Server] Received A request for domain 'slscr.update.microsoft.com'.
05/19/23 12:34:56 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:56 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:57 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:58 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:34:58 AM [DNS Server] Received PTR request for domain '47.56.168.192.in-addr.arpa'.
05/19/23 12:35:00 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:35:00 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:35:01 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:35:02 AM [Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
05/19/23 12:35:02 AM [DNS Server] Received PTR request for domain '48.56.168.192.in-addr.arpa' system Window
```

## Wireshark

770	115.141996	192.168.112.131	23.55.155.27	TCP	54 49262 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
772	115.142020	192.168.112.131	23.55.155.27	HTTP	220 PROPFIND /admin\$/ HTTP/1.1
773	115.142133	23.55.155.27	192.168.112.131	TCP	60 80 → 49262 [ACK] Seq=1 Ack=167 Win=64240 Len=0

Widzimy, że NotPetya próbuje wysłać zapytanie HTTP ze ścieżką admin\$.

1032	256.949326	192.168.112.131	192.168.112.129	SMB2	162 Negotiate Protocol Request
1033	256.949635	192.168.112.129	192.168.112.131	SMB2	260 Negotiate Protocol Response
1034	256.950284	192.168.112.131	192.168.112.129	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
1035	256.950824	192.168.112.129	192.168.112.131	SMB2	299 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
1036	256.951128	192.168.112.131	192.168.112.129	SMB2	635 Session Setup Request, NTLMSSP_AUTH, User: WIN-006HFMLC6IV\Crystal
1037	256.951828	192.168.112.129	192.168.112.131	SMB2	139 Session Setup Response
1038	256.952101	192.168.112.131	192.168.112.129	SMB2	178 Tree Connect Request Tree: \\192.168.112.129\admin\$
1039	256.952413	192.168.112.129	192.168.112.131	SMB2	131 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1040	256.952444	192.168.112.131	192.168.112.129	SMB2	126 Session Logoff Request

Jest sporo zapytań SMB2, które mogą służyć do przeszukiwania sieci w celu znalezienia innych urządzeń w niej (Tree Connect Request)

715	114.978169	192.168.112.131	192.168.112.1	SMB2	162 Negotiate Protocol Request
717	114.985313	192.168.112.131	192.168.112.1	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
719	114.985978	192.168.112.131	192.168.112.1	SMB2	713 Session Setup Request, NTLMSSP_AUTH, User: WIN-006HFMLC6IV\Crystal
725	114.990525	192.168.112.131	192.168.112.1	SMB2	162 Negotiate Protocol Request
727	114.993620	192.168.112.131	192.168.112.1	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
729	114.994217	192.168.112.131	192.168.112.1	SMB2	713 Session Setup Request, NTLMSSP_AUTH, User: WIN-006HFMLC6IV\Crystal
735	114.996934	192.168.112.131	192.168.112.1	SMB2	162 Negotiate Protocol Request
740	115.078830	192.168.112.131	192.168.112.1	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
742	115.079447	192.168.112.131	192.168.112.1	SMB2	713 Session Setup Request, NTLMSSP_AUTH, User: WIN-006HFMLC6IV\Crystal
748	115.082917	192.168.112.131	192.168.112.1	SMB2	162 Negotiate Protocol Request
750	115.085765	192.168.112.131	192.168.112.1	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
752	115.086468	192.168.112.131	192.168.112.1	SMB2	713 Session Setup Request, NTLMSSP_AUTH, User: WIN-006HFMLC6IV\Crystal
758	115.089833	192.168.112.131	192.168.112.1	SMB2	162 Negotiate Protocol Request
760	115.093851	192.168.112.131	192.168.112.1	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
762	115.094340	192.168.112.131	192.168.112.1	SMB2	713 Session Setup Request, NTLMSSP_AUTH, User: WIN-006HFMLC6IV\Crystal
312	66.347755	192.168.112.131	192.168.112.129	SMB2	162 Negotiate Protocol Request
314	66.350003	192.168.112.131	192.168.112.129	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
316	66.352374	192.168.112.131	192.168.112.129	SMB2	318 Session Setup Request, NTLMSSP_AUTH, User: \
318	66.353103	192.168.112.131	192.168.112.129	SMB2	156 Tree Connect Request Tree: \\REMNUX\IPC\$
585	89.695213	192.168.112.131	192.168.112.129	SMB2	126 Tree Disconnect Request
587	89.696019	192.168.112.131	192.168.112.129	SMB2	126 Session Logoff Request
1032	256.949326	192.168.112.131	192.168.112.129	SMB2	162 Negotiate Protocol Request

## Podsumowanie Wstępnej Analizy Dynamicznej

- NotPetya po włączeniu zmienia i odczytuje rejestry w celu znalezienia jak największej ilości informacji o systemie.
- Próbuje także nawiązać połączenie z siecią.
- Za pomocą SMB2 przeszukuje sieć w celu znalezienia innych podłączonych do niej komputerów, aby się rozprzestrzenić.
- Ustawia w Harmonogramie zadań restart komputera.
- Po wykonaniu restartu malware szyfruje pliki
- Następnie ukazana jest informacja o żądaniu okupu.

# Zaawansowana Analiza Dynamiczna

## Biblioteka i funkcje UI

Malware używa takich funkcji jak LoadLibraryExW, aby załadować bibliotekę.

75A88D59	56	PUSH ESI	Arg2
75A88D5A	FF75 F4	PUSH DWORD PTR SS:[LOCAL.3]	Arg1 => [LOCAL.3]
75A88D5D	E8 7EF3FFFF	CALL LoadLibraryExW	KERNELBASE.LoadLibraryExW
75A88D62	8BF0	MOV ESI, EAX	
75A88D64	8D45 F8	LEA EDI, [LOCAL.4]	

W czasie działania funkcji LoadCursor zapisuje w rejestrze ESI ścieżkę do pliku malware.

```
EBP 0019F664
ESI 00624240 ASCII "C:\Users\julia\Desktop\MALWARE\NotPetya.dll"
EDI 00000000
```

W funkcji USER32.MbToWCSEx wykonuje operacje na stringu "LoadDLLClass"

- usuwa od początku po jednym znaku
- odczytuje od początku po jednym znaku
- porównuje rejestry

76998000	57	PUSH EDI	Arg1
76998001	E8 1A32FFFF	CALL MBToWCSEx	USER32.MBToWCSEx
76998006	85C0	TEST EAX, EAX	
76998009	8B48 28	MOV ECX, DWORD PTR DS:[EBX+28]	ASCII "LoadDLLClass"
76982403	3B05 B45CA071	CMP EAX, DWORD PTR DS:[76A05CB4]	
76982409	74 13	JE SHORT 769824EE	
7698240B	8B48 28	MOV ECX, DWORD PTR DS:[EBX+28]	ASCII "LoadDLLClass"
7698240E	33D2	XOR EDX, EDX	
769824E0	42	INC EDX	

```
Registers (FPU)
EAX 0019FD6C
ECX 004021AA ASCII "ass"
EDX 004021A2 ASCII "oadDLLClass"
EBX 00000000
ESP 0019FCF8
EBP 0019FD08
ESI FFFFFFFF
EDI FFFFFFFF
```

77381F8A	> 8B35 4063447	MOV ESI, DWORD PTR DS:[77446940]		Registers (FPU)
77381F90	33C9	XOR ECX, ECX		EAX 0000004C
77381F92	85D2	TEST EDI, EDI		ECX 00000006
77381F94	> 74 17	JZ SHORT 77381FAD		EDX 00000000
77381F96	> 8B7D 14	MOV EDI, DWORD PTR SS:[ARG.4]		EBX 00625900 UNICODE "LoadDL"
77381F99	> 85D0 08	MOV EBX, DWORD PTR SS:[ARG.1]		ESP 0019FCC4
77381F9C	> 0FB60439	MOVZX EAX, BYTE PTR DS:[EDI+ECX]		EBP 0019FDC0
77381FA0	> 66180446	MOV AX, WORD PTR DS:[EAX*2+ESI]		ESI 77FB001C
77381FA4	> 66180446	MOV WORD PTR DS:[ECX*2+EBX], AX		EDI 004021A1 ASCII "LoadDLLClass"
77381FA8	> 41	INC ECX		EIP 77381FAB ntdll.77381FAB
77381FAB	> 3BCA	CMP ECX, EDX		C 1 ES 002B 32bit 0(FFFFFFFF)
77381FAD	> 72 EF	JNB SHORT 77381F9C		P 1 CS 0023 32bit 0(FFFFFFFF)
77381FAE	> 5F	POP EDI		A 1 SS 002B 32bit 0(FFFFFFFF)
77381FAF	> 5B	POP ESI		Z 0 DS 002B 32bit 0(FFFFFFFF)
77381FB0	> 33C0	XOR EAX, EAX		S 1 FS 0053 32bit 370000(FFF)
77381FB2	> C9	LEAVE		T 0 GS 002B 32bit 0(FFFFFFFF)
77381FB3	> C2 1400	RETN 14		D 0
77381FB6	> 8D0412	LEA EAX, [EDX+EDX]		D 0 LastErr: 00000000 ERROR_SUCCESS
77381FB9	> 9B01	MOV DWORD PTR DS:[ECX], EAX		EFL 00000297 (NO, B, NE, BE, S, PE, L, LE)
77381FBB	> EB CD	JMP SHORT 77381F8A		ST0 empty 0.0
77381FBD	> 8BFF	MOV EDI, EDI		

Razem ze stringiem znajdują się takie napisy jak "Button", "Edit", "ComboBox". Malware może próbować manipulować elementami interfejsu użytkownika, takimi jak przyciski ("Button"), rozwijane listy ("ComboBox") lub pola tekstowe ("Edit"), aby wprowadzić użytkownika w błąd lub uzyskać pewne dane. W tym kontekście,

“LoadDLLClass” może wskazywać na ładowanie klasy, która dostarcza dodatkowe funkcje manipulacji interfejsem użytkownika w ramach działań malware'u.

769906B2	• 397C24 14	CMP DWORD PTR SS:[LOCAL.15],EDI	
769906B6	• 0F85 0F010000	JNE 769907CB	
769906BC	• 8B86 B4500071	MOV EAX,DWORD PTR DS:[ESI+76A050] PTR to UNICODE "Button"	
769906C2	• A9 0000FFFF	TEST EAX,FFFFFF00	
769906C7	• 74 18	JZ SHORT 769906E1	
769906C9	• 397C24 1C	CMP DWORD PTR SS:[LOCAL.15],EDI	

76990690	> 8B5424 10	MOV EDX,DWORD PTR SS:[LOCAL.16]	
769906A1	• 8B0F	MOV EBX,EDI	
769906A3	• 8BF7	MOV ESI,EDI	
769906A5	> A1 B85CA076	MOV EAX,DWORD PTR DS:[76A05CB8]	
769906AA	• 8BCB	MOV ECX,EBX	
769906AC	• D3E8	SHR EAX,CL	
769906AE	• A3 01	TEST AL,01	
769906B0	• 75 2F	JNZ SHORT 769906E1	
769906B2	• 397C24 14	CMP DWORD PTR SS:[LOCAL.15],EDI	
769906B6	• 0F85 0F010000	JNE 769907CB	
769906BC	• 8B86 B4500071	MOV EAX,DWORD PTR DS:[ESI+76A050] PTR to UNICODE "Button"	
769906C2	• A9 0000FFFF	TEST EAX,FFFFFF00	
769906C7	• 74 18	JZ SHORT 769906E1	
769906C9	• 397C24 1C	CMP DWORD PTR SS:[LOCAL.15],EDI	

Registers (FPU)		
EAX	76965B08	UNICODE "ComboBox"
ECX	00000001	
EDX	004021A1	ASCII "LoadDLLClass"
EBX	00000001	
ESP	0019FD28	
EBP	0019FD78	
ESI	00000024	
EDI	00000000	
EIP	769906C2	USER32.769906C2
C 0	ES 002B	32bit 0(FFFFFFFF)
P 1	CS 0023	32bit 0(FFFFFFFF)

Registers (FPU)		
EAX	00000001	
ECX	76965C24	ASCII "Edit"
EDX	004021A1	ASCII "LoadDLLClass"
EBX	00000004	
ESP	0019FD28	
EBP	0019FD78	

75266E67	• 8BF7	MOV EDI,ECX	
75266E6B	• BB 10FB3FE75	MOV EBX,OFFSET 753FEB11	
75266E70	• 68 24C11E75	PUSH 751EC124	Arg1 = ASCII "onecore\com\combase\class\compobj.cxx"
75266E75	• 8BCB	MOV ECX,EBX	
75266E77	• 8BF2	MOV ESI,EDX	
75266E79	• E8 B29C0400	CALL 752B0B30	combase.752B0B30

771B43B5	• 56	PUSH ESI	
771B43B6	• BE C0A51C77	MOV ESI,OFFSET 771CA5C0	
771B43BB	• 56	PUSH ESI	
771B43BC	• FF15 68B21C7	CALL DWORD PTR DS:[<&n	pCriticalSection => 771CA5C0
771B43C2	• 833D 34A01C7	CMP DWORD PTR DS:[771C	NTDLL.RtlEnterCriticalSection
771B43C9	• 75 0B	JNE SHORT 771B43D6	
771B43CB	• FF15 C0B01C7	CALL DWORD PTR DS:[&K	KERNEL32.TlsAlloc
771B43D1	• A3 34A01C77	MOV DWORD PTR DS:[771C	
771B43D6	> 56	PUSH ESI	
771B43D7	• FF15 6CB21C7	CALL DWORD PTR DS:[<&n	pCriticalSection = 771CA5C0
771B43DD	• 5E	POP ESI	NTDLL.RtlLeaveCriticalSection
771B43DE	• C3	RETN	



## Antywirus

```

771B30D9 8B BE 28 00 00 00 MOV EDI,DWORD PTR DS:[I
771B30DF 03 39          ADD EDI,DWORD PTR DS:[I UNICODE "ecurity-antitheft-l1-1-0"
771B30E1 8B 86 2C 00 00 00 MOV EAX,DWORD PTR DS:[I
771B30E7 13 41 04       ADC EAX,DWORD PTR DS:[I

```

W tym miejscu malware sprawdza czy na komputerze jest antywirus Kaspersky, Norton czy Symantec.

0x6403527E - Kaspersky AV

0x2E21B44 - Norton Security

0x651B3005 - Symantec

W zależności jaki antywirus odkrył używa innej flagi w celu ustawienia sobie odpowiednich uprawnień

Flaga o numerze 1 - ustawienie SeShutdownPrivilege

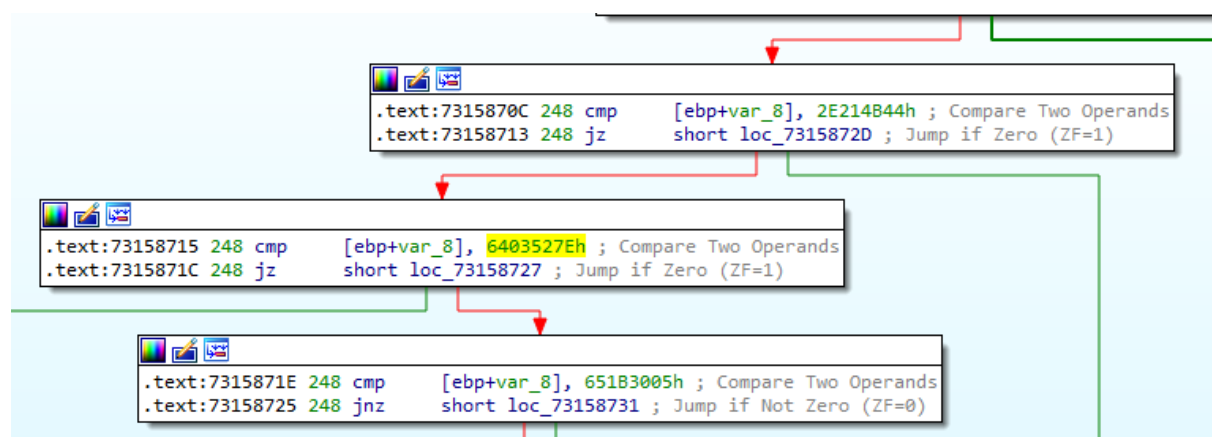
Flaga o numerze 2 - ustawienie SeDebugPrivilege

Flaga o numerze 3 - ustawienie SeShutdownPrivilege i SeDebugPrivilege

```

7315870H 72 06          JCB SHORT 731586E2
7315870C 81 7D F8 44 4B CMP DWORD PTR SS:[LOC
73158713 74 18          JE SHORT 7315872D
73158715 81 7D F8 7E 52 CMP DWORD PTR SS:[LOC
7315871C 74 09          JE SHORT 73158727
7315871E 81 7D F8 05 30 CMP DWORD PTR SS:[LOC
73158725 75 0A          JNE SHORT 73158731
73158727 > 83 65 FC FB   AND DWORD PTR SS:[LOC
7315872B > EB 04         JMP SHORT 73158731
7315872D > 83 65 FC F7   AND DWORD PTR SS:[LOC
73158731 > 8B 85 C8 FD FF IFA FAX.FI NCAL .1421

```





## Informacje o sieci

Malware wykonuje sekwencję funkcji w celu zdobycia jak największej ilości informacji o sieci:

- GetIpNetTable - służy do pobierania tabeli adresów IP
- NetServerEnum - razem z 3 argumentami (arg2 - ilość informacji jakie zostaną przeszukane, Arg1 - servername (null)) służy do pobrania listy serwerów w domenę
- NetServerGetInfo - pobiera bieżące informacje o serwerze. Jeżeli funkcja nie zwróci nulla zostają wywołane inne funkcje wyszukujące informacje o serwerze DHCP
- DhcpEnumSubnets służy do pobrania listy podsieci na serwerze.
- DhcpGetSubnetInfo wyrzuca wartość dla każdej podsieci na liście

```
MOV DWORD PTR SS:[LOCAL.1]
MOV DWORD PTR SS:[LOCAL.1]
CALL ESI
CMP EAX,0E8
JNE SHORT 73157897
CALL ESI

LEA EAX,[LOCAL.1]
PUSH EAX
PUSH 65
PUSH ESI
MOV DWORD PTR SS:[LOCAL.1]
MOV DWORD PTR SS:[LOCAL.1]
MOV DWORD PTR SS:[LOCAL.1]
MOV DWORD PTR SS:[LOCAL.1]
57 CALL DWORD PTR DS:[<&N]
CMP EAX,ESI

PUSH 65
PUSH ESI
2 CALL DWORD PTR DS:[<&N]
MOV ECX,DWORD PTR SS:[LOCAL.1]
TEST EAX,EAX

PUSH EAX
CALL DWORD PTR DS:[<&N]
TEST EAX,EAX
JNZ 731591F1
MOV EAX,DWORD PTR SS:[LOCAL.1]
MOV EAX,DWORD PTR DS:[LOCAL.1]
MOV DWORD PTR SS:[LOCAL.1]
CMP EAX,EDI
JBE 731591E8
LEA EAX,[LOCAL.4]
PUSH EAX
MOV EAX,DWORD PTR SS:[LOCAL.1]
MOV EAX,DWORD PTR DS:[LOCAL.1]
PUSH DWORD PTR DS:[EBX]
PUSH EDI
CALL DWORD PTR DS:[<&N]
TEST EAX,EAX
JNZ 731591D8
MOV EAX,DWORD PTR SS:[LOCAL.1]
CMP DWORD PTR DS:[EAX]
JNE 731591D8
LEA EAX,[LOCAL.15]
PUSH EAX
LEA EAX,[LOCAL.8]
PUSH EAX
LEA EAX,[LOCAL.3]
PUSH EAX
PUSH 10000
LEA EAX,[LOCAL.10]
PUSH EAX
MOV EAX,DWORD PTR SS:[LOCAL.1]
MOV EAX,DWORD PTR DS:[LOCAL.1]
PUSH DWORD PTR DS:[EBX]
PUSH EDI
CALL DWORD PTR DS:[<&N]
TEST EAX,EAX
```

IPHLPAPI.GetIpNetTable

Arg3 = 0  
Arg2 = 65  
Arg1 => 0

NETAPI32.NetServerEnum

Arg2 = 65  
Arg1 => 0

SRUCL1.NetServerGetInfo

Arg1 => OFFSET LOCAL.145

DHCPAPI.DhcpEnumSubnets

Arg3 => OFFSET LOCAL.4  
Arg2  
Arg1

DHCPAPI.DhcpGetSubnetInfo

Arg7 => OFFSET LOCAL.15  
Arg6 => OFFSET LOCAL.8  
Arg5 => OFFSET LOCAL.3  
Arg4 = 10000  
Arg3 => OFFSET LOCAL.10

Arg2  
Arg1

DHCPAPI.DhcpEnumSubnetClients

## Odczytywanie rejestrów

Po przejściu dalej możemy zauważyć w process monitorze, że malware zaczął odczytywać rejestry m.in. rejestry HKLM i HKCU

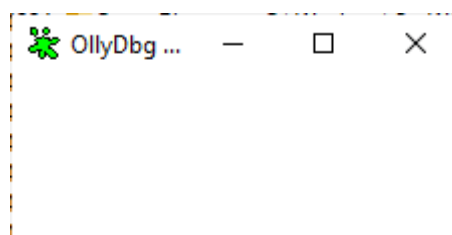
```
7699BAF2 8BEC MOV EBP,ESP
7699BAF5 83EC 18 SUB ESP,18
7699BAF8 56 PUSHESI
7699BAF9 C745 F0 0000 MOV DWORD PTR SS:[LOCAL.6],0
7699BB00 C745 F8 0000 MOV DWORD PTR SS:[LOCAL.7],0
7699BB07 C745 FC 0000 MOV DWORD PTR SS:[LOCAL.8],0
7699BB0E 8B75 08 MOVESI,DWORD PTR SS:[LOCAL.6]
7699BB11 FF76 14 PUSH DWORD PTR DS:[ESI+14]
7699BB14 FF76 10 PUSH DWORD PTR DS:[ESI+10]
7699BB17 FF76 0C PUSH DWORD PTR DS:[ESI+0C]
7699BB1A FF76 08 PUSH DWORD PTR DS:[ESI+08]
7699BB1D FF76 04 PUSH DWORD PTR DS:[ESI+04]
7699BB20 FF36 PUSH DWORD PTR DS:[ESI+36]
7699BB22 8B76 18 MOVESI,DWORD PTR DS:[ESI+18]
7699BB25 8BCE MOVECX,ESI
7699BB27 FF15 54A0A077 CALL DWORD PTR DS:[7754A0A0]
7699BB2D FFD6 CALLESI
7699BB2F 6A 00 PUSH0
7699BB31 8945 E8 MOV DWORD PTR SS:[LOCAL.6],E8
7699BB34 8D45 E8 LEAEAX,[LOCAL.6]
7699BB37 6A 18 PUSH18
7699BB39 50 PUSHEAX
7699BB3A C745 EC 0000 MOV DWORD PTR SS:[LOCAL.6],0
7699BB41 FF15 6C26A077 CALL DWORD PTR DS:[776C26A0]
7699BB47 5E POPESI
7699BB48 8BE5 MOVESP,EBP
```

Arg3 = 0  
Arg2 = 18  
Arg1 => OFFSET LOCAL.6  
ntdll.NtCallbackReturn

02:50:...	load.dll.exe	5596	CreateFile	C:\Windows\SystemResources\USER32.dll.mun	NAME NOT FOUND	Desired Access: 0x00000000
02:51:...	load.dll.exe	5596	RegOpenKey	HKCU	SUCCESS	Desired Access: 0x00000000
02:51:...	load.dll.exe	5596	RegQueryValue	HKCU	SUCCESS	Query: Handle
02:51:...	load.dll.exe	5596	RegQueryValue	HKCU	SUCCESS	Query: Name
02:51:...	load.dll.exe	5596	RegOpenKey	HKCU\Keyboard Layout\Toggle	SUCCESS	Desired Access: 0x00000000
02:51:...	load.dll.exe	5596	RegSetInfoKey	HKCU\Keyboard Layout\Toggle	SUCCESS	KeySetInformation: 0x00000000
02:51:...	load.dll.exe	5596	RegCloseKey	HKCU	SUCCESS	
02:51:...	load.dll.exe	5596	RegQueryValue	HKCU\Keyboard Layout\Toggle\Language Hotkey	NAME NOT FOUND	Length: 16
02:51:...	load.dll.exe	5596	RegQueryValue	HKCU\Keyboard Layout\Toggle\Hotkey	NAME NOT FOUND	Length: 16
02:51:...	load.dll.exe	5596	RegQueryValue	HKCU\Keyboard Layout\Toggle\Layout Hotkey	NAME NOT FOUND	Length: 16
02:51:...	load.dll.exe	5596	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Ids\pl-PL	NAME NOT FOUND	Length: 90
02:51:...	load.dll.exe	5596	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Ids\pl	SUCCESS	Type: REG_SZ
02:51:...	load.dll.exe	5596	RegCloseKey	HKCU\Keyboard Layout\Toggle	SUCCESS	

## Okienko OllyDbg

Gdy włącza się malware w Ollydbg to funkcją CreateWindow pojawia się okienko i dopiero po jego wyłączeniu malware robi dalsze kroki.



```
00401127 50 PUSH 0
00401126 FF35 44204000 PUSH DWORD PTR DS:[40204444]
0040112C 6A 00 PUSH 0
0040112E 6A 00 PUSH 0
00401130 6A 78 PUSH 78
00401132 68 F0000000 PUSH 0F000000
00401137 68 00000000 PUSH 00000000
0040113C 68 00000000 PUSH 00000000
00401141 68 0000CF10 PUSH 00CF0000
00401146 68 88214000 PUSH OFFSET 00402188
0040114B 68 A1214000 PUSH OFFSET 004021A1
00401150 6A 00 PUSH 0
00401152 E8 63040000 CALL <JMP.&USER32.CreateWindowExA>
00401157 A3 48204000 MOV DWORD PTR DS:[40204448],0
```

hInst = 00400000  
hMenu = NULL  
hParent = NULL  
Height = 120  
Width = 240  
Y = CW\_USEDEFAULT  
X = CW\_USEDEFAULT  
Style = WS\_OVERLAPPEDWINDOW|WS\_VISIBLE  
WindowName = "OllyDbg v2.01 DLL Loader"  
ClassName = "LoadDLLClass"  
ExtStyle = 0  
USER32.CreateWindowExA

## Szyfrowanie

NotPetya wywołuje funkcję DeviceIoControl w celu uzyskania fizycznej lokalizacji dysku

```
7315113F . 50 PUSH EAX
73151140 . FF15 ACD1157 CALL DWORD PTR DS:[<&K hDevice
73151142 . 85C0 TEST EAX,EAX
73151143 . 75 1C JNZ SHORT 73151146
```

Następnie odczytuje MBR i koduje go za pomocą operacji XOR z kluczem 0x7. Za pomocą CryptGenRandom jest generowany klucz, który później jest wykorzystywany przy szyfrowaniu Salsa20. Jest on także w późniejszym czasie wykorzystywany do stworzenia osobistego klucza instalacji użytkownika na ekranie powitalnym. (czerwone literki) Szyfrowany jest także MFT (zawiera wpisy o plikach i folderach) za pomocą Salsa20.

```
73151429 . 56 PUSH ESI
7315142A . 57 PUSH EDI
7315142B . 68 000000F0 PUSH F0000000
7315142C . 33C0 XOR EAX,EAX
7315142D . 6A 01 PUSH 1
7315142E . 50 PUSH EAX
7315142F . 50 PUSH EAX
73151430 . 8945 FC MOV DWORD PTR SS:[LOCAL.1],EAX
73151431 . 8D45 FC LEA EAX,[LOCAL.1]
73151432 . 50 PUSH EAX
73151433 . FF15 04D0157 CALL DWORD PTR DS:[<&ADVAPI32.CryptAcquireContextA>
73151434 . 8B1D 00D1157 MOV EBX,DWORD PTR DS:[<&KERNEL32.GetLastError>]
73151435 . BF FFFF0000 MOV EDI,0FFFF
73151436 . BE 00000780 MOV ESI,80070000
73151437 . 85C0 TEST EAX,EAX
73151438 . 75 13 JNZ SHORT 7315146A
73151439 . FFD3 CALL EBX
7315143A . 85C0 TEST EAX,EAX
7315143B . 7E 04 JLE SHORT 73151461
7315143C . 23C7 AND EAX,EDI
7315143D . 08C6 OR EAX,ESI
7315143E . A3 F8F81673 MOV DWORD PTR DS:[7316F8F8],EAX
7315143F . 85C0 TEST EAX,EAX
73151440 . 78 22 JS SHORT 7315148C
73151441 . FF75 08 PUSH DWORD PTR SS:[ARG.1]
73151442 . FF75 0C PUSH DWORD PTR SS:[ARG.2]
73151443 . FF75 FC PUSH DWORD PTR SS:[LOCAL.1]
73151444 . FF15 00D0157 CALL DWORD PTR DS:[<&ADVAPI32.CryptGenRandom>]
73151445 . 85C0 TEST EAX,EAX
73151446 . 75 0F JNZ SHORT 7315148C
```

## Podsumowanie Analizy Dynamicznej

Podczas analizy dynamicznej wirusa NotPetya ujawniono jego zaawansowane funkcje i metody propagacji.

Wirus wykorzystuje różnorodne techniki, takie jak manipulacja interfejsem użytkownika, odczyt i modyfikacja rejestrów systemowych oraz komunikacja sieciowa.

Wykryto próby nawiązywania połączenia z Internetem i przeszukiwania sieci w celu zidentyfikowania innych urządzeń.

Istotnym aspektem jest także proces szyfrowania MBR i MFT, co prowadzi do niemożności dostępu do ważnych plików.

Analiza uwidoczniła również dostosowanie zachowań wirusa w zależności od obecności konkretnych programów antywirusowych, co świadczy o złożoności i inteligencji zastosowanych technik.