

# Raport Analiza Malware

Wykonali: Mieszko Makowski, Mateusz Jackiewicz, Wiktor Deka

## Wykorzystane narzędzia:

### 1. Lista narzędzi użytych umożliwiających przeprowadzenie analizy statycznej:

#### PEiD

PEiD to narzędzie służące do identyfikacji packerów, kompresorów i kryptorów stosowanych w plikach wykonywalnych Windows PE. Jest szczególnie przydatne w analizie plików binarnych, pozwalając na szybkie rozpoznanie użytych technik ukrywania kodu.



#### PE-bear

PE-bear to narzędzie do analizy i edycji plików PE (Portable Executable), które oferuje funkcje takie jak przeglądanie struktury pliku, modyfikowanie sekcji i eksploracja nagłówków. Jest cenione za intuicyjny interfejs i możliwości głębokiej inspekcji plików binarnych.



#### PEStudio

PEStudio to narzędzie do wstępnej analizy plików PE, które pozwala na ocenę potencjalnych zagrożeń bez ich uruchamiania. Umożliwia przeglądanie zależności, analizę importowanych i eksportowanych funkcji, a także wykrywanie wskaźników kompromitacji.



## Detect It Easy

Detect It Easy (DIE) to zaawansowane narzędzie do analizy plików wykonywalnych, które identyfikuje użyte packery, kryptory i kompresory. Umożliwia także dekompresję plików oraz dostarcza szczegółowe informacje o strukturze plików PE.



## IDA Pro

IDA Pro to interaktywne narzędzie do dekompilacji i analizy binarnej, które umożliwia inżynierię wsteczną złośliwego oprogramowania. Pozwala na statyczną i dynamiczną analizę kodu, oferując rozbudowane funkcje dekompilacji i wizualizacji.



## VirusTotal.com

VirusTotal to internetowa usługa umożliwiająca skanowanie plików i adresów URL przy użyciu wielu silników antywirusowych i narzędzi do wykrywania zagrożeń. Pozwala na szybkie zidentyfikowanie potencjalnie złośliwego oprogramowania i uzyskanie szczegółowych raportów na temat analizowanych próbek.



## 2. Lista narzędzi umożliwiających przeprowadzenie analizy dynamicznej:

### RegShot

RegShot to narzędzie do monitorowania zmian w rejestrze Windows. Umożliwia tworzenie zrzutów stanu rejestru przed i po wykonaniu podejrzanego pliku, co pozwala na identyfikację modyfikacji wprowadzonych przez malware.



## Process Monitor

Process Monitor to narzędzie do monitorowania aktywności systemu plików, rejestru i procesów w czasie rzeczywistym. Jest używane do śledzenia działań złośliwego oprogramowania i analizy jego wpływu na system operacyjny.



## Process Explorer

Process Explorer to zaawansowany menedżer procesów, który oferuje szczegółowe informacje o uruchomionych procesach i otwartych przez nie zasobach. Jest przydatny do identyfikacji podejrzanych procesów i ich powiązań.



## x64\_dbg

x64\_dbg to darmowy debugger dla systemów Windows, obsługujący zarówno aplikacje 32-bitowe, jak i 64-bitowe. Umożliwia dynamiczną analizę kodu i debugowanie złośliwego oprogramowania.



## VMPDump

VMPDump to narzędzie służące do dekompilacji plików zabezpieczonych za pomocą VMProtect. Umożliwia ekstrakcję oryginalnego kodu, co ułatwia dalszą analizę złośliwego oprogramowania.



## Hybrid-Analysis.com sandbox

Hybrid Analysis to internetowa platforma do dynamicznej analizy złośliwego oprogramowania w środowisku sandbox. Zapewnia szczegółowe raporty na temat działania próbki, w tym jej zachowania sieciowego, zmian systemowych i innych wskaźników kompromitacji.



## 3. Lista narzędzi umożliwiających przeprowadzenie analizy sieciowej:

### FakeNet-NG

FakeNet-NG to narzędzie do symulacji środowiska sieciowego, które pozwala na przechwytywanie i analizę ruchu sieciowego generowanego przez złośliwe oprogramowanie. Pomaga w badaniu zachowań sieciowych malware bez ryzyka dla rzeczywistej infrastruktury.



### Wireshark

Wireshark to popularny analizator protokołów sieciowych, który umożliwia przechwytywanie i szczegółową analizę ruchu sieciowego. Jest używany do badania komunikacji sieciowej złośliwego oprogramowania i identyfikacji podejrzanych aktywności.



## Próbka numer 1: ProAim D&D.exe

### Podsumowanie wykonawcze:

Mój znajomy kupił cheat do gry Dark and Darker. Nie mogąc się doczekać anihilacji przeciwników, wpierw poprosił mnie o sprawdzenie tego programu. Mimo, że poznane na zajęciach sposoby analizy nie zapewniają pełnego zrozumienia działania próbki, to uważam, że jest to ciekawy przypadek i warto spróbować wyciągnąć minimum indykatorów.

Próbka pochodzi ze strony

<https://cosmocheats.com/store/product/508-proaim-dd-1-day-key/>

Po wykonaniu przelewu na określone konto, pracownik serwisu kontaktuje się z nami w wiadomości prywatnej na platformie Discord i przesyła plik wykonywalny.

Po wprowadzeniu odpowiedniego klucza API, próbka odnajduje grę na dysku i zapewnia nakładkę pozwalającą na oszukiwanie w czasie rzeczywistym.

Próbkę można pobrać z GitHuba: [https://github.com/wiktorDeka/Malware\\_sample](https://github.com/wiktorDeka/Malware_sample)

## Skrót analizy

Próbka to plik wykonywalny, który został wielokrotnie zgłoszony na **VirusTotal** jako Trojan i VMProtect. Program został skompilowany stosunkowo niedawno. Importuje jedynie KERNEL32.dll i CloseHandle, co przy jego dużym rozmiarze (~30MB) sugeruje, że kod został obfuskowany. Analiza narzędziem strings jest przez to nieskuteczna. Po uruchomieniu próbka otwiera puste okno cmd i samoistnie się wyłącza, modyfikując rejestr systemowy. Process Monitor wykazuje, że próbka modyfikuje rejestr, manipuluje procesami oraz tworzy i usuwa plik. Wykryto sztuczny EntryPoint, co sugeruje zaawansowaną obfuskację. Dotychczasowa analiza nie potwierdza ani nie wyklucza szkodliwości próbki. Próbka modyfikuje rejestr, aby uruchamiać się przy starcie systemu, instaluje się tylko na kompatybilnych systemach po spełnieniu określonych warunków (np. dostęp do sieci, obecność odpowiednich bibliotek) i używa VMProtect w połączeniu z innymi metodami obfuskacji, co znacznie utrudnia inżynierię wsteczną.

## Kompleksowa analiza

Pierwszym krokiem wobec naszej próbki jest użycie **VirusTotal**. Informuje on nas, że próbka została już zgłoszona kilka razy i ciągle napływają nowe zgłoszenia. Ponadto oznacza ją jako Trojan i vmprotect

Program został skompilowany stosunkowo niedawno  
sobota, 30.03.2024 22:59:16 UTC

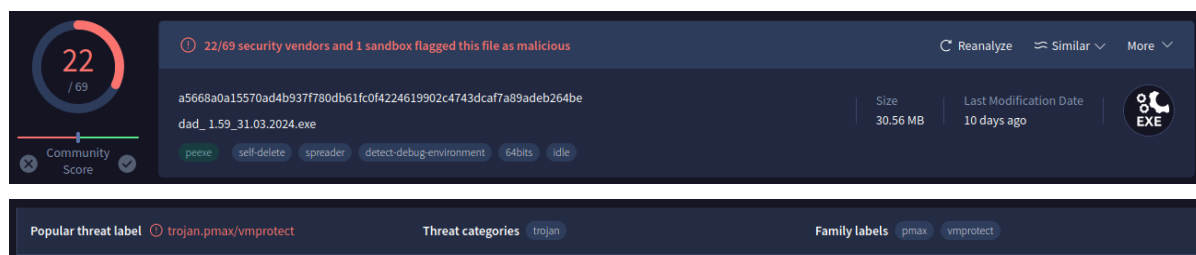


Fig 1: Próbka w VirusTotal

### Program importuje

- KERNEL32.dll
- CloseHandle

Tak mała ilość importów w stosunku do rozmiaru pliku (~30MB) sugeruje, że kod został obfuskowany.

Disasm: _2	General	Strings	DOS Hdr	File Hdr	Optional Hdr	Section Hdrs	Imports	Resource
Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder		
AED0F0	KERNEL32.dll	1	FALSE	2492B18	0	0		
KERNEL32.dll [ 1 entry ]								
Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint		
19A5000	CloseHandle	-	2DC761E	2DC761E	-	0		

Fig 2: Import

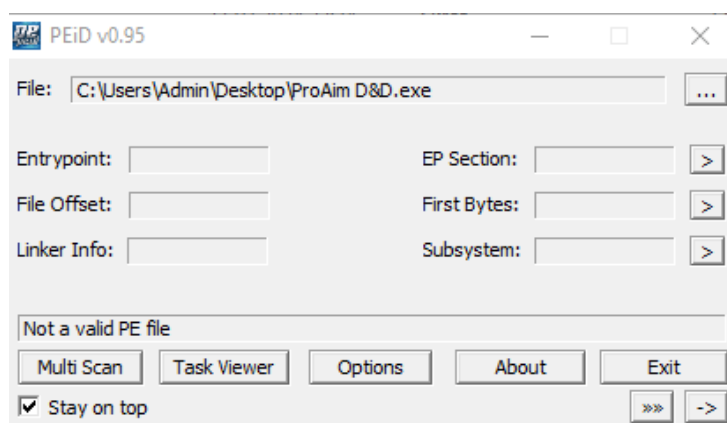


Fig 3 : PEiD

Program **PEiD** nie pozwala w jednoznaczny sposób określić, czy program został spakowany. Nie mniej jednak VirusTotal oznacza nam próbkę jako **vmprotect**.

**VMProtect** to metoda uruchamiania programu w wirtualnym kontenerze, w celu utrudnienia inżynierii wstecznej. Wykorzystuje technikę wirtualizacji kodu, co oznacza, że kod oryginalnego programu jest przekształcany na kod pośredni (bytecode), który następnie jest wykonywany przez wirtualną maszynę VMProtect.

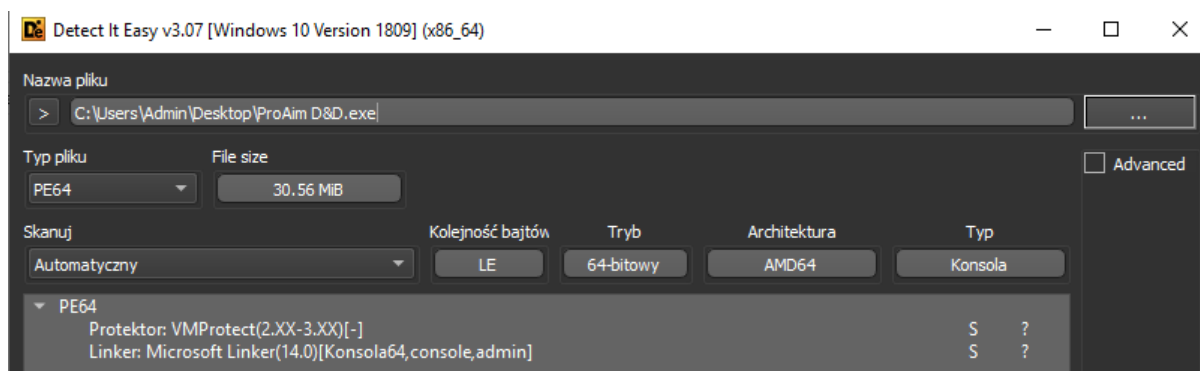


Fig 4: Detect it Easy

Program „**Detect it Easy**” tak samo jak **PEiD** nie dostajemy jednoznacznej odpowiedzi czy program został spakowany.

Z powodu **vmprotect**, strings nie podpowiada nam niczego ciekawego

1	4d	A	41	!This program cannot be run in DOS mode.\$
2	180	A	5	.text
3	1a7	A	7	`.rdata
4	1cf	A	6	@.data
5	1f8	A	6	.pdata
6	21f	A	7	@.00cfg
7	247	A	6	@.gxfg
8	26f	A	9	@.retplne
9	298	A	6	_RDATA
10	337	A	6	h.rsrc
11	659	A	5	)(roF
12	7c1	A	5	"r+}n
13	7f9	A	6	)lwabv
14	80f	A	5	UOdHZ
15	8de	A	5	FsX)n

Fig 5: Strings

Przez całe strings przewija się losowy junk (tak jak w liniach 11-15)

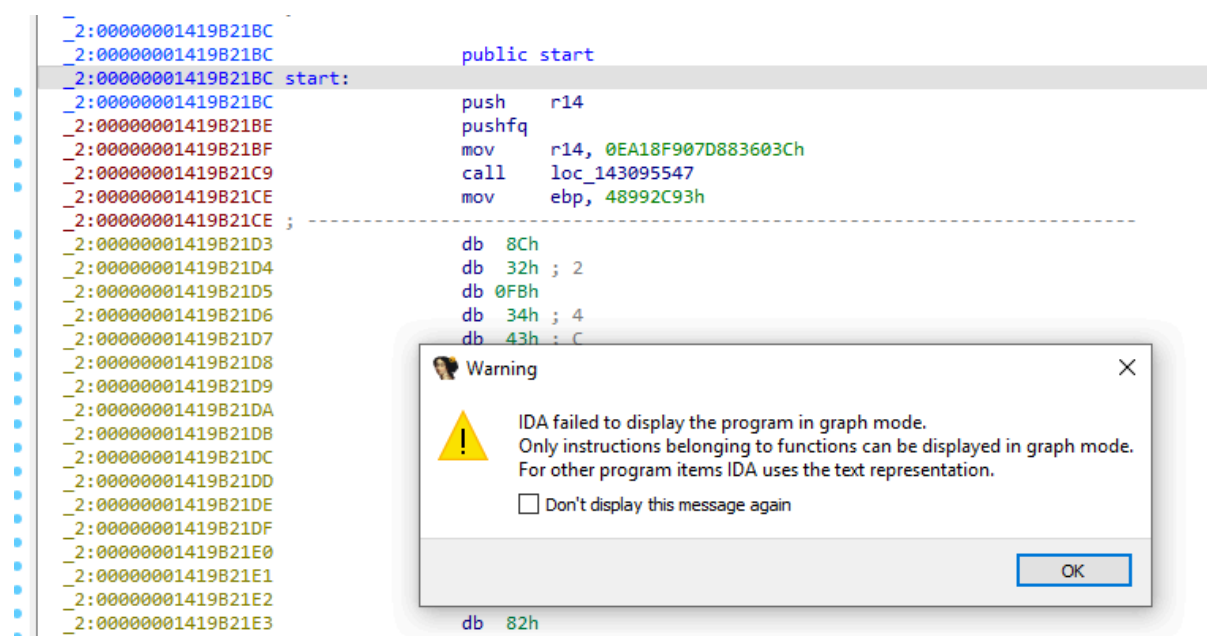


Fig 6: IDA Pro

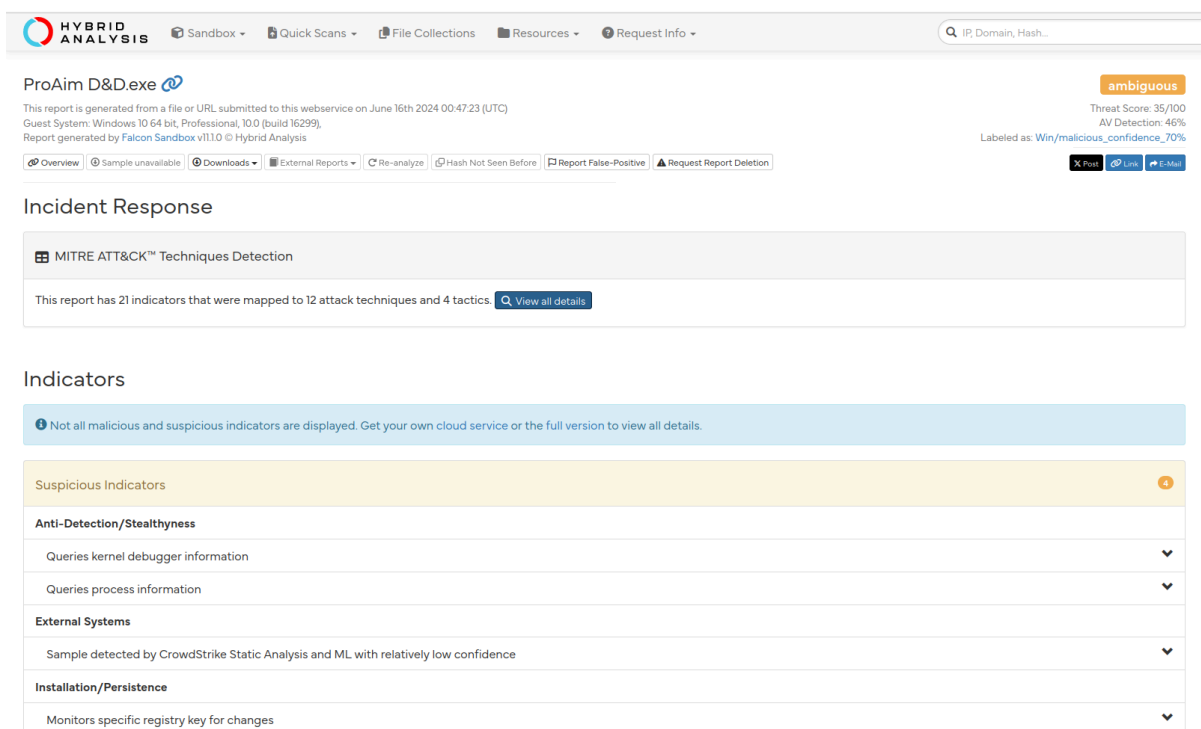
Kod jest mocno obfuskowany. **IDA** nie radzi sobie z programem. Nie potrafi stworzyć też grafu. IDA wykrywa tylko 2 (przy okazji bardzo duże) funkcje. Prawdopodobnie są odpowiedzialne za **vmprotect**

Pełna i poprawna deasemblacja jest na tym etapie niemożliwa.

name	signature	location	entropy	language
icon	icon	.rsrc:0x01E74BD8	2.493	Russian
manifest	manifest	.rsrc:0x01E8F0A0	4.700	English-US
icon-group	icon-group	.rsrc:0x01E8F040	2.799	Russian
icon	icon	.rsrc:0x01E75040	2.025	Russian
icon	icon	.rsrc:0x01E760E8	1.808	Russian
icon	icon	.rsrc:0x01E78690	1.644	Russian
icon	icon	.rsrc:0x01E7C8B8	1.325	Russian
icon	icon	.rsrc:0x01E8D0E0	7.894	Russian

Fig 7: Icon

Icon sugeruje, że program został napisany przez Rosjan.



The screenshot shows the Hybrid Analysis interface for a file named 'ProAim D&D.exe'. The report was generated on June 16th, 2024, at 00:47:23 (UTC). The guest system is Windows 10 64 bit, Professional, 10.0 (build 16299). The report was generated by Falcon Sandbox v11.10.0. The report is labeled as 'Win/malicious\_confidence\_70%'. The report shows a threat score of 35/100 and an AV detection rate of 46%. The report is categorized as 'Incident Response' and 'MITRE ATT&CK™ Techniques Detection'. The report has 21 indicators that were mapped to 12 attack techniques and 4 tactics. The report also shows a section for 'Indicators' with a message: 'Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.' The 'Suspicious Indicators' section is expanded, showing 'Anti-Detection/Stealthiness' and 'External Systems'.

Fig 8: Sandbox

Sandbox <https://hybrid-analysis.com/> oznaczył próbkę jako podejrzaną



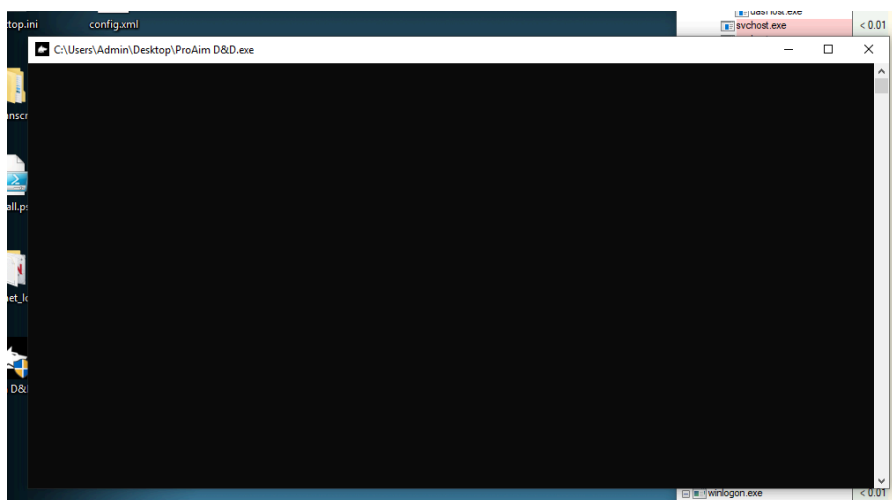


Fig 9: Uruchomienie

Próbka uruchamia puste okienko cmd po czym samoistnie się wyłącza. W tym czasie edytowany jest rejestr systemowy. Poza tym podstawowa analiza dynamiczna, nic nie mówi.

Możliwe potrzeby:

- brakujące parametry uruchomienia programu
- brakujące biblioteki

```
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-06-15 20:49:19, 2024-06-15 20:50:54
Computer: DESKTOP-SR2L7I2, DESKTOP-SR2L7I2
Username: Admin, Admin

-----
Keys added: 3
-----
Values added: 3
-----
Values modified: 15
-----
```

Fig 10: RegShot

Do ciekawszych zmian w rejestrze należą wpisy:

**HKU\S-1-5-21-3992777276-1445507506-558448409-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32**

- Ten wpis może wskazywać na próbę ukrycia lub manipulacji sesjami użytkownika.

**HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3992777276-1445507506-558448409-1001\Device\HarddiskVolume2\Users\Admin\Desktop\ProAim D&D.exe**

- Ten wpis w kontekście BAM (Background Activity Moderator) może sugerować próbę utrzymania aktywności aplikacji nawet w tle, co jest typowe dla malware.

## HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Schedule\TaskCache\Tasks{6462C646-DD43-41FB-B5CC-43C72C793710}

- Zmiany w zadaniach harmonogramu zadań mogą świadczyć o próbie ustanowienia trwałego zadania, które uruchamia złośliwe oprogramowanie w określonych odstępach czasu lub przy starcie systemu.

22:55:...	ProAim D&D.exe	2316	RegOpenKey	HKLM\Software\Policies\Microsoft\IMUI...	NAME NOT FOUND	Desired Access: Read
22:55:...	ProAim D&D.exe	2316	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access
22:55:...	ProAim D&D.exe	2316	RegOpenKey	HKCU\Control Panel\Desktop\MuiCach...	SUCCESS	Desired Access: Read
22:55:...	ProAim D&D.exe	2316	RegQueryValue	HKCU\Control Panel\Desktop\MuiCach...	BUFFER OVERFL...	Length: 12
22:55:...	ProAim D&D.exe	2316	RegQueryValue	HKCU\Control Panel\Desktop\MuiCach...	SUCCESS	Type: REG_MULTI_SZ, Length: 12, Data: pl-PL
22:55:...	ProAim D&D.exe	2316	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
22:55:...	ProAim D&D.exe	2316	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
22:55:...	ProAim D&D.exe	2316	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
22:55:...	ProAim D&D.exe	2316	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
22:55:...	ProAim D&D.exe	2316	RegCloseKey	HKCU\Control Panel\Desktop\MuiCach...	SUCCESS	
22:55:...	ProAim D&D.exe	2316	RegCloseKey	HKCU	SUCCESS	
22:55:...	ProAim D&D.exe	2316	CreateFile	C:\Users\Admin\Desktop\ProAim D&D...	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous...
22:55:...	ProAim D&D.exe	2316	CreateFileMapp...	C:\Users\Admin\Desktop\ProAim D&D...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE...
22:55:...	ProAim D&D.exe	2316	QueryStandardI...	C:\Users\Admin\Desktop\ProAim D&D...	SUCCESS	AllocationSize: 32 047 104, EndOfFile: 32 043 520, NumberOfLinks: 1, D...
22:55:...	ProAim D&D.exe	2316	CreateFileMapp...	C:\Users\Admin\Desktop\ProAim D&D...	SUCCESS	SyncType: SyncTypeOther
22:55:...	ProAim D&D.exe	2316	CloseFile	C:\Users\Admin\Desktop\ProAim D&D...	SUCCESS	
22:55:...	ProAim D&D.exe	2316	Thread Exit		SUCCESS	Thread ID: 3468, User Time: 2.7500000, Kernel Time: 0.1093750
22:55:...	ProAim D&D.exe	2316	Process Exit		SUCCESS	Exit Status: -559038242, User Time: 2.7500000 seconds, Kernel Time: 0...
22:55:...	ProAim D&D.exe	2316	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Desired Access: All Access
22:55:...	ProAim D&D.exe	2316	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 23 64 32 5D 66 BF DA 01 00 00...
22:55:...	ProAim D&D.exe	2316	RegSetValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 6B B1 ED 5E 66 BF DA 01 00 0...
22:55:...	ProAim D&D.exe	2316	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	
22:55:...	ProAim D&D.exe	2316	CloseFile	C:\Users\Admin\Desktop	SUCCESS	

Fig 11: Process monitor

## Próbka:

- modyfikuje rejestr systemowy
- manipuluje procesami
- tworzy/usuwa pliki

explorer.exe	< 0.01	70 556 K	147 380 K	4448 Eksplorator Windows	Microsoft Corporation
SecurityHealthSystray.exe		1 712 K	8 372 K	5964 Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2 848 K	11 704 K	5348 VirtualBox Guest Additions Tr...	Oracle Corporation
ZoomIt64.exe		1 948 K	8 560 K	888 Sysinternals Screen Magnifier	Sysinternals - www.sysinter...
cmd.exe		3 276 K	3 928 K	1292 Windows Command Processor	Microsoft Corporation
conhost.exe		8 572 K	22 816 K	6660 Host okna konsoli	Microsoft Corporation
fakenet.exe		1 416 K	4 356 K	2924	
fakenet.exe	< 0.01	25 184 K	31 492 K	1108	
proccxp.exe		4 472 K	11 884 K	4128 Sysinternals Process Explorer	Sysinternals - www.sysinter...
proccxp64.exe	1.54	28 120 K	52 072 K	5740 Sysinternals Process Explorer	Sysinternals - www.sysinter...
ProAim D&D.exe	25.00	26 860 K	48 452 K	5256	
conhost.exe		7 284 K	17 408 K	3396 Host okna konsoli	Microsoft Corporation

Fig 12: Process explorer

Program wywołuje conhost.exe, który wygląda na bezpieczny. **Process Explorer** weryfikuje go jako integralną część Windowsa

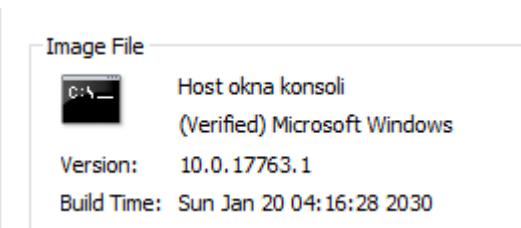


Fig 13: Image File

## Process Explorer weryfikuje go jako integralną część Windowsa

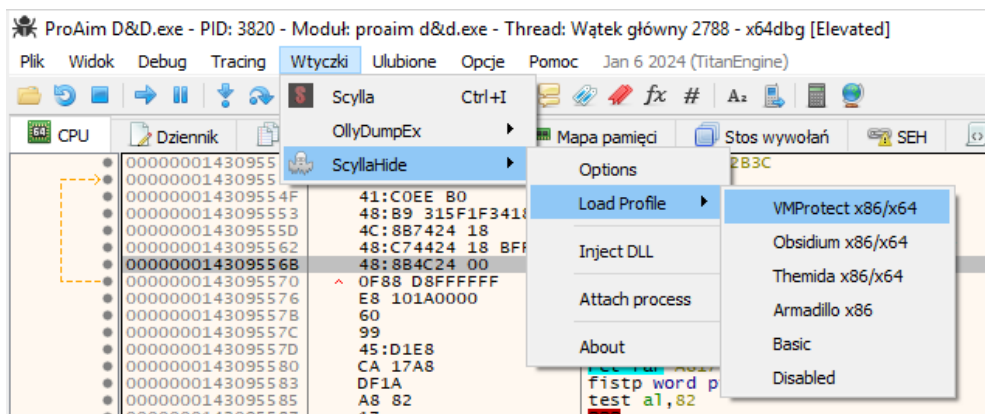


Fig 14: x64\_dbg

W celu poprawnego poruszania się po debuggerze musimy najpierw zaimportować profil ukrywający debuggera. Umożliwia nam to **ScyllaHide**.

Typ	Adres	Module/Label/Exception	Stan	Disassembly	Hits
Oprogramowanie	00007FEEA4E925D0	<kernelbase.dll.VirtualProtectEx>	Aktywny	mov rax, rsp	0
	00007FEEA4EED280	<kernelbase.dll.VirtualAlloc>	Aktywny	sub rsp, 38	0
	00007FEEA4EF7A80	<kernelbase.dll.VirtualProtect>	Aktywny	mov rax, rsp	0

Fig 15: Wykrycie sztucznego EntryPoint

Po uruchomieniu próbki, debugger wykrywa sztuczny EntryPoint

### OptionalHeader.AddressOfEntryPoint

00007FEEA4EF7A80	48:8BC4	mov rax, rsp	VirtualProtect
00007FEEA4EF7A83	48:8958 18	mov qword ptr ds:[rax+18], rbx	
00007FEEA4EF7A87	55	push rbp	
00007FEEA4EF7A88	56	push rsi	rsi:"LdrpInitializeProcess"
00007FEEA4EF7A89	57	push rdi	
00007FEEA4EF7A8A	48:83EC 30	sub rsp, 30	
00007FEEA4EF7A8E	49:8BF1	mov rsi, r9	rsi:"LdrpInitializeProcess"
00007FEEA4EF7A91	4C:8948 D8	mov qword ptr ds:[rax-28], r9	
00007FEEA4EF7A95	45:8BC8	mov r9d, r8d	
00007FEEA4EF7A98	48:8950 08	mov qword ptr ds:[rax+8], rdx	
00007FEEA4EF7A9C	41:8BE8	mov ebp, r8d	
00007FEEA4EF7A9F	48:8948 10	mov qword ptr ds:[rax+10], rcx	rcx:NtQueryInformationThread+14
00007FEEA4EF7AA3	4C:8D40 08	lea r8, qword ptr ds:[rax+8]	rcx:NtQueryInformationThread+14
00007FEEA4EF7AA7	48:83C9 FF	or rcx, FFFFFFFF	
00007FEEA4EF7AAB	48:8D50 10	lea rdx, qword ptr ds:[rax+10]	
00007FEEA4EF7AAF	48:FF15 5A3E1300	call qword ptr ds:[<NtProtectVirtualMem>	
00007FEEA4EF7AB6	0F1F4400 00	nop dword ptr ds:[rax+rax], eax	
00007FEEA4EF7ABB	33DB	xor ebx, ebx	
00007FEEA4EF7ABD	8BF8	mov edi, eax	
00007FEEA4EF7ABF	85C0	test eax, eax	
00007FEEA4EF7AC1	0F88 45290400	js kernelbase.7FEEA4F3A40C	
00007FEEA4EF7AC7	BB 01000000	mov ebx, 1	
00007FEEA4EF7ACC	8BC3	mov eax, ebx	
00007FEEA4EF7ACE	48:8B5C24 60	mov rbx, qword ptr ss:[rsp+60]	
00007FEEA4EF7AD3	48:83C4 30	add rsp, 30	
00007FEEA4EF7AD7	5F	pop rdi	
00007FEEA4EF7AD8	5E	pop rsi	rsi:"LdrpInitializeProcess"
00007FEEA4EF7AD9	5D	pop rbp	
00007FEEA4EF7ADA	5D	ret	

Fig 16: VMprotect

Próbujemy znaleźć **OEP** (Original Entry Point). W tym celu ustawiamy entrypoint zanim VMprotect zacznie działać. Niestety **wyłącza się** zanim header VMprotect zacznie się wykonywać. VMProtect tworzy nadmiarowe odgałęzienia w postaci przeskoków-atrap oraz funkcji-atrap aby ukryć oryginalny EntryPoint.

C:\> Administrator: Admin Command Prompt

```
FLARE-VM 16.06.2024 1:34:43,92
C:\Users\Admin\Desktop>VMPDump.exe 1816 "" -ep=19B21BC -disable-reloc
** Successfully opened process ProAim D&D.exe, PID 0x718
** Selected module: C:\Users\Admin\Desktop\ProAim D&D.exe
** Found 0 calls to 0 imports
** Converting 0 calls
** New ImageBase: 0x140000000, SizeOfImage: 0x3837000
** File written to: C:\Users\Admin\Desktop\ProAim D&D.VMPDump.exe

FLARE-VM 16.06.2024 1:35:02,71
C:\Users\Admin\Desktop>
```

Fig 17: VMPDump

Przy pomocy narzędzia **VMPDump** skanuje wszystkie sekcje wykonywalne w poszukiwaniu odgałęzień. To również nie pomogło w odnalezieniu **OEP**

Możliwe przyczyny takiego zachowania próbki:

- wielowarstwowa obfuskacja  
Próbka poza VMProtect może korzystać z innych metod obfuskacji np. Themida, Armadillo.
- zaawansowana kontrola integralności  
Próbka może kontrolować czy w trakcie wykonywania programu nie doszło do jego.
- nieprawidłowe działanie ScyllaHide
- własna metoda obfuskacji  
Twórcy programu mogli użyć własnoręcznie zmodyfikowanego narzędzia do obfuskacji

Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Num. of Linenum.
> .text	0	0	1000	1ACA9	60000020	0	0	0
> .rdata	0	0	1C000	9494	40000040	0	0	0
> .data	0	0	26000	CC41B0	C0000040	0	0	0
> .pdata	0	0	CEB000	11DC	40000040	0	0	0
> .00cfg	0	0	CED000	38	40000040	0	0	0
> .gxf	0	0	CEE000	1100	40000040	0	0	0
> .retplne	0	0	CF0000	8C	0	0	0	0
> _RDATA	0	0	CF1000	15C	40000040	0	0	0
> _0	0	0	CF2000	CB2938	60000020	0	0	0
> _1	400	200	19A5000	40	C0000040	0	0	0
> _2	600	1E74400	19A6000	1E74280	68000060	0	0	0
> .rsrc	1E74A00	1A800	381B000	1A7EE	40000040	0	0	0

Fig 18:Custom header

**Custom headers** potwierdzają powyższe teorie:

- Brak typowego dla VMProtect nagłówka .vmp0, .vmp1
- .00cfg czy \_2 to zwykle niespotykane nagłówki

## Wnioski

Dotychczasowa analiza nie potwierdza, ani nie wyklucza szkodliwości próbki.

W wyniku przeprowadzonego dochodzenia próbka:

- Modyfikuje rejestr w celu automatycznego uruchomienia się przy starcie systemu
- Instaluje się wyłącznie na kompatybilnych systemach po spełnieniu wszystkich warunków (m.in dostęp do sieci, posiadanie innych programów i bibliotek)
- Posiada wielowarstwowy mechanizm obfuskacji znacznie utrudniający inżynierię wsteczną.
  - Próbka wykorzystuje VMProtect w połączeniu z innymi metodami obfuskacji

*“VMProtect protects code by executing it on a virtual machine with non-standard architecture that makes it extremely difficult to analyze and crack the software. Besides that, VMProtect generates and verifies serial numbers, limits free upgrades and much more.”*

*~Opis z programu Detect It Easy*

## Próbka numer II : Trojan

### Pochodzenie:

Próbka pochodzi z dostępnych repozytoriów zamieszczonych na platformie GitHub.

- a) <https://github.com/mstfknn/malware-sample-library/tree/master/Ransomware>

### VirusTotal

40 / 69

Community Score

40/69 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

317849c236aa238bd3287ed58effeef15db1c7d63cf54bbba...

Size 72.44 KB

Last Modification Date 16 days ago

EXE

wow\_helper.exe

peexe assembly overlay revoked-cert signed via-tor 64bits invalid-signature

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

Alibaba	Trojan:Win32/AgentSmall.87ab9f77	ALYac	Trojan.Generic.8268230
Arcabit	Trojan.Generic.D7E29C6	Max size: 650MB	Win64:Trojan-gen
Avert Labs	Artemis!A1233745DC77	AVG	Win64:Trojan-gen
BitDefender	Trojan.Generic.8268230	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	DeepInstinct	MALICIOUS
Emsisoft	Trojan.Generic.8268230 (B)	eScan	Trojan.Generic.8268230
ESET-NOD32	A Variant Of Generik.LQGYHOS	GData	Trojan.Generic.8268230
Google	Detected	Ikarus	Trojan-Downloader.AgentSmall
Jiangmin	Trojan.Agent.ceea	Kaspersky	Trojan.Win32.Agent.bwao

BitDefender	Trojan.Generic.8268230	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	DeepInstinct	MALICIOUS
Emsisoft	Trojan.Generic.8268230 (B)	eScan	Trojan.Generic.8268230
ESET-NOD32	A Variant Of Generik.LQGYHOS	GData	Trojan.Generic.8268230
Google	Detected	Ikarus	Trojan-Downloader.AgentSmall
Jiangmin	Trojan.Agent.ceea	Kaspersky	Trojan.Win32.Agent.bwao
Lionic	Trojan.Win32.Agent.4lc	MAX	Malware (ai Score=100)
McAfee-GW-Edition	Artemis!Trojan	Microsoft	TrojanDownloader:Win32/AgentSmall.M
NANO-Antivirus	Trojan.Win64.Agent.crchzy	Panda	Trj/CIA
Rising	Downloader.AgentSmall!8.8B9 (CLOUD)	Sophos	Mal/Generic-S
Symantec	Trojan.Gen.MBT	Tencent	Win32.Trojan.FalseSign.Zchl
Trapmine	Suspicious.low.ml.score	Trellix (FireEye)	Trojan.Generic.8268230
TrendMicro	TROJ_GEN.R002C0DCF23	TrendMicro-HouseCall	TROJ_GEN.R002C0DCF23
VBA32	Trojan.Agent	VIPRE	Trojan.Generic.8268230
ViRobot	Trojan.Win32.S.Agent.74176.A	Webroot	W32.Malware.Gen
Xcitium	Malware@fv2nzs2csfdc8	Yandex	Trojan.AgentLee/tAz+CCN8
Zillya	Trojan.Agent.Win32.402335	ZoneAlarm by Check Point	Trojan.Win32.Agent.bwao

Virustotal wykrył że jest to malware oraz większość vendorów oznacza tą próbkę jako malicious.

## Imports

Jedyną biblioteką importowaną jest KERNEL32.dll. Także nic ciekawego.

library (1)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (65)	group	description
<a href="#">KERNEL32.dll</a>	-	-	0x0000F318	0x0000C000	implicit	<a href="#">65</a>	-	Windows NT BASE API Client

## PEiD

product-id (7)	build-id (4)	count
Utc1500_C	Visual Studio 2008 - 9.0	76
Masm900	Visual Studio 2008 - 9.0	10
Implib800	Visual Studio 2005 - 08.00	3
Import	Visual Studio	81
Utc1500_CPP	Visual Studio 2008 - 9.0	41
Cvtres900	Visual Studio 2008 - 9.0	1
Linker900	Visual Studio 2008 - 9.0	1

Program został skompilowany w Visual Studio 2008

general		
<a href="#">compiler-stamp</a>	0x5012E78E	Fri Jul 27 19:10:06 2012   UTC
<a href="#">size-of-optional-header</a>	0x00F0	240 bytes

Skompilowany 27 czerwca 2012 roku.

## PEStudio



section:rdata	-	import	reconnaissance	T1124   System Time Discovery	GetTickCount
section:rdata	x	import	reconnaissance	T1057   Process Discovery	GetCurrentProcessId
section:rdata	x	import	memory	T1055   Process Injection	WriteProcessMemory
section:rdata	x	import	memory	T1055   Process Injection	VirtualProtectEx
section:rdata	x	import	memory	T1055   Process Injection	ReadProcessMemory
section:rdata	-	import	memory	-	RtlVirtualUnwind
section:rdata	-	import	memory	-	HeapAlloc
section:rdata	-	import	memory	-	HeapFree
section:rdata	-	import	memory	-	HeapSetInformation
section:rdata	-	import	memory	-	HeapCreate
section:rdata	-	import	memory	-	HeapSize
section:rdata	-	import	memory	-	GetStringType
section:rdata	-	import	memory	-	GetStringType
section:rdata	-	import	memory	-	HeapReAlloc
section:rdata	x	import	file	-	WriteFile
section:rdata	-	import	file	-	GetFileType
section:rdata	-	import	file	T1124   System Time Discovery	GetSystemTimeAsFileTime
section:rdata	x	import	execution	T1055   Process Injection	OpenProcess
section:rdata	x	import	execution	-	RtlLookupFunctionEntry
section:rdata	x	import	execution	-	TerminateProcess
section:rdata	x	import	execution	T1057   Process Discovery	GetCurrentProcess
section:rdata	-	import	execution	-	RtlCaptureContext
section:rdata	x	import	execution	T1057   Process Discovery	GetCurrentThreadId

W importach znajduje się parę ciekawych rzeczy między innymi GetTickCount służący do poznania jaki czas jest obecnie na danym systemie.

ascii	11	section:rdata	-	import	dynamic-library	T1106   Execution through API	LoadLibrary
ascii	17	section:rdata	x	import	diagnostic	-	RtlPcToFileHeader
ascii	12	section:rdata	-	import	diagnostic	-	SetLastError
ascii	12	section:rdata	-	import	diagnostic	-	GetLastError
ascii	23	section:rdata	x	-	desktop	-	GetProcessWindowStation
ascii	24	section:rdata	x	-	desktop	-	GetUserObjectInformation
ascii	12	section:rdata	-	import	console	-	GetStdHandle
ascii	25	certificate	-	url-pattern	-	-	http://ocsp.verisign.com0
ascii	25	certificate	-	url-pattern	-	-	http://ocsp.verisign.com0
ascii	30	certificate	-	url-pattern	-	-	https://www.verisign.com/cps0*
ascii	29	certificate	-	url-pattern	-	-	https://www.verisign.com/rpa0
ascii	26	certificate	-	url-pattern	-	-	http://ocsp.verisign.com01
ascii	34	certificate	-	url-pattern	-	-	http://crl.verisign.com/pca3.crl0
ascii	29	certificate	-	url-pattern	-	-	https://www.verisign.com/rpa0
ascii	26	certificate	-	url-pattern	-	-	http://ocsp.verisign.com0?
unicode	9	version	-	url-pattern	-	-	10.1.4.38
unicode	9	version	-	url-pattern	-	-	10.1.4.38
ascii	19	section:data	-	rtti	-	-	:AVbad_alloc@std@@
ascii	19	section:data	-	rtti	-	-	:AVexception@std@@
ascii	21	section:data	-	rtti	-	-	:AVlogic_error@std@@
ascii	22	section:data	-	rtti	-	-	:AVlength_error@std@@
ascii	22	section:data	-	rtti	-	-	:AVout_of_range@std@@
ascii	15	section:data	-	rtti	-	-	:AVtype_info@@
ascii	23	section:data	-	rtti	-	-	:AVbad_exception@std@@
ascii	19	section:rdata	-	import	-	-	WideCharToMultiByte
ascii	11	section:rdata	-	import	-	-	RtlUnwindEx
ascii	13	section:rdata	-	import	-	-	EncodePointer
ascii	13	section:rdata	-	import	-	-	DecodePointer
ascii	11	section:rdata	-	import	-	-	FlsGetValue
ascii	11	section:rdata	-	import	-	-	FlsSetValue
ascii	8	section:rdata	-	import	-	-	FlsAlloc
ascii	9	section:rdata	-	import	-	-	GetCPlInfo
ascii	8	section:rdata	-	import	-	-	GetOEMCP
ascii	15	section:rdata	-	import	-	-	IsValidCodePage
ascii	14	section:rdata	-	import	-	-	SetHandleCount
ascii	13	section:rdata	-	import	-	-	GetLocaleInfo
ascii	11	section:rdata	-	import	-	-	LCMaoString

Po analizie zakładki string znalazłem dużo indyktorów sieciowych odnoszących się do strony verisign.com. Importy głównie służą sprawdzeniu certyfikatów strony prawdopodobnie aby użyć ich dalej jako zaufanych i uniknąć detekcji.

certificate	-	url-pattern	-	-	http://ocsp.verisign.com0
certificate	-	url-pattern	-	-	http://ocsp.verisign.com0
certificate	-	url-pattern	-	-	https://www.verisign.com/cps0*
certificate	-	url-pattern	-	-	https://www.verisign.com/rpa0
certificate	-	url-pattern	-	-	http://ocsp.verisign.com01
certificate	-	url-pattern	-	-	http://crl.verisign.com/pca3.crl0
certificate	-	url-pattern	-	-	https://www.verisign.com/rpa0
certificate	-	url-pattern	-	-	http://ocsp.verisign.com0?

Na liście znajduje się też prywatny adres 10.1.4.38 jednak ciężko stwierdzić na razie po co jest on tutaj wpisany.

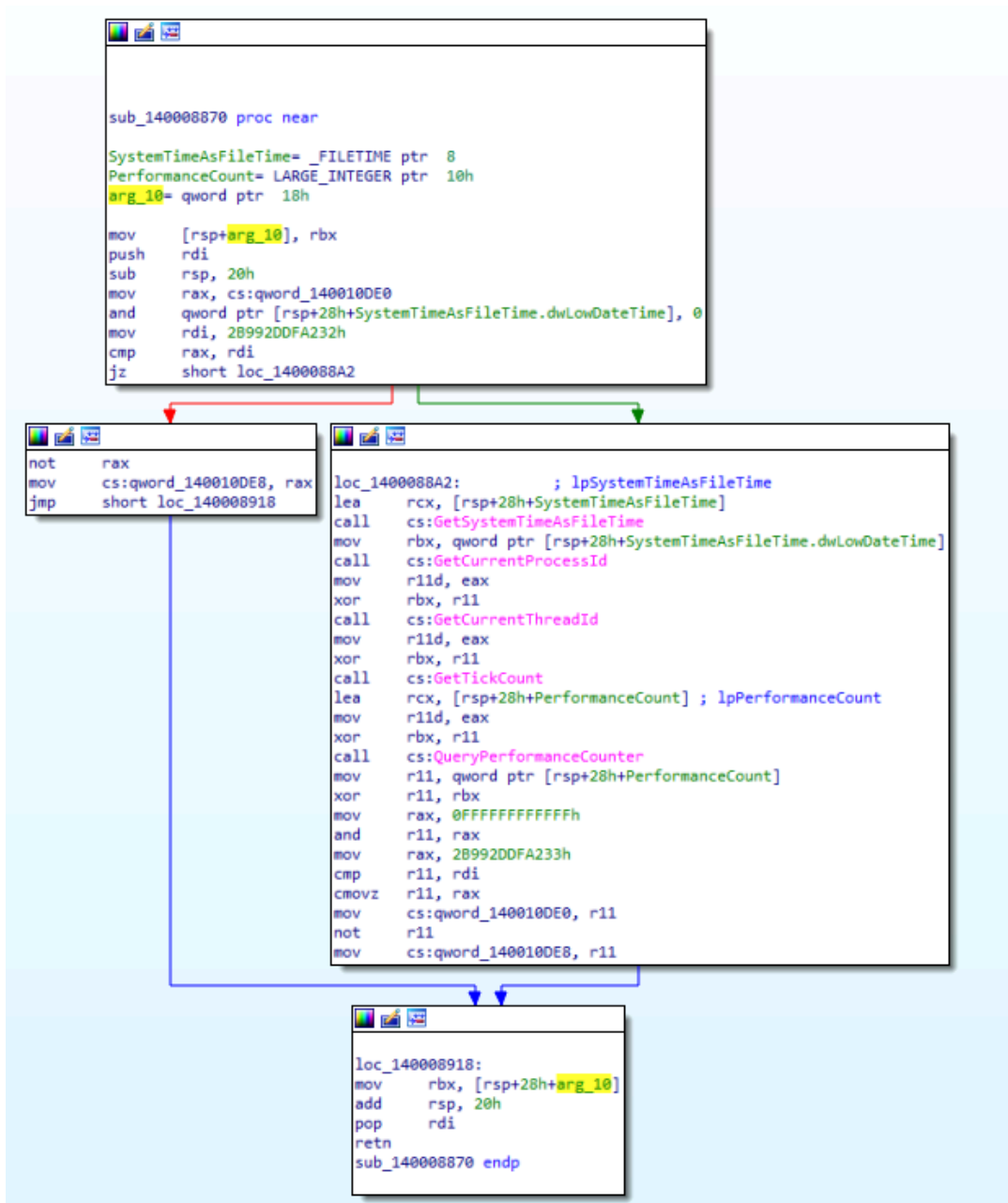
property	value
certificate	
revision	0x0200 (WIN_CERT_REVISION_2_0)
type	0x0002 (WIN_CERT_TYPE_PKCS_SIGNED_DATA)
file-offset-from	0x00010C00
file-offset-to	0x000121C0
size-certificate	0x15C0 (5568 bytes)
size-PKCS7	0x15AE (5550 bytes)
size-PKCS7-null-padding	6 bytes
footprint > sha256	D634FAAEA09652A59D0427927799AB59B908DECAED587F575B23329DFD2EA3C1
issued-to	
name	<b>Adobe Systems, Incorporated</b>
signature-info	Cyfrowy podpis obiektu nie został zweryfikowany.
issued-by	VeriSign Class 3 Code Signing 2009-2 CA
signing-time	Fri Jul 27 22:36:21 2012
valid-from	Mon Sep 28 02:00:00 2009
valid-to	Mon Nov 05 01:59:59 2012
serial-number	0290965E913340CDA6634CEF31F7FD07
thumbprint	9163233616937D326C8C45B966D98B6B0E739366
signature-algorithm	sha1RSA
program-name	wow_helper.exe
email	n/a
more-info-url	n/a
tail	

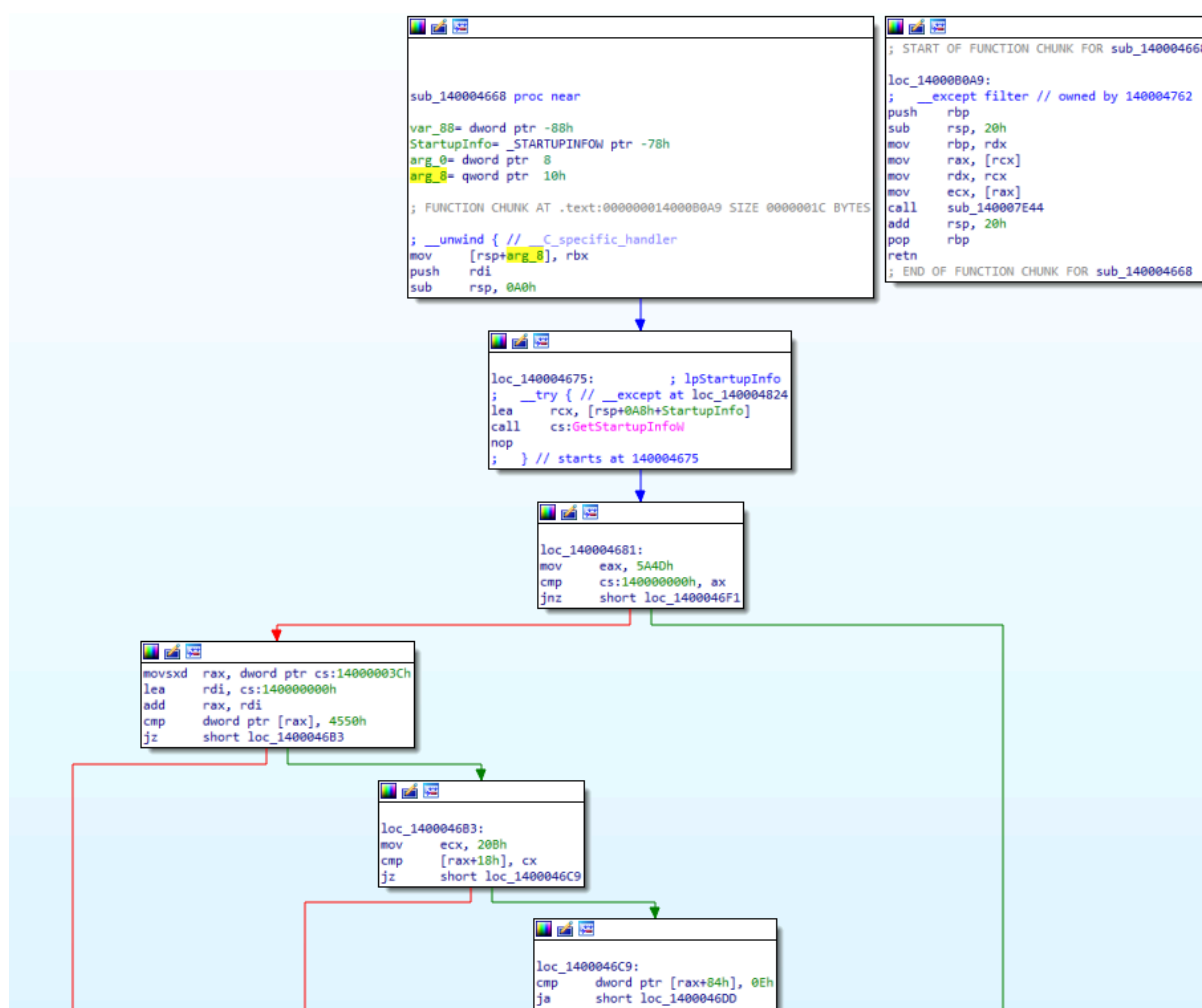
Jeżeli spojrzymy na certyfikat możemy zauważyć że program próbuje podrobić go tak aby wyglądało jakby to był program wydany przez Adobe.

version	-	-	-	-	040904e4
version	-	-	-	-	CompanyName
version	-	-	-	-	Adobe Systems, Inc
version	-	-	-	-	FileDescription
version	-	-	-	-	Adobe Reader WOW Helper
version	-	-	-	-	FileVersion
version	-	-	-	-	LegalCopyright
version	-	-	-	-	Copyright 2010-2012 Adobe Systems Incorporated and its licensors. All rights reserved.
version	-	-	-	-	InternalName
version	-	-	-	-	OriginalFilename
version	-	-	-	-	ProductName
version	-	-	-	-	Adobe Reader WOW Helper
version	-	-	-	-	ProductVersion
version	-	-	-	-	VarFileInfo
version	-	-	-	-	Translation
certificate	-	-	-	-	wow_helper.ex

Informacje w strings pozwalają nam zauważyć że program nazywa się Adobe Reader WOW Helper. W tym momencie analizy możemy stwierdzić, że może chodzić albo o Wow (Windows on Windows) czyli subsystemie pozwalającym uruchomić Pierwsza funkcja jaka jest wywoływana przez program zbiera dużo danych dotyczących maszyny na której jest między innymi ID procesu i godzinę a następnie wykonuje serię operacji AND i XOR możliwe aby zablokować dane.programy 32-bitowe na 64-bitowym systemie dodatkowo próbując ukryć swoje działania.

## IDA Pro





Następnie program używa **GetStartupInfo** by uzyskać informacje o procesie. Bardzo możliwe, że w celu sprawdzenia w jaki sposób został uruchomiony aby uniknąć detekcji przez niektóre narzędzia.

```

; FUNCTION CHUNK AT .text:000000014000AF80 SIZE 00000018 BYTES
; __unwind { // __CxxFrameHandler3
mov [rsp+arg_10], r8
mov [rsp+arg_8], rdx
mov [rsp+hProcess], rcx
sub rsp, 0D8h
mov [rsp+0D8h+var_10], 0FFFFFFFFFFFFFFFh
lea rax, aNtdllDll_0 ; "ntdll.dll"
mov [rsp+0D8h+lpModuleName], rax
mov rcx, [rsp+0D8h+lpModuleName] ; lpModuleName
call cs:GetModuleHandleW
mov [rsp+0D8h+var_48], rax
cmp [rsp+0D8h+var_48], 0
jnz short loc_140001C6C
  
```

Program w pewnym momencie próbuje znaleźć **ntdll.dll**. Jest to plik w którym w 2003 znaleziono lukę jednak została ona załatwana. Prawdopodobnie program próbuje wykorzystać lukę w nim w celu zainfekowania urządzenia.

## Podsumowanie

Z samej analizy statycznej programu ciężko stwierdzić jego funkcję. Jednak najprawdopodobniej próbuje się podszyć pod program Adobe może być wykorzystywany w celu zbierania informacji o systemie i osobie korzystającej z niego.

## Uruchomienie próbki

Malware zaraz po uruchomieniu wykonuje próbę połączenia się ze stroną `Watson.events.data.microsoft.com` prawdopodobnie by zmylić ewentualną osobę analizującą sieć.

```
06/06/24 03:31:43 PM [ DNS Server] Received A request for domain 'disc601.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:31:43 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
06/06/24 03:31:44 PM [ Divter] msedge.exe (4880) requested UDP 239.255.255.250:1900
06/06/24 03:31:51 PM [ Divter] svchost.exe (2192) requested UDP 192.168.56.102:53
06/06/24 03:31:51 PM [ DNS Server] Received A request for domain 'disc601.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:31:51 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
06/06/24 03:32:02 PM [ Divter] System (4) requested UDP 192.168.56.255:138
06/06/24 03:32:06 PM [ Divter] svchost.exe (2192) requested UDP 192.168.56.102:53
06/06/24 03:32:06 PM [ DNS Server] Received A request for domain 'disc601.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:32:06 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
06/06/24 03:32:48 PM [ Divter] svchost.exe (2192) requested UDP 192.168.56.102:53
06/06/24 03:32:48 PM [ DNS Server] Received A request for domain 'disc601.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:32:48 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
06/06/24 03:33:41 PM [ Divter] msedge.exe (4880) requested UDP 239.255.255.250:1900
06/06/24 03:34:23 PM [ Divter] svchost.exe (2192) requested UDP 192.168.56.102:53
06/06/24 03:34:23 PM [ DNS Server] Received A request for domain 'disc601.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:34:23 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
06/06/24 03:34:23 PM [ Divter] svchost.exe (2192) requested UDP 192.168.56.102:53
06/06/24 03:34:23 PM [ DNS Server] Received A request for domain 'geover.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:34:23 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
06/06/24 03:34:23 PM [ Divter] svchost.exe (2192) requested UDP 192.168.56.102:53
06/06/24 03:34:23 PM [ DNS Server] Received A request for domain 'kv601.prod.do.dsp.mp.microsoft.com'.
06/06/24 03:34:23 PM [ Divter] svchost.exe (4380) requested TCP 192.0.2.123:443
```

Następnie próbuje wykonać **request DNS** do innych serwerów związanych z Microsoftem

31	38.131070	10.0.2.15	20.42.73.29	TCP	74 49924 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=641853 TSecr=0
32	38.244750	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
33	38.245806	10.0.2.15	20.42.73.29	TCP	54 49924 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
34	38.246919	10.0.2.15	20.42.73.29	TLSv1.2	253 Client Hello (SN=watson.events.data.microsoft.com)
35	38.247345	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=1 Ack=200 Win=65535 Len=0
36	38.365523	20.42.73.29	10.0.2.15	TCP	1514 443 → 49924 [ACK] Seq=1 Ack=200 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
37	38.365523	20.42.73.29	10.0.2.15	TCP	1514 443 → 49924 [PSH, ACK] Seq=1461 Ack=200 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
38	38.365595	10.0.2.15	20.42.73.29	TCP	54 49924 → 443 [ACK] Seq=200 Ack=1921 Win=64240 Len=0
39	38.365853	20.42.73.29	10.0.2.15	TCP	1514 443 → 49924 [ACK] Seq=2921 Ack=200 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
40	38.365853	20.42.73.29	10.0.2.15	TLSv1.2	158 Server Hello, Certificate, Server Key Exchange, Server Hello Done
41	38.365907	10.0.2.15	20.42.73.29	TCP	54 49924 → 443 [ACK] Seq=200 Ack=4485 Win=64240 Len=0
42	38.368326	10.0.2.15	20.42.73.29	TLSv1.2	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
43	38.368504	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=4485 Ack=358 Win=65535 Len=0
44	38.482757	20.42.73.29	10.0.2.15	TLSv1.2	185 Change Cipher Spec, Encrypted Handshake Message
45	38.494045	10.0.2.15	20.42.73.29	TLSv1.2	259 Application Data
46	38.494493	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=4536 Ack=563 Win=65535 Len=0
47	38.494556	10.0.2.15	20.42.73.29	TCP	2974 49924 → 443 [ACK] Seq=563 Ack=4536 Win=64189 Len=2920 [TCP segment of a reassembled PDU]
48	38.494835	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=4536 Ack=2023 Win=65535 Len=0
49	38.494835	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=4536 Ack=3483 Win=65535 Len=0
50	38.494850	10.0.2.15	20.42.73.29	TLSv1.2	1259 Application Data
51	38.495058	10.0.2.15	20.42.73.29	TLSv1.2	693 Application Data
52	38.495222	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=4536 Ack=4688 Win=65535 Len=0
53	38.495222	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=4536 Ack=5327 Win=65535 Len=0
54	38.784598	20.42.73.29	10.0.2.15	TLSv1.2	921 Application Data
55	38.785824	10.0.2.15	20.42.73.29	TCP	54 49924 → 443 [FIN, ACK] Seq=5327 Ack=5403 Win=63322 Len=0
56	38.786388	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [ACK] Seq=5403 Ack=5328 Win=65535 Len=0
57	38.903978	20.42.73.29	10.0.2.15	TCP	60 443 → 49924 [FIN, ACK] Seq=5403 Ack=5328 Win=65535 Len=0

Dodatkowo po uruchomieniu widać że komunikuje się z serwerem

```
HKLM\SOFTWARE\Classes\pdf\ShellEx{8B95B1C6-B414-4d1c-a562-0d564250836f}\{"384F9C2-6164-485C-A709-4B27F8AC009E"}
HKLM\SOFTWARE\Classes\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\PDF Preview Handler
HKLM\SOFTWARE\Classes\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\DisplayName="PDF Preview Handler"
HKLM\SOFTWARE\Classes\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\AppID="{6d2b5079-2f0b-48dd-ab7f-97cec514d30b}"
HKLM\SOFTWARE\Classes\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\EnablePreviewHandler: 0x00000001
HKLM\SOFTWARE\Classes\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\InProcServer32: "C:\Program Files (x86)\Microsoft\Edge\Application\125.0.2535.92\PdfPreview\PdfPreviewHandler.dll"
HKLM\SOFTWARE\Classes\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\InProcServer32\ThreadingModel="Apartment"
HKLM\SOFTWARE\Classes\WOW6432Node\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\PDF Preview Handler
HKLM\SOFTWARE\Classes\WOW6432Node\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\DisplayName="PDF Preview Handler"
HKLM\SOFTWARE\Classes\WOW6432Node\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\AppID="{6d2b5079-2f0b-48dd-ab7f-97cec514d30b}"
HKLM\SOFTWARE\Classes\WOW6432Node\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\EnablePreviewHandler: 0x00000001
HKLM\SOFTWARE\Classes\WOW6432Node\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\InProcServer32: "C:\Program Files (x86)\Microsoft\Edge\Application\125.0.2535.92\PdfPreview\PdfPreviewHandler.dll"
HKLM\SOFTWARE\Classes\WOW6432Node\CLSID{384F9C2-6164-485C-A709-4B27F8AC009E}\InProcServer32\ThreadingModel="Apartment"
```

Dodatkowo widzimy klucze dodane do rejestru przez malware podszywa on się pod program do podglądu PDF-ów. Stąd też prawdopodobnie jego próba do upodobnienia się do programu Adobe.

## x64\_dbg

[illegible]

Wykonując dalszą analiza natrafiamy na coś co nazywa się Installer\_NotifyShims. Prawdopodobnie trojan próbuje zainstalować dodatkowy malware.

```
000000002
00010FECB0
00010FEC10
C76372120      L"TerminalServices-RemoteConnectionManager-AllowAppServerMode"
00010FEC28
00010FEBD8
000000011C      L'G'
0000000124      L'H'
```

Dalej analizując znajdujemy kolejny indyktor sieciowy mówiący o tym że aplikacja próbuje się z czymś połączyć.

00007FFC762BE969	44:8B5CF8 08	mov rbx,rcx and ptr ds:[rax+r15*8+8]	rbx	ukry3 FPU
00007FFC762BE965	44:8B5D	test rbx,rbx	rbx	
00007FFC762BE968	74 74	jnz ntdll1.F7FC762BE96E	rbx	C73C4B98 kernelbase.00007FFC73C4B98 &"GetVersionExWSwitch"
00007FFC762BE96A	33FE	xor esi,esi	rbx	
00007FFC762BE96C	5973 44	cmp dword ptr ds:[rbx+44],esi	rbx	C73D0670
00007FFC762BE96F	76 12	jbe ntdll1.F7FC762BE988	rbx	0000000003
00007FFC762BE971	3C9	xor ecx,ecx	rbx	0000000003
00007FFC762BE973	1940 38	cmp dword ptr esi:[rbp+3C],ecx	rbx	000110078
00007FFC762BE976	0F87 FC190500	jnz ntdll1.F7FC762B3078	rbx	00010FA30
00007FFC762BE97C	FFC6	inc esi	rbx	0000000002
00007FFC762BE97E	3B73 44	cmp esi,dword ptr ds:[rbx+44]	rbx	0000000000
00007FFC762BE981	72 EC	jbe ntdll1.F7FC762BE978	rbx	0000000000
00007FFC762BE983	44:8B53 44	mov r10,dword ptr ds:[rbx+44]	rbx	0000000000A
00007FFC762BE987	41:3BF2	cmp esi,r10d	rbx	00010FA68
00007FFC762BE98A	72 52	jbe ntdll1.F7FC762BE98E	rbx	0000000003
00007FFC762BE98C	33FE	xor esi,esi	rbx	00000000346 L**
00007FFC762BE98E	45:8B02	test r10d,r10d	rbx	0000000040 "g"
00007FFC762BE991	74 44	jnz ntdll1.F7FC762B307F	rbx	C73C4188 "KLSN"
00007FFC762BE993	8BE	mov ebx,esi	rbx	C73D070F kernelbase.00007FFC73D070F
00007FFC762BE995	48:804C24 38	lea rcx,dword ptr esi:[esp+38]	rbx	0000000003
00007FFC762BE997	48:C1E5 07	shl r10,10	rbx	
00007FFC762BE999	48:83C5 48	add rbp,48	rbx	
00007FFC762BE99A	89FE	mov esi,esi	rbx	
00007FFC762BE99C	48:03EB	add rbp,rbx	rbx	C762BE97C ntdll1.00007FFC762BE97C
00007FFC762BE9A4	48:03EB	add rbp,rbx	rbx	
00007FFC762BE9A7	48:8B05	mov rdx,rbp	rbx	0000000010246
00007FFC762BE9AA	E8 C5000000	call ntdll1.F7FC762BEA74	rbx	0000000000000000
00007FFC762BE9AF	33BF 01	cmp eax,1	rbx	0000000000000000
00007FFC762BE9B2	74 09	jnz ntdll1.F7FC762BE9BD	rbx	0000000000000000
00007FFC762BE9B4	FFC6	inc esi	rbx	0000000000000000
00007FFC762BE9B6	41:3BF2	cmp esi,r10d	rbx	0000000000000000
00007FFC762BE9B9	72 D8	jbe ntdll1.F7FC762BE993	rbx	0000000000000000
00007FFC762BE9BB	C9 15	cmp ntdll1.F7FC762BE982	rbx	0000000000000000
00007FFC762BE9BD	48:C1E7 07	shl rdi,7	rbx	0000000000000000
00007FFC762BE9C1	48:837C10 00	cmp rdi,rcx and ptr ds:[rdi+rbx+50],0	rbx	0000000000000000
00007FFC762BE9C7	0F84 161A0500	jnz ntdll1.F7FC762B3078	rbx	0000000000000000
00007FFC762BE9CD	48:89CF6E 10	mov dword ptr ds:[r14+r15*8+10],rbp	rbx	0000000000000000
00007FFC762BE9D2	48:8B6C24 20	mov rbp,dword ptr esi:[esp+20]	rbx	0000000000000000
00007FFC762BE9D7	3BF2	cmp esi,edx	rbx	0000000000000000
00007FFC762BE9DC	73 48	jbe ntdll1.F7FC762BEA29	rbx	0000000000000000
00007FFC762BE9DE	49:8845 18	mov esi,dword ptr ds:[r13+18]	rbx	0000000000000000
00007FFC762BE9E2	41:FFC7	inc r15	rbx	0000000000000000
00007FFC762BE9E5	44:39B8	cmp r15,dword ptr ds:[rax]	rbx	0000000000000000
00007FFC762BE9E8	0F82 72FFFFF	jnz ntdll1.F7FC762BE960	rbx	0000000000000000
00007FFC762BE9F4	45:804C24 30	mov esi,dword ptr esi:[esp+30]	rbx	0000000000000000
00007FFC762BE9F3	B8 01000000	mov eax,1	rbx	0000000000000000
00007FFC762BE9F8	49:890E	mov dword ptr ds:[r14],ecx	rbx	0000000000000000
00007FFC762BE9FA	8B4C24 20	mov rcx,dword ptr esi:[esp+20]	rbx	0000000000000000
00007FFC762BE9FF	41:894E 08	mov dword ptr ds:[r14+8],ecx	rbx	0000000000000000
00007FFC762BEA00	48:8B4C24 48	mov rcx,dword ptr esi:[esp+48]	rbx	0000000000000000



Następnie program próbuje dowiedzieć się jaka wersja windowsa jest na komputerze.

Po podłączeniu komputera do internetu program zmienił swoje działanie.

0F100C11	movups xmm1,xmmword ptr ds:[rcx+rdx]	rcx+rdx*1:L"OCESOR5=12"
0F105411 10	movups xmm2,xmmword ptr ds:[rcx+rdx+10]	rcx+rdx*1+10:L"=12"
0F105C11 20	movups xmm3,xmmword ptr ds:[rcx+rdx+20]	rcx+rdx*1+20:L"rive=C:\\Users\\admin\\OneDrive"
0F106411 30	movups xmm4,xmmword ptr ds:[rcx+rdx+30]	rcx+rdx*1+30:L"Users\\admin\\OneDrive"
0F2941 F0	movaps xmmword ptr ds:[rcx-10],xmm0	
48:83C1 40	add rcx,40	
49:FFC9	dec r9	
0F2949 C0	movaps xmmword ptr ds:[rcx-40],xmm1	
0F2951 D0	movaps xmmword ptr ds:[rcx-30],xmm2	
0F2959 E0	movaps xmmword ptr ds:[rcx-20],xmm3	
0F29C4	movaps xmm0,xmm4	
75 D1	jmp ntdll.7FFC762F3F40	

Zaczął szukać jakiegoś pliku na dysku

	89 E0FF0000	mov ecx,FF00																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									</
--	-------------	--------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

00007FFC762B1FBA	49:8B02	mov rax,qword ptr ds	rax:NtCreateFile, [r10]:NtCreateFile
00007FFC762B1FBD	45:33C0	xor r8d,r8d	
00007FFC762B1FCE	0F1000	movups xmm0,xmmword	rax:NtCreateFile
00007FFC762B1FCE	F2:0F1048 10	movsd xmm1,qword ptr	rax+10:ZwCreateFile+10
00007FFC762B1FCE	48:8D05 D0BA0C00	lea rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	0F114424 38	movups xmmword ptr	
00007FFC762B1FCE	F2:0F114C24 48	movsd qword ptr ss:[	
00007FFC762B1FCE	44:0FB608	movzx r9d,byte ptr	rax:NtCreateFile
00007FFC762B1FCE	49:83F9 18	cmp r9,18	
00007FFC762B1FCE	0F83 FE000000	jbe ntdll.7FFC762B20	
00007FFC762B1FCE	44:03C6	add r8d,esi	
00007FFC762B1FCE	42:C6440C 38 00	mov byte ptr ss:[rsp	
00007FFC762B1FCE	48:03C6	add rax,rax	rax:NtCreateFile
00007FFC762B1FCE	41:83F8 04	cmp r8d,4	
00007FFC762B1FCE	72 E0	jbe ntdll.7FFC762B1FD	
00007FFC762B1FCE	48:8B05 1F771000	mov rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	48:284424 38	sub rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	75 1A	jne ntdll.7FFC762B20	
00007FFC762B1FCE	48:8B05 19771000	mov rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	48:284424 40	sub rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	75 0C	jne ntdll.7FFC762B20	
00007FFC762B1FCE	48:8B05 13771000	mov rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	48:284424 48	sub rax,qword ptr ds	rax:NtCreateFile
00007FFC762B1FCE	48:85C0	test rax,rax	rax:NtCreateFile
00007FFC762B1FCE	0F85 EDC40500	jbe ntdll.7FFC7630E5	

Malware próbuje tworzyć nowe pliki

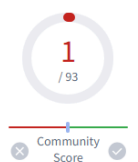
```
EXCEPTION_DEBUG_INFO:
  dwFirstChance: 1
  ExceptionCode: C000001D (EXCEPTION_ILLEGAL_INSTRUCTION)
  ExceptionFlags: 00000000
  ExceptionAddress: 317849c236aa238bd3287ed58effeef15db1c7d63cf54bbba1f88b3d97d6c7a.00007FF663B64AB2
  NumberParameters: 0
First chance exception on 00007FF663B64AB2 (C000001D, EXCEPTION_ILLEGAL_INSTRUCTION)!
Process stopped with exit code 0xC000001D (STATUS_ILLEGAL_INSTRUCTION)
Zapisywanie bazy danych do c:\tools\x64dbg\release\x64\db\317849c236aa238bd3287ed58effeef15db1c7d63cf54bbba1f88b3d97d6c7a.exe.dd64 0ms
Zatrzymano debugowanie!
```

Program po pewnym czasie napotyka wyjątek i się wyłącza

## Windows Vista

Po zmianie systemu na windows Vista program zaczął wysyłać żądania do serwera używając losowych znaków jako linku do pliku.

133	29.093938	152.199.19.74	10.0.2.15	TCP	60 80-49260 [ACK] Seq=1852 Ack=1548 Win=65535 Len=0
134	29.106057	152.199.19.74	10.0.2.15	OCSP	425 Response
135	29.121545	10.0.2.15	192.229.221.95	HTTP	194 GET /ThawteTimestampingCA.crl HTTP/1.1
136	29.122870	192.229.221.95	10.0.2.15	TCP	60 80-49261 [ACK] Seq=1848 Ack=265 Win=65535 Len=0
137	29.133882	192.229.221.95	10.0.2.15	PKIX-C...	779 Certificate Revocation List
138	29.156378	10.0.2.15	152.199.19.74	HTTP	287 GET /HFEwTzBMWESwSTA3BglrDgKCGUABBT03jA3oCaQZuo7K2B2q3hdK4D6wpuQQUqkwaVo1A5mAvIL8uAwdOcH2iFUCEHm1pYX58RVCe9m4Pva2je083D HTTP/1.1
139	29.156723	152.199.19.74	10.0.2.15	TCP	60 80-49260 [ACK] Seq=2223 Ack=1781 Win=65535 Len=0
140	29.167141	152.199.19.74	10.0.2.15	OCSP	425 Response
141	29.188497	10.0.2.15	152.199.19.74	HTTP	330 GET /HFEwTzBMWESwSTA3BglrDgKCGUABBT03jA3oCaQZuo7K2B2q3hdK4D6wpuQQUqkwaVo1A5mAvIL8uAwdOcH2iFUCEHm1pYX58RVCe9m4Pva2je083D HTTP/1.1
142	29.188698	152.199.19.74	10.0.2.15	TCP	60 80-49260 [ACK] Seq=2594 Ack=2057 Win=65535 Len=0
143	29.201559	152.199.19.74	10.0.2.15	OCSP	425 Response
144	29.215240	10.0.2.15	192.229.221.95	HTTP	180 GET /tss-ca.crl HTTP/1.1
145	29.215575	192.229.221.95	10.0.2.15	TCP	60 80-49261 [ACK] Seq=2573 Ack=391 Win=65535 Len=0



1/93 security vendor flagged this IP address as malicious

Reanalyze Similar Graph API

US Last Analysis Date 7 hours ago

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

Security vendors' analysis

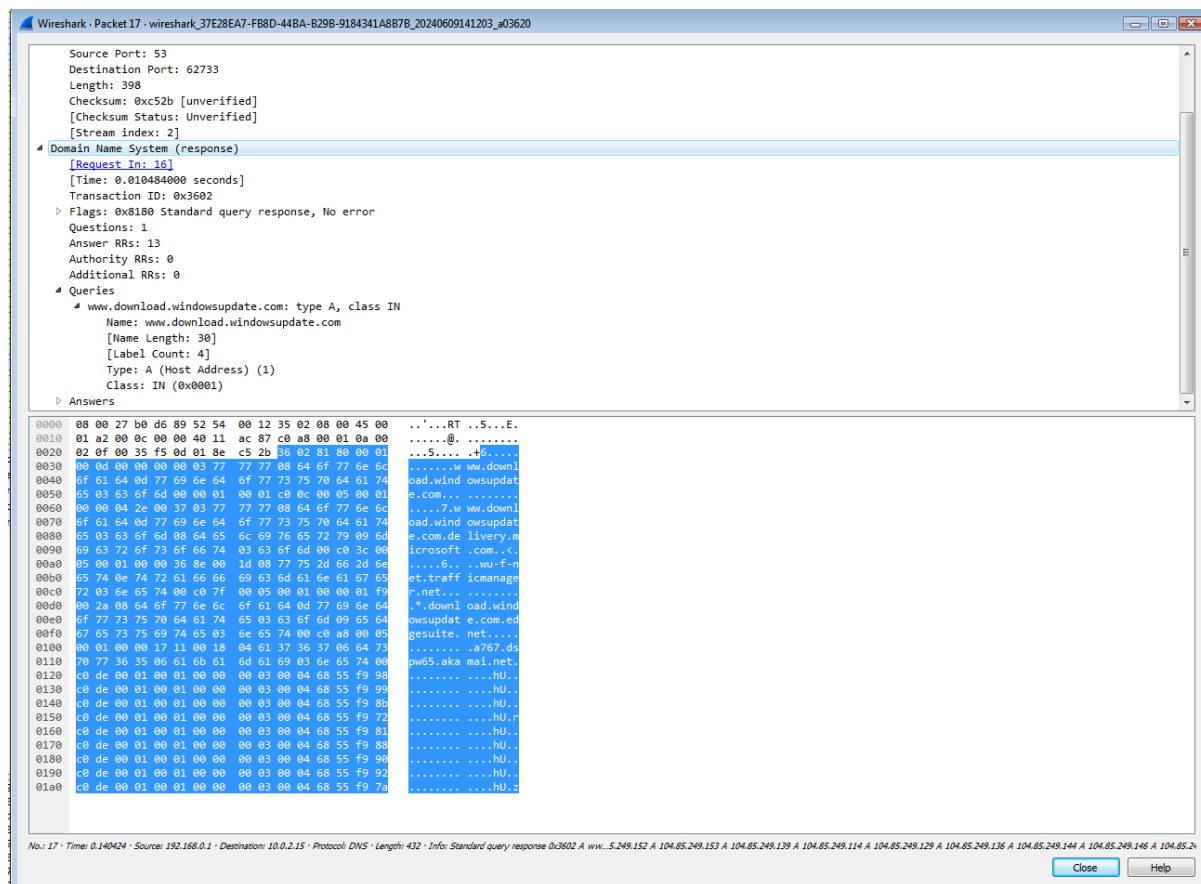
Do you want to automate checks?

SOCradar	Malicious	Abusix	Clean
----------	-----------	--------	-------

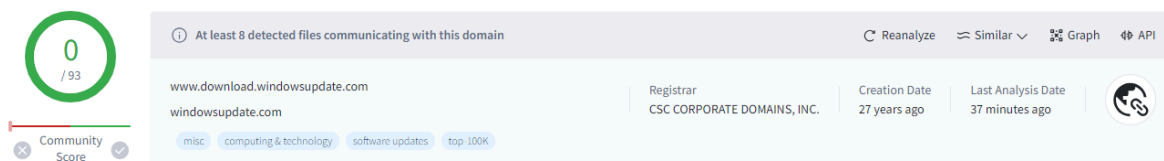
Adres ten przez jednego vendora został zaznaczony jako malicious



## Wireshark



## Wnioski



Program wygląda na program który próbuje podszyć się pod program do przeglądania PDF-ów jednak w rzeczywistości stara się pobrać pliku ze zdalnego serwera. Serwer jest już niedostępny więc malware automatycznie się wyłącza.