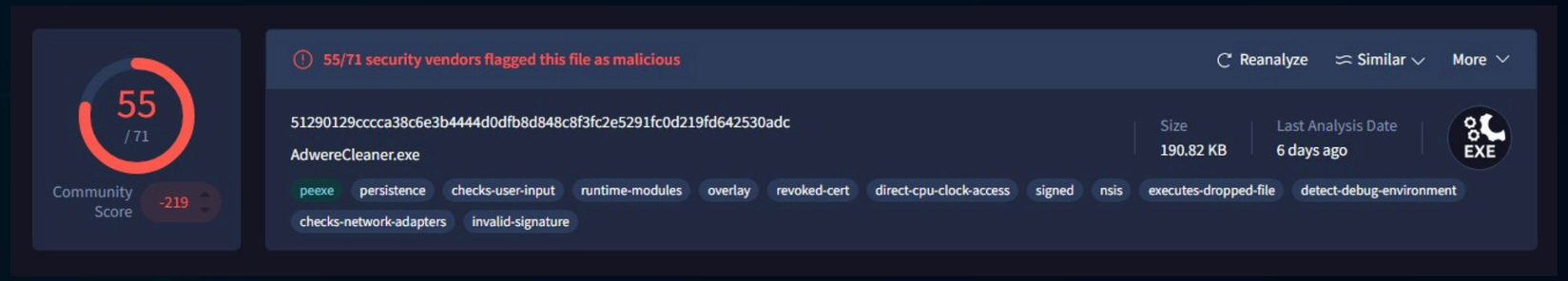
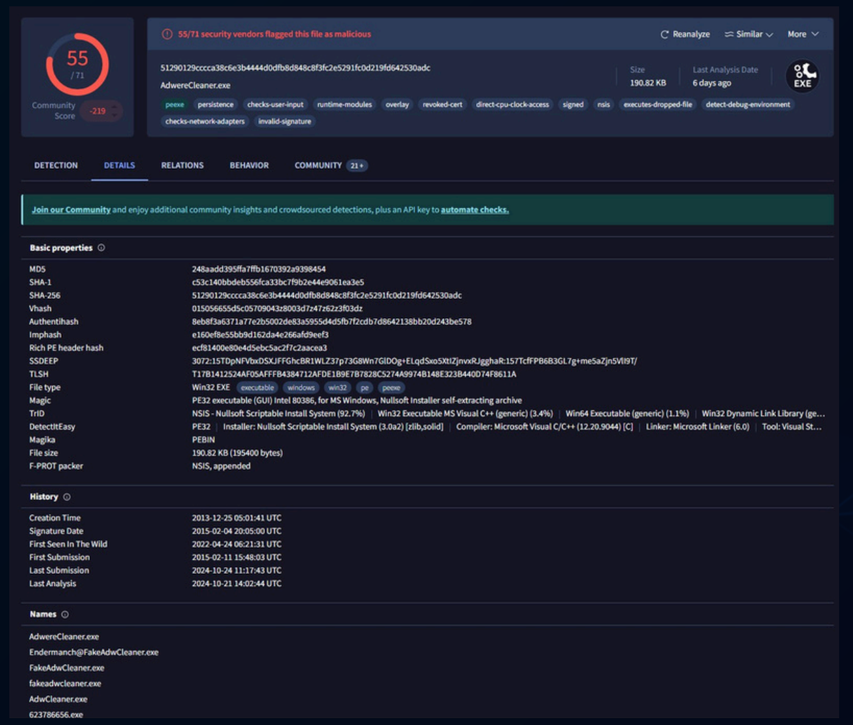
MALWARE ANALYSIS

PantherPwners

VIRUSTOTAL SCANNING



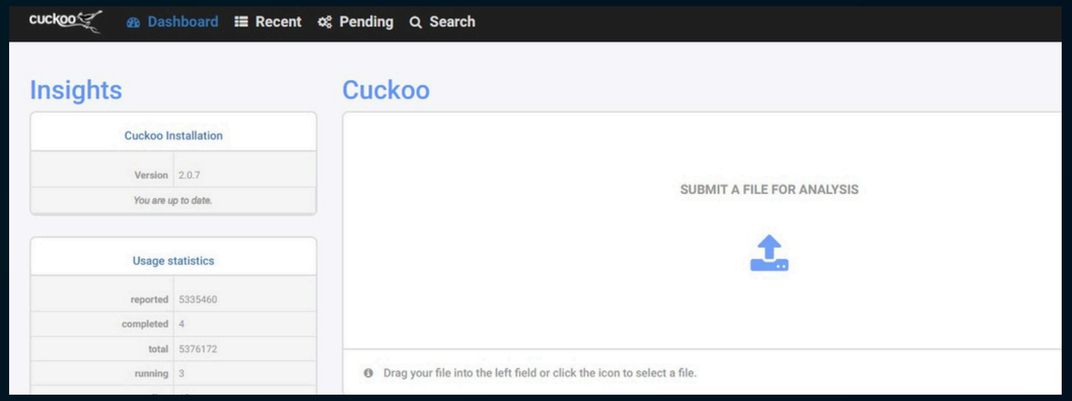


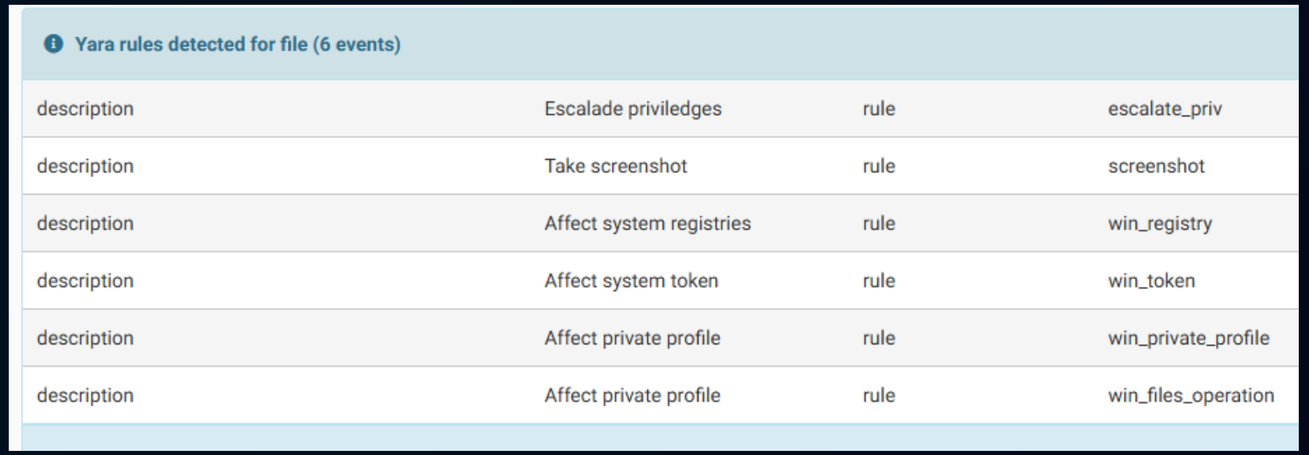
Utilizziamo il tool VirusTotal per effettuare una prima analisi, sul file AdwereCleaner.exe
55/71 security vendors flagged this file as malicious

Adwere.exe è potenzialmente dannoso

PantherPwners

SANDBOX CUCKOO



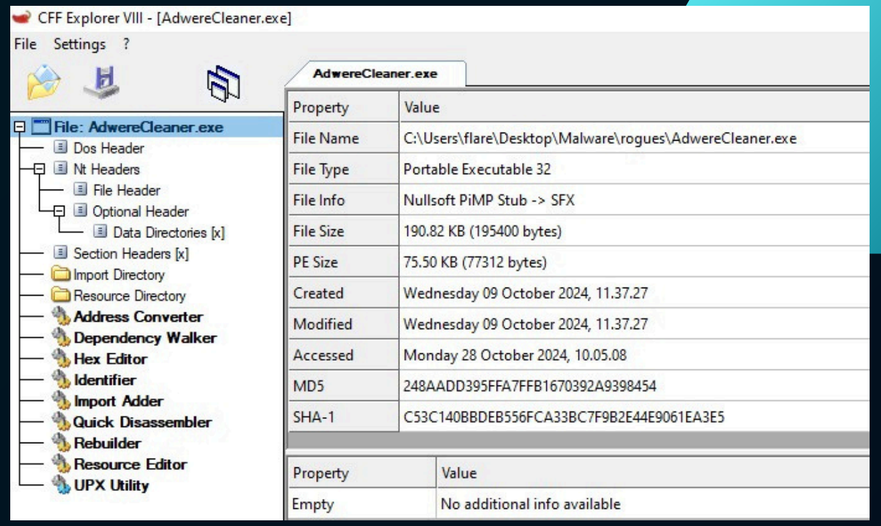


Escalade_priv: Tentativi di ottenere privilegi elevati.
Screenshot: Il malware tenta di acquisire screenshot del sistema.
Win_registry: Modifica delle chiavi di registro di sistema.
Win_token: Manipolazione dei token di sistema.
Win_private_profile: Accesso o modifica ai profili privati.
Win_files_operation: Operazioni sui file privati dell'utente.

PantherPwners

Avviamo CFF Explorer, per un ulteriore analisi del Malware.

Andando su Section Header, troviamo le varie Sezioni dell'eseguibile



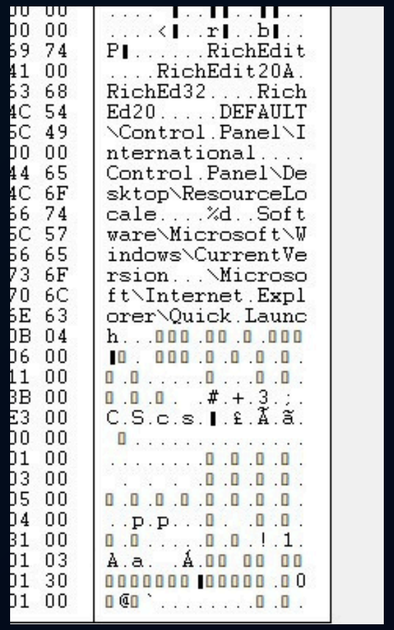
Property	Value
File Name	C:\Users\flare\Desktop\Malware\rogues\AdwereCleaner.exe
File Type	Portable Executable 32
File Info	Nullsoft PiMP Stub -> SFX
File Size	190.82 KB (195400 bytes)
PE Size	75.50 KB (77312 bytes)
Created	Wednesday 09 October 2024, 11.37.27
Modified	Wednesday 09 October 2024, 11.37.27
Accessed	Monday 28 October 2024, 10.05.08
MD5	248AADD395FFA7FFB1670392A9398454
SHA-1	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5

Property	Value
Empty	No additional info available

AdwereCleaner.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...
000001E8	000001F0	000001F4	000001F8	000001FC	00000200	00000204	00000208
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word
.text	00005DE2	00001000	00005E00	00000400	00000000	00000000	0000
.rdata	000012DA	00007000	00001400	00006200	00000000	00000000	0000
.data	00025498	00009000	00000400	00007600	00000000	00000000	0000
.ndata	00008000	0002F000	00000000	00000000	00000000	00000000	0000
.rsrc	0000B268	00037000	0000B400	00007A00	00000000	00000000	0000

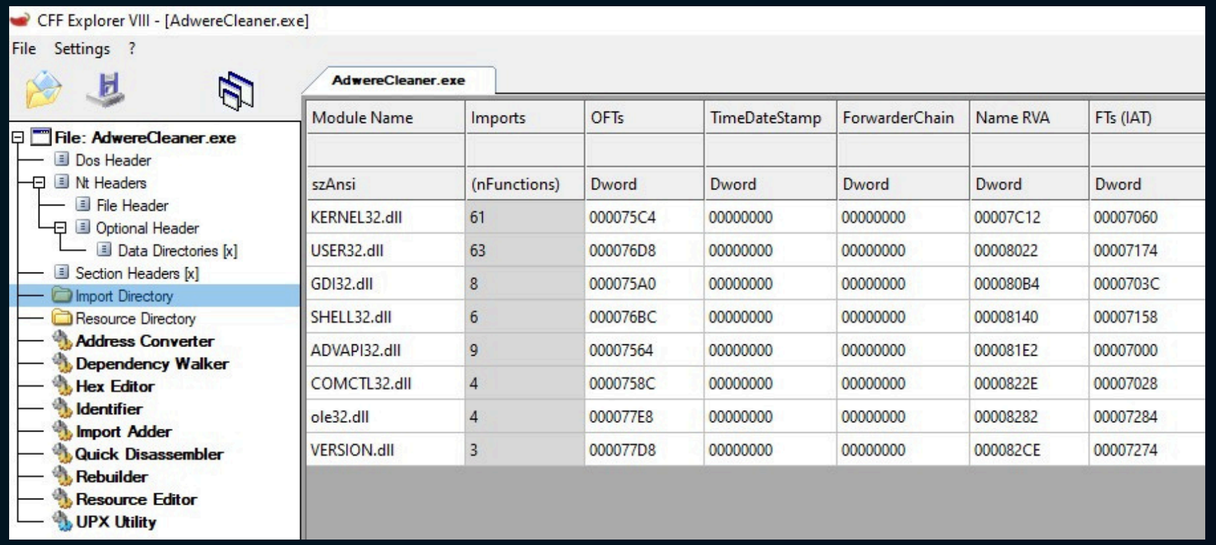
.rdata: Contiene dati di sola lettura come puntatori e stringhe costanti



Analizzando la Sezione di ".rdata" troviamo una richiesta di far partire con un Quick Launch, Internet Explorer

PantherPwners

Nella voce “Import Directory” invece, vediamo le liste DLL



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
VERSION.dll	3	000077D8	00000000	00000000	000082CE	00007274

AdwereCleaner.exe

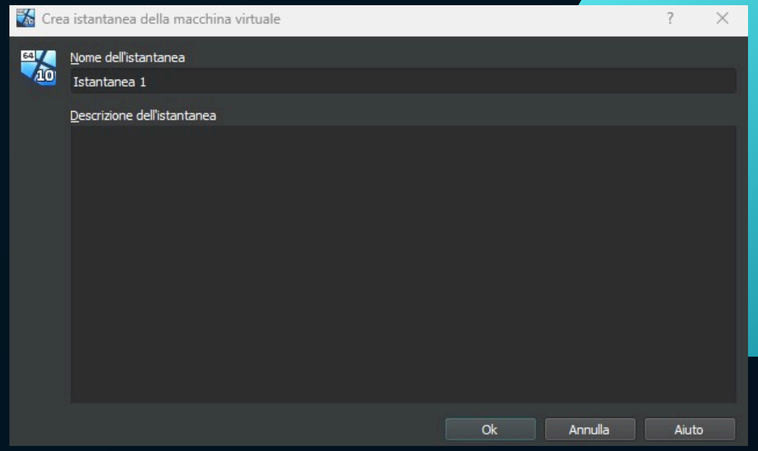
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00006E12	N/A	000066B0	000066B4	000066B8	000066BC	000066C0
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
VERSION.dll	3	000077D8	00000000	00000000	000082CE	00007274

La presenza di funzioni come:
LoadLibraryA
CreateThread
CreateProcessA
RemoveDirectoryA
GetTempFileNameA

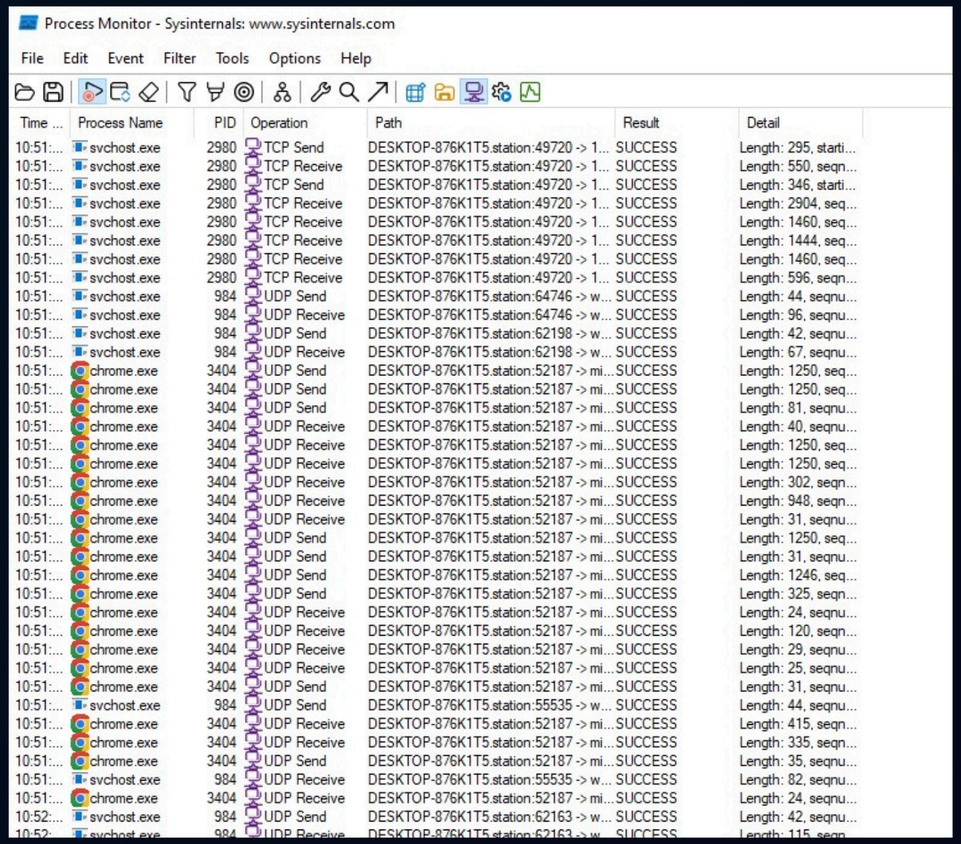
Suggerisce che questo software:
Carica altre librerie dinamicamente
Crea nuovi processi e thread
Manipola file e directory temporanee
Rimuove directory

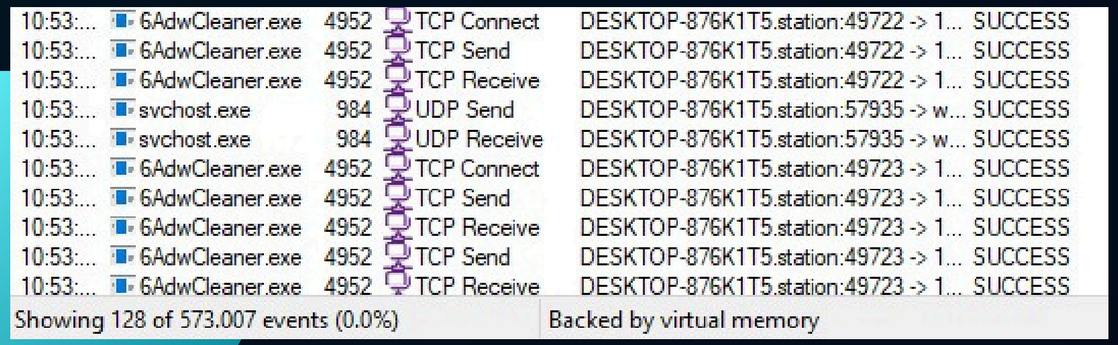
Dword	Dword	Word	szAnsi
00007A40	00007A40	01DF	GetTickCount
000079B0	000079B0	0169	GetFullPathNameA
000079C4	000079C4	026E	MoveFileA
000079D0	000079D0	030A	SetCurrentDirectoryA
000079E8	000079E8	015E	GetFileAttributesA
000079FE	000079FE	0171	GetLastError
00007A0E	00007A0E	004B	CreateDirectoryA
00007A22	00007A22	0319	SetFileAttributesA
0000798E	0000798E	02DB	SearchPathA
0000799C	0000799C	01B5	GetShortPathNameA
00007A50	00007A50	0163	GetFileSize
00007A5E	00007A5E	017D	GetModuleFileNameA
00007A74	00007A74	0142	GetCurrentProcess
00007A88	00007A88	0043	CopyFileA
00007A94	00007A94	00B9	ExitProcess
00007AA2	00007AA2	0313	SetEnvironmentVariableA
00007ABC	00007ABC	01F3	GetWindowsDirectoryA
00007AD4	00007AD4	01D5	GetTempPathA
00007A38	00007A38	0356	Sleep
00007960	00007960	0034	CloseHandle
00007B06	00007B06	0252	LoadLibraryA
00007B16	00007B16	03CC	lstrlenA
00007B22	00007B22	03C9	lstrcpynA
00007B2E	00007B2E	014D	GetDiskFreeSpaceA
00007B42	00007B42	020A	GlobalUnlock
00007B52	00007B52	0203	GlobalLock
00007B60	00007B60	006F	CreateThread
00007B70	00007B70	0066	CreateProcessA
00007B82	00007B82	02C4	RemoveDirectoryA
00007B96	00007B96	0053	CreateFileA
00007BA4	00007BA4	01D3	GetTempFileNameA

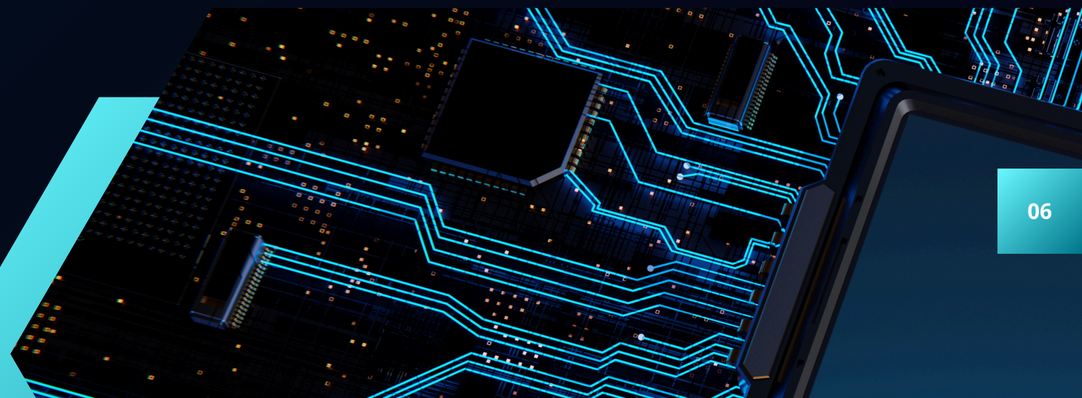
Prima di avviare il malware, abbiamo creato un istantanea della macchina virtuale, per lavorare in sicurezza e non compromette la macchina



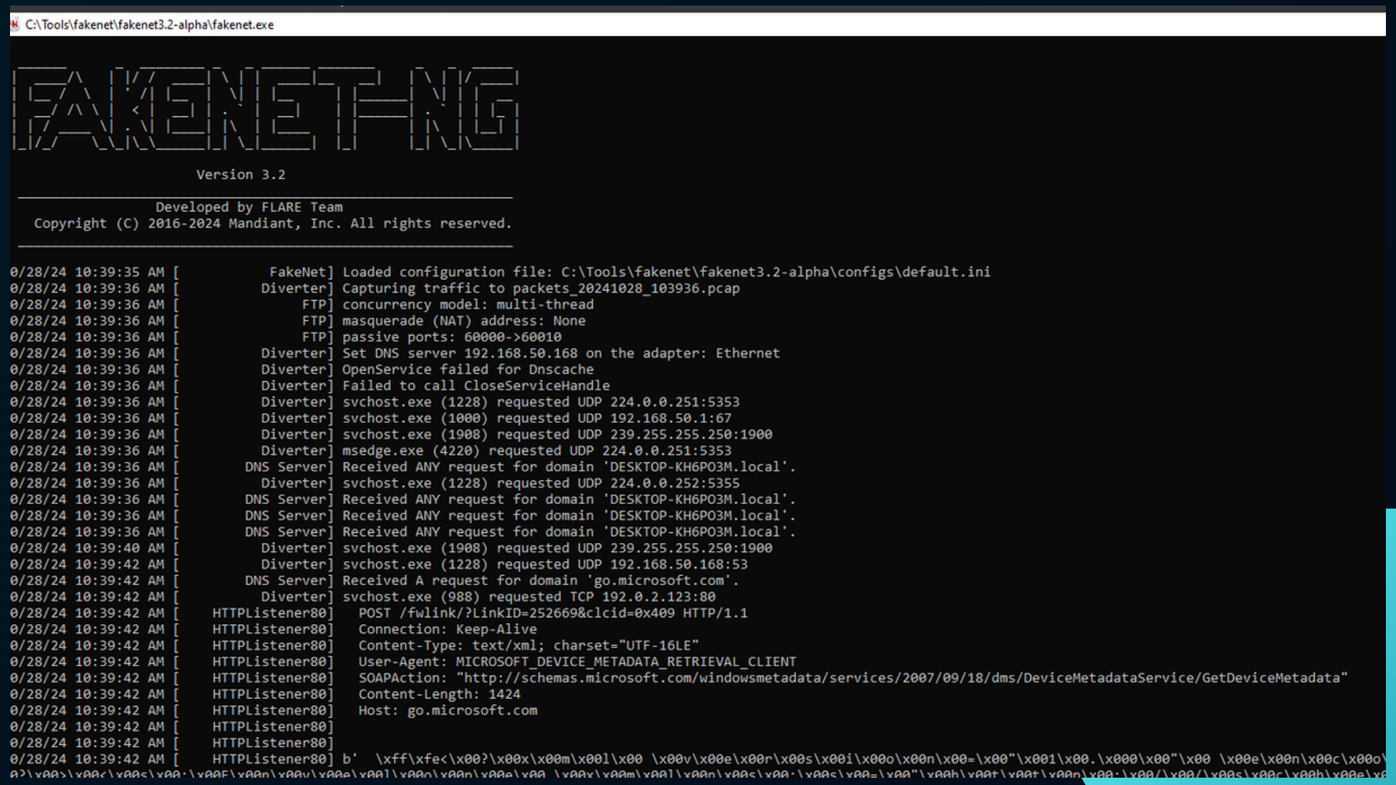
Con Procmon, abbiamo notato che una volta avviato il malware, inizia a inviare richieste TCP



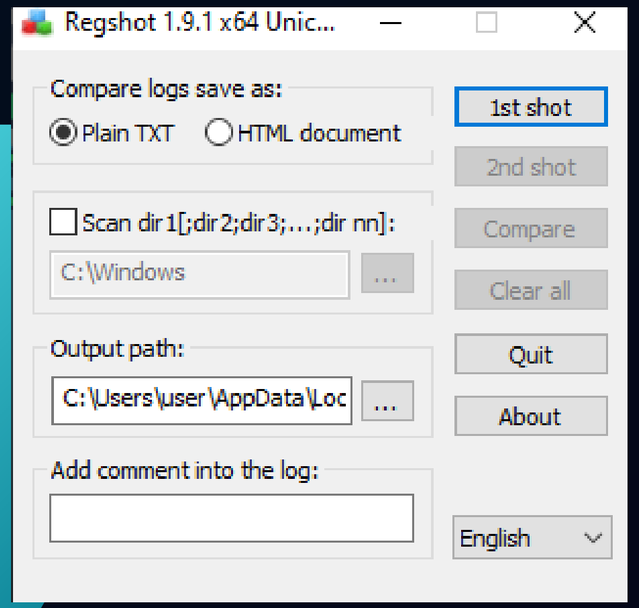




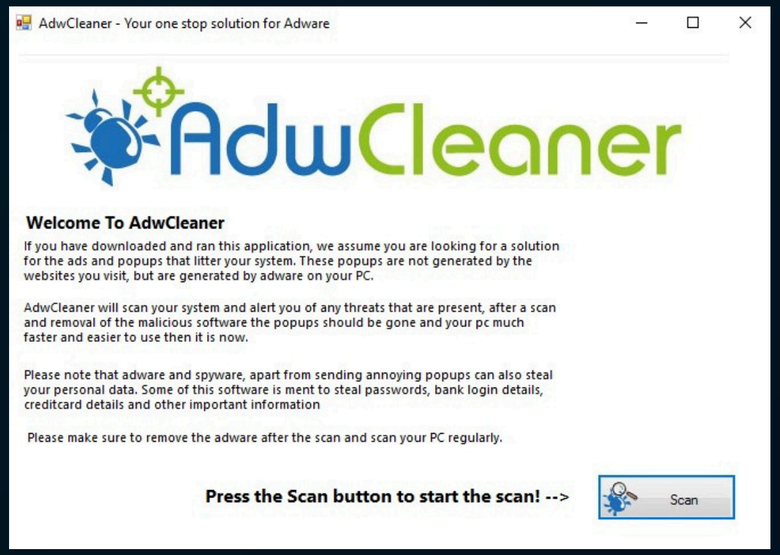
Avviamo Fakenet: uno strumento utile per analizzare malware in ambienti controllati, simulando un ambiente di rete.

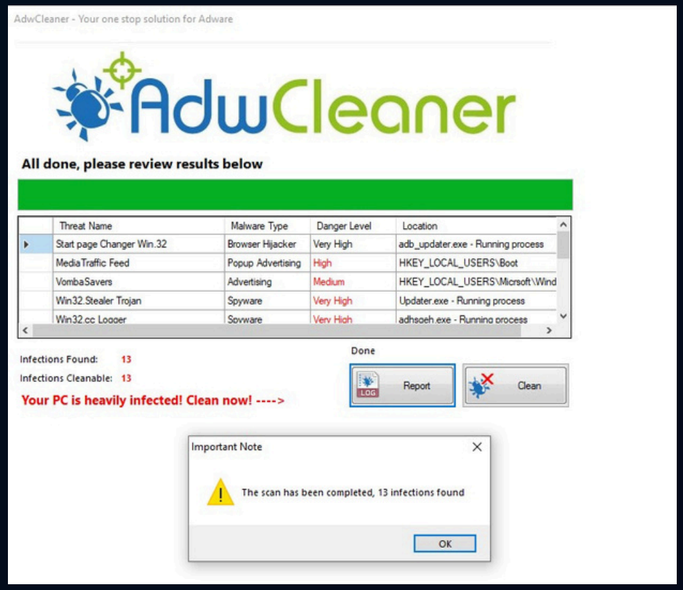


Avviamo anche Regshot, cosi da poter verificare i relativi danni causati da un Malware, avviato dopo aver cliccato “1st shot”



Avviando il Malware scaricato, notiamo che dopo la scansione, ci chiede di pagare il programma, per eliminare i file





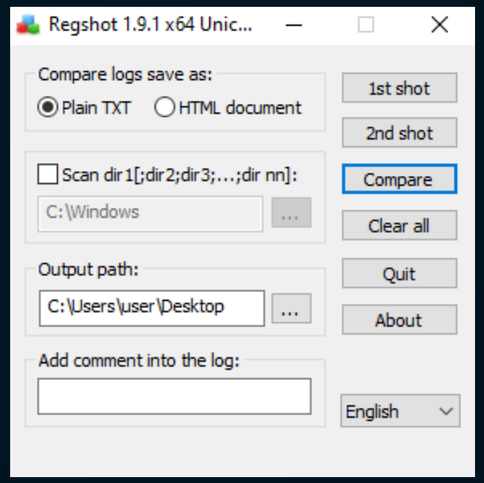
Dopo aver avviato il Malware possiamo notare su Fakenet un incremento del traffico di rete, dopo che il malware ha finito la sua “Scansione”.

```
10/28/24 10:53:39 AM [     HTTPListener80]   Host: ocsp.usertrust.com
10/28/24 10:53:39 AM [     HTTPListener80]
10/28/24 10:53:39 AM [     HTTPListener80]
10/28/24 10:53:39 AM [     HTTPListener80] b'  0Q0O0M0K0I0\t\x06\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14|\xb1fT\x9c\xab\xdbD
\xeeb&\x16\xad\xf4e{\xf7z\xd5\x94\x04\x14\xad\xbd\x98z4\xb4&\xf7\xfa\xc4&T\xef\x03\xbd\xe0$\xcbT\x1a\x02\x10B\x1a\xf2\x9
4\t\x84\x19\x1fR'
10/28/24 10:53:39 AM [     HTTPListener80] b'  K\xc6$&\xa7K'
10/28/24 10:53:39 AM [     HTTPListener80] Storing HTTP POST headers and data to http_20241028_105339.txt.
10/28/24 10:53:39 AM [          Diverter] svchost.exe (1228) requested UDP 192.168.50.168:53
10/28/24 10:53:39 AM [        DNS Server] Received A request for domain 'crl.usertrust.com'.
10/28/24 10:53:39 AM [          Diverter] 6AdwCleaner.exe (5844) requested TCP 192.0.2.123:80
10/28/24 10:53:39 AM [     HTTPListener80]   GET /AddTrustExternalCARoot.crl HTTP/1.1
10/28/24 10:53:39 AM [     HTTPListener80]   Connection: Keep-Alive
10/28/24 10:53:39 AM [     HTTPListener80]   Accept: */*
10/28/24 10:53:39 AM [     HTTPListener80]   User-Agent: Microsoft-CryptoAPI/10.0
10/28/24 10:53:39 AM [     HTTPListener80]   Host: crl.usertrust.com
10/28/24 10:53:39 AM [     HTTPListener80]
10/28/24 10:53:39 AM [     HTTPListener80]
10/28/24 10:53:45 AM [          Diverter] msedge.exe (4692) requested UDP 192.168.50.168:53
10/28/24 10:53:45 AM [        DNS Server] Received A request for domain 'edge.microsoft.com'.
10/28/24 10:53:45 AM [        DNS Server] Received HTTPS request for domain 'edge.microsoft.com'.
10/28/24 10:53:45 AM [          Diverter] msedge.exe (4692) requested TCP 192.0.2.123:443
10/28/24 10:53:57 AM [          Diverter] svchost.exe (1228) requested UDP 192.168.50.168:53
10/28/24 10:53:57 AM [        DNS Server] Received A request for domain 'tlu.dl.delivery.mp.microsoft.com'.
10/28/24 10:53:57 AM [          Diverter] ICMP type 8 code 0 192.168.50.168->192.0.2.123
10/28/24 10:53:57 AM [          Diverter] Modifying ICMP packet (type 8, code 0):
10/28/24 10:53:57 AM [          Diverter]   from: 192.168.50.168->192.0.2.123
10/28/24 10:53:57 AM [          Diverter]   to:   192.168.50.168->192.168.50.168
10/28/24 10:53:57 AM [          Diverter] ICMP type 0 code 0 192.168.50.168->192.168.50.168
```

PantherPwners

HKEY_LOCAL_MACHINE contiene le informazioni relative alla configurazione del Computer

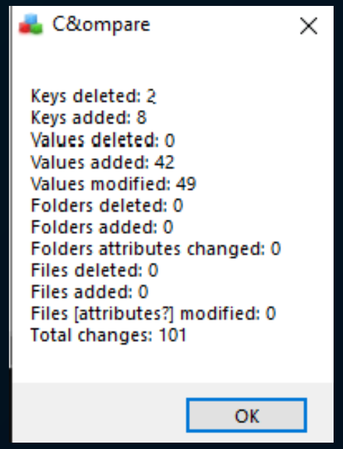
```
---------------------------------
Keys deleted: 2
---------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\367a6d02-dd5a-46cb-b31c-c1208007f9a1
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\367a6d02-dd5a-46cb-b31c-c1208007f9a1

---------------------------------
Keys added: 8
---------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\a324e26c-85c9-4e3d-80bb-aa03513a4a8e
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\a324e26c-85c9-4e3d-80bb-aa03513a4a8e
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Google\Chrome\ThirdParty
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000404A6
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001003E6
HKU\S-1-5-21-604460268-1048137326-3628289992-1001\Software\AdwCleaner
```



Possiamo anche vedere il report sotto forma di testo, per poterlo analizzare meglio.
Notiamo che sono state rimosse delle policy dal nostro PC

Cercando con chat Gpt, ci dice che:
HKLM\SOFTWARE\Microsoft\Tracing...: indica che ci sono vari tentativi di connessione da parte del Malware che tenta di cambiare le configurazioni di Sistema e/o Servizi di Rete

Una volta che il Malware ha terminato la sua esecuzione, clicchiamo su "Compare", per ricevere il report finale



Inoltre notiamo nel report che ci sono vari tentativi di connessione e accesso alle risorse di sistema e alle chiavi di registro, e anche prove di accesso ai Server ed i Domini

```
 _____     _ _____ _____ _____ _____ _____     _ _____ _____
|  ___/\   | |/ / ___| \ | |  ___|_   _|  | \ | |/ ___|
| |__ /  \  | ' /| |_  |  \| | |_    | |  |  \| | |  _
|  __/ /\ \ |  < |  _| | . ` |  _|   | |  | . ` | | |_| |
| | / ___ \| . \| |___| |\  | |___   | |  | |\  | |__| |
|_|/_/   \_\_|\_\_____|_| \_|_____|  |_|  |_| \_|\____|

                    H T T P   L I S T E N E R
</pre></b>

<p>FakeNet-NG is a next generation dynamic network analysis tool for malware
analysts and penetration testers. It is open source and designed for the latest
versions of Windows.</p>

<p>The tool allows you to intercept and redirect all or specific network traffic
while simulating legitimate network services. Using FakeNet-NG, malware analysts
can quickly identify mal
ware's functionality and capture network signatures.
Penetration testers and bug hunters will find FakeNet-NG's configurable
interception engine and modular framework highly useful when testing
application's specific functionality and prototyping PoCs.</p>

<p>FakeNet-NG is based on the excellent Fakenet tool developed
by Andrew Honig and Michael Sikorski.</p>

<h3>Contact</h3>

For bugs, crashes, or other comments please contact <b>The FLARE Team</b> by email
<b>FakeNet@mandiant.com</b>.
</body>
</html>"
HKU\S-1-5-21-604460268-1048137326-3628289992-1001_Classes\Local Settings\MuiCache\86\FE2848FA\@%systemroot%\system32\FirewallControlPanel.d
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\86\FE2848FA\@%SystemRoot%\System32\ngcsvc.dll,-100: "Microsoft Passport"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\86\FE2848FA\@%SystemRoot%\System32\NgcCtnrSvc.dll,-1: "Contenitore Microsoft Passport
```

THANK YOU