

Build Week 3

Esercizio 1

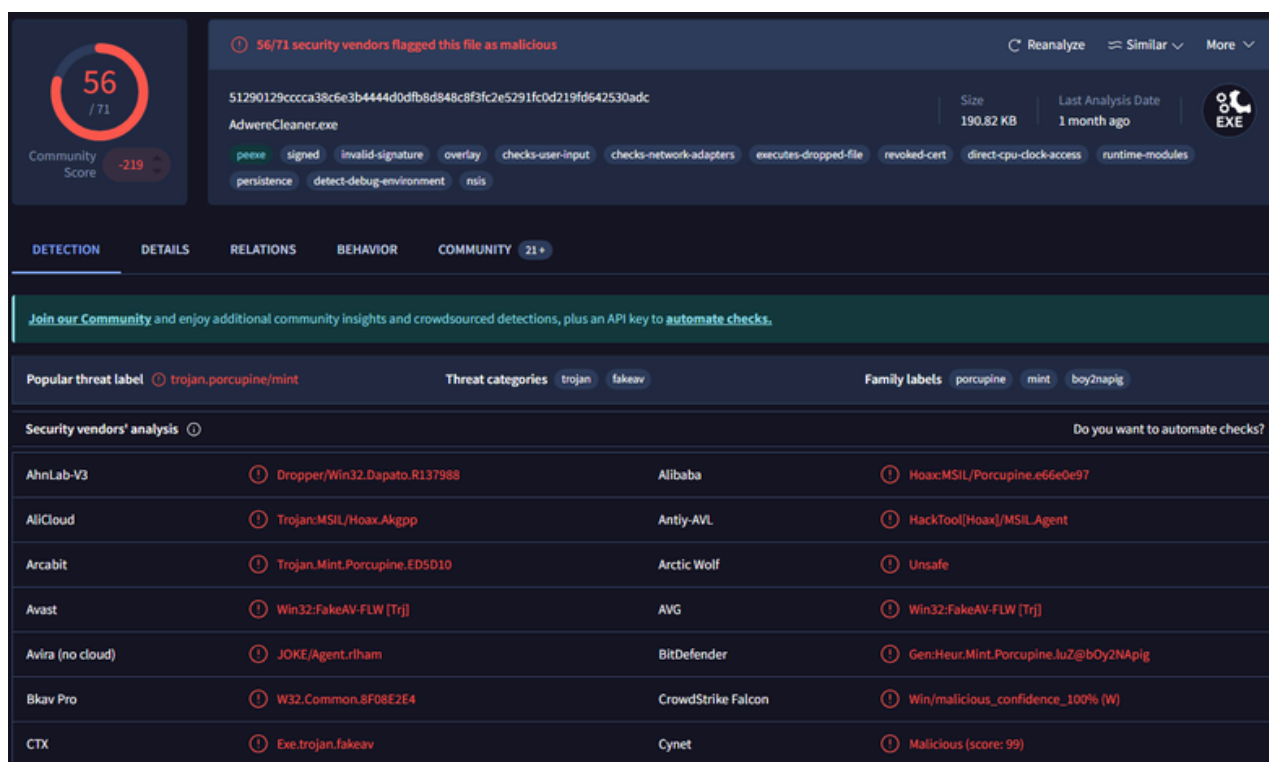


LANDA
TRACKER SPA

Scaricare il MALWARE presente in questo link, effettuare un'analisi completa, pulire le tracce e creare un report:

<https://github.com/Da2dalus/The-MALWARE-Repo/blob/master/rogues/AdwereCleaner.exe>

Innanzitutto inseriamo il file malevolo su **VirusTotal** per ottenere le prime indicazioni sulla tipologia di malware:



The screenshot shows the VirusTotal analysis interface for the file **AdwereCleaner.exe**. The file's SHA-256 hash is `51290129cccca38c6e3b4444d0dfb8d848c8f3c2e5291fc0d219fd642530adc`. The file size is 190.82 KB, and the last analysis was performed 1 month ago. The file is flagged as malicious by 56 out of 71 security vendors, with a community score of -219. The analysis shows several suspicious behaviors, including persistence, detection of debug environments, and execution of dropped files. The file is identified as a trojan, specifically a trojan.porcupine/mint variant. The security vendors' analysis table is as follows:

Security vendor	Detection	Threat category	Family label
AhnLab-V3	ⓘ Dropper/Win32.Dapato.R137988	trojan	ⓘ Hoax:MSIL/Porcupine.e66e0e97
AliCloud	ⓘ Trojan:MSIL/Hoax.Akgpp	trojan	ⓘ HackTool[Hoax]/MSIL.Agent
Arcabit	ⓘ Trojan.Mint.Porcupine.ED5D10	trojan	ⓘ Unsafe
Avast	ⓘ Win32:FakeAV-FLW [Trj]	trojan	ⓘ Win32:FakeAV-FLW [Trj]
Avira (no cloud)	ⓘ JOKE/Agent.rlhnm	trojan	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2NApig
Bkav Pro	ⓘ W32.Common.8F08E2E4	trojan	ⓘ Win/malicious_confidence_100% (W)
CTX	ⓘ Exe.trojan.fakeav	trojan	ⓘ Malicious (score: 99)

Notiamo subito un punteggio elevato, pari a **56/71**.

Notiamo inoltre l'identificazione da parte di diversi antivirus come **Trojan**, questo perchè a conti fatti il malware finge di essere un software lecito, ovvero un antivirus.



Basic properties ⓘ	
MDS	248aadd395ffa7ffb1670392a9398454
SHA-1	c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5
SHA-256	51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
Vhash	01505665d5d05709043z8003d7z47z62z3f03dz
Authentihash	8eb8f3a6371a77e2b5002de83a5955d4d5fb7f2cdb7d8642138bb20d243be578
Imphash	e160ef8e55bb9d162da4e266afd9eef3
Rich PE header hash	ecf81400e80e4d5ebc5ac277c2aacea3
SSDEEP	3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GLD0g+ELqdSxo5XtZjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjnsVI9T/
TLSH	T17B1412524AF05AFFFB4384712AFDE1B9E7B7828C5274A9974B148E323B440D74F8611A
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
TrID	NSIS - Nullsoft Scriptable Install System (92.7%) Win32 Executable MS Visual C++ (generic) (3.4%) Win64 Executable (generic) (1.1%) Win32 Dynamic Link Library (ge...
DetectItEasy	PE32 Installer: Nullsoft Scriptable Install System (3.0a2) [zlib,solid] Compiler: Microsoft Visual C/C++ (12.20.9044) [C] Linker: Microsoft Linker (6.0) Tool: Visual St...
Magika	PEBIN
File size	190.82 KB (195400 bytes)
F-PROT packer	NSIS, appended
Varist packer	NSIS

History ⓘ

Creation Time	2013-12-25 05:01:41 UTC
Signature Date	2015-02-04 20:05:00 UTC
First Seen In The Wild	2022-04-24 06:21:31 UTC
First Submission	2015-02-11 15:48:03 UTC
Last Submission	2025-09-29 11:06:57 UTC
Last Analysis	2025-08-27 10:05:20 UTC

Names ⓘ

AdwereCleaner.exe
 AdwereCleaner (1).exe
 FakeAdwCleaner.exe
 fakeadwcleaner.exe
 Endermanch@FakeAdwCleaner.exe
 7ac27f7b8c68f4c5d547891d991001661a1a6af1-d659d96d15c7a1206f44eb36ed72495563140859
 bf832162-104c-4773-9c5e-9a9aaa876444.exe
 858858dd-26e0-4876-bd5d-4ecb3d200fee.exe
 91440ed8-e5ef-4a38-ada2-6666b60726a4.exe
 AdwereCleaner.zOtfFhsJ.exe.part



ANALISI STATICA

Per l'analisi statica utilizzeremo il software **CFF Explorer** all'interno di una VM con sistema operativo Windows 10 Pro.

Import Directory

Ora ci concentreremo sulla sezione Import Directory per analizzare le librerie utilizzate ed individuare quelle anomale:

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

Notiamo la presenza di librerie lecite come:

- **KERNEL32.dll**
- **USER32.dll**
- **GDI32.dll**

Queste invece le librerie su cui concentrarci data la presenza anomala:

- **SHELL32.dll**: Contiene funzioni per l'interazione con la shell di Windows (es. creazione di collegamenti, gestione della shell di Esplora file). Può essere usata per l'installazione o l'avvio automatico.
- **ADVAPI32.dll**: Contiene funzioni avanzate di sicurezza e accesso al Registro di sistema (Registry). È la libreria che i malware usano per creare chiavi di persistenza, modificare politiche o creare servizi. Questo è un forte segnale di potenziale attività malevola o di persistenza.
- **COMCTL32.dll**: Librerie relative ai controlli comuni di Windows e alla tecnologia OLE/COM. Standard per un'applicazione con GUI.
- **VERSION.dll**: Usata per ottenere informazioni sulla versione del sistema operativo o del file stesso. Non sospetta di per sé.
- **ole32.dll**: Tale presenza indica che il programma utilizza il Component Object Model (COM) e la tecnologia Object Linking and Embedding (OLE) di Windows.



Section Headers

Ci spostiamo poi all'interno di Section Headers che contiene informazioni di mappatura delle sezioni del file e che sarà necessario al loader di Windows per l'avvio:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00005DE2	00001000	00005E00	00000400	00000000	00000000	0000	0000	60000020
.rdata	000012DA	00007000	00001400	00006200	00000000	00000000	0000	0000	40000040
.data	00025498	00009000	00000400	00007600	00000000	00000000	0000	0000	C0000040
.ndata	00008000	0002F000	00000000	00000000	00000000	00000000	0000	0000	C0000080
.rsrc	0000B268	00037000	0000B400	00007A00	00000000	00000000	0000	0000	40000040

- **.text:** Questa è la parte più importante: contiene il codice eseguibile vero e proprio. Sono le istruzioni che la **CPU** esegue. Se voglio modificare il comportamento del programma o analizzare cosa fa, è qui che vado a cercare. È una sezione in sola lettura e marcata come eseguibile.
- **.rdata:** Questa sezione contiene dati di sola lettura, come stringhe costanti, tabelle di importazione/esportazione e informazioni statiche. Non può essere modificata durante l'esecuzione. Qui possiamo trovare riferimenti a funzioni esterne, nomi di librerie o dati che non cambiano. È una sezione marcata come leggibile ma non scrivibile né eseguibile.
- **.data:** Qui ci sono i dati modificabili, come le variabili globali e statiche. Durante l'esecuzione, il programma può leggere e scrivere in questa sezione. Se ci sono contatori, flag, buffer o strutture che cambiano nel tempo, probabilmente sono presenti qui.
- **.ndata:** Questa non è una sezione standard del formato PE. Se la trovo in un file, può indicare una sezione personalizzata creata da un compilatore, da un packer o da un malware. Il contenuto può variare: dati offuscati, configurazioni, codice nascosto o payload. Per capire cosa contiene, è necessario analizzarla manualmente, verificare se è referenziata dal codice e controllare i suoi attributi. Potrebbe essere leggibile, scrivibile o persino eseguibile, a seconda di come è stata definita.
- **.rsrc:** Questa sezione contiene tutte le risorse del programma: icone, immagini, menu, dialoghi, stringhe localizzate. Non è eseguibile, ma è fondamentale per la parte visiva ed interattiva. Se il programma ha una GUI, molto di ciò che è visibile a schermo proviene da qui.



Dopo aver fornito una panoramica generale degli elementi all'interno del malware, volgiamo la nostra attenzione su una libreria specifica:

SHELL32.dll.

Questa libreria, come suggerisce il nome, contiene generalmente funzioni che consentono al programma di interagire con la **Shell** di Windows (Esplora file, desktop, ecc.):

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00008122	00008122	00C3	SHGetSpecialFolderLocation
0000810A	0000810A	00BC	SHGetPathFromIDListA
000080F4	000080F4	0079	SHBrowseForFolderA
000080E2	000080E2	00AC	SHGetFileInfoA
000080D2	000080D2	0107	ShellExecuteA
000080BE	000080BE	009A	SHFileOperationA

Di seguito le funzioni illustrate nel dettaglio:

- **SHGetSpecialFolderLocation:** Permette al programma di trovare percorsi noti e nascosti nel sistema, come AppData, la cartella di avvio (Startup) o la cartella System32. Critica per la scelta del percorso di installazione o del payload.
- **SHGetPathFromIDListA:** Recupera il percorso del file system da un ID (identificatore interno della Shell). Questo permette al programma di risolvere i percorsi speciali trovati con la funzione precedente.
- **SHBrowserForFolderA:** Apre la classica finestra di dialogo "Sfoggia per cartella". Non direttamente malevola, ma indica un'applicazione con GUI che interagisce con l'utente.
- **SHGetFileInfoA:** Ottiene informazioni sui file (icona, tipo, ecc.). Standard per le applicazioni con GUI.
- **ShellExecuteA:** Permette al programma di eseguire un file o un programma come se fosse avviato dall'utente (ad esempio, facendo doppio clic o usando il comando "Esegui"). Spesso usata per lanciare il payload principale o i componenti aggiuntivi.
- **SHFileOperationA:** Funzione ad alto impatto. Usata per eseguire operazioni standard di file system come copiare, spostare, rinominare o eliminare file e cartelle. Cruciale per l'installazione e la rimozione (pulizia) del mal



Ora, tornando sulla sezione Import Directory, ci concentriamo su un'altra libreria particolare:

ADVAPI32.dll.

Dal momento che si tratta di una libreria generalmente usata per creare chiavi di persistenza, modificare politiche o creare servizi potremmo trovarci di fronte alla libreria su cui l'interò malware farà affidamento per raggiungere il suo obiettivo.

Di seguito le funzioni importate dalla libreria:

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000081A2	000081A2	01CB	RegCloseKey
000081D2	000081D2	01EC	RegOpenKeyExA
000081C2	000081C2	01D4	RegDeleteKeyA
000081B0	000081B0	01D8	RegDeleteValueA
0000814C	0000814C	01E1	RegEnumValueA
00008190	00008190	01D1	RegCreateKeyExA
0000817E	0000817E	0204	RegSetValueExA
0000816A	0000816A	01F7	RegQueryValueExA
0000815C	0000815C	01DD	RegEnumKeyA

I nomi delle funzioni in questa tabella indicano chiaramente che il programma non solo legge il Registro, ma è configurato per modificarlo attivamente e pulire le tracce del suo passaggio.

Analizziamo però ogni singola funzione nel dettaglio per avere un'idea chiara di ciò che è in grado di fare la libreria in questo contesto:

- **RegCloseKey**: Funzione di pulizia standard dopo la manipolazione del Registro.
- **RegOpenKeyExA**: Necessaria per accedere e modificare i percorsi noti di persistenza.
- **RegDeleteKeyA**: Può essere usata per pulire le tracce del malware o per rimuovere i dati di altri malware (se è un rogue o un adware cleaner).
- **RegDeleteValueA**: Può essere usata per pulire le tracce lasciate dalla sua installazione o da altri file.
- **RegEnumValueA**: Usata per la mappatura dell'ambiente o per trovare valori specifici.
- **RegCreateKeyExA**: Indicazione primaria di persistenza, utilizzata per impostare nuove voci in Run, servizi, o chiavi di sistema meno note.
- **RegSetValueExA**: La funzione più **critica**. Permette di salvare il percorso dell'eseguibile nella chiave di persistenza, garantendo l'avvio automatico.
- **RegQueryValueExA**: Usata per la configurazione o per verificare l'ambiente prima di agire.
- **RegEnumKeyA**: Usata per la mappatura dell'ambiente o per trovare chiavi specifiche.

In definitiva tramite l'analisi statica possiamo notare come lo scopo principale del malware sia quello di alterare il registro di sistema tramite creazione, modifica e rimozione di chiavi e valori.

La combinazione di **ADVAPI32.dll** e **SHELL32.dll** rivela che:

- Usa *SHGetSpecialFolderLocation* per trovare un luogo sicuro dove nascondersi (ad esempio, %APPDATA%).
- Installazione/Disinstallazione: Usa *SHFileOperationA* per copiare se stesso o un payload, e anche per cancellare tracce o file di software concorrente (come suggerito dai RegDelete... di ADVAPI32.dll).
- Esecuzione: Usa *ShellExecuteA* per lanciare i suoi componenti.
- Persistenza: Usa *RegCreateKeyExA* / *RegSetValueExA* (da ADVAPI32.dll) per assicurarsi di riavviarsi insieme al sistema.



L'analisi statica dei file di questo campione rivela un comportamento progettato per l'installazione nascosta, l'assicurazione di persistenza e la manipolazione aggressiva del sistema operativo.

Il programma è un'**applicazione Windows** con **GUI** (confermato dalle importazioni di USER32.dll e GDI32.dll).

Dal punto di vista dell'installazione e dell'ambiente, l'uso di **SHELL32.dll** e funzioni come **SHGetSpecialFolderLocation** e **SHFileOperationA** permette al malware di localizzare cartelle speciali (es. %APPDATA%) e di copiare, spostare o eliminare file, attività cruciali sia per l'installazione furtiva che per la pulizia di software concorrente.

Il fulcro del malware risiede nella possibilità di interazione con il Registro di sistema, evidente dalle importazioni delle funzioni da **ADVAPI32.dll**.

Le funzioni **RegCreateKeyExA** e **RegSetValueExA** indicano chiaramente il tentativo di stabilire la persistenza scrivendo il percorso del file copiato in chiavi di avvio automatico.

Ancor più significativa è la presenza di **RegDeleteKeyA** e **RegDeleteValueA** che conferma la sua capacità di **cancellare le proprie tracce** o di eliminare le voci di registro di altri programmi.

L'inclusione di **ShellExecuteA** gli permette di lanciare componenti o payload con un'esecuzione simile a quella dell'utente, mentre **ole32.dll** suggerisce la possibilità di interazioni più complesse con gli oggetti di sistema.

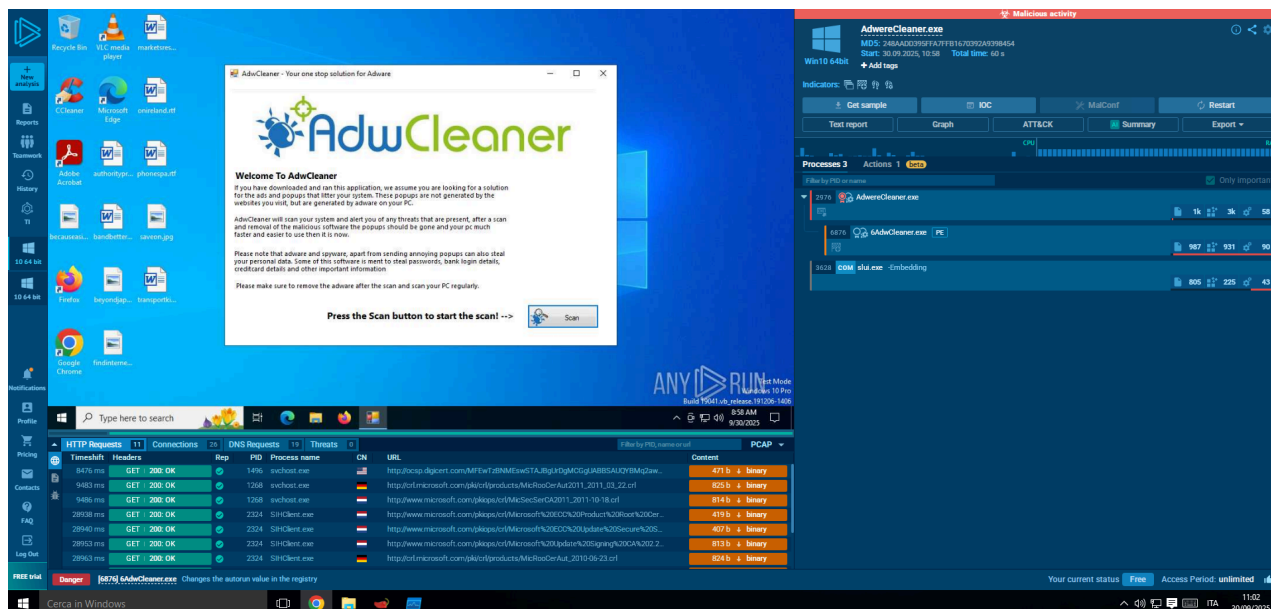


ANALISI DINAMICA

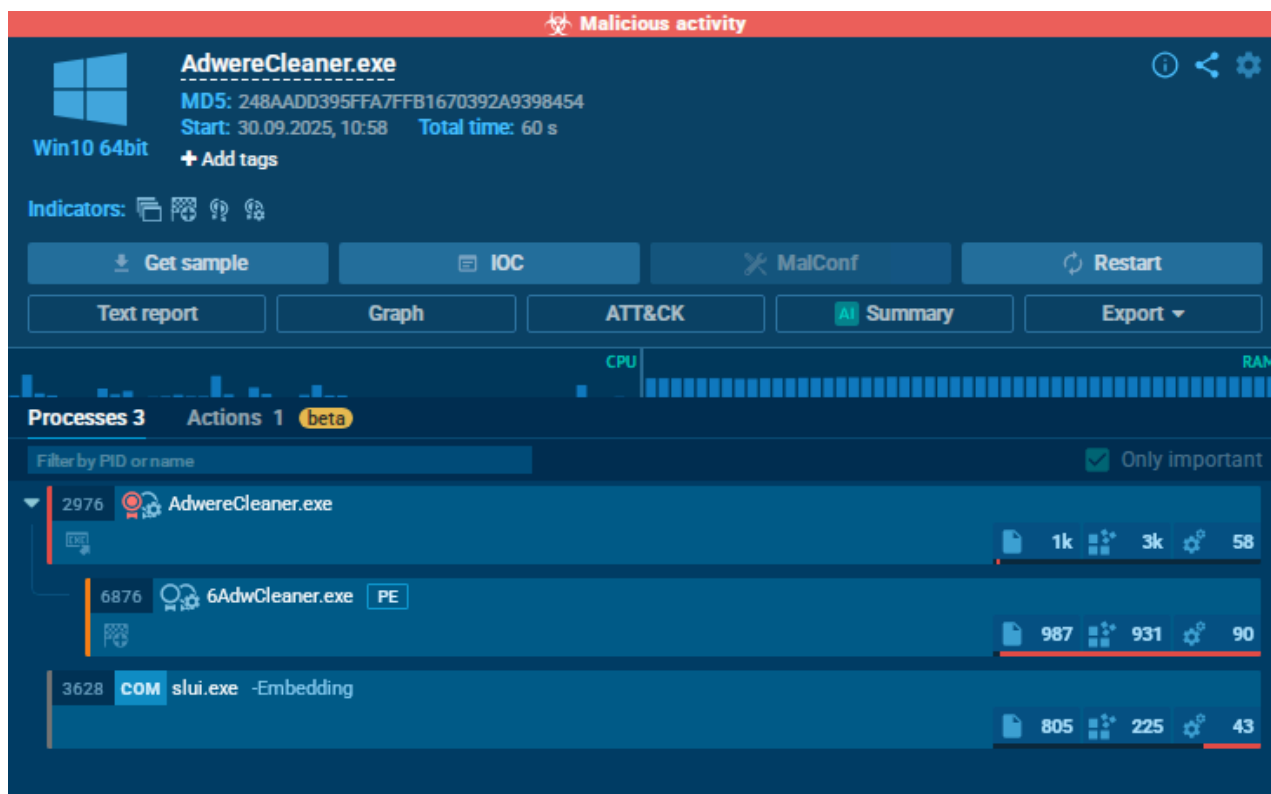
Per l'analisi dinamica ci sposteremo sul famoso tool online **AnyRun**.

Dopo aver effettuato l'accesso con mail aziendale abbiamo la possibilità di caricare il malware Adwrecleaner.exe in modo da poter osservare il comportamento in un ambiente sandbox.

Una volta caricato eseguiamo l'analisi e ci ritroveremo davanti alla seguente schermata:



Possiamo notare da subito la suddivisione di tre processi sul lato destro:



Di conseguenza andremo ad analizzare nel dettaglio ciascuno di essi partendo da **AdwareCleaner.exe**:

[2976] AdwareCleaner.exeC:\Users\admin\AppData\Local\Temp\AdwareCleaner.exe

Threat Verdict

100
OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username:

admin

SID:

S-1-5-21-1693682860-607145093-2874071422-1001

IL:

MEDIUM

Start:

4.94 s

File information

Command line

A1

"C:\Users\admin\AppData\Local\Temp\AdwareCleaner.exe"

Timeline of the process?

0 s4.94 s5.17 s

4.94 s

Danger 1

Executing a file with an untrusted certificate

Warning 4

T1012 Query Registry (2)

Reads the date of Windows installation

Reads security settings of Internet Explorer

T1082 System Information Discovery (1)

Reads the date of Windows installation

T1497.003 Time Based Evasion (1)

Reads the date of Windows installation

Executable content was dropped or overwritten

Other 4

T1614 System Location Discovery (1)

Process checks computer location settings

T1012 Query Registry (2)

Reads the computer name

Checks supported languages

T1082 System Information Discovery (2)

Reads the computer name

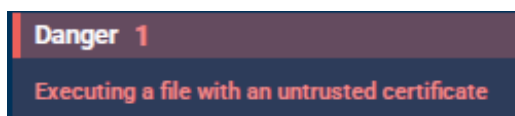
Checks supported languages

Creates files or folders in the user directory

Il processo presenta un punteggio di 100 su 100 per quanto riguarda l'essere malevolo.

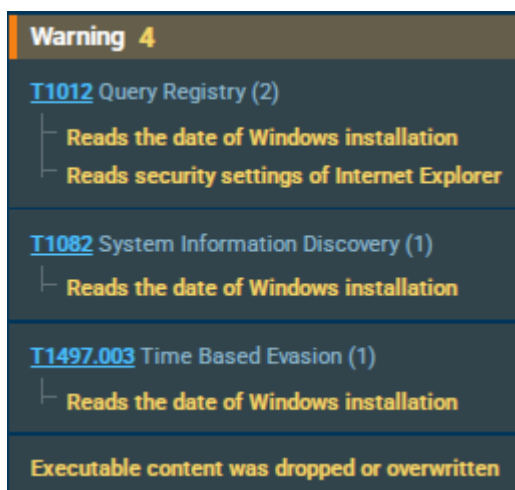
Nella pagina seguente viene analizzato nel dettaglio ogni singolo evento.





Esecuzione di un file con un certificato non attendibile. Questo è un segnale di allarme immediato che indica che il file non proviene da una fonte verificata e potrebbe essere una minaccia mascherata:

C:\Users\admin\AppData\Local\Temp\AdwereCleaner.exe



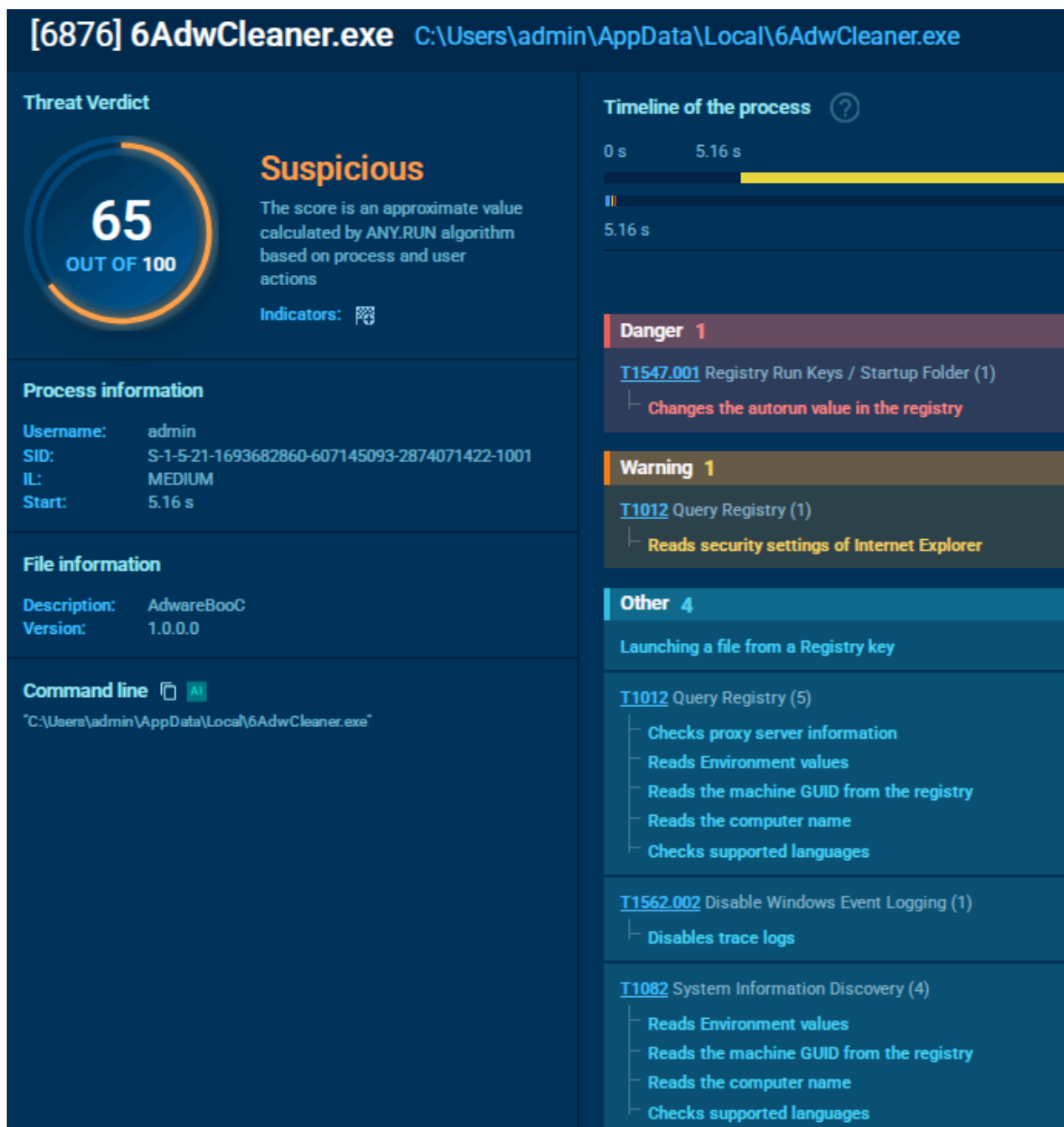
- **T1012 Query Registry:** Legge la data di installazione di Windows e Legge le impostazioni di sicurezza di Internet Explorer. Questa attività è usata per la ricognizione e per capire l'ambiente:
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Security
- **T1082 System Information Discovery:** Legge la data di installazione di Windows. Anche questo è un passo di ricognizione per l'adattamento (Environment Discovery):
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion
- **T1497.003 Time Based Evasion:** Legge la data di installazione di Windows. Questa tecnica può essere usata per l'evasione. Il malware potrebbe usare queste informazioni per capire se è in un ambiente di sandboxing o se è stato installato di recente per un'analisi:
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion
- **Executable content was dropped or overwritten:** Indica che il processo ha scaricato o modificato altro codice eseguibile:
 - C:\Users\admin\AppData\Local\6AdwCleaner.exe



Other 4
T1614 System Location Discovery (1) Process checks computer location settings
T1012 Query Registry (2) Reads the computer name Checks supported languages
T1082 System Information Discovery (2) Reads the computer name Checks supported languages
Creates files or folders in the user directory

- **T1614 System Location Discovery:** Verifica le impostazioni di localizzazione del computer. Usato per capire la posizione geografica del sistema, talvolta per evitare l'esecuzione in determinate regioni:
 - HKEY_CURRENT_USER\Control Panel\International\Geo
- **T1012 Query Registry:** Legge il nome del computer e Verifica le lingue supportate. Riconnessione standard:
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale
- **T1082 System Information Discovery:** Legge il nome del computer e Verifica le lingue supportate. Riconnessione standard:
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale
- **Creates files or folders in the user directory:** Creazione di file o cartelle, in questo caso crea il file **6AdwCleaner.exe**:
 - C:\Users\admin\AppData\Local\6AdwCleaner.exe

Ci spostiamo di conseguenza sul file appena creato, 6AdwCleaner.exe, visibile nella pagina successiva.



Come chiaramente visibile dalla panoramica, il suo comportamento è focalizzato sulla **persistenza**, la **ricognizione** e l'**evasione**.



Danger 1

T1547.001 Registry Run Keys / Startup Folder (1)

└ **Changes the autorun value in the registry**

T1547.001 Registry Run Keys / Startup Folder: Cambia il valore di autorun nel registro. Questo è l'indicatore più pericoloso. Significa che il file si sta rendendo persistente sul sistema, assicurandosi di essere eseguito automaticamente ad ogni riavvio o accesso dell'utente:

- **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- **Value:** "C:\Users\admin\AppData\Local\6AdwCleaner.exe" -auto

Warning 1

T1012 Query Registry (1)

└ **Reads security settings of Internet Explorer**

T1012 Query Registry: Legge le impostazioni di sicurezza di Internet Explorer.

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security



Other 4
Launching a file from a Registry key
T1012 Query Registry (5) <ul style="list-style-type: none"> Checks proxy server information Reads Environment values Reads the machine GUID from the registry Reads the computer name Checks supported languages
T1562.002 Disable Windows Event Logging (1) <ul style="list-style-type: none"> Disables trace logs
T1082 System Information Discovery (4) <ul style="list-style-type: none"> Reads Environment values Reads the machine GUID from the registry Reads the computer name Checks supported languages

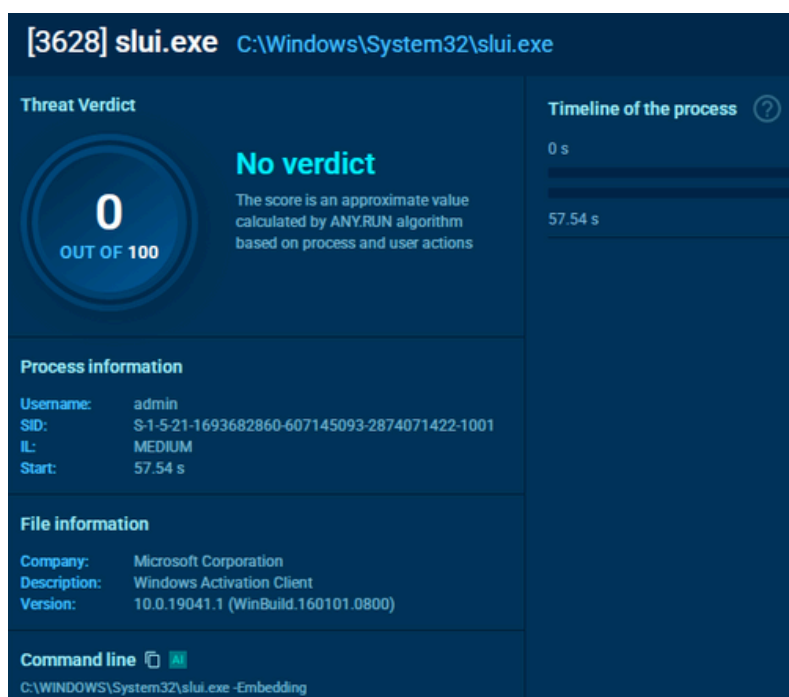
- **Launching a file from a Registry key:** Indica l'uso del registro anche per l'avvio, in linea con l'indicatore di persistenza:
 - **Key:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
 - **Value:** `"C:\Users\admin\AppData\Local\6AdwCleaner.exe" -auto`
- **T1012 Query Registry:** Ricognizione estesa del registro.
 - Verifica le informazioni del server proxy:
 - `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`
 - Legge i valori d'ambiente:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`
 - Legge il GUID della macchina dal registro:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography`
 - Legge il nome del computer:
 - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Active ComputerName`
 - Verifica le lingue supportate:
 - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale`
- **T1562.002 Disable Windows Event Logging:** Disabilita le tracce di log. Questo è un chiaro tentativo di evasione della difesa e di offuscamento delle tracce, rendendo più difficile l'analisi forense e il rilevamento:
 - **Key:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32`
 - **Value:** `0`



- **T1082 System Information Discovery:** Ricognizione estesa del sistema.
 - **Legge i valori d'ambiente:**
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`
 - **Legge il GUID della macchina dal registro:**
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography`
 - **Legge il nome del computer:**
 - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Active ComputerName`
 - **Verifica le lingue supportate:**
 - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale`

Il risultato dell'analisi totale mostra come si tratti con ogni probabilità di uno spyware.

Accenno finale, per dovere di cronaca, al processo slui.exe che però non rileva nulla di anomalo:



Ora non resta che analizzare il report generale di AnyRun per verificare la presenza di connessioni di rete stabilite dal malware per tentare di capire dove vengono inviati i dati ottenuti. I PID sono i seguenti:

- `AdwereCleaner.exe` (2976)
- `6AdwCleaner.exe` (6876)

Le schermate sono presenti nella pagina seguente.



Network activity

☒ Add for printing

HTTP(S) requests

11

TCP/UDP connections

26

DNS requests

19

Threats

0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1496	svchost.exe	GET	200	172.66.2.5:80	http://ocsp.digicert.com/MFEwTzBNMESwSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPIGxvDi7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
1268	svchost.exe	GET	200	23.216.77.28:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted
1268	svchost.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	23.216.77.28:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.1.crl	unknown	—	—	whitelisted
2324	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.1.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	—	—	—	whitelisted
5944	MoUsCoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
2112	RUXIMICS.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
1496	svchost.exe	20.190.160.131:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1496	svchost.exe	172.66.2.5:80	ocsp.digicert.com	—	US	whitelisted
1268	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	23.216.77.28:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
1268	svchost.exe	95.101.149.131:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
5944	MoUsCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
2336	svchost.exe	172.211.123.249:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
5944	MoUsCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
2324	SIHClient.exe	135.232.92.137:443	slscr.update.microsoft.com	LUCENT-CIO	US	whitelisted
2324	SIHClient.exe	95.101.149.131:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
2324	SIHClient.exe	23.216.77.28:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
2324	SIHClient.exe	20.242.39.171:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4544	slui.exe	20.83.72.98:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

Previous 1 Next

60



Domain	IP	Reputation
settings-win.data.microsoft.com	4.231.128.59 51.104.136.2 40.127.240.158	whitelisted
google.com	142.250.185.78	whitelisted
www.vikingwebscanner.com	—	malicious
login.live.com	20.190.160.131 40.126.32.74 20.190.160.64 20.190.160.66 40.126.32.136 40.126.32.138 20.190.160.130 40.126.32.72	whitelisted
ocsp.digicert.com	172.66.2.5 162.159.142.9	whitelisted
crl.microsoft.com	23.216.77.28 23.216.77.6	whitelisted
www.microsoft.com	95.101.149.131	whitelisted
client.wns.windows.com	172.211.123.249	whitelisted
slscr.update.microsoft.com	135.232.92.137	whitelisted
fe3cr.delivery.mp.microsoft.com	20.242.39.171	whitelisted
self.events.data.microsoft.com	20.50.73.11	whitelisted
activation-v2.sls.microsoft.com	20.83.72.98	whitelisted

I **PDI 2976** e **6876** non sono presenti in alcuna comunicazione di rete, eppure l'unico segnale anomalo è presente nella categoria di richieste DNS in cui viene citato vikingwebscanner.com.

Brevi ricerche hanno confermato che si tratta di un pop-up ad, risultato di un PC infetto:

If you are seeing random pop-up ads from **vikingwebscanner.com** within Internet Explorer, Firefox or Google Chrome, then your computer is infected with an adware or a potentially unwanted program.

Il motivo per cui la richiesta DNS non è andata potrebbe fare riferimento ad una tecnica di evasione.

Dal momento che effettua una lettura estesa dell'ambiente è assai probabile che il codice abbia rilevato l'ambiente di sandboxing di AnyRun ed abbia intenzionalmente annullato la connessione per evitare l'analisi completa, lasciando comunque una traccia nel report.

CONCLUSIONI

Il software analizzato, mascherato da **AdwereCleaner.exe**, opera come un Malware Multi-Fase classificabile come **Spyware**.

Si tratta di un malware progettato per l'installazione furtiva, l'ottenimento della persistenza e la ricognizione estesa del sistema.

Nella prima fase fa una rapida valutazione dell'ambiente e rilascia un payload secondario (**6AdwCleaner.exe**) che è il vero malware.

Questo payload si concentra immediatamente sulla Persistenza (**T1547.001**), modificando le chiavi di autorun del registro per assicurare l'esecuzione ad ogni avvio.

Parallelamente esegue una ricognizione (**T1082, T1012**) invasiva raccogliendo dati sensibili sull'ambiente (GUID della macchina, impostazioni di rete, configurazione locale).

Il malware manifesta tecniche di evasione della difesa (**T1562.002**) tentando di disabilitare i log di sistema e includendo indicatori di evasione basata sul tempo. Infine, ha tentato di stabilire un contatto con un server tramite un dominio malevolo (**vikingwebscanner.com**), sebbene la connessione vera e propria sia stata probabilmente interrotta per evasione nell'ambiente di sandboxing di **AnyRun**. L'obiettivo complessivo è l'accesso remoto e l'esfiltrazione dei dati raccolti.

