

# Relazione Tecnica Finale: Progetto Cyber Security & Ethical Hacking

**Team:** Secure Sentinels

**Modulo:** Cybersecurity & Ethical Hacking (Epicode)

**Data:** 23 Febbraio 2026

## 1. Gestione dell'Analisi Statica e Triage Iniziale

Il laboratorio è iniziato con l'obiettivo di decostruire il malware **6AdwCleaner.exe**, un binario che tenta di mimetizzarsi come un noto strumento di rimozione adware. Utilizzando **pestudio** e **Detect It Easy (DiE)**, abbiamo subito isolato i primi indizi critici: il file è un eseguibile **.NET** (v4.0.30319).

La prima anomalia riscontrata riguarda il **typosquatting** e il mascheramento dei metadati: sebbene il file si presenti esternamente come un tool legittimo, i campi interni rivelano il nome originale del progetto, **AdwareBooC.exe**, e un percorso di debug che punta alla cartella di sviluppo dell'autore (**C:\Users\PresFox\...**).

property	value
file > sha256	4F0033E811FE2497B38F0D45DF958B29D01933EBE7D331079EEFC8E38FBFAA61
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00
file > first 32 bytes (text)	MZ.....@.....
file > info	size: 172648 bytes, entropy: 7.624
file > type	executable, 32-bit, GUI
file > version	1.0.0
file > description	AdwareBooC
entry-point > first 32 bytes (hex)	FF 25 00 20 40 00
entry-point > location	0x000299FE
file > signature	Microsoft Linker 11.0

stamps	
stamp > compiler	Wed Feb 04 20:00:00 2015 (UTC)
stamp > debug	Wed Feb 04 20:00:00 2015 (UTC)
stamp > resource	n/a
stamp > import	n/a
stamp > export	n/a

names	
file > name	c:\users\flarevm\desktop\malware\rogues\adwcleaner\6adwcleaner.exe
debug > file	c:\Users\PresFox\Documents\Visual Studio 2013\Projects\AdwareBooC\Adw
export	n/a
version > original-file-name	AdwareBooC.exe
manifest	MyApplication.app
.NET > module > name	AdwareBooC.exe
certificate > program-name	n/a

*Assessment iniziale in pestudio: identificazione del compilatore e discrepanza dei metadati interni.*

Approfondendo l'analisi della struttura, abbiamo calcolato un'entropia di **7.624**, un valore estremamente elevato che suggerisce l'uso di un **packer** o di tecniche di offuscamento del codice. Esaminando le stringhe estratte, è possibile notare numerosi frammenti di codice ASCII privi di senso compiuto, tipici di un payload cifrato che attende di essere decriptato in memoria.

c:\users\flarevm\Desktop\malware\rogues\adwre cleaner.exe (read-only)					
	encoding (2)	size (bytes)	offset	flag (46)	value (5734)
ascii	3	0x000016989	-	4cv	
ascii	5	0x000025B32	-	4e\$)	
ascii	55	0x0002F541	-	4http://crf3.digicert.com/DigiCertAssuredIDRootCA.crl0:	
ascii	54	0x0002F57D	-	4http://crf4.digicert.com/DigiCertAssuredIDRootCA.crl0	
ascii	3	0x000025090	-	4i-	
ascii	3	0x000000CE5	-	4j1	
ascii	4	0x00002D84F	-	4kel	
ascii	5	0x0000A0CBB	-	4IU3l	
ascii	5	0x0002A348	-	4p)Mg	
ascii	3	0x000025077	-	4p@	
ascii	3	0x0000019C1	-	4q@	
ascii	3	0x000019F1	-	4q@	
ascii	3	0x00002244	-	4q@	
ascii	3	0x000024A9	-	4q@	
ascii	3	0x00004E1D	-	4q@	
ascii	3	0x000219B6	-	4qf	
ascii	3	0x0001CE01	-	4r5	
ascii	3	0x000010A7	-	4r@	
ascii	3	0x000010D2	-	4r@	
ascii	3	0x00002E5A	-	4r@	
ascii	3	0x0000303E	-	4r@	
ascii	3	0x000031B1	-	4r@	
ascii	3	0x0000346B	-	4r@	
ascii	3	0x000034F5	-	4r@	
ascii	3	0x00003710	-	4r@	
ascii	3	0x000041D6	-	4r@	
ascii	3	0x00004580	-	4r@	
...:::	3	~.~~~~~1111A	-	Arc	

*Analisi delle stringhe offuscate presenti nel binario.*

Un elemento fondamentale per comprendere le capacità del malware è l'esame della **Import Address Table (IAT)**. Abbiamo rilevato l'importazione di librerie come **ADVAPI32.dll** e **VERSION.dll**, che indicano chiaramente l'intento del software di manipolare il registro di sistema e di effettuare un fingerprinting della versione del sistema operativo ospite.

c:\users\flarevm\Desktop\malware\rogues\adwre cleaner.exe (read-only)					
	library (8)	flag (0)	type	imports (158)	description
	KERNEL32.dll	-	Implicit	61	Windows NT BASE API Client
	USER32.dll	-	Implicit	63	Multi-User Windows USER API Client Library
	GDI32.dll	-	Implicit	8	GDI Client Library
	SHELL32.dll	-	Implicit	6	Windows Shell Library
	ADVAPI32.dll	-	Implicit	9	Advanced Windows 32 Base API
	COMCT132.dll	-	Implicit	4	Common Controls Library
	OLE32.dll	-	Implicit	4	Microsoft OLE for Windows
	VERSION.dll	-	Implicit	2	Version Checking and File Installation Library

*Elenco delle librerie importate per l'interazione con le API di sistema.*

## 2. Ingegneria Sociale e Struttura della GUI

Analizzando le stringhe relative all'interfaccia grafica, il team **securesentinels** ha identificato la vera natura della minaccia: un **Rogue Software**. Sono stati isolati riferimenti a componenti UI come **ProgressBar**, **infections**, e testi allarmistici progettati per indurre paura nell'utente.

ascii	236	0x00003C7E	-	If you have downloaded and ran this application, we assume you are looking for a solution ...
ascii	215	0x00003D6D	-	AdwCleaner will scan your system and alert you of any threats that are present, after a scan...
ascii	228	0x00003E47	-	Please note that adware and spyware, apart from sending annoying popups can also steal y...
ascii	82	0x00003F41	-	QSystem.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
ascii	21	0x00003F99	-	System.Drawing.Bitmap
ascii	4	0x00003FB3	-	Data
ascii	4	0x00003FD2	-	JFIF
ascii	5	0x00003FE4	-	Adobe
ascii	4	0x00003FF4	-	Exif
ascii	5	0x0000400C	-	Ducky
ascii	29	0x0000401E	-	<http://ns.adobe.com/xap/1.0/
ascii	17	0x0000403C	-	<?xpacket begin="
ascii	150	0x00004050	-	" id="W5M0MpCeihHzreSzNTczkc9d"?>\n<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xm...
ascii	69	0x000040E3	-	<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">\n<rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM...
ascii	350	0x00004128	-	<xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A17E05C78F9911E48FD0912E94936E89" s...
ascii	144	0x00004287	-	</rdf:Description>\n</rdf:Description>\n</rdf:RDF>\n<x:xmpmeta>\n<?xpacket end='w'?>
ascii	22	0x00004317	-	1AQ
ascii	49	0x0000432C	-	Raq
ascii	3	0x00004435	-	t67
ascii	3	0x00004439	-	S\$T
ascii	5	0x000044A6	-	3AQq2
ascii	4	0x000044B3	-	BRr4
ascii	6	0x000044DA	-	op@8Qx
ascii	6	0x000044F3	-	op@8Qx
ascii	6	0x0000450C	-	op@8Qx
ascii	6	0x00004539	-	op@8Qx
ascii	6	0x00004552	-	op@8Qx
ascii	6	0x0000456B	-	op@8Qx

*Evidenze dell'interfaccia utente: messaggi di scareware e controlli grafici simulati.*

L'esame forense delle risorse tramite **CFF Explorer** ha mostrato metadati Adobe e Ducky legati a risorse bitmap. Questo dimostra che il malware utilizza icone e grafiche rubate da software professionali per simulare un ambiente di scansione antivirus fake, volto a estorcere dati o denaro alla vittima.

ascii	145	0x0000C8B0	-	ISystem.Resources.ResourceReader, mscorelib, Version=4.0.0.0, Culture=neutral, PublicKeyT...
ascii	111	0x0000C94D	-	hSystem.Drawing.Bitmap, System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyTok...
ascii	82	0x0000C9FE	-	QSystem.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
ascii	21	0x0000CA56	-	System.Drawing.Bitmap
ascii	4	0x0000CA70	-	Data
ascii	4	0x0000CA8F	-	JFIF
ascii	5	0x0000CAA1	-	Adobe
ascii	4	0x0000CAB1	-	Exif
ascii	5	0x0000CAC9	-	Ducky
ascii	29	0x0000CADB	-	<http://ns.adobe.com/xap/1.0/
ascii	17	0x0000CAF9	-	<?xpacket begin="
ascii	150	0x0000CB0D	-	" id="W5M0MpCeihHzreSzNTczkc9d"?>\n<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xm...
ascii	69	0x0000CBA0	-	<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">\n<rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM...
ascii	350	0x0000CBF5	-	<xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A81B867F8FB211E4B89DDF8909EB666D"...
ascii	144	0x0000CD44	-	</rdf:Description>\n</rdf:RDF>\n<x:xmpmeta>\n<?xpacket end='w'?>
ascii	22	0x0000CDD4	-	
ascii	49	0x0000CDE9	-	

*Didascalia: Estrazione dei metadati dalle risorse grafiche per validare l'uso di loghi contraffatti.*

### 3. Strategie di Evasione e Analisi Dinamica (ProcMon)

Un punto critico emerso è la scoperta dello script `[NSIS].nsi` nella directory di lavoro. La direttiva `SilentInstall silent` istruisce l'installer a operare senza alcun feedback visivo, permettendo al malware di stabilirsi nel sistema in modo furtivo prima di mostrare la propria GUI.

encoding (1)	size (bytes)	offset	flag (0)	value (12)
ascii	20	0x00000000	-	; NSIS script NSIS-3
ascii	9	0x00000016	-	; Install
ascii	13	0x00000023	-	Unicode false
ascii	18	0x00000032	-	SetCompressor zlib
ascii	22	0x00000048	-	; -----
ascii	19	0x00000050	-	; HEADER SIZE: 2193
ascii	24	0x00000075	-	; START HEADER SIZE: 300
ascii	25	0x0000008F	-	; MAX STRING LENGTH: 1024
ascii	19	0x000000AA	-	; STRING CHARS: 515
ascii	18	0x000000C1	-	OutFile [NSIS].exe
ascii	24	0x000000D5	-	linclude WinMessages.nsh
ascii	1610	0x000000F1	-	SilentInstall silent\v\n\v\n\v\n\v-----\v\n; LANG TABLES: 1\v\n; LANG STRINGS...

Configurazione NSIS per l'installazione silenziosa e non interattiva.

Durante l'esecuzione controllata in FlareVM, abbiamo utilizzato **Process Monitor (ProcMon)** per osservare il comportamento a runtime, focalizzandoci sulle interazioni con il cuore del sistema operativo.

#### 3.1 Investigazione sulle Registry Keys (RegKey)

Il malware effettua una massiccia attività di ricognizione interrogando il registro di sistema (T1012). Attraverso i filtri di ProcMon, abbiamo isolato migliaia di eventi di `RegQueryValue` e `RegOpenKey`:

- **Enumerazione Policy:** Il processo analizza le chiavi sotto `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies` per verificare la presenza di restrizioni di sistema o software di protezione attivi.
- **Fingerprinting dell'Utente:** Sono state intercettate letture costanti alla chiave `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`, probabilmente per determinare le impostazioni di visualizzazione dell'utente e nascondere meglio i propri file temporanei.
- **Persistenza:** L'analisi suggerisce che il malware cerchi i path di "Run" o "RunOnce" per garantirsi l'esecuzione automatica a ogni riavvio del sistema.

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Policies\Microsoft\... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\WOW6432Node\Polic... REPARSE	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Policies\Microsoft\... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegQueryKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		Query: HandleTag...
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Window... NAME NOT FOUND Desired Access: Q...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\WOW6432Node\Polic... REPARSE	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Policies\Microsoft\... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Window... REPARSE	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\WOW6432Node\Micr... REPARSE	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegSetInfoKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		KeySetInformation...
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSOFTWARE\Microsoft\Window... NAME NOT FOUND Length: 20		
6:19:3...	AdwereCleaner...	1860	RegCloseKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\WOW6432Node\Micr... REPARSE	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegSetInfoKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		KeySetInformation...
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSOFTWARE\Microsoft\Window... NAME NOT FOUND Length: 20		
6:19:3...	AdwereCleaner...	1860	RegCloseKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Windows N... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Policies\Microsoft\Win... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKCU\Software\Policies\Microsoft\Win... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKCU\Control Panel\Desktop\... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKCU\Control Panel\Desktop\EnableP... NAME NOT FOUND Length: 20		
6:19:3...	AdwereCleaner...	1860	RegCloseKey	HKCU\Control Panel\Desktop\... SUCCESS		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Wow6432Node\Micro... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSOFTWARE\WOW6432Node\... NAME NOT FOUND Length: 172		
6:19:3...	AdwereCleaner...	1860	RegCloseKey	HKLMSOFTWARE\WOW6432Node\... SUCCESS		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Wow6432Node\Micro... NAME NOT FOUND Desired Access: R...		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLM\... SUCCESS		Desired Access: M...
6:19:3...	AdwereCleaner...	1860	RegQueryKey	HKLM\... SUCCESS		Query: HandleTag...
6:19:3...	AdwereCleaner...	1860	RegQueryKey	HKLM\... SUCCESS		Query: Name
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\WOW6432Node\Micro... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegSetInfoKey	HKLMSOFTWARE\WOW6432Node\... SUCCESS		KeySetInformation...
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSOFTWARE\WOW6432Node\... SUCCESS		Type: REG_DWO...
6:19:3...	AdwereCleaner...	1860	RegCloseKey	HKLMSOFTWARE\WOW6432Node\... SUCCESS		
6:19:3...	AdwereCleaner...	1860	RegQueryKey	HKLMSOFTWARE\Microsoft\Window... SUCCESS		Query: HandleTag...
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Window... NAME NOT FOUND Desired Access: Q...		
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr... NAME NOT FOUND Length: 528		
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr... NAME NOT FOUND Length: 528		
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr... NAME NOT FOUND Length: 528		
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr... NAME NOT FOUND Length: 528		
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr... NAME NOT FOUND Length: 528		
6:19:3...	AdwereCleaner...	1860	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr... NAME NOT FOUND Length: 528		
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKCU\... SUCCESS		Desired Access: R...
6:19:3...	AdwereCleaner...	1860	RegCloseKey	HKCU\... SUCCESS		
6:19:3...	AdwereCleaner...	1860	RegQueryKey	HKLM\... SUCCESS		Query: HandleTag...
6:19:3...	AdwereCleaner...	1860	RegQueryKey	HKLM\... SUCCESS		Query: Name
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\WOW6432Node\... REPARSE	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegOpenKey	HKLMSOFTWARE\Microsoft\Ole... SUCCESS	Desired Access: R...	
6:19:3...	AdwereCleaner...	1860	RegSetInfoKey	HKLMSOFTWARE\Microsoft\Ole... SUCCESS		KeySetInformation...

Showing 10,616 of 419,253 events (2.5%) Backed by virtual memory

*Monitoraggio delle attività di sistema: dettaglio dell'enumerazione delle RegKey per la ricognizione delle policy e dell'ambiente utente.*

### 3.2 Analisi delle API e Buffer Overflow

Un dettaglio tecnico interessante è la comparsa di risultati **BUFFER OVERFLOW** durante l'accesso a certe DLL di sistema come **imm32.dll**. Abbiamo determinato che si tratta di una normale negoziazione della memoria delle Windows API: il sistema segnala che il buffer fornito dal malware è troppo piccolo per i dati richiesti, costringendo il software a riallocare memoria. Non si tratta, quindi, di un tentativo di exploit, ma di un comportamento strutturale del binario .NET.

Time ...	Process Name	PID	Operation	Path	Result	Detail
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\Prefetch\ADWERECLEA...	NAME NOT FOUND	Desired Access: G...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Desired Access: E...
:19:3...	AdwereCleaner....	1860	QueryNameInfo...	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows\...
:19:3...	AdwereCleaner....	1860	QueryNameInfo...	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows\...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	QueryBasicInfor...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Creation Time: 12/3...
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WI...	SyncType: SyncTy...
:19:3...	AdwereCleaner....	1860	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTy...
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
:19:3...	AdwereCleaner....	1860	QueryNameInfo...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Name: \Windows\...
:19:3...	AdwereCleaner....	1860	QueryNameInfo...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Name: \Windows\...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Users\FlareVm\AppData\Local\Tem...	BUFFER OVERFL...	Information: Owner
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Information: Owner
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\SysWOW64\vtdll.dll	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\vtdll.dll	BUFFER OVERFL...	Information: Owner
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\vtdll.dll	SUCCESS	Information: Owner
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\SysWOW64\vtdll.dll	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFL...	Information: Owner
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Information: Owner
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	Desired Access: R...
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\kernelBase.dll	BUFFER OVERFL...	Information: Owner
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	Information: Owner
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G...
:19:3...	AdwereCleaner....	1860	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,0...
:19:3...	AdwereCleaner....	1860	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,0...
:19:3...	AdwereCleaner....	1860	CreateFileMapp...	C:\Windows\apppatch\sysmain.sdb	FILE LOCKED WI...	SyncType: SyncTy...
:19:3...	AdwereCleaner....	1860	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,0...
:19:3...	AdwereCleaner....	1860	CreateFileMapp...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Desired Access: G...
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Information: Owner...
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G...
:19:3...	AdwereCleaner....	1860	QueryBasicInfor...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	CreationTime: 12/3...
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
:19:3...	AdwereCleaner....	1860	QueryBasicInfor...	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	CreationTime: 2/23...
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	
:19:3...	AdwereCleaner....	1860	CreateFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Desired Access: G...
:19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	Information: Owner...
:19:3...	AdwereCleaner....	1860	QueryBasicInfor...	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	CreationTime: 2/23...
:19:3...	AdwereCleaner....	1860	CloseFile	C:\Users\FlareVm\AppData\Local\Tem...	SUCCESS	
:19:3...	AdwereCleaner	1860	CloseFile	C:\Windows\svnpatch\svsmain.srh	SUCCESS	

### Negoziazione delle Windows API: dettaglio del risultato Buffer Overflow a runtime.

Al termine della fase di installazione silenziosa e della ricognizione delle RegKey, il malware avvia finalmente la sua GUI: un finto software di pulizia che allerta l'utente su pericoli inesistenti per indurlo a pagare per una "soluzione" fittizia.



*Interfaccia grafica del FakeAV attivata al termine della fase stealth.*

## 4. Network Intelligence e Conclusioni

L'ultima fase ha analizzato le minacce di rete tramite **FakeNet-NG (Diverter)**. Il binario tenta di contattare domini come [ocsp.comodoca.com](http://ocsp.comodoca.com) per validare i propri certificati scaduti, utilizzando un User-Agent di sistema ([Microsoft-CryptoAPI/10.0](#)) per mimetizzarsi nel traffico legittimo di Windows.

```

02/23/26 06:42:11 AM [ HTTPListener80] Host: ocsp.comodoca.com
02/23/26 06:42:11 AM [ HTTPListener80]
02/23/26 06:42:11 AM [ HTTPListener80]
02/23/26 06:42:11 AM [ Diverter] 6AdwCleaner.exe (5184) requested UDP 192.168.56.102:53
02/23/26 06:42:11 AM [ DNS Server] Received A request for domain 'ocsp.comodoca.com' from 6AdwCleaner.exe (5184)
02/23/26 06:42:11 AM [ Diverter] 6AdwCleaner.exe (5184) requested TCP 192.0.2.123:80
02/23/26 06:42:11 AM [ HTTPListener80] POST / HTTP/1.1
02/23/26 06:42:11 AM [ HTTPListener80] Cache-Control: no-cache
02/23/26 06:42:11 AM [ HTTPListener80] Connection: Keep-Alive
02/23/26 06:42:11 AM [ HTTPListener80] Pragma: no-cache
02/23/26 06:42:11 AM [ HTTPListener80] Content-Type: application/ocsp-request
02/23/26 06:42:11 AM [ HTTPListener80] Accept: */
02/23/26 06:42:11 AM [ HTTPListener80] User-Agent: Microsoft-CryptoAPI/10.0
02/23/26 06:42:11 AM [ HTTPListener80] Content-Length: 83
02/23/26 06:42:11 AM [ HTTPListener80] Host: ocsp.comodoca.com
02/23/26 06:42:11 AM [ HTTPListener80]
02/23/26 06:42:11 AM [ HTTPListener80]
02/23/26 06:42:11 AM [ HTTPListener80] b' 0Q000M0K0I0\t\x06\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14\x8e%\xa16\x1f\x88Ga\x0c\x
02/23/26 06:42:11 AM [ HTTPListener80] x10\x04\x14\x1e\xc5\xb1,\x87\xda\x02h%\xcb\x0c\x07\x84?\xb6\xcf\xde\xf1\x02\x100\x82\xe5\xb2J\xce&\x89'\xc5K6\xe7\x1d\x02'
02/23/26 06:42:11 AM [ HTTPListener80] Storing HTTP POST headers and data to http_20260223_064211.txt.
02/23/26 06:42:11 AM [ Diverter] 6AdwCleaner.exe (5184) requested UDP 192.168.56.102:53
02/23/26 06:42:11 AM [ DNS Server] Received A request for domain 'crl.comodoca.com' from 6AdwCleaner.exe (5184)
02/23/26 06:42:11 AM [ Diverter] 6AdwCleaner.exe (5184) requested TCP 192.0.2.123:80
02/23/26 06:42:11 AM [ HTTPListener80] GET /COMODOCodeSigningCA2.crl HTTP/1.1
02/23/26 06:42:11 AM [ HTTPListener80] Connection: Keep-Alive
02/23/26 06:42:11 AM [ HTTPListener80] Accept: */
02/23/26 06:42:11 AM [ HTTPListener80] User-Agent: Microsoft-CryptoAPI/10.0
02/23/26 06:42:11 AM [ HTTPListener80] Host: crl.comodoca.com
02/23/26 06:42:11 AM [ HTTPListener80]

```

*Richieste di rete intercettate dirette ai server di validazione certificati.*

Il verdetto finale di **VirusTotal** conferma l'analisi del team: 54 vendor su 72 classificano il file come maligno (**Hoax.MSIL/FakeAV**).

In conclusione, questo laboratorio ha dimostrato che la sicurezza non può basarsi solo sulle firme. Solo integrando l'analisi statica dei metadati con il monitoraggio comportamentale dei processi è possibile smascherare minacce sofisticate che abusano di strumenti legittimi per scopi malevoli.

The screenshot shows the VirusTotal analysis interface for the file 4f0033e811fe2497b38f0d45df958829d01933ebe7d331079eefc8e38fbbeaa61. The summary indicates that 54 out of 72 security vendors flagged the file as malicious. The file is identified as AdwareBooC.exe (PE executable). Threat categories listed are trojan, fakeav, and msil. Popular threat labels include trojan.jatif/joke, trojan, and fakeav. A table below shows the analysis from various security vendors, such as AhnLab-V3, Alibaba, AliCloud, ALYac, Anti-AVL, Arcabit, Avast, AVG, Avira, BitDefender, CrowdStrike Falcon, CTX, DeepInstinct, DrWeb, Elastic, Emsisoft, eScan, ESET-NOD32, Fortinet, GData, Google, Gridinsoft, and Kaspersky. Each entry includes the vendor name, detection name, and associated threat label.

Validazione finale tramite Threat Intelligence e verdetto multi-scanner.

## 6. Consigli Strategici di Mitigazione e Soluzioni

L'analisi del malware effettuata dal team ha evidenziato che le minacce moderne sfruttano la fiducia dell'utente e la malleabilità delle configurazioni di sistema. Di seguito sono riportate le contromisure raccomandate:

### 6.1 Rafforzamento delle Policy di Sistema (Hardening)

- **Limitazione dei privilegi (LUAS):** Impedire agli utenti standard di eseguire file con privilegi amministrativi riduce drasticamente la capacità del malware di modificare chiavi di registro critiche in **HKLM**.
- **Controllo dell'esecuzione (AppLocker):** Implementare policy di restrizione del software per bloccare l'esecuzione di binari non firmati o provenienti da directory temporanee come **%TEMP%**, dove gli installer NSIS estraggono solitamente i payload.

- **Monitoraggio dell'integrità del registro:** Configurare avvisi per modifiche non autorizzate alle chiavi di "Run" e "RunOnce", intercettate durante l'analisi dinamica come vettori di persistenza.

## 6.2 Sicurezza a Livello di Rete ed Endpoint

- **Filtraggio DNS e URL:** Bloccare preventivamente l'accesso a domini sospetti identificati nelle fasi di ricognizione, come [vikingwebscanner.com](http://vikingwebscanner.com), per interrompere la catena di comando e controllo (C2).
- **Ispezione del traffico SSL/TLS:** Poiché il malware tenta di validare certificati contraffatti tramite OCSP, l'ispezione del traffico può rilevare anomalie negli User-Agent non standard come [Microsoft-CryptoAPI/10.0](https://github.com/Microsoft/CryptoAPI).

## 6.3 Formazione e Incident Response

- **Security Awareness Training:** Educare il personale a riconoscere le tattiche di Scareware e l'inganno visivo del finto antivirus, evitando di cliccare su pulsanti di "Scan" o "Rimuovi minacce" da software non autorizzati dall'IT.
- **Adozione di EDR/XDR:** L'uso di soluzioni di Endpoint Detection and Response permette di identificare comportamenti anomali (come la scansione ricorsiva delle registry keys) che sfuggono ai tradizionali antivirus basati solo sulle firme.