Relazione Tecnica Finale: Progetto Cyber Security & Ethical Hacking

Team: Secure Sentinels

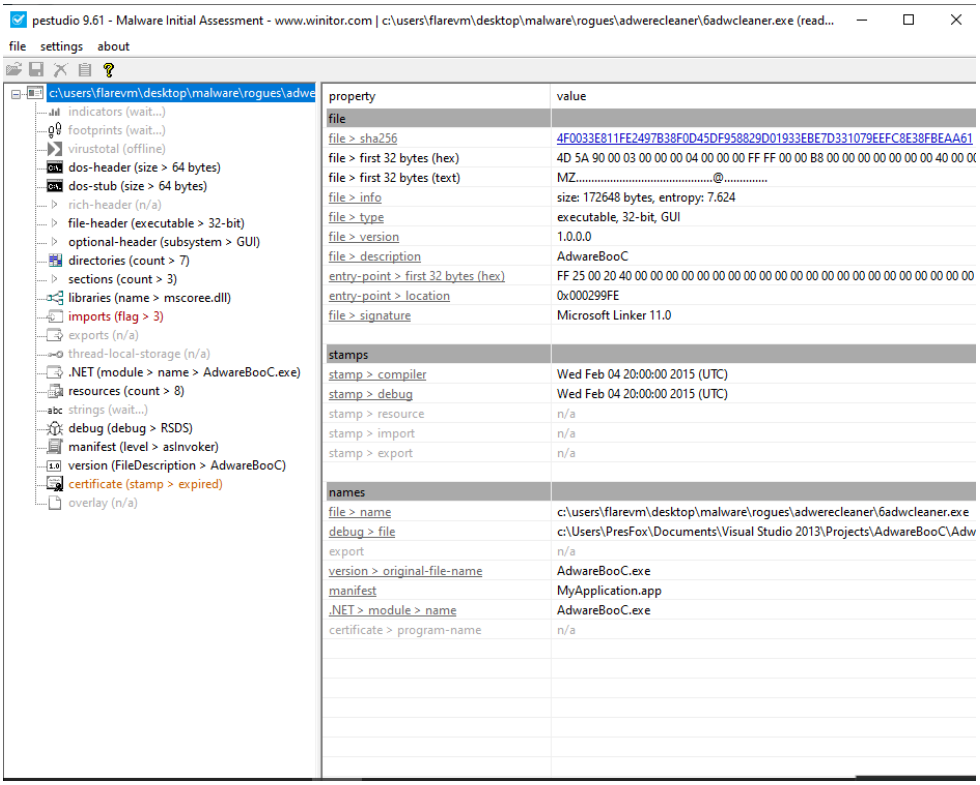
Modulo: Cybersecurity & Ethical Hacking (Epicode)

Data: 23 Febbraio 2026

1. Gestione dell'Analisi Statica e Triage Iniziale

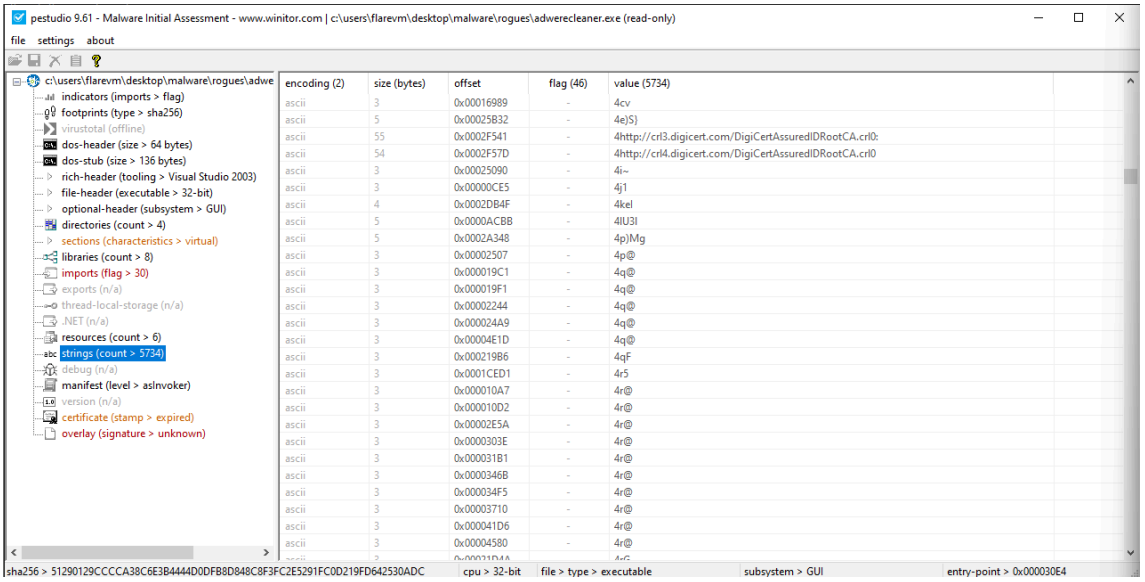
Il laboratorio è iniziato con l'obiettivo di decostruire il malware `6AdwCleaner.exe`, un binario che tenta di mimetizzarsi come un noto strumento di rimozione adware. Utilizzando **pestudio** e **Detect It Easy (DiE)**, abbiamo subito isolato i primi indizi critici: il file è un eseguibile **.NET**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



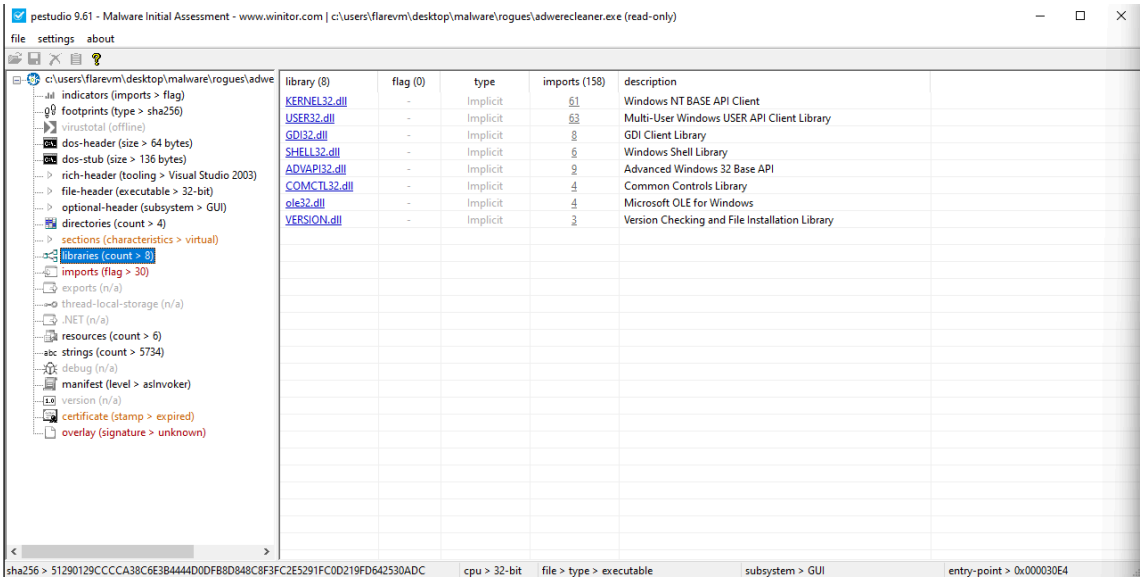
Assessment iniziale in pestudio: identificazione del compilatore e discrepanza dei metadati interni.

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.



Analisi delle stringhe offuscate presenti nel binario.

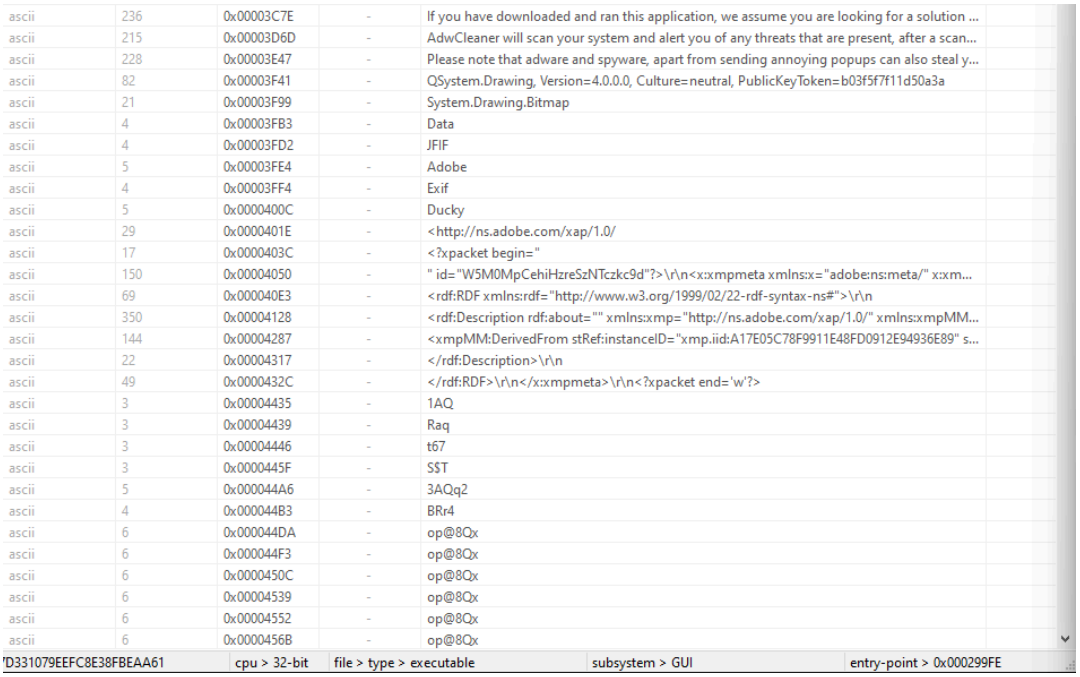
Un elemento fondamentale per comprendere le capacità del malware è l'esame della **Import Address Table (IAT)**. Abbiamo rilevato l'importazione di librerie come `ADVAPI32.dll` e `VERSION.dll`, che indicano chiaramente l'intento del software di manipolare il registro di sistema e di effettuare un fingerprinting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



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

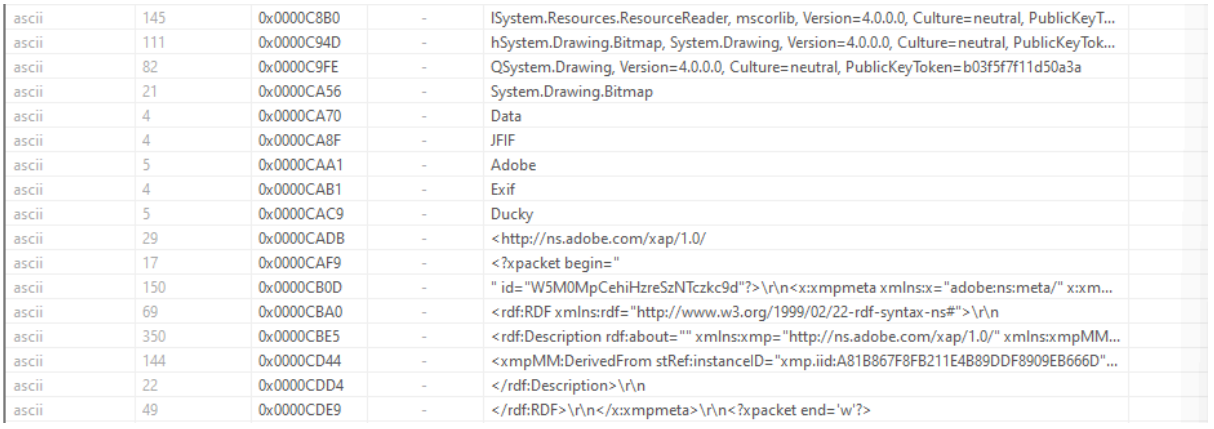
2. Ingegneria Sociale e Struttura della GUI

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.



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

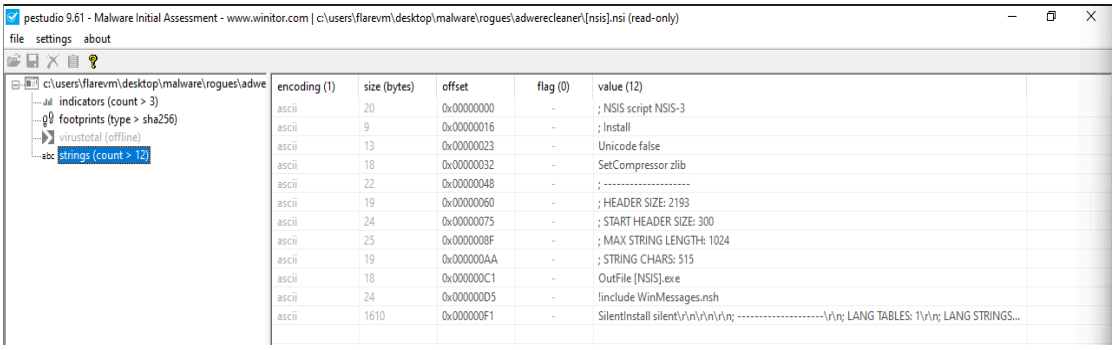
L'esame forense delle risorse tramite **CFF Explorer** ha mostrato metadati Adobe e Ducky legati a risorse bitmap. Questo dimostra che il malware utilizza icone e grafiche rubate da software professionali per simulare un ambiente di scansione antivirus fake, volto a estorcere dati o denaro alla vittima.



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.



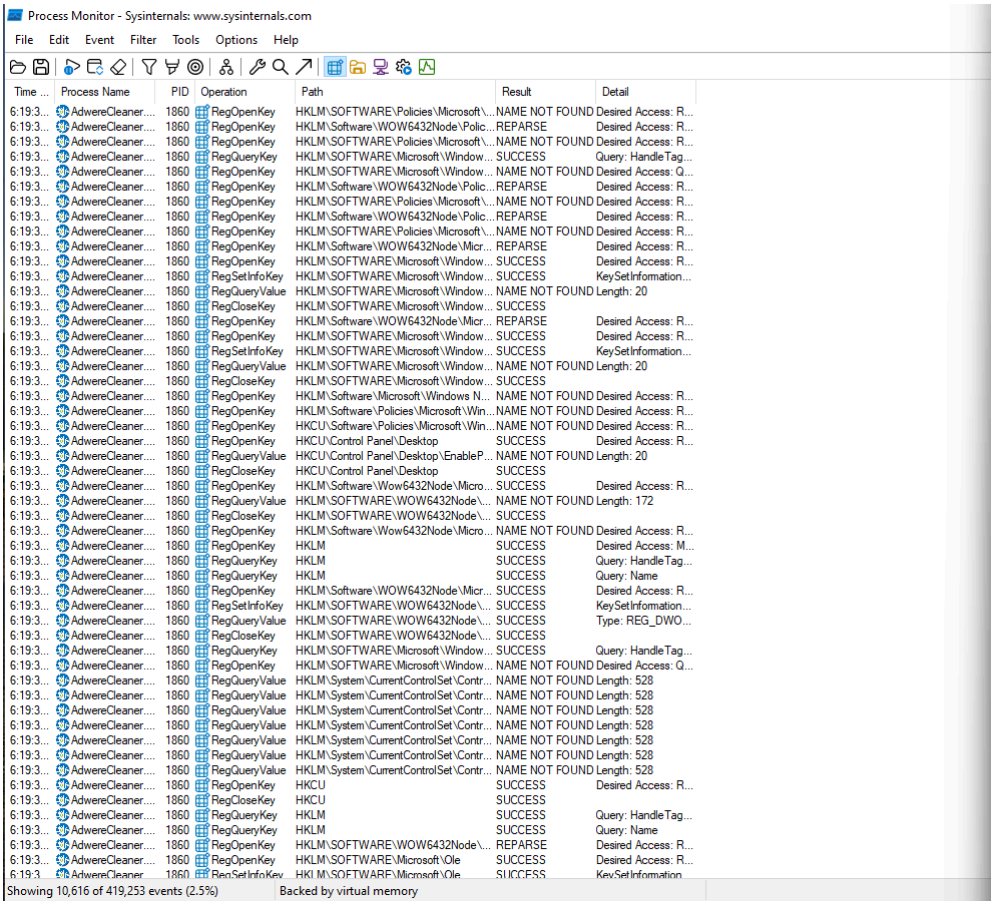
Configurazione NSIS per l'installazione silenziosa e non interattiva.

*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`**:*

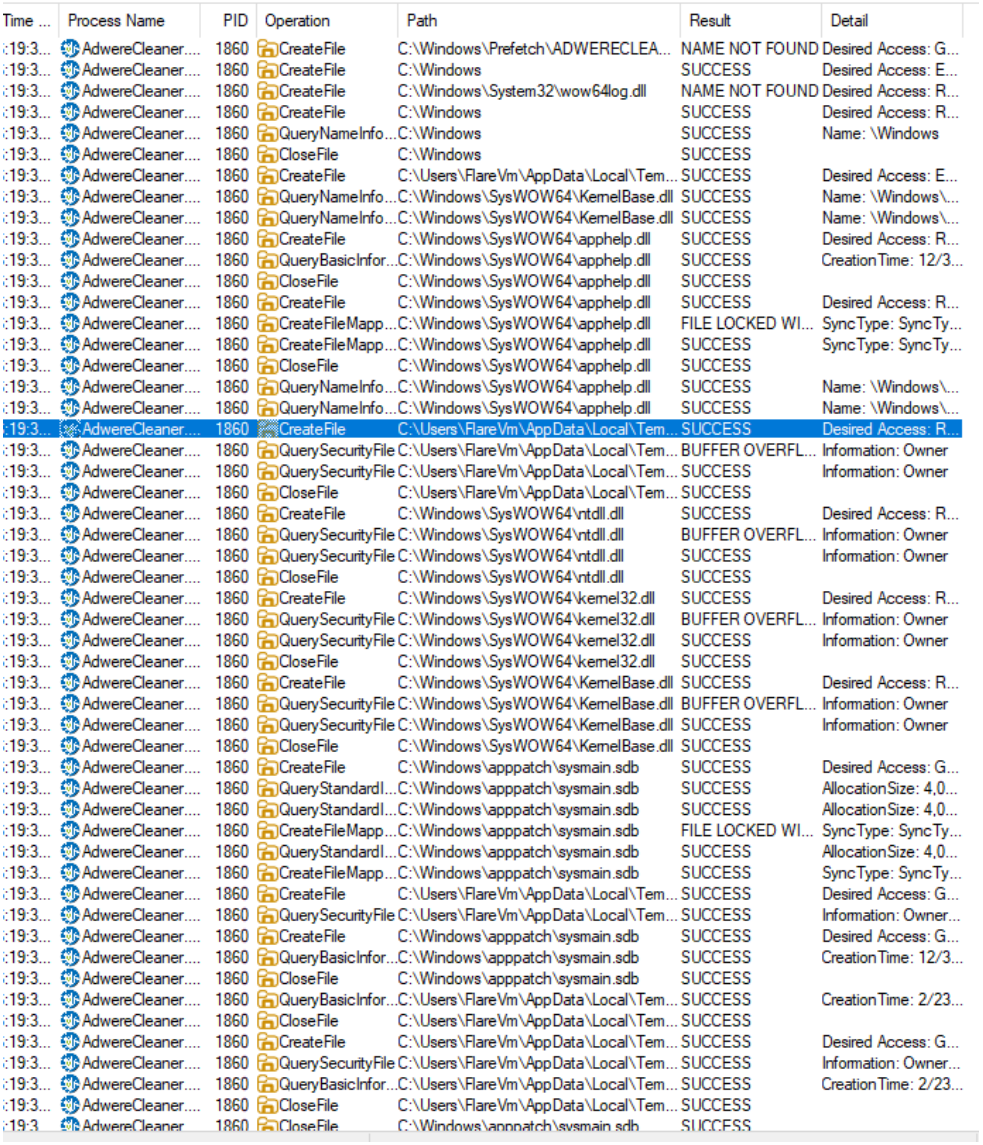
- ***Enumerazione Policy:** Il processo analizza le chiavi sotto `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies` per verificare la presenza di restrizioni di sistema o software di protezione attivi.*
- ***Fingerprinting dell'Utente:** Sono state intercettate letture costanti alla chiave `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`, 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.*



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	CreationTime: 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\ntdll.dll	SUCCESS	Desired Access: R...
19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	BUFFER OVERFL...	Information: Owner
19:3...	AdwereCleaner....	1860	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Information: Owner
19:3...	AdwereCleaner....	1860	CloseFile	C:\Windows\SysWOW64\ntdll.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\apppatch\sysmain.sdb	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

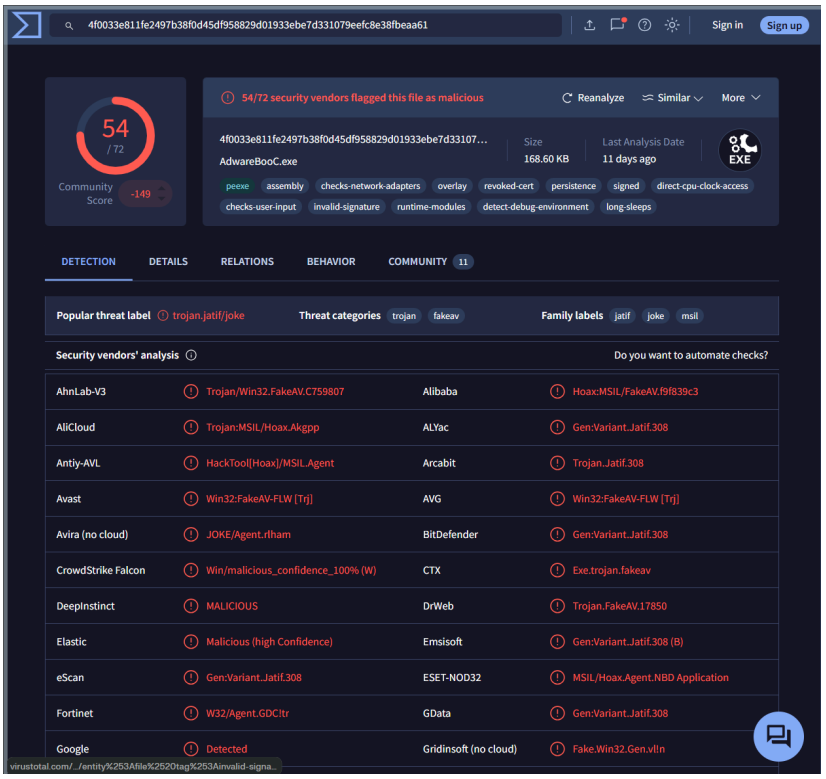
L'ultima fase ha analizzato le minacce di rete tramite **FakeNet-NG (Diverter)**. Il binario tenta di contattare domini come `ocsp.comodoca.com` per validare i propri certificati scaduti, utilizzando un User-Agent di sistema (`Microsoft-CryptoAPI/10.0`) per mimetizzarsi nel traffico legittimo di Windows.

```
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'  0Q0O0M0K0I0\t\x06\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14\x8e%\xa16\x1f\x88Ga\x0c\x
x10\x04\x14\x1e\xc5\xb1,}\x87\xda\x02h|%\xbc\x0c\x07\x84?\xb6\xcf\xde\xf1\x02\x10Q\x82\xe5\xb2JK\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]
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.



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 (LUA):** 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`*, 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`*.*

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.*