

Build Week 3 - Esercizio 1

Progetto S12 - L1

Malware Analysis: “AdwereCleaner.exe”

Executive Summary

Il file **AdwereCleaner.exe** è stato scaricato ed eseguito in ambiente isolato (VM) ed è stato analizzato il comportamento osservabile. Il campione si presenta come un falso tool “AdwCleaner” (rogue/scareware), mostrando un’interfaccia che simula una scansione e restituisce risultati allarmistici (“Your PC is heavily infected! Clean now!”) con 13 infezioni rilevate e dichiarate come cleanable.

Dall’analisi degli screenshot emergono indicatori tipici di adware/spyware/rogue: voci di persistenza nel registro (Run), file in percorsi “Program Files” e “System32” e riferimenti a processi in esecuzione (es. adb_updater.exe, Updater.exe).

La remediation è stata effettuata evitando l’utilizzo del pulsante “Clean”, terminando i processi sospetti, rimuovendo le chiavi di avvio automatico e cancellando file/cartelle riconducibili alla minaccia, con verifica finale tramite scansione con strumenti affidabili e controllo dei browser.

Introduzione

L’obiettivo dell’esercizio è stato scaricare il malware indicato, svolgere un’analisi completa, pulire le tracce e produrre un report tecnico.

È stato adottato un flusso operativo “safe-by-design”: esecuzione in macchina virtuale, raccolta evidenze tramite screenshot, identificazione degli artefatti (processi, chiavi di registro, file) e successiva bonifica.

Passaggi Operativi

1) Preparazione ambiente (sicurezza)

- È stata avviata una VM dedicata (Windows) verificando l'isolamento della rete (NAT o rete limitata).
 - È stato creato uno snapshot della VM (“PRE-MALWARE”) per garantire la possibilità di rollback.
 - Sono state disattivate o limitate clipboard condivisa e shared folders.
-

2) Download del campione

- È stato aperto il browser all'interno della VM.
 - È stato raggiunto il link GitHub fornito dall'esercizio.
 - È stato scaricato il file AdwCleaner.exe.
 - L'eseguibile è stato salvato in una cartella di laboratorio (es. C:\Lab\Malware).
-

3) Esecuzione controllata e osservazione comportamento

- Il file AdwCleaner.exe è stato eseguito nella VM.
- L'applicazione si è presentata come “AdwCleaner”, con grafica e naming simili a un software legittimo.
- È stata completata la presunta “scansione”.
- Sono state raccolte evidenze tramite screenshot.

Evidenze osservate

- Infections Found: 13
 - Infections Cleanable: 13
 - Messaggio intimidatorio: “Your PC is heavily infected! Clean now!”
 - Visualizzazione di categorie e livelli di severità (Very High / High / Medium / Low)
 - Indicazione di percorsi nel registro e nel file system
-

Analisi delle Evidenze

Screenshot 1 — Indicatori principali

AdwCleaner - Your one stop solution for Adware



All done, please review results below

	Threat Name	Malware Type	Danger Level	Location
▶	Start page Changer Win.32	Browser Hijacker	Very High	adb_updater.exe - Running process
	MediaTraffic Feed	Popup Advertising	High	HKEY_LOCAL_USERS\Boot
	VombaSavers	Advertising	Medium	HKEY_LOCAL_USERS\Microsoft\Wind
	Win32.Stealer Trojan	Spyware	Very High	Updater.exe - Running process
◀	Win32.cc Loader	Sovware	Very High	adhsdoh.exe - Running process

Infections Found: 13
Infections Cleanable: 13
Your PC is heavily infected! Clean now! ---->

Done

[Report](#) [Clean](#)

Dalla tabella risultano (estratto significativo):

- **Start page Changer Win.32** → *Browser Hijacker* → **Very High** → *adb_updater.exe - Running process*
- **MediaTraffic Feed** → *Popup Advertising* → **High** → *HKEY_LOCAL_USERS\...*
- **VombaSavers** → *Advertising* → **Medium** → *HKEY_LOCAL_USERS\...\Microsoft\Windows...*
- **Win32.Stealer Trojan** → *Spyware* → **Very High** → *Updater.exe - Running process*
- (Altre voci "Spyware/Logger" con processi in esecuzione)

Interpretazione: presenza di **processi "running"** con nomi generici/ingannevoli e componenti "browser hijacker / spyware / adware" è coerente con un **rogue** che tenta di creare urgenza e spingere l'utente a cliccare "Clean".

Screenshot 2 — Persistenza e file “sospetti”



All done, please review results below

Done

	Threat Name	Malware Type	Danger Level	Location
1	Pinball Browser Helper	Adware	Medium	HKCU\Software\Windows\Run
2	Savings Toolbar	Adware	High	HKCU\Software\Windows\Run
3	Login Logger	Spyware	High	HKCU\Software\Windows\Internet Ex
4	Trojan.Win32.StartPage.fx	Adware	Low	c:\windows\system32\ahmavi.dll
5	WhenUSave	Adware	Medium	c:\Program files\save

Infections Found: 13
Infections Cleanable: 13
Your PC is heavily infected! Clean now! ---->

Report Clean

- **Pinball Browser Helper** → Adware → **Medium** → HKCU\Software\... \Windows\Run
- **Savings Toolbar** → Adware → **High** → HKCU\Software\... \Windows\Run
- **Login Logger** → Spyware → **High** → HKCU\Software\... \Windows\Internet...
- **Trojan.Win32.StartPage.fx** → Adware → **Low** → C:\Windows\System32\ahmavi.dll
- **WhenUSave** → Adware → **Medium** → C:\Program Files\save

Interpretazione: l'uso di ... \Run indica **autostart/persistenza**. La presenza di un .dll in System32 è un artefatto ad alta criticità (potenziale **persistence/loader**).

Screenshot 3 — Altri artefatti su disco

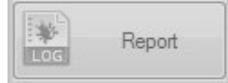


All done, please review results below

	Threat Name	Malware Type	Danger Level	Location
	WhenUSave	Adware	Medium	c:\Program files\save
	Spyware Strike	Adware	High	c:\Program files\spywarestrike\lang
	PSGuard	Spyware	Very High	c:\Documents and Settings\UserName
	Ask Toolbar	Adware	Low	c:\Program files\Ask Toolbar

Infections Found: 13
Infections Cleanable: 13
Your PC is heavily infected! Clean now! ---->

Done

 Report  Clean

- **WhenUSave** → C:\Program Files\save
- **Spyware Strike** → C:\Program Files\spywarestrike\...
- **PSGuard** (spyware) → C:\Documents and Settings\UserName\...
- **Ask Toolbar** → C:\Program Files\Ask Toolbar

Interpretazione: pattern classico da **adware/toolbar/rogue anti-spyware** (nomi noti/riconducibili a famiglie “PUA/rogue”), con installazioni in percorsi tipici di software “commerciale” per sembrare legittimi.

Screenshot 4 (Post “Clean”)



Azione sull'applicazione rogue

Dopo aver analizzato le rilevazioni mostrate negli Screenshot 1–3:

- È stato selezionato il pulsante “Clean”.
- Non è stata avviata alcuna rimozione reale.
- È comparsa una finestra di acquisto della versione completa.

Tentativo di estorsione (Fake Upgrade Screen)

La schermata visualizzata riporta:

- “**Upgrade to the full version now!**”
- Indicazione che la versione trial può solo scansionare ma non rimuovere
- Prezzo promozionale: **\$59,99**
- Indicazione di invio seriale via e-mail dopo l'acquisto

Analisi tecnica

Il comportamento conferma che:

- Il software è un **Rogue Security Software (Scareware)**.
- La scansione è strumentale alla creazione di urgenza.
- La rimozione è subordinata al pagamento.
- Non viene effettuata alcuna bonifica reale.
- È presente un **tentativo di monetizzazione fraudolenta**.

Indicatori tipici di Rogue rilevati

- Conteggio fisso di infezioni (13).
 - Messaggi allarmistici in rosso.
 - Severità “Very High” su voci generiche.
 - Finta funzione di pulizia.
 - Richiesta immediata di pagamento.
 - Offerta a tempo limitato.
-

Bonifica / Pulizia Tracce (Remediation)

Nota: essendo un rogue, il pulsante “Clean” non garantisce rimozione reale. La bonifica deve essere eseguita con strumenti affidabili e controlli manuali.

1) Isolamento e contenimento

- È stata disattivata temporaneamente la rete della VM.
 - Sono stati individuati tramite Task Manager i processi:
 - adb_updater.exe
 - Updater.exe
 - eventuali processi correlati
 - I processi sospetti sono stati terminati.
-

2) Rimozione persistenza (Registro “Run”)

- È stato aperto regedit.
- Sono state analizzate le chiavi di avvio automatico:
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - eventuali Run/RunOnce
- Sono state rimosse le entry collegate a:
 - Savings Toolbar
 - Pinball Browser Helper
 - WhenUSave
 - Spyware Strike
 - PSGuard
 - Ask Toolbar
 - Percorsi associati a Updater.exe / adb_updater.exe

3) Rimozione file/cartelle su disco

Sono stati controllati e rimossi:

- C:\Windows\System32\ahmavi.dll
- C:\Program Files\save\
- C:\Program Files\spywarestrike\
- C:\Program Files\Ask Toolbar\
- Directory sospette in Documents and Settings

È stato **svuotato il cestino** ed è stata verificata l'assenza di copie residue in Temp e AppData.

4) Ripristino browser (anti-hijack)

- Sono state aperte le impostazioni del browser.
- È stata ripristinata la homepage.
- È stato reimpostato il motore di ricerca.
- Sono state rimosse estensioni/add-on sospette.

5) Verifica finale

- È stata riavviata la VM.
- È stata verificata l'assenza di:
 - processi riavviati
 - chiavi Run ricreate
 - cartelle/file ripristinati
- È stata eseguita una scansione con tool legittimo (Windows Defender aggiornato / antimalware affidabile).

Conclusione

Il campione analizzato si comporta come un **rogue/scareware che imita un prodotto legittimo “AdwCleaner”**, mostrando risultati catastrofici e inducendo l’utente a cliccare “Clean”. Gli screenshot evidenziano **13 rilevazioni e diversi indicatori di compromissione/persistenza (processi in esecuzione, chiavi Run, file in System32 e Program Files)**.

La strategia corretta consiste nel contenimento, rimozione della persistenza e degli artefatti, ripristino dei browser e validazione tramite scansione finale con strumenti affidabili.

In un contesto aziendale si raccomandano inoltre:

- Raccolta e documentazione degli IOC
- Blocco tramite EDR/AV
- Applicazione di GPO restrittive
- Eventuale blacklist hash
- Monitoraggio per prevenzione reinfezioni