



SMART  
WORKERS

# MALWARE ANALYSIS

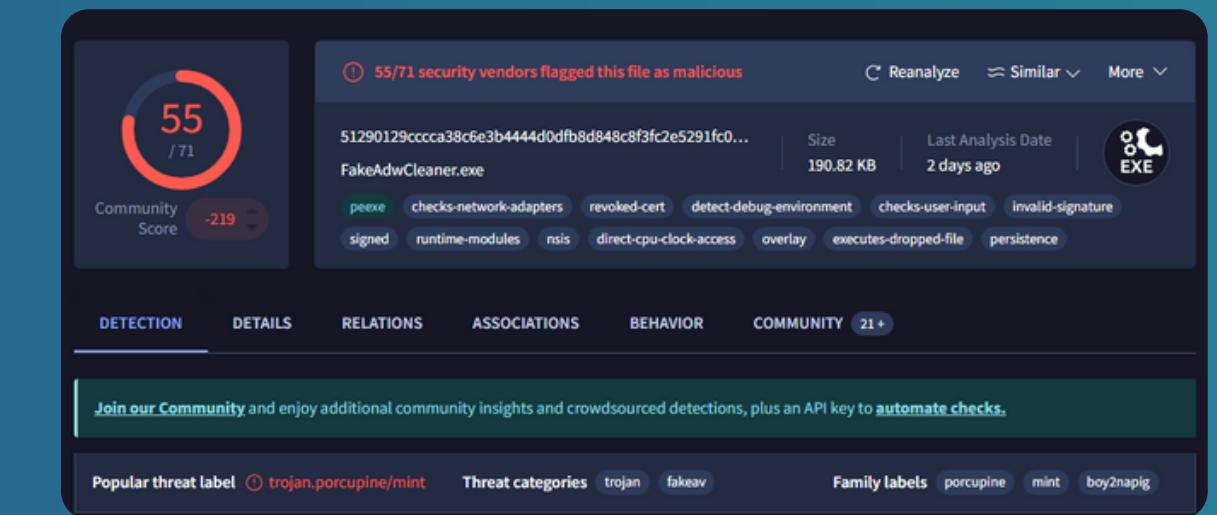


# ADWERECLEANER.EXE



## IDENTIKIT

- Nome del file: AdwereCleaner.exe
  - Verdetto: Attività Malevola
  - Data di analisi: 17 Dicembre 2024
- Sistema Operativo Analizzato: Windows 10 Professional (Build 19045, 64-bit)
- Indicatori Hash:
  - MD5: 74B6CB94FA7823F226CFE862DoD8F65
  - SHA1: 8210DFDE1A045EA09A7683CC04081BD316205470
  - SHA256: 6515BDA500BF9E89FBCA8D507FE098C11EB298CDC544405A5B1B1E4FBB12D2



Risultato di VirusTotal,  
prima analisi statica



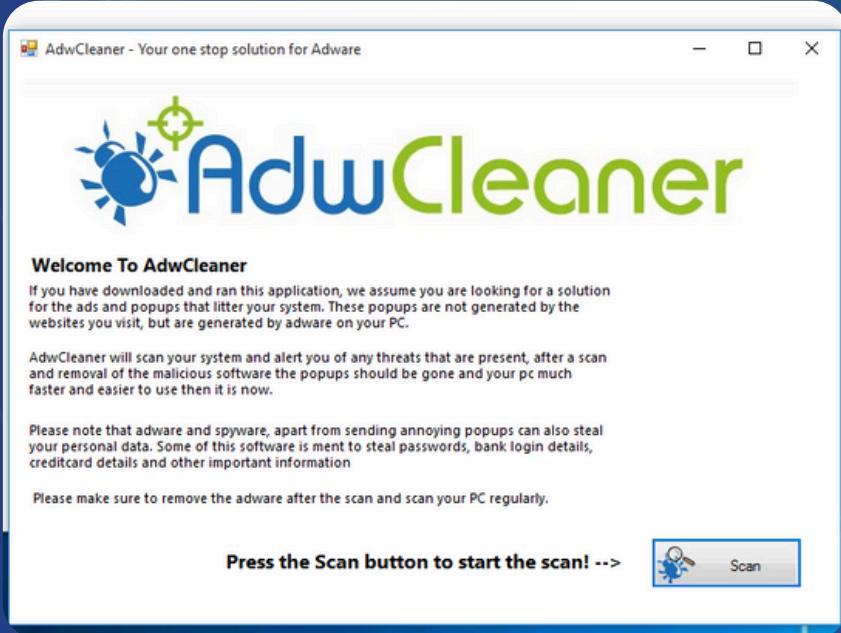
# PRIMO CAMPANELLO

Già senza una preparazione in tema di CyberSecurity, l'errore di battitura nella scrittura di AdwareCleaner.exe, scritto invece AdwereCleaner.exe, ci può far pensare a un software non ufficiale e di cui quindi non fidarsi a prescindere. Questo sottolinea la responsabilità individuale di un utente di controllare anche le informazioni più banali.

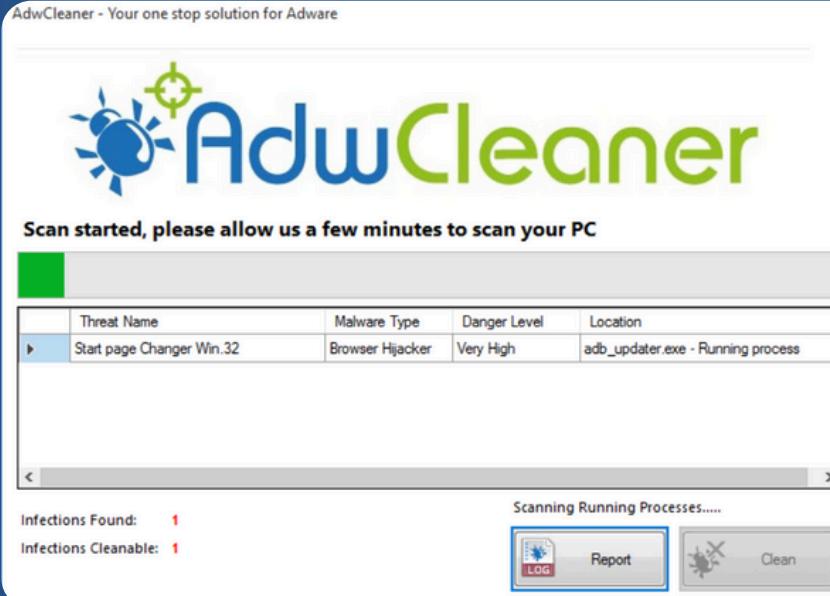
Nome	Ultima modifica	Tipo	Dimensione
AdwereCleaner	17/12/2024 15:28	Applicazione	191 KB



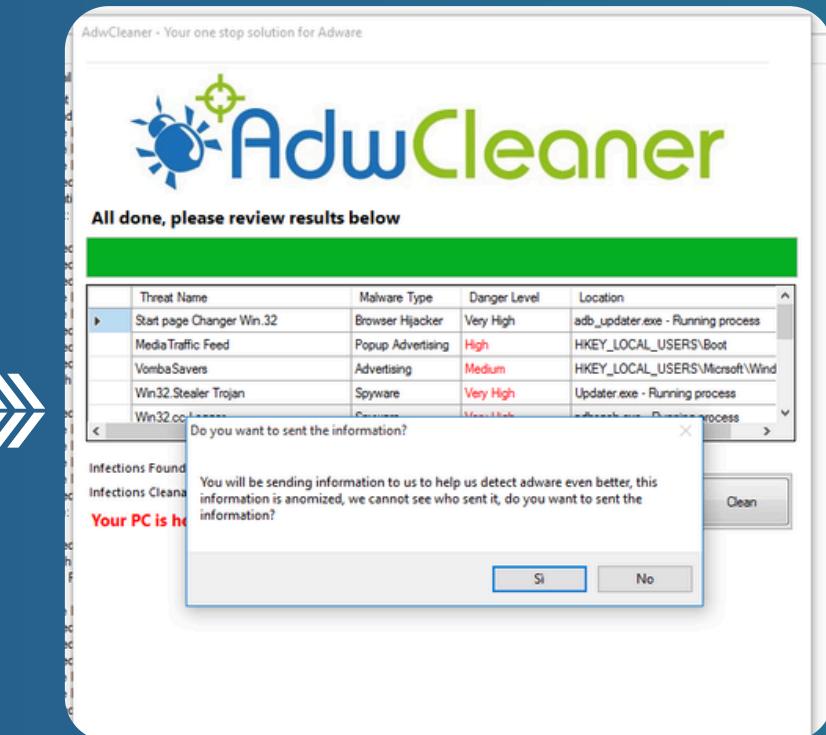
# FUNZIONAMENTO PRATICO



Il programma chiede di eseguire uno scan del PC per individuare minacce all'interno del sistema



Il programma procede alla "scansione" del sistema



Il programma individua sempre 13 minacce, per il quale si può inviare un log di report attraverso il tasto "Report"



Si può anche chiedere la pulizia totale del sistema attraverso il pagamento della versione premium

# ANALISI STATICÀ - CFFEXPLORER

L'analisi statica consiste nell'esaminare un file senza eseguirlo, studiandone struttura e dipendenze. CFF Explorer è uno strumento utile per esplorare header PE, librerie importate e altre informazioni binarie.

**KERNEL32.dll, USER32.dll, GDI32.dll, SHELL32.dll** e ADVAPI32.dll sono librerie di sistema essenziali per il funzionamento di Windows, spesso sfruttate anche dai malware per le loro attività dannose. KERNEL32.dll gestisce operazioni di basso livello come processi, memoria e file, rendendola una scelta comune per manipolazioni del sistema. USER32.dll e GDI32.dll supportano l'interazione grafica e

l'interfaccia utente, utilizzate per mostrare finestre o simulare attività legittime. SHELL32.dll offre accesso al file system e comandi di shell, utili per modificare file o creare persistenza.

Infine, ADVAPI32.dll permette l'accesso avanzato al registro di sistema e ai meccanismi di sicurezza, spesso usati per eludere le protezioni.

Module Name	Imports	OFTs	TimeStamp	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

# RISULTATI CUCKOO

Abbiamo utilizzato la sandbox di Cuckoo per analizzare in un ambiente sicuro l'eseguibile. Qui di fianco potete notare i risultati.

## Score e Yara

Le regole Yara e lo score di 10/10 ci hanno praticamente assicurato che si tratta di un malware potenzialmente molto pericoloso.

## Eventi e firme

Similmente alla sezione di sommario, nella sezione firme troviamo altri comportamenti sospetti segnalati da Cuckoo.

Andremo ora ad analizzare i risultati più nel dettaglio.

The screenshot displays two main sections of the Cuckoo Sandbox analysis interface:

**Summary** (Top Section):

- File:** AdwereCleaner.exe
- Score:** Very suspicious, with a score of 10 out of 10!
- Summary Details:** Size: 190.8KB, Type: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, MD5: 248aadd395ffa7ffb1670392a9398454, SHA1: c53c140bbdeb556fcfa33bc7f9b2e44e9061ea3e5, SHA256: 51290129ccccca38c6e3b444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc, SHA512: Show SHA512, CRC32: 124412D7, ssdeep: None.
- Yara Rules:** A list of detected behaviors including escalate\_priv, screenshot, win\_registry, win\_token, win\_private\_profile, and win\_files\_operation.

**Signatures** (Bottom Section):

- Yara rules detected for file (6 events)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)
- Creates executable files on the filesystem (1 event)
- Drops a binary and executes it (1 event)
- Drops an executable to the user AppData folder (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- File has been identified by 12 AntiVirus engine on IRMA as malicious (12 events)
- File has been identified by 55 AntiVirus engines on VirusTotal as malicious (50 out of 55 events)

# ATTIVITÀ SOSPETTE

## **escalate\_priv - Escalade privileges:**

Il malware tenta di acquisire privilegi elevati per accedere a funzionalità o dati protetti del sistema operativo.

## **screenshot - Take screenshot**

Cattura immagini dello schermo del sistema, potenzialmente per rubare informazioni sensibili come credenziali o documenti.

## **win\_registry - Affect system registries**

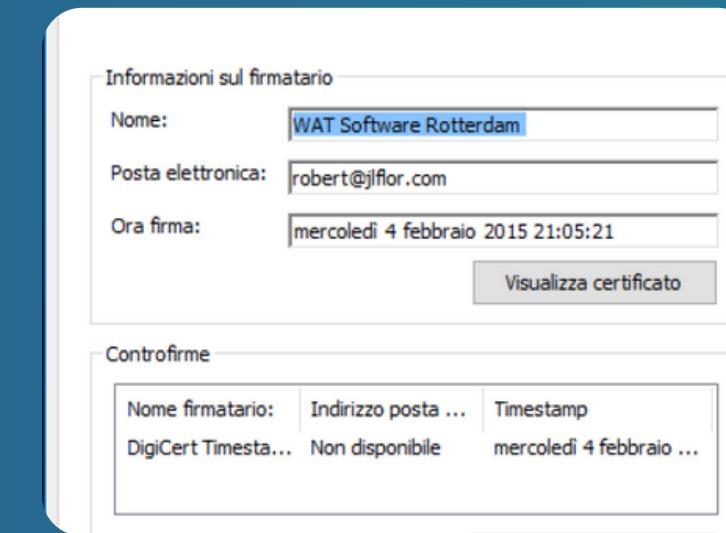
Modifica le chiavi del registro di sistema per garantire persistenza o alterare configurazioni di sicurezza.

## **win\_token - Affect system token**

Manipola i token di sicurezza per aggirare le autorizzazioni e accedere a risorse riservate.

## **Esecuzione con un certificato non affidabile**

Sebbene il file sia firmato digitalmente, la validità della firma non viene correttamente verificata. Questo permette a file malevoli di apparire legittimi.



## **The binary likely contains encrypted or compressed data**

Il file binario potrebbe contenere dati compressi o crittografati, indicativi di offuscamento tramite packer.



# ATTIVITÀ SOSPETTE

## **win\_private\_profile - Affect private profile**

Interferisce con i profili privati degli utenti per compromettere dati personali o configurazioni.

## **win\_files\_operation**

Esegue operazioni dannose sui file personali, come sovrascrittura o eliminazione.

## **The executable contains unknown PE section names:**

L'eseguibile include sezioni PE sconosciute, suggerendo l'uso di un packer per offuscare il codice.

## **Drops a binary and executes it**

Rilascia un file binario sul sistema e lo esegue, spesso per introdurre ulteriori componenti malware.

## **Drops an executable to the user AppData folder:**

- Deposita file eseguibili nella cartella AppData, un metodo comune per eludere controlli di sicurezza.



## Filtro per nome processo

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process Name	is	AdwereCleaner.exe	Include
<input checked="" type="checkbox"/> Process Name	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Procexp.exe	Exclude

## Risultati ProcMon

Un breve sguardo ai risultati della cattura di ProcMon evidenziano la correttezza delle nostre ipotesi sul funzionamento del malware e della scrittura nei registri di sistema

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:43...	AdwereCleaner....	2948	Process Start		SUCCESS	Parent PID: 3824, ...
12:43...	AdwereCleaner....	2948	Thread Create		SUCCESS	Thread ID: 3224
12:43:41,5532852	Cleaner....	2948	Load Image	C:\Users\user\Downloads\AdwereClea...	SUCCESS	Image Base: 0x400...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fd...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77b...
12:43...	AdwereCleaner....	2948	CreateFile	C:\Windows\Prefetch\ADWERECLEA...	SUCCESS	Desired Access: G...
12:43...	AdwereCleaner....	2948	QueryStandard...	C:\Windows\Prefetch\ADWERECLEA...	SUCCESS	AllocationSize: 12...
12:43...	AdwereCleaner....	2948	ReadFile	C:\Windows\Prefetch\ADWERECLEA...	SUCCESS	Offset: 0, Length: 9...
12:43...	AdwereCleaner....	2948	CloseFile	C:\Windows\Prefetch\ADWERECLEA...	SUCCESS	
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
12:43...	AdwereCleaner....	2948	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x68b...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x68b...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\Software\Microsoft\WOW64	SUCCESS	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\Software\MICROSOFT\WIN...	NAME NOT FOUND	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegQueryValue	HKLM\Software\MICROSOFT\WO...	NAME NOT FOUND	Length: 532
12:43...	AdwereCleaner....	2948	RegCloseKey	HKLM\Software\MICROSOFT\WO...	SUCCESS	
12:43...	AdwereCleaner....	2948	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x1d0...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x7f9...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x1d0...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x450...
12:43...	AdwereCleaner....	2948	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
12:43...	AdwereCleaner....	2948	QueryNameInfo...	C:\Windows	SUCCESS	Name: '\Windows
12:43...	AdwereCleaner....	2948	CloseFile	C:\Windows	SUCCESS	
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\Software\Microsoft\Wow64\%86	SUCCESS	Desired Access: R...
12:43...	AdwereCleaner....	2948	RegQueryValue	HKLM\Software\MICROSOFT\WO...	NAME NOT FOUND	Length: 520
12:43...	AdwereCleaner....	2948	RegQueryValue	HKLM\Software\MICROSOFT\WO...	SUCCESS	Type: REG_SZ, Le...
12:43...	AdwereCleaner....	2948	RegCloseKey	HKLM\Software\MICROSOFT\WO...	SUCCESS	
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x68c...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
12:43...	AdwereCleaner....	2948	CreateFile	C:\Users\user\Downloads	SUCCESS	Desired Access: E...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x7f9...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x77a...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\Software\Wow6432Node\Policies	REPARSE	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegOpenKey	HKLM\Software\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
12:43...	AdwereCleaner....	2948	RegSetInfoKey	HKLM\Software\Policies\Microsoft\...	SUCCESS	KeySetInformation...
12:43...	AdwereCleaner....	2948	RegQueryValue	HKLM\Software\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
12:43...	AdwereCleaner....	2948	RegCloseKey	HKLM\Software\Policies\Microsoft\...	SUCCESS	
12:43...	AdwereCleaner....	2948	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x75b...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\gd32.dll	SUCCESS	Image Base: 0x760...
12:43...	AdwereCleaner....	2948	Thread Create		SUCCESS	Thread ID: 3776
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x764...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\msvcr.dll	SUCCESS	Image Base: 0x759...
12:43...	AdwereCleaner....	2948	Load Image	C:\Windows\SysWOW64\windows.sto...	SUCCESS	Image Base: 0x752...

Potete trovare qui sotto il link al log completo di ProcMon durante tutta l'esecuzione del malware sulla macchina virtuale.

**LINK LOG .CSV DI PROCMON**

<https://www.dropbox.com/scl/fi/fb44vi3axhq2zefuofvr4/LogFile.CSV?rlkey=3ay7cqrpmrk521nt7iqpcnknm&st=dxwboljd&dl=0>

# RISULTATI PROCMON



# MITIGAZIONE

## Eliminazione e Isolamento del File

Rimuovere immediatamente il file identificato come malevolo e isolarlo in un ambiente sicuro per ulteriori analisi. Evitare di riavviare il sistema prima di aver eliminato il malware per prevenire ulteriori danni.

## Formazione ai Dipendenti

Educare i dipendenti sulle buone pratiche di sicurezza informatica, come evitare il download di file sospetti e il clic su link non verificati. Questo aiuta a prevenire l'introduzione di malware tramite comportamenti umani non sicuri.

## Gestione dei Privilegi (escalate\_priv)

Limitare i privilegi utente ai minimi necessari e utilizzare account separati per operazioni amministrative. Configurare politiche di sicurezza che impediscono l'elevazione non autorizzata dei privilegi.

## Monitoraggio del Registro di Sistema (win\_registry)

Implementare strumenti che monitorino e rilevino modifiche sospette alle chiavi di registro critiche, con la possibilità di bloccare o annullare modifiche non autorizzate.

## Protezione dei File di Sistema (Creates executable files on the filesystem)

Configurare il controllo dell'accesso ai file e abilitare un sistema di rilevamento delle modifiche che avvisi l'amministratore in caso di creazione o modifica di eseguibili non autorizzati.

## Prevenzione della Cattura dello Schermo (screenshot)

Configurare strumenti di sicurezza per rilevare e bloccare processi non autorizzati che tentano di accedere al buffer dello schermo, e abilitare politiche di controllo per limitare l'accesso alle API di cattura dello schermo solo alle applicazioni fidate.



# GRAZIE!