

CS0424IT — ESERCITAZIONE S10L2
ANALISI DINAMICA MALWARE ADWCLEANER

Simone La Porta



30 luglio 2024

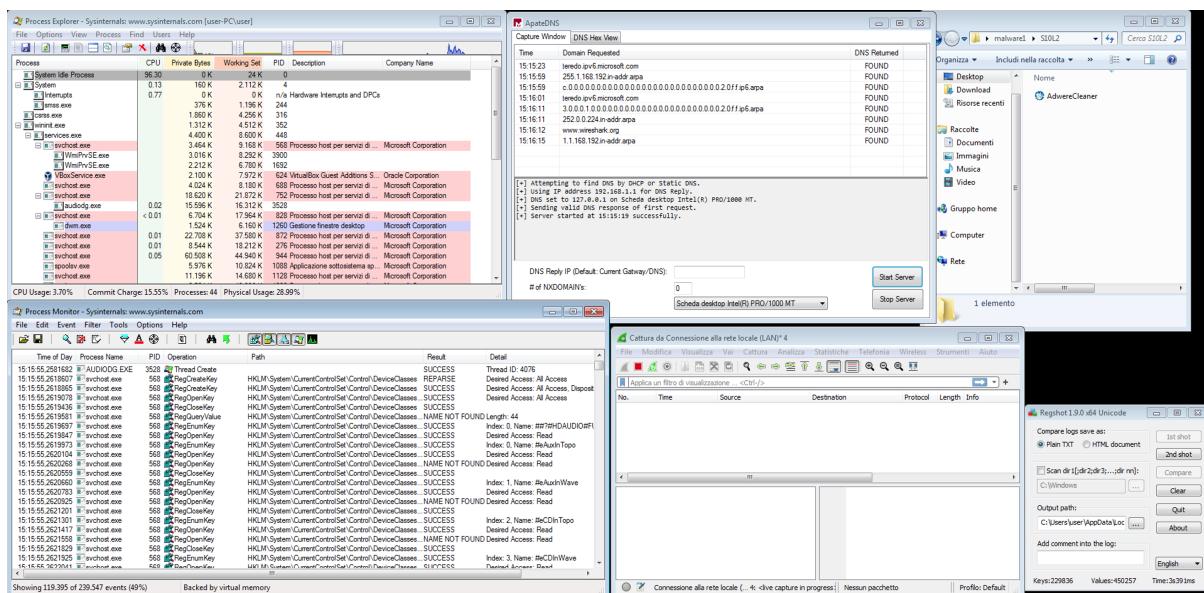
INDICE

1	TRACCIA	3
2	SVOLGIMENTO	4
2.1	Azioni sul File System	5
2.2	Azioni su Processi e Thread	6
2.3	Modifiche del Registro	7
2.4	Profilazione del Malware	8

1 TRACCIA

Con riferimento al file eseguibile AdwCleaner presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

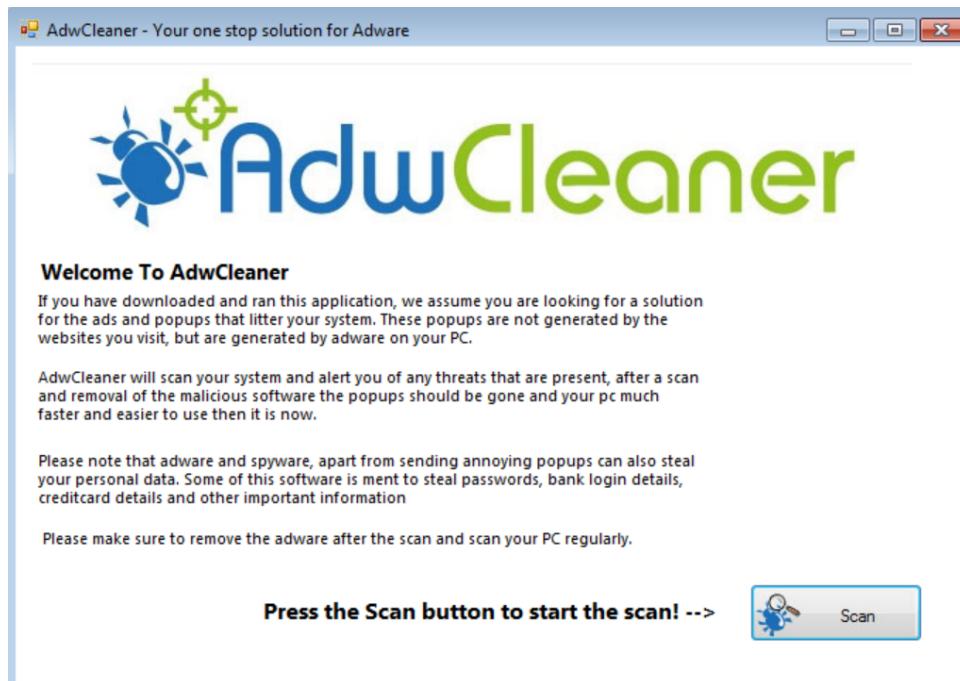
1. Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon).
 2. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor.
 3. Modifiche del registro dopo il malware (le differenze).
 4. Provare a profilare il malware in base alla correlazione tra «operation» e path.



2. SVOLGIMENTO

2 SVOLGIMENTO

Questa relazione fornisce un'analisi dettagliata del malware AdwCleaner, basata sulle sue azioni sul file system, sui processi, sui thread e sulle modifiche al registro. L'analisi è stata eseguita utilizzando gli strumenti Process Monitor (ProcMon) e RegShot su una macchina virtuale dedicata all'analisi dei malware.



Analysis Overview

[Request Report Deletion](#)

Submission name:	AdwereCleaner.exe
Size:	191KiB
Type:	pexe executable
Mime:	application/x-dosexec
SHA256:	51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
Operating System:	Windows
Last Anti-Virus Scan:	06/18/2024 07:49:50 (UTC)
Last Sandbox Report:	06/18/2024 07:49:47 (UTC)

malicious
Threat Score: 100/100
AV Detection: 78%
Labeled As: Mint.Porcupine.Generic
[#evasive](#)
[X Post](#) [🔗 Link](#) [✉️ E-Mail](#)

Anti-Virus Results

[⚠️ Updated 1 month ago - Click to Refresh](#)

CrowdStrike Falcon 🔗 Static Analysis and ML	MetaDefender 🔗 Multi Scan Analysis
Malicious (100%)	Malicious (13/23)
X No Additional Data	More Details

2.1 Azioni sul File System

AdwCleaner ha eseguito diverse azioni sul file system, tra cui lettura e creazione di file, nonché interrogazione di informazioni sui file.

Le seguenti operazioni sono state osservate nel file di log prodotto tramite ProcessMonitor:

- ReadFile:** Il malware ha tentato di leggere il contenuto di directory e file specifici.
- CreateFile:** Il malware ha creato o aperto diversi file e directory.
- QueryBasicInformationFile:** Il malware ha interrogato informazioni di base su file di sistema.

Queste azioni suggeriscono che il malware sta cercando di raccogliere informazioni sul sistema e potenzialmente prepararsi per ulteriori operazioni dannose.

15:17:18.2992547	6AdvCleaner.exe	1984	QueryDirectory	C:\Windows\Microsoft.NET Framework64	NO MORE FILES
15:17:18.2992676	6AdvCleaner.exe	1984	CloseFile	C:\Windows\Microsoft.NET Framework64	SUCCESS
15:17:18.3018180	6AdvCleaner.exe	1984	CreateFile	C:\Windows\System32\imm32.dll	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: None, AllocationSize: 16777216, EndOfFile: 16777216, NumberOfLinks: 1, DeletePending: False, Directory: False, CreationTime: 14/07/2009 01:38:08, LastAccessTime: 14/07/2009 01:38:08, LastWriteTime: 14/07/2009 ...
15:17:18.3738266	6AdvCleaner.exe	1984	QueryBasicInformation	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3732792	6AdvCleaner.exe	1984	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3732981	6AdvCleaner.exe	1984	CreateFile	C:\Windows\System32\imm32.dll	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Non-AI, SyncType: SyncTypeCreateSection, PageProtection:
15:17:18.3734814	6AdvCleaner.exe	1984	CreateFileMapping	C:\Windows\System32\imm32.dll	FILE LOCKED WI...
15:17:18.3734920	6AdvCleaner.exe	1984	QueryStandardInforma...	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3735144	6AdvCleaner.exe	1984	CreateFileMapping	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3735573	6AdvCleaner.exe	1984	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3737226	6AdvCleaner.exe	1984	CreateFile	C:\Windows\System32\imm32.dll	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: None, AllocationSize: 16777216, EndOfFile: 16777216, NumberOfLinks: 1, DeletePending: False, Directory: False, CreationTime: 14/07/2009 01:38:08, LastAccessTime: 14/07/2009 01:38:08, LastWriteTime: 14/07/2009 ...
15:17:18.3738383	6AdvCleaner.exe	1984	QueryBasicInformation	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3738489	6AdvCleaner.exe	1984	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3740446	6AdvCleaner.exe	1984	CreateFile	C:\Windows\System32\imm32.dll	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Non-AI, SyncType: SyncTypeCreateSection, PageProtection:
15:17:18.3745446	6AdvCleaner.exe	1984	CreateFileMapping	C:\Windows\System32\imm32.dll	FILE LOCKED WI...
15:17:18.3745564	6AdvCleaner.exe	1984	QueryStandardInforma...	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3745764	6AdvCleaner.exe	1984	CreateFileMapping	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3746146	6AdvCleaner.exe	1984	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3747911	6AdvCleaner.exe	1984	CreateFile	C:\Windows\System32\imm32.dll	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: None, AllocationSize: 16777216, EndOfFile: 16777216, NumberOfLinks: 1, DeletePending: False, Directory: False, CreationTime: 14/07/2009 01:38:08, LastAccessTime: 14/07/2009 01:38:08, LastWriteTime: 14/07/2009 ...
15:17:18.3749018	6AdvCleaner.exe	1984	QueryBasicInformation	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3749116	6AdvCleaner.exe	1984	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3750297	6AdvCleaner.exe	1984	CreateFile	C:\Windows\System32\imm32.dll	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Sync...
15:17:18.3751064	6AdvCleaner.exe	1984	CreateFileMapping	C:\Windows\System32\imm32.dll	FILE LOCKED WI...
15:17:18.3751491	6AdvCleaner.exe	1984	CreateFileMapping	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3752621	6AdvCleaner.exe	1984	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS
15:17:18.3772418	6AdvCleaner.exe	1984	CreateFile	C:\Users\user\AppData\Local\6AdvCleaner.exe.config	NAME NOT FOUND Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, A...
15:17:18.3774695	6AdvCleaner.exe	1984	CreateFile	C:\Users\user\AppData\Local\6AdvCleaner.exe	SUCCESS
15:17:18.3774795	6AdvCleaner.exe	1984	QueryStandardInforma...	C:\Users\user\AppData\Local\6AdvCleaner.exe	Desired Access: Generic Read, Disposition: Open, Options: Sequential Access, Synchronous IO Non-Alert, ...
15:17:18.3775168	6AdvCleaner.exe	1984	CreateFileMapping	C:\Users\user\AppData\Local\6AdvCleaner.exe	FILE LOCKED WI...
15:17:18.3775267	6AdvCleaner.exe	1984	QueryStandardInforma...	C:\Users\user\AppData\Local\6AdvCleaner.exe	SUCCESS
15:17:18.3776128	6AdvCleaner.exe	1984	CreateFileMapping	C:\Users\user\AppData\Local\6AdvCleaner.exe	SUCCESS
15:17:18.3777201	6AdvCleaner.exe	1984	CloseFile	C:\Users\user\AppData\Local\6AdvCleaner.exe	SUCCESS
15:17:18.3777373	6AdvCleaner.exe	1984	QueryStandardInforma...	C:\Users\user\AppData\Local\6AdvCleaner.exe	Desired Access: Generic Read, Disposition: Open, Options: Sequential Access, Synchronous IO Non-Alert, ...
15:17:18.3777480	6AdvCleaner.exe	1984	CreateFileMapping	C:\Users\user\AppData\Local\6AdvCleaner.exe	FILE LOCKED WI...

Figura 1: Modifiche al File System

2.2 Azioni su Processi e Thread

AdwCleaner ha eseguito diverse azioni relative ai processi e ai thread, inclusi l'avvio di nuovi processi e la creazione di thread.

Le seguenti operazioni sono state osservate nel file di log prodotto tramite ProcessMonitor:

- Process Start:** Il malware ha avviato un nuovo processo AdwreCleaner.exe, indicando un tentativo di eseguire il proprio codice in modo indipendente.
- Thread Create:** Il malware ha creato nuovi thread per eseguire operazioni in parallelo.
- Load Image:** Il malware ha caricato diverse immagini di sistema e di sé stesso, mostrando un comportamento tipico di esecuzione di codice malevolo.

Queste azioni indicano che il malware è progettato per eseguire operazioni multiple simultaneamente e per caricare moduli aggiuntivi se necessario.

15:17:18.1044415	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\cfmpg32.dll	SUCCESS	Image Base: 0x77380000, Image Size: 0x21e000
15:17:18.1043222	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Image Base: 0x759e0000, Image Size: 0x12000
15:17:18.1253493	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x74120000, Image Size: 0x6000
15:17:18.1447646	AdwreCleaner.exe	3984	Thread Create		SUCCESS	Thread ID: 2844
15:17:18.1870884	AdwreCleaner.exe	3984	Thread Create		SUCCESS	Thread ID: 3972
15:17:18.2008124	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\aphelp.dll	SUCCESS	Image Base: 0x73c30000, Image Size: 0x4e000
15:17:18.2056504	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x6f5e0000, Image Size: 0x2e000
15:17:18.2064459	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x6f450000, Image Size: 0x2e000
15:17:18.2072003	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x6f5e0000, Image Size: 0x2e000
15:17:18.2116262	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\shdocvw.dll	SUCCESS	Image Base: 0x6f450000, Image Size: 0x2e000
15:17:18.2133995	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x28400000, Image Size: 0x44e000
15:17:18.2200745	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\usermon.dll	SUCCESS	Image Base: 0x759e0000, Image Size: 0x100000
15:17:18.2220764	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\userinit.dll	SUCCESS	Image Base: 0x77380000, Image Size: 0x49e000
15:17:18.2232461	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x770e0000, Image Size: 0x16b000
15:17:18.2284361	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x777e0000, Image Size: 0x122000
15:17:18.2295587	AdwreCleaner.exe	3984	Load Image	C:\Windows\SysWOW64\msasn1.dll	SUCCESS	Image Base: 0x777e0000, Image Size: 0xc000
15:17:18.2342249	AdwreCleaner.exe	3984	Thread Create		SUCCESS	Thread ID: 2328
15:17:18.2820076	AdwreCleaner.exe	3984	Process Create	C:\Users\user\AppData\Local\6AdvCleaner.exe	SUCCESS	PID: 1984, Command line: "C:\Users\user\AppData\Local\6AdvCleaner.exe"
15:17:18.2820076	6AdvCleaner.exe	1984	Process Start		SUCCESS	Parent PID: 3984, Command line: "C:\Users\user\AppData\Local\6AdvCleaner.exe", Current directory: C:\..
15:17:18.2820133	6AdvCleaner.exe	1984	Thread Create		SUCCESS	Thread ID: 3680
15:17:18.2823943	AdwreCleaner.exe	3984	Load Image	C:\Users\user\AppData\Local\6AdvCleaner.exe	SUCCESS	Image Base: 0x2980000, Image Size: 0x2e000
15:17:18.2861874	AdwreCleaner.exe	3984	Thread Exit		SUCCESS	Thread ID: 3284, User Time: 0.000000, Kernel Time: 0.0156250
15:17:18.2862824	AdwreCleaner.exe	3984	Thread Exit		SUCCESS	Thread ID: 2844, User Time: 0.000000, Kernel Time: 0.0000000
15:17:18.2863665	AdwreCleaner.exe	3984	Thread Exit		SUCCESS	Thread ID: 3284, User Time: 0.000000, Kernel Time: 0.0000000
15:17:18.2864508	AdwreCleaner.exe	3984	Thread Exit		SUCCESS	Thread ID: 2328, User Time: 0.000000, Kernel Time: 0.0000000
15:17:18.2865370	AdwreCleaner.exe	3984	Thread Exit		SUCCESS	Thread ID: 3165, User Time: 0.000000, Kernel Time: 0.1093750
15:17:18.2903705	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x759e0000, Image Size: 0x2e000
15:17:18.2910583	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77ae0000, Image Size: 0x19000
15:17:18.2921928	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\mscoree.dll	SUCCESS	Image Base: 0x7ef2e2000, Image Size: 0x9f000
15:17:18.2923078	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\kernbase.dll	SUCCESS	Image Base: 0x779e0000, Image Size: 0x1f000
15:17:18.2924380	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7effd70000, Image Size: 0x6e000
15:17:18.2940127	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x7effd20000, Image Size: 0xb0000
15:17:18.2941017	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\msvcr7.dll	SUCCESS	Image Base: 0x7effd10000, Image Size: 0x9f000
15:17:18.2949975	6AdvCleaner.exe	1984	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7effd0000, Image Size: 0x1f000

Figura 2: Azioni su processi e Thread

2.3 Modifiche del Registro

AdwCleaner ha effettuato diverse modifiche al registro di sistema, aggiungendo e modificando chiavi e valori, principalmente per garantire la propria persistenza nel sistema e tracciare le proprie attività.

Le modifiche al registro sono state osservate utilizzando RegShot. Le principali modifiche includono:

- Chiavi aggiunte:** Il malware ha creato chiavi nel registro per tracciare le proprie attività e garantire l'avvio automatico all'accensione del sistema.
- Valori eliminati:** Alcuni valori del registro sono stati eliminati per nascondere le tracce delle sue operazioni.
- Valori aggiunti e modificati:** Sono stati aggiunti e modificati valori per configurare la traccia delle proprie operazioni e garantirne la persistenza.

Le modifiche al registro indicano che il malware è progettato per resistere alle rimozioni semplici e per mantenere una traccia delle sue attività nel sistema infetto.

```
[+] cat CS04241T/UNIT_3/week10/S10L2/compare_reghost.txt
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/7/30 13:15:36 , 2024/7/30 13:19:48
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 3
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASMANCS
HKU\S-1-5-21-3771313050-58785377-345263501-1001\Software\AdwCleaner

-----
Values deleted: 2
HKU\S-1-5-21-3771313050-58785377-345263501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\{C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Wireshark.lnk: 0x00000001
HKU\S-1-5-21-3771313050-58785377-345263501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\{C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Wireshark.lnk: 0x00000001

-----
Values added: 29
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\MaxFileSize: 0x00100000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\Directory: "%windir%\tracing"
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASMANCS\EnableConsoleTracing: 0x00000000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASMANCS\FileTracingMask: 0xFFFF0000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKLM\Software\Microsoft\Tracing\AdwCleaner_RASMANCS\MaxFileSize: 0x00100000
```

Figura 3: Modifiche al registro

2.4 Profilazione del Malware

In base alle azioni osservate e alla correlazione tra operazioni e percorsi, è possibile profilare il comportamento del malware AdwCleaner:

- **Persistenza:** Il malware modifica le impostazioni del registro per garantire l'avvio automatico ad ogni avvio del sistema. Questo è evidente dalle chiavi aggiunte nel registro che configurano l'esecuzione automatica del malware.
- **Evasione:** Il malware elimina valori del registro e utilizza tecniche di caricamento di immagini non convenzionali per evitare la rilevazione da parte di strumenti di sicurezza. Le operazioni di lettura e creazione di file in directory di sistema come C:\Windows\Prefetch e C:\Windows\System32 indicano tentativi di evitare la rilevazione e l'analisi.
- **Raccolta Informazioni:** Il malware legge e interroga file di sistema per raccogliere informazioni sull'ambiente in cui è eseguito. Le operazioni di query sui file di sistema suggeriscono che sta raccogliendo informazioni per adattare il suo comportamento in base all'ambiente specifico.
- **Esecuzione parallela:** Il malware crea thread multipli per eseguire operazioni simultanee, aumentando l'efficienza delle sue operazioni malevoli. La creazione di thread aggiuntivi e l'avvio di processi indicano una struttura di esecuzione complessa, progettata per massimizzare l'efficienza delle sue attività dannose.

AdwCleaner è un malware sofisticato progettato per garantire la propria persistenza e raccogliere informazioni dal sistema infetto. Le sue operazioni sul file system, sui processi e sulle modifiche del registro evidenziano un comportamento tipico di malware avanzati, con tecniche di evasione e persistenza ben definite.