



# **ESERCITAZIONE**

**S10 - L2**



MICHELANGELO BORROMEO

# TRACCIA

In base al Malware  [AdwCleaner](#) fornito:

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

# MALWARE ANALYSIS

Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)

Una volta avviato **Process Monitor** (Procmon)

Filtrando la ricerca con il nome **6AdwCleaner.exe** (Malware)



Siamo riusciti a unificare tutte le operazioni che il programma in questione ha eseguito, troveremo per la maggior parte dei casi:

**ReadFile**

**RegQueryKey**

**RegOpenkey**

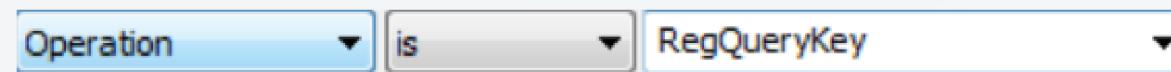
Process Monitor - Sysinternals: www.sysinternals.com

14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 773.120, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 756.736, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 735.744, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\System32\imm32.dll	SUCCESS	Offset: 132.608, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\System32\user32.dll	SUCCESS	Offset: 631.808, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7.528.960, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.771.392, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.677.184, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.628.032, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.726.336, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.709.952, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 13.810.688, ...
14:56:...	6AdwCleaner.exe	1484	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
14:56:...	6AdwCleaner.exe	1484	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\Kn...	NAME NOT FOUND	Desired Access: R...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 2.776.064, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.615.744, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.869.696, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.820.544, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 2.776.064, ...
14:56:...	6AdwCleaner.exe	1484	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
14:56:...	6AdwCleaner.exe	1484	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\Kn...	NAME NOT FOUND	Desired Access: R...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7.471.616, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 7.406.080, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 3.902.464, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 13.913.088, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 479.744, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 1.289.728, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 1.289.728, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 184.832, Le...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 9.262.592, ...
14:56:...	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 242.176, Le...
14:5C:	6AdwCleaner.exe	1484	ReadFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Offset: 994.916, Le...

# MALWARE ANALYSIS

Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)

per trovare le attività che hanno a che fare con la manipolazione delle chiavi di registro, andiamo ad immettere **RegOpenKey**, **RegQueryValue** come filtro di operazioni.



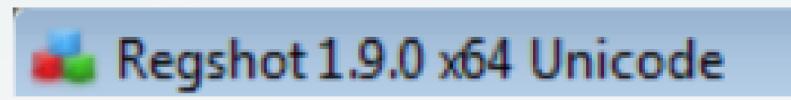
in questo caso **AdwCleaner** ha effettuato molte attività di manipolazione delle chiavi di registro.

6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusi...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKCU	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\System\CurrentControlSet\servic...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\System\CurrentControlSet\servic...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\System\CurrentControlSet\servic...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\System\CurrentControlSet\servic...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\System\CurrentControlSet\servic...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM\System\CurrentControlSet\servic...	SUCCESS
6AdwCleaner.exe	3304	RegQueryKey	HKLM	SUCCESS

# MALWARE ANALYSIS

## Modifiche del registro dopo il malware (le differenze)

Con il Software Regshot siamo riusciti a scovare diverse operazioni: Modifiche effettuate durante l'esecuzione del programma.



```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/7/30 12:35:15 , 2024/7/30 12:36:10
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 3
-----
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\software\AdwCleaner

-----
Values added: 16
-----
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\Directory: "%windir%\tracing"
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\Directory: "%windir%\tracing"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F4174
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F4174
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Run\AdwCleaner: ""C:\Users\user\AppData\Local\6AdwClea
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner\id: "0"
```

# MALWARE ANALYSIS

```
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32  
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANS  
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner
```

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASAPI32

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASMANS

HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner

**Come possiamo notare al lancio del malware sono state aggiunte 3 Hkeys con le seguenti caratteristiche:**

HKEY\_LOCAL\_MACHINE: include le impostazioni comuni per tutti gli utenti del sistema indipendentemente dalle loro preferenze

HKEY\_USERS: raggruppa le impostazioni di tutti gli utenti connessi al sistema

# MALWARE ANALYSIS

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASAPI32

HKLM\SOFTWARE\MICROSOFT\Tracing\6AdwCleaner\_RASAPI32

La chiave di **tracing** di solito contiene sottoclassi e valori che consentono il monitoraggio e la registrazione delle attività di rete di un'applicazione.

**RASAPI32** indica che la chiave potrebbe essere correlata alle chiamate all'API di Accesso Remoto (Remote Access Service), una libreria che gestisce le connessioni di rete.

# MALWARE ANALYSIS

**HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASMANCS**

**HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner\_RASMANCS**

La chiave di **tracing** di solito contiene sottoclassi e valori che consentono il monitoraggio e la registrazione delle attività di rete di un'applicazione.

**RASMANCS** suggerisce che il tracing è correlato al servizio Remote Access Connection Manager (RASMAN), il quale gestisce le connessioni di accesso remoto come VPN e dial-up.

# MALWARE ANALYSIS

**HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner**

**HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner**

contiene le impostazioni e i dati specifici di AdwCleaner per un utente specifico. Questa chiave è utile per memorizzare le preferenze dell'utente, i dati delle scansioni e altre configurazioni specifiche dell'applicazione.

# MALWARE ANALYSIS

Con il Software **Process Explorer**

Selezionando il Malware in questione e ispezionando le DLL possiamo trovare le seguenti librerie importate:

**kemel32.dll**

DLL client di Windows

**Kernel32.dll**

Fornisce funzioni principali per la gestione della memoria, processi e thread

**advapi32.dll**

API Windows 32 Base

**advapi32.dll**

contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

**msvcrt.dll**

Windows NT CRT DLL

**msvcrt.dll**

Fornisce le funzioni per eseguire applicazioni scritte in C e C++.

The screenshot shows the Process Explorer interface with a list of processes and their imported DLLs. The main table lists processes like procexp.exe, lsass.exe, explorer.exe, and several instances of 6AdwCleaner.exe. The bottom section shows a detailed view of the DLLs imported by one of the 6AdwCleaner.exe processes, including kernel32.dll, advapi32.dll, mscoree.dll, mscoreei.dll, mscoreui.dll, mscorelib.dll, mscorec.dll, and msctf.dll.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
procexp.exe	3.692 K	9.448 K	2212 Sysinternals Process Explorer	Sysinternals - www.sysinter...		
lsm.exe	2.352 K	4.556 K	496			
lsass.exe	< 0.01	3.748 K	10.804 K	488 Local Security Authority Proc...	Microsoft Corporation	
Intempts	< 0.01	0 K	0 K	n/a Hardware Intempts and DPCs		
explorer.exe	0.71	35.288 K	50.640 K	820 Esplora risorse	Microsoft Corporation	
dwm.exe	< 0.01	1.732 K	6.544 K	340 Gestione finestre desktop	Microsoft Corporation	
dinotify.exe		1.632 K	5.840 K	1136 Installazione dispositivo Win...	Microsoft Corporation	
csrss.exe	< 0.01	2.004 K	4.984 K	336		
csrss.exe	< 0.01	2.080 K	6.652 K	392		
audiogd.exe		15.540 K	16.240 K	2584		
6AdwCleaner.exe	< 0.01	37.200 K	39.656 K	576 AdwareBooC		
6AdwCleaner.exe	< 0.01	33.352 K	31.716 K	4024 AdwareBooC		
6AdwCleaner.exe	< 0.01	34.408 K	31.644 K	3304 AdwareBooC		

Handles	DLLs	Threads

Name	Description	Company Name	Path
imageres.dll	Windows Image Resource	Microsoft Corporation	C:\Windows\System32\imageres.dll
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll
IPHLPAPI.DLL	API helper IP	Microsoft Corporation	C:\Windows\System32\IPHLPAPI.DLL
kemel32.dll	DLL client di Windows NT BASE A...	Microsoft Corporation	C:\Windows\System32\kemel32.dll
KernelBase.dll	DLL client di Windows NT BASE A...	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
KernelBase.dll.mui	DLL client di Windows NT BASE A...	Microsoft Corporation	C:\Windows\System32\it-IT\KernelBase.dll.mui
locale.nls			C:\Windows\System32\locale.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\Windows\System32\lpk.dll
mscoree.dll	Microsoft .NET Runtime Execution...	Microsoft Corporation	C:\Windows\System32\mscoree.dll
mscoreei.dll	Microsoft .NET Runtime Execution...	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\msc...
mscorlib.ni.dll	Microsoft Common Language Runt...	Microsoft Corporation	C:\Windows\assembly\NativeImages_v4.0.30319_64\msco...
mscorrc.dll	Microsoft .NET Runtime resources	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\msc...
msctf.dll	MSCTF Server DLL	Microsoft Corporation	C:\Windows\System32\msctf.dll