ESERCITAZIONE

S10 - L2

NET.
REBELS.

MICHELANGELO BORROMEO

TRACCIA

In base al Malware 

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 ANALISYS

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

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

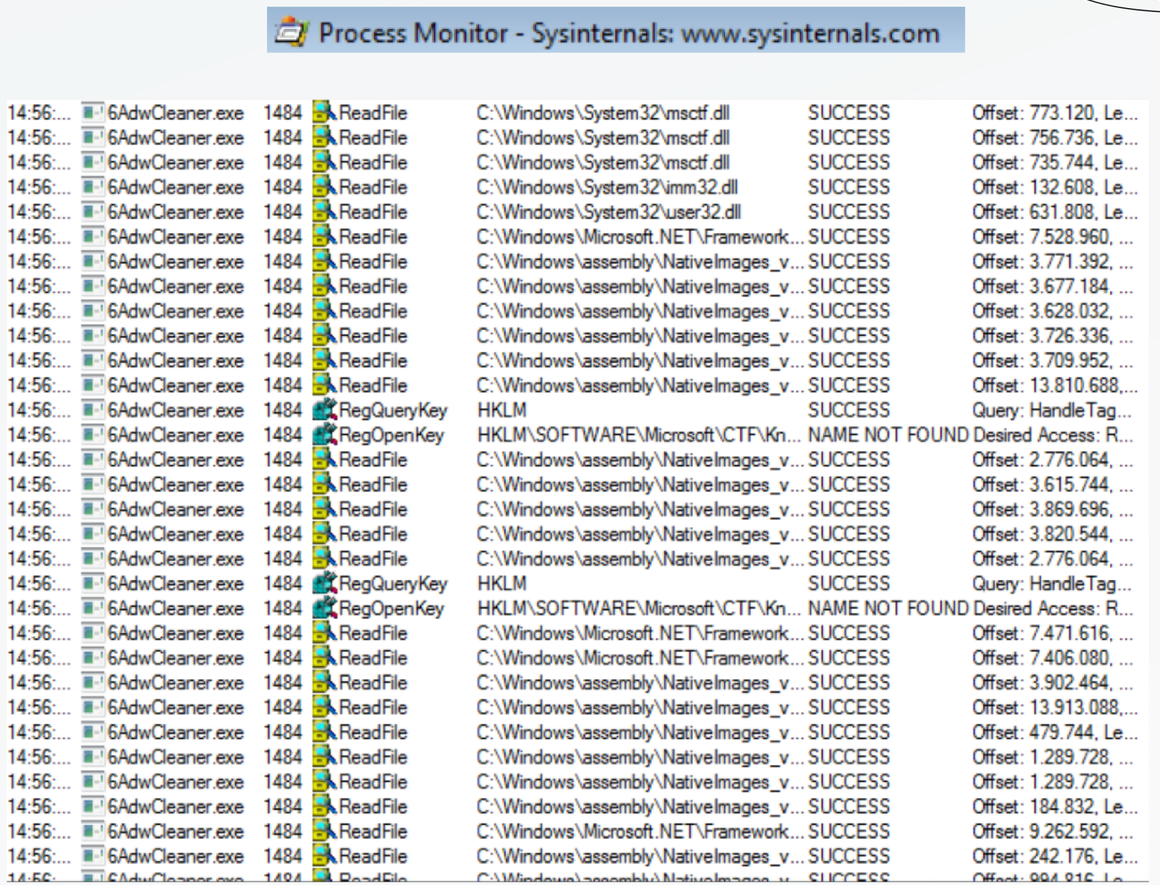
Filtrando la ricerca con il nome 6AdwCleaner.exe (Malware)

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

ReadFile

RegQueryKey

RegOpenkey



MALWARE ANALISYS

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.

Operation	is	RegQueryKey

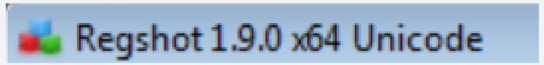
in questo caso **AdwCleaner** ha effettuato molte attività di manipolazione delle chiavi di registro.

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	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	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	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	SUCCESS

MALWARE ANALISYS

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\FileDirectory: "%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\FileDirectory: "%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 ANALISYS

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

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS

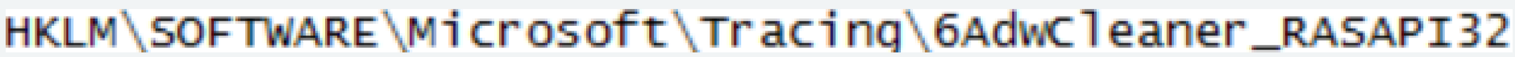
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AdwCleaner

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 ANALISYS



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 ANALISYS

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 ANALISYS

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 ANALISYS

Con il Software **Process Explorer**

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

Kernel32.dll
Fornisce funzioni principali per la gestione della memoria, processi e thread

advapi32.dll
contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

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