

Analisi Dinamica del Malware 1

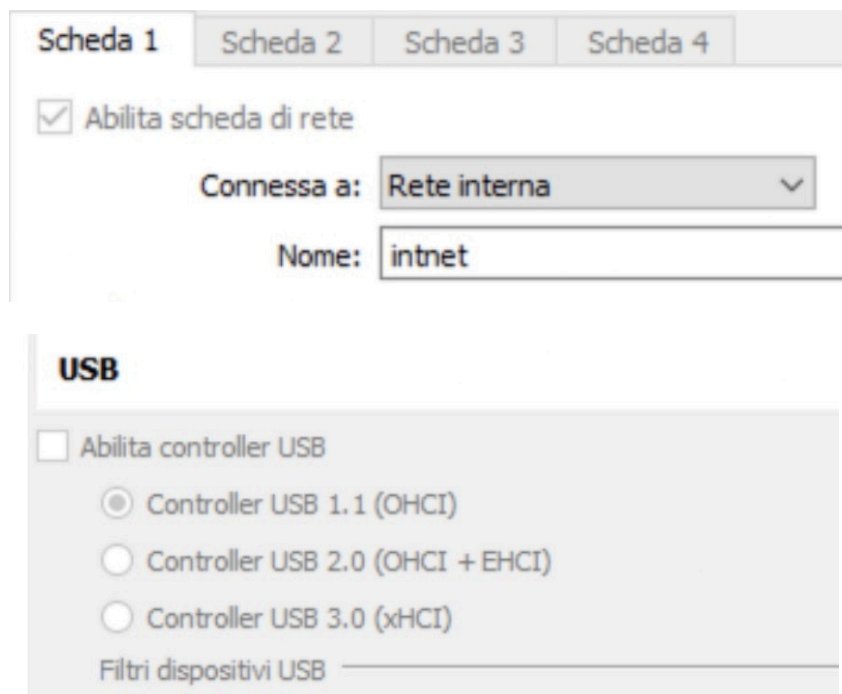
Traccia:

1. Configurare la macchina virtuale per l'analisi dinamica.
2. Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon).
3. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor.
4. Modifiche del registro dopo il malware (le differenze).

1. Configurazione macchina:

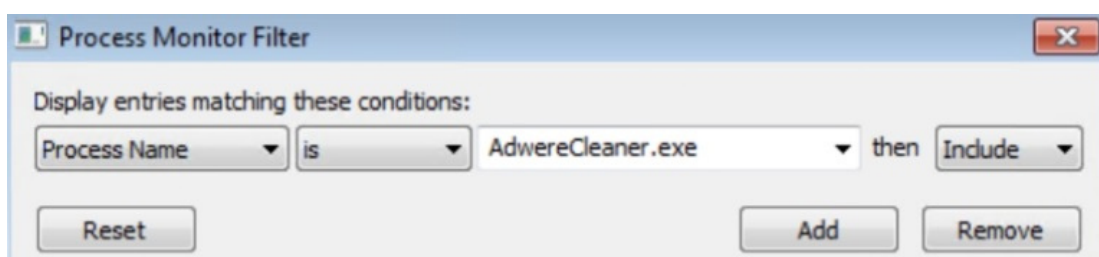
La macchina virtuale è configurata in modo da essere isolata dalla rete per prevenire la diffusione del malware.

È stata effettuata un'istantanea della macchina per poterla ripristinare facilmente.



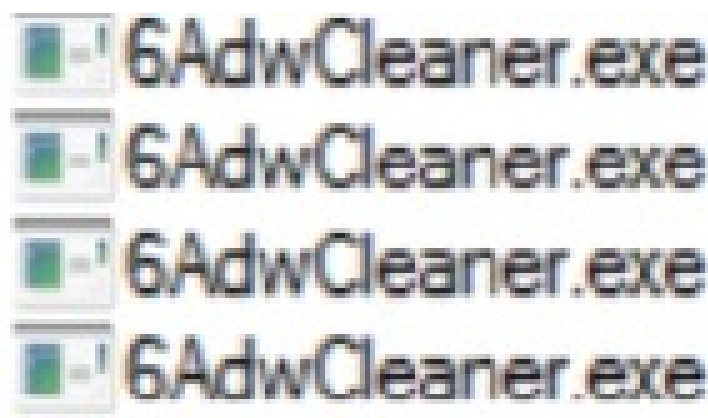
2. Azioni sul file system:

Utilizzando Process Monitor, è stato osservato che il malware esegue numerose operazioni di lettura e scrittura su file di sistema, identificando processi come AdwCleaner.exe e 6AdwCleaner.exe.



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:17:...	AdwareCleaner....	2484	Process Start		SUCCESS	Parent PID: 1404, ...
16:17:...	AdwareCleaner....	2484	Thread Create		SUCCESS	Thread ID: 2428
16:17:...	AdwareCleaner....	2484	Load Image	C:\Users\user\Desktop\MALWARE\Ad...	SUCCESS	Image Base: 0x400...
16:17:...	AdwareCleaner....	2484	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x773...
16:17:...	AdwareCleaner....	2484	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x775...
16:17:...	AdwareCleaner....	2484	Read File	C:	SUCCESS	Offset: 0, Length: 4...
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows\Prefetch\ADWERECLEA...	NAME NOT FOUND	Desired Access: G...
16:17:...	AdwareCleaner....	2484	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
16:17:...	AdwareCleaner....	2484	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
16:17:...	AdwareCleaner....	2484	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
16:17:...	AdwareCleaner....	2484	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16:17:...	AdwareCleaner....	2484	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
16:17:...	AdwareCleaner....	2484	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:17:...	AdwareCleaner....	2484	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 30/0...
16:17:...	AdwareCleaner....	2484	Close File	C:\Windows\System32\wow64.dll	SUCCESS	
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:17:...	AdwareCleaner....	2484	CreateFile Mapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:17:...	AdwareCleaner....	2484	CreateFile Mapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
16:17:...	AdwareCleaner....	2484	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x749...
16:17:...	AdwareCleaner....	2484	Close File	C:\Windows\System32\wow64.dll	SUCCESS	
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:17:...	AdwareCleaner....	2484	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 30/0...
16:17:...	AdwareCleaner....	2484	Close File	C:\Windows\System32\wow64win.dll	SUCCESS	
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:17:...	AdwareCleaner....	2484	CreateFile Mapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:17:...	AdwareCleaner....	2484	CreateFile Mapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
16:17:...	AdwareCleaner....	2484	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x748...
16:17:...	AdwareCleaner....	2484	Close File	C:\Windows\System32\wow64win.dll	SUCCESS	
16:17:...	AdwareCleaner....	2484	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...



Questi possono essere trovati tramite filtri:













Ho anche effettuato un'istantanea della macchina prima di eseguire il malware, per poterla ripristinare facilmente.

3. Azioni del malware sui processi e thread:




I filtri di Process Monitor hanno permesso di identificare i processi e thread creati o chiusi dal malware, mostrando un'attività intensa di creazione e terminazione di thread.

	Operation	is	Thread Create	Include
	Operation	is	Thread Exit	Include

16:17:...	 AdwareCleaner....	2484	 Process Start	SUCCESS	Parent PID: 1404, ...
16:17:...	 AdwareCleaner....	2484	 Process Create	SUCCESS	C:\Users\user\AppData\Local\6AdwCl... PID: 2400, Comma...
16:17:...	 6AdwCleaner.exe	2400	 Process Start	SUCCESS	Parent PID: 2484, ...
16:17:...	 AdwareCleaner....	2484	 Process Exit	SUCCESS	Exit Status: 0, User...
16:18:...	 6AdwCleaner.exe	2400	 Process Exit	SUCCESS	Exit Status: 0, User...

4. Modifiche del registro da parte del malware:

Per trovare le differenze nel registro da prima dell'esecuzione del malware a dopo ho utilizzato un tool opensource chiamato Regshot, ovviamente ho prima ripristinato lo stato della macchina grazie all'istantanea salvata prima.

	Regshot-x64-ANSI.exe	MIRROR	5 years ago
	Regshot-x64-Unicode.exe	MIRROR	5 years ago
	Regshot-x86-ANSI.exe	MIRROR	5 years ago

Questo tool permette di scansionare tutte le directory del sistema due volte e compararle, dando in output tutte le variazioni che ci sono state dalla prima alla seconda scansione.

```

-----
files added: 11
-----
:ProgramData\Microsoft\Windows Defender\Scans\History\Results\Resource\{D84C29D5-AF83-493B-BAB4-5599D00A9325}
:Users\All Users\Microsoft\Windows Defender\Scans\History\Results\Resource\{D84C29D5-AF83-493B-BAB4-5599D00A9325}
:Users\user\AppData\Local\6AdwCleaner.exe
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B8CC409ACDBF2A2FE04C56F2875B1FD6
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F4D9C889B7AEBFC4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B8CC409ACDBF2A2FE04C56F2875B1FD6
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F4D9C889B7AEBFC4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84
:Users\user\AppData\Roaming\Microsoft\Windows\Recent\1shot.hivu.tnk
:Users\user\Desktop\1shot.hivu

-----
files deleted: 2
-----
:Windows\Temp\TMP00000021D5C45BCFD0489823
:Windows\Temp\TMP000000231F33E17DD94F6D2F

-----
files [attributes?] modified: 13
-----
:ProgramData\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log
:Users\All Users\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log
:Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
:Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
:Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA748D0D0E0426DC8F8008506
:Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
:Users\user\NTUSER.DAT

```