

EPICODE-CS0124

S10/L2 - Pratica

Flaviano Sedici

Indice

1. Traccia	3
1.1. Definizioni	4
1.2. Analisi statica del Malware	4
1.2.1. Analisi delle librerie	4
1.2.2. Analisi con VirusTotal	4
1.3. Analisi dinamica del Malware	6
1.3.1. Configurazione dell'ambiente di analisi	6
1.3.2. Esecuzione del Malware	6
1.3.3. Esecuzione del Malware senza difese	7

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	26/03/2024

1. Traccia

Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito).

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- 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.

Suggerimento:

Per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione Create File su path noti (ad esempio il path dove è presente l'eseguibile del malware).

Creare istantanea da Virtualbox della macchina Windows 7 prima di avviare il malware per poter ripristinare in caso di problemi (o al limite fare il clone)

1.1. Definizioni

Malware Analysis

L'analisi del malware è il processo di esame approfondito dei software dannosi per comprendere le loro funzionalità, comportamenti e impatti sui sistemi informatici. Include l'identificazione delle caratteristiche del malware, l'analisi del codice sorgente, l'esecuzione in un ambiente sicuro per osservarne il comportamento e lo sviluppo di contromisure e soluzioni di sicurezza per mitigare o neutralizzare la minaccia. L'analisi del malware è essenziale per comprendere e contrastare le sempre più sofisticate minacce informatiche e proteggere gli utenti e le organizzazioni dai danni causati dal software dannoso.

Procmon

ProcMon, abbreviazione di Process Monitor, è un'utilità di monitoraggio del sistema per sistemi operativi Windows. Essa consente di monitorare in tempo reale l'attività dei processi, inclusi file system, registro di sistema, attività di rete e altro ancora. ProcMon è utilizzato per diagnosticare problemi di sistema, tracciare l'attività dei malware e analizzare le prestazioni del sistema.

Registro di sistema

Il registro di sistema è un database di sistema utilizzato dai sistemi operativi Windows per memorizzare configurazioni, impostazioni e informazioni sulle applicazioni, i dispositivi hardware e il sistema stesso. È organizzato in una struttura ad albero e contiene voci per varie componenti del sistema, consentendo agli utenti e ai programmi di accedere e modificare le impostazioni del sistema.

1.2. Analisi statica del Malware

1.2.1. Analisi delle librerie

Analizzando il malware fornito dalla traccia tramite l'utilizzo del software CFF Explorer, recandoci nella cartella "Import Directory", è possibile visionare l'elenco delle librerie che vengono richiamate dal malware.

KERNEL32.DLL - libreria di sistema di Windows che fornisce funzioni essenziali per la gestione della memoria, la gestione dei file, l'accesso ai dispositivi hardware e altre operazioni di basso livello. È fondamentale per il funzionamento stabile del sistema operativo Windows.

Dalla libreria in questione vengono richiamate 54 funzioni il cui censimento ci fa intuire che il malware tenta di ritirare molte informazioni inerenti alle attività dell'utente in tempo reale.

Tra le possibilità a nostra disposizione si può ipotizzare di posizionare il malware nella categoria Keylogger.

1.2.2. Analisi con VirusTotal


VirusTotal ci restituisce una traccia sulle attività del Malware, indirizzandoci verso l'ipotesi di un Trojan.




Malware_U3_W2_L2.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
00004548	00004548	001B	CloseHandle			
00004556	00004556	02BF	VirtualFree			
00004564	00004564	0218	ReadFile			
00004570	00004570	02B8	VirtualAlloc			
00004580	00004580	0112	GetFileSize			
0000458E	0000458E	0034	CreateFileA			
0000459C	0000459C	022C	ResumeThread			
000045AC	000045AC	0283	SetThreadContext			
000045C0	000045C0	02E9	WriteProcessMemory			
000045D6	000045D6	02BC	VirtualAllocEx			
000045E8	000045E8	013E	GetProcAddress			
000045FA	000045FA	0126	GetModuleHandleA			
0000460E	0000460E	021C	ReadProcessMemory			
00004622	00004622	0167	GetThreadContext			
00004636	00004636	0044	CreateProcessA			
00004648	00004648	00B6	FreeResource			
00004658	00004658	0295	SizeofResource			
0000466A	0000466A	01D5	LockResource			
0000467A	0000467A	01C7	LoadResource			
0000468A	0000468A	00A3	FindResourceA			

Malware_U3_W2_L2.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
0000469A	0000469A	0159	GetSystemDirectoryA			
000046B0	000046B0	0296	Sleep			
000046C6	000046C6	00CA	GetCommandLineA			
000046D8	000046D8	0174	GetVersion			
000046E6	000046E6	007D	ExitProcess			
000046F4	000046F4	029E	TerminateProcess			
00004708	00004708	00F7	GetCurrentProcess			
0000471C	0000471C	02AD	UnhandledExceptionFilter			
00004738	00004738	0124	GetModuleFileNameA			
0000474E	0000474E	00B2	FreeEnvironmentStringsA			
00004768	00004768	00B3	FreeEnvironmentStringsW			
00004782	00004782	02D2	WideCharToMultiByte			
00004798	00004798	0106	GetEnvironmentStrings			
000047B0	000047B0	0108	GetEnvironmentStringsW			
000047CA	000047CA	026D	SetHandleCount			
000047DC	000047DC	0152	GetStdHandle			
000047EC	000047EC	0115	GetFileType			
000047FA	000047FA	0150	GetStartupInfoA			
0000480C	0000480C	019D	HeapDestroy			
0000481A	0000481A	019B	HeapCreate			

Malware_U3_W2_L2.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
000047CA	000047CA	026D	SetHandleCount			
000047DC	000047DC	0152	GetStdHandle			
000047EC	000047EC	0115	GetFileType			
000047FA	000047FA	0150	GetStartupInfoA			
0000480C	0000480C	019D	HeapDestroy			
0000481A	0000481A	019B	HeapCreate			
00004828	00004828	019F	HeapFree			
00004834	00004834	022F	RtlUnwind			
00004840	00004840	02DF	WriteFile			
0000484C	0000484C	0199	HeapAlloc			
00004858	00004858	00BF	GetCPInfo			
00004864	00004864	00B9	GetACP			
0000486E	0000486E	0131	GetOEMCP			
0000487A	0000487A	01A2	HeapReAlloc			
00004888	00004888	01C2	LoadLibraryA			
00004898	00004898	01E4	MultiByteToWideChar			
000048AE	000048AE	01BF	LCMapStringA			
000048BE	000048BE	01C0	LCMapStringW			
000048CE	000048CE	0153	GetStringTypeA			
000048E0	000048E0	0156	GetStringTypeW			

Analisi Statica - Funzioni



[Sign in](#)
[Sign up](#)

60

/71

Community Score

60/71 security vendors and 2 sandboxes flagged this file as malicious

Reanalyze

Similar

More

ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce

Size

52.00 KB

Last Modification Date

1 hour ago

EXE

Lab03-03.exe

peexe

checks user input

idle

detect-debug environment

persistence

armadillo

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY 27

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.explorerhijack/a09u3p

Threat categories

trojan

dropper

Family labels

explorerhijack

a09u3p

keylogger

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3

Dropper/Win32.Agent.R194628

Alibaba

TrojanSpy:Win32/KeyLogger.570e4f43

VirusTotal

In ogni caso notiamo come sia possibile identificare alcune azioni che il malware esegue all'interno del sistema tramite ProcMon.

Notiamo come provi a scrivere sul file system a seguito di alcune modifiche effettuate sul registro di sistema.

Inoltre è evidente che durante l'esecuzione del Malware vengono registrati degli errori "File locked with only readers" che sicuramente sono legati all'errore di esecuzione sopracitato.

Le modifiche registrate sul sistema da RegShot sono 348, mentre ApatDNS e Wireshark non ci forniscono alcun riscontro concreto.

```
Regshot 1.9.0 x64 unicode
Comments:
Datettime: 2024/3/26 13:36:42 , 2024/3/26 13:38:56
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 16
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\3\0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\92
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\92\Shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\92\Shell\{5C4F28B5-F869-4E84-8E60-F11D0B97C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\93
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\93\Shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\93\Shell\{5C4F28B5-F869-4E84-8E60-F11D0B97C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\3\0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\92\Shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\92\Shell\{5C4F28B5-F869-4E84-8E60-F11D0B97C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\93
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\93\Shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\93\Shell\{5C4F28B5-F869-4E84-8E60-F11D0B97C5C7}

-----
values deleted: 88
HKLM\SYSTEM\ControlSet001\services\BFE\Parameters\Policy\BootTimeFilter\{dc95b53e-01cf-4058-821d-350b3d0d4676}: 01 10 08 00 CC CC CC 98 00 00 00 00 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\services\BFE\Parameters\Policy\BootTimeFilter\{2dd96961-5757-434f-b617-34e732517c0e}: 01 10 08 00 CC CC CC A8 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).left: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).left: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).top: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).top: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).right: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).right: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).bottom: 0x0000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\Nodeslots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\Nodeslots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\WRUListEx: 0A 00 00 00 03 00 00 00 0B 00 00 00 01 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\WRUListEx: 0A 00 00 00 01 00 00 00 03 00 00 00 0B 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\WRUListEx: 03 00 00 00 00 00 00 00 02 00 00 00 01 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\WRUListEx: 00 00 00 00 03 00 00 00 02 00 00 00 01 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\WRUListEx: 00 00 00 00 02 00 00 00 01 00 00 00 00 FF FF
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\WRUListEx: 03 00 00 00 00 00 00 00 02 00 00 00 00 01 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).left: 0x00000014A
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).left: 0x0000000E4
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).top: 0x00000007E
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).top: 0x000000033
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).right: 0x000000574
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).right: 0x00000050E
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).bottom: 0x000000206
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\winPos1706x872x96(1).bottom: 0x00000028B

-----
Total changes: 348
-----
```

Risultati Regshot

1.3.3.Esecuzione del Malware senza difese

Per ovviare all'errore abbiamo provato ad eseguire nuovamente il malware eliminando tutte le difese di Windows (firewall, defender e controllo utente), spostando anche il malware eseguibile in altre cartelle con maggiori diritti di utente e addirittura facendolo partire come amministratore e in modalità di compatibilità con Windows XP service pack 2.

Sfortunatamente abbiamo rilevato che la modifica di tutti questi parametri non ha portato ai risultati sperati in quanto sembrano essere assenti alcune chiavi di registro che sono tipiche di Windows XP e non di Windows 7 (che è la macchina fornita dalla traccia).

Ne deduciamo quindi che l'architettura di Windows 7 non sia compatibile con il malware che se invece eseguito su una macchina Windows XP funziona correttamente.