

# EPICODE-CS0124 S10/L2 - Pratica

Flaviano Sedici



## Indice

accia	3
efinizioni	4
alisi statica del Malware	
1.Analisi delle librerie	2
2.Analisi con VirusTotal	
alisi dinamica del Malware	6
1.Configurazione dell'ambiente di analisi	6
2. Esecuzione del Malware	
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.

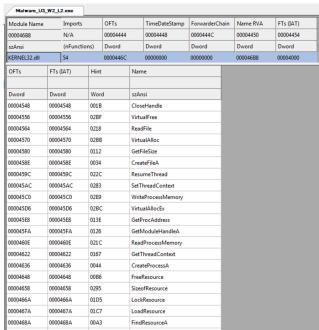
Dalla libreria in questione vengono richiamate 54 funzioni il cui censimento ci fa intuire che il malware tenta di ritirare molte informazioni inerenti alle attività dell'utente in tempo reale.

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

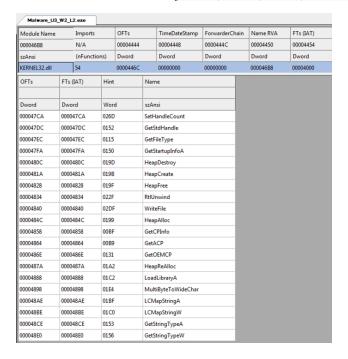
#### 1.2.2. Analisi con VirusTotal

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

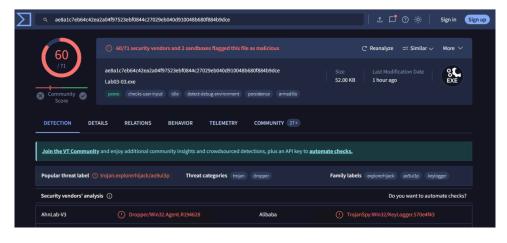




Module Name Imports   000046B8 N/A   szAnsi (nFunction   KERNEL32.dll 54		Imports	OFTs			TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
				00004444 Dword	00004448 Dword	0000444C Dword	00004450	00004454 Dword 00004000	
							Dword 000046B8		
		0000446C		5C 00000000	00000000	00000000			
OFTs	FTs	(IAT)	Hint		Nam	ie			
Dword	Dwo	Dword V		ord szAr		si	_		
0000469A	0000469A		0159		GetSystemDirectoryA				
000046B0	0046B0 000046B0		0296	Sleep					
000046C6 000046C6		00CA	A GetCommandLineA						
000046D8	000046D8		0174		GetV	GetVersion			
000046E6	000046E6		0070		ExitP	ExitProcess			
000046F4	000046F4		029E		TerminateProcess				
00004708	00004708		00F7		GetC	GetCurrentProcess			
0000471C	0000471C		02AE	)	Unha	andledExceptionFilter			
00004738	00004738		0124		GetN	ModuleFileNameA			
0000474E	0000474E		00B2		Freel	reeEnvironmentStringsA			
00004768	0004768 00004768		00B3		FreeEnvironmentStringsW		sW		
00004782 00004782		02D2		WideCharToMultiByte					
00004798	0000	4798	0106		GetEnvironmentStrings				
000047B0	0000	47B0	0108		GetE	GetEnvironmentStringsW			
000047CA	0000	47CA	0260		SetH	SetHandleCount			
000047DC	0000	47DC	0152		GetS	tdHandle			
000047EC	0000	47EC	0115		GetF	ileType			
000047FA	0000	47FA	0150		GetS	tartupInfoA			
0000480C	0000	480C	0190		Heap	Destroy			
0000481A	0000	481A	019B		Heap	Create			



Analisi Statica - Funzioni



**VirusTotal** 



#### 1.3. Analisi dinamica del Malware

#### 1.3.1. Configurazione dell'ambiente di analisi

Procediamo con la configurazione e l'apertura dei seguenti programmi:

- ProcMon
- Wireshark
- ApateDNS
- · RegShot

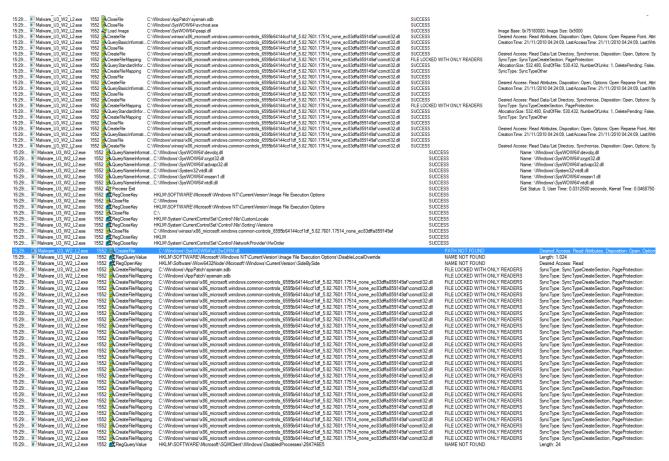
Proseguiamo con l'esecuzione del Malware.

#### 1.3.2. Esecuzione del Malware

Eseguendo il Malware, il sistema ci restituisce il seguente errore:



#### Errore di esecuzione



Risultati ProcMon



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 ApateDNS e Wireshark non ci forniscono alcun riscontro concreto.

```
| Replication | 1.0.0 | X64 Unicode | Comments | Commen
```

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.