PROGETTO SETTIMANALE

FUNDAMENTALS MALWARE ANALYSIS AND REVERSE ENGINEERING

EPICODE

Giovanni Pisapia

1. INDIVIDUARE LE LIBRERIE IMPORTATE

- **STEP 1:**
  Individuare le librerie importate dal file eseguibile (malware):

Per individuare le librerie di un malware o di un semplice file eseguibile, è necessario effettuare un'analisi statica del file sospetto utilizzando strumenti specifici come CFF Explorer. Questo tipo di analisi consente di identificare le librerie importate dal file, comprese quelle potenzialmente dannose.

Le librerie **kernel32.dll** e **wininet.dll** sono parti importanti del sistema operativo Windows che aiutano il computer a funzionare correttamente. Tuttavia, se un programma dannoso come un malware utilizza queste librerie, può arrecare danno al sistema compromesso.

- **Libreria kernel32.dll:** Questa libreria è fondamentale per il funzionamento del sistema e fornisce una serie di funzioni di basso livello. Un malware può utilizzare questa libreria per accedere, modificare e nascondere file nel sistema operativo Windows, oltre a iniettare codice malevolo in altri processi.
- **Libreria wininet.dll:** Un malware può sfruttare questa libreria per stabilire connessioni di rete non autorizzate, scaricare file dannosi e rubare informazioni sensibili dall'utente. Ad esempio, un malware può sfruttare la libreria wininet.dll per stabilire connessioni di rete non autorizzate e comunicare con server di comando e controllo remoti.

Malware_U3_W2_L5.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000065EC	N/A	000064DC	000064E0	000064E4	000064E8	000064EC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

2. INDIVIDUARE LE SEZIONI DEL MALWARE

- **STEP 2:**
  Individuare le sezioni importate dal file eseguibile (malware):

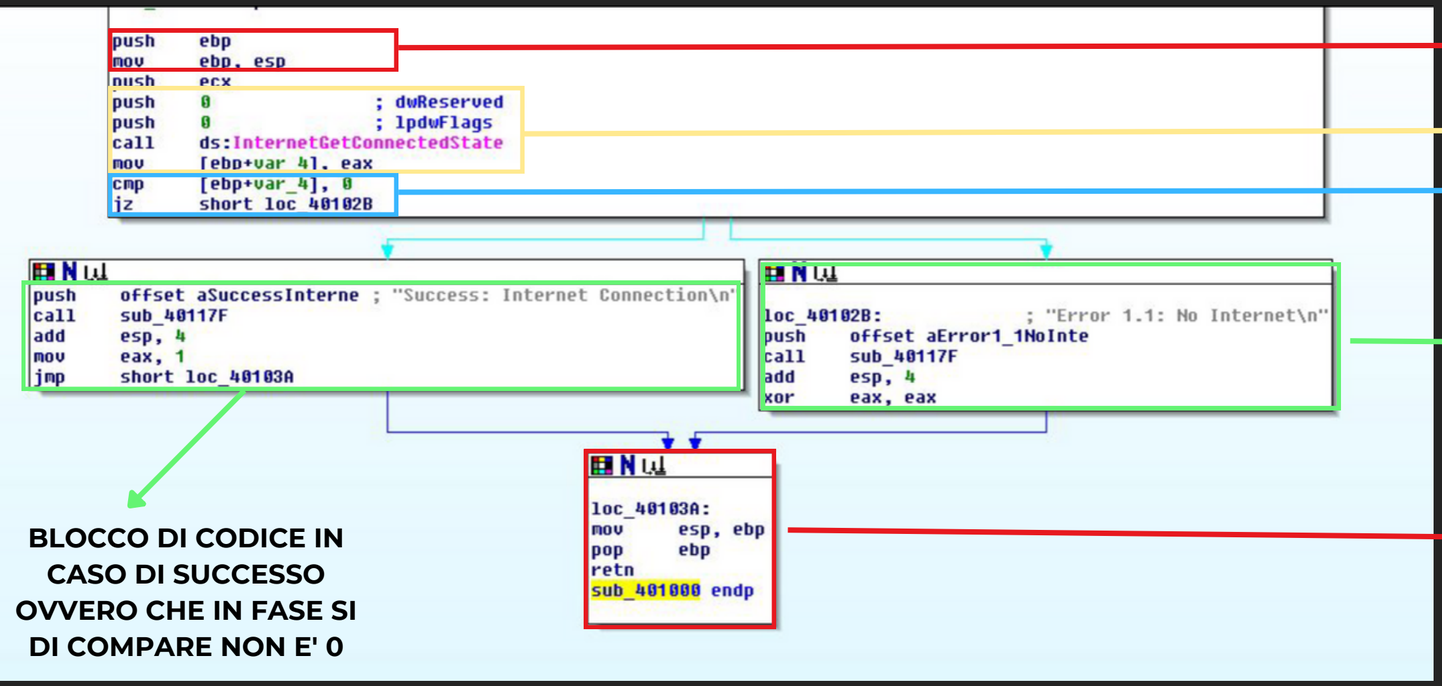
Per individuare le sezioni di un eseguibile o di un malware, utilizzeremo l'analisi statica di base con il tool CFF Explorer. In particolare, selezioneremo la sezione "Section Headers" per visualizzare le informazioni sulle sezioni del file. Questo ci permetterà di identificare le diverse parti del file, come il codice eseguibile, i dati, le risorse e altre sezioni rilevanti.

Le sezioni trovate nel malware sono:

- **.text:** Questa sezione contiene il codice eseguibile del malware. È la parte del file che viene interpretata e eseguita dall'operating system o dal processo in cui il malware è attivo.
- **.rdata:** Questa sezione contiene dati di sola lettura (read-only data) che possono essere utilizzati dal malware durante l'esecuzione. Ad esempio, potrebbe contenere stringhe di testo, costanti o tabelle di lookup.
- **.data:** Questa sezione contiene dati modificabili (read-write data) utilizzati dal malware durante l'esecuzione. Ad esempio, potrebbe contenere variabili, strutture dati o altre informazioni che vengono manipolate o aggiornate dal malware durante la sua attività.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
00000230	00000238	0000023C	00000240	00000244	00000248	0000024C	00000250	00000252	00000254
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

3. INDIVIDUARE COSTRUTTI NOTI



CREAZIONE DELLO STACK

INIZIALIIZZAZIONI DELLE VARIABILI-CHIAMATA FUNZIONE

BLOCCO CONDIZIONALE
IF

BLOCCO DI CODICE IN CASO DI ERRORE OVVERO CHE IN FASE SI DI COMPARE E' 0

BLOCCO DI CODICE IN CASO DI SUCCESSO OVVERO CHE IN FASE SI DI COMPARE NON E' 0

BLOCCO DI PULIZIA DELLO STACK E RITORNO

4. COMPORTAMENTO DELLA FUNZIONALITA IMPLEMENTATA

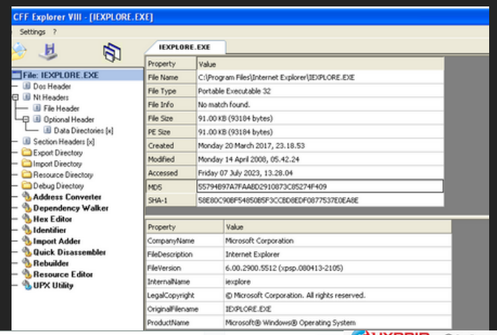
- Il codice sembra essere finalizzato a verificare lo stato di connessione a Internet utilizzando la funzione **InternetGetConnectedState** e a gestire i risultati in base a tale stato. Se lo stato di connessione è diverso da zero, viene chiamata la funzione **sub_40105F** e viene restituito il valore 1 come risultato. Altrimenti, viene chiamata la funzione **sub_40117F** e viene restituito il valore 0 come risultato.

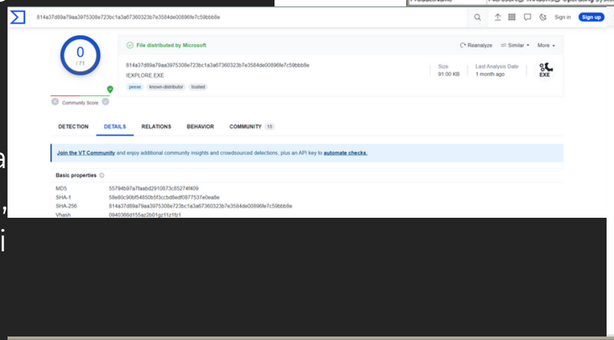
5. BONUS: SENIOR SOC

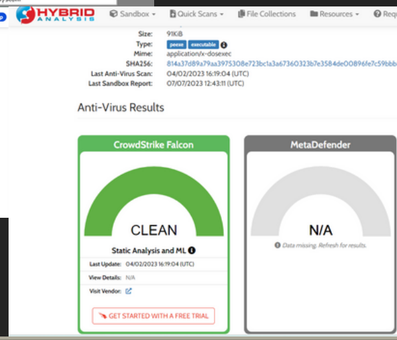
Come membro senior del SOC, comprendiamo l'importanza di indagare attentamente su file segnalati che potrebbero rappresentare una minaccia per la nostra azienda. Anche se a prima vista l'eseguibile sembra legittimo, non dobbiamo dare nulla per scontato. I malware potrebbero nascondersi creando eseguibili con lo stesso nome per confondersi tra i processi e nelle varie posizioni delle cartelle.

ANALISI STATICA:

- Per iniziare, eseguiamo un'analisi statica dell'eseguibile per cercare il suo hash utilizzando strumenti come CFF Explorer o comandi da riga di comando come "md5deep". Successivamente, procediamo ad analizzarlo con VirusTotal. Tuttavia, non possiamo basare unicamente la nostra valutazione sull'analisi con gli antivirus, poiché alcuni malware sono progettati per eludere la rilevazione.
- analisi basica stati cff explore
- Dalla analisi dinamica ho scoperto che l'eseguibile "IEXPLORE.EXE" importa diverse librerie, tra cui:
- Le librerie come msvcrt.dll, kernel32.dll, user32.dll, shlwapi.dll e shdocvw.dll importate da "IEXPLORE.EXE" sono librerie comuni necessarie per il funzionamento di molte applicazioni, compreso Internet Explorer. L'importazione di queste librerie è coerente con le applicazioni attendibili sviluppate da Microsoft da ricerche effettuate online.





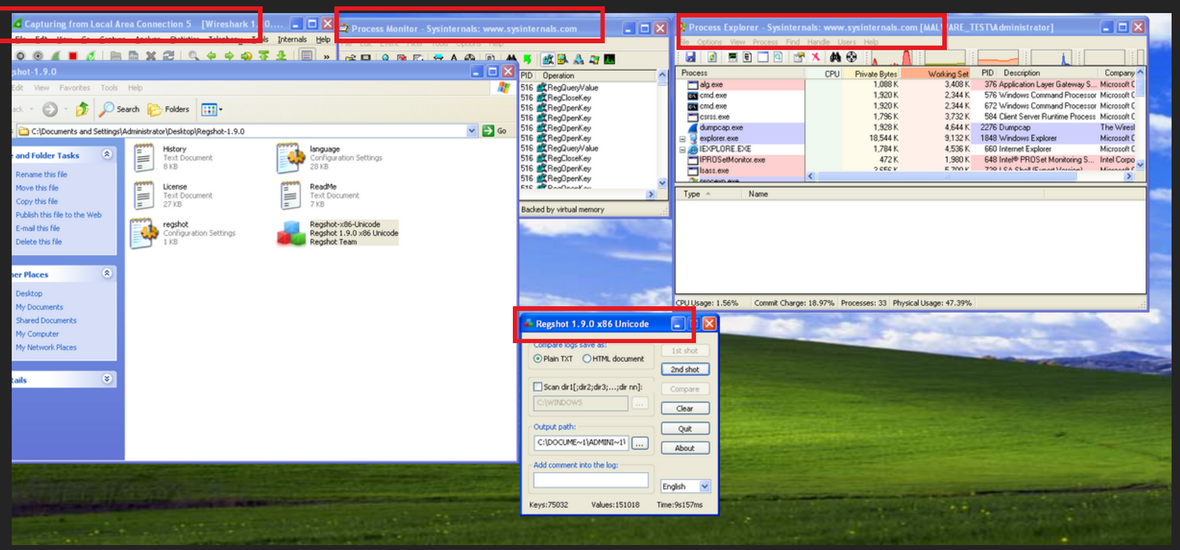


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
msvcrt.dll	1	00002830	FFFFFFFF	FFFFFFFF	0000284C	00001144
KERNEL32.dll	43	000026EC	FFFFFFFF	FFFFFFFF	00002B66	00001000
USER32.dll	16	000027EC	FFFFFFFF	FFFFFFFF	00002C8C	00001100
SHLWAPI.dll	16	000027A8	FFFFFFFF	FFFFFFFF	00002D30	000010BC
SHDOCVW.dll	2	0000279C	FFFFFFFF	FFFFFFFF	00002D3C	000010B0

5. BONUS: SENIOR SOC

ANALISI DINAMICA:

- Le best practice per eseguire un'analisi dinamica sicura sono le seguenti:
- Creare uno snapshot o una copia: Prima di eseguire l'analisi dinamica, crea uno snapshot o una copia della macchina o dell'ambiente di test. In questo modo, puoi ripristinare facilmente lo stato precedente dell'ambiente se si verificano problemi o infezioni durante l'analisi.
- Utilizzare un ambiente isolato come una sandbox: Esegui l'analisi dinamica all'interno di un ambiente isolato come una sandbox o una macchina virtuale. Questo previene la contaminazione del sistema principale e fornisce un ambiente controllato per l'esecuzione del file sospetto.
- Limitare l'accesso a Internet: Se possibile, disabilita l'accesso a Internet nell'ambiente di test. Questo aiuta a prevenire la comunicazione del malware con server di comando e controllo o l'infezione di altri sistemi all'interno della rete.
- Evitare cartelle condivise: Assicurati che non ci siano cartelle condivise tra la sandbox o la macchina virtuale e il sistema principale. Questo previene la possibilità di trasferimento accidentale del malware o di altri file dannosi tra i due ambienti.
- Per iniziare l'analisi dinamica, avviamo i seguenti strumenti disponibili: Process Explorer, RegShot, ProcMon e Wireshark. Successivamente, avviamo l'eseguibile del file sospetto e interrompiamo l'esecuzione di Wireshark e ProcMon. Salviamo una seconda istantanea con RegShot per confrontare le modifiche nel sistema prima e dopo l'esecuzione del file.
- Ora analizziamo tutte le informazioni avute dalla analisa basica e dinamica.



5. BONUS: SENIOR SOC

- Gentile signor Luca Sempronio, Grazie per la sua segnalazione. È sempre consigliabile segnalare file sospetti e non lasciare nulla al caso. Sulla base della sua segnalazione, ho effettuato un'analisi approfondita del file in questione. Dopo diverse analisi, ho constatato che il file sembra essere completamente legittimo. Ho verificato l'autenticità del file tramite firme digitali e durante l'esecuzione non ha mostrato comportamenti anomali, come un utilizzo eccessivo della CPU. Ho monitorato attentamente il suo comportamento simulando una connessione di rete, ma non ha tentato di connettersi a indirizzi IP o server remoti sconosciuti. Ho anche verificato se venivano apportate modifiche anomale alle chiavi di registro. Al momento, il file sembra essere completamente legittimo. Per garantire ulteriormente la sicurezza, sottoporremo il file al team di analisi malware per ulteriori verifiche.
- in allegato i file delle analisi