Report Tecnico: Estrazione di un Eseguibile da un PCAP + BONUS 1

Obiettivo: Identificare e analizzare un potenziale download di malware rilevato nel traffico HTTP per confermarne la natura, l'origine e l'avvenuto trasferimento.

Indice

Cosa sono tutti quei simboli mostrati nella finestra Follow TCP Stream? Sono rumore di connessione? Dati? Spiega. Ci sono alcune parole leggibili sparse tra i simboli. Perché sono lì?

punti, lettere a caso, parentesi sono il contenuto di un file eseguibile (.exe), non è rumore di connessione, ma qualcosa di molto più pericoloso.

Le parole scritte in "chiaro" servono al sistema operativo per far funzionare i files:
"This program cannot be run in DOS mode": è una frase standard che si trova in quasi tutti i file eseguibili di Windows (formato PE). Comunica ai vecchi computer che il programma è troppo moderno per loro.
msvcrt .dll NTDLL.dll KERNEL32.dll: Sono i nomi dei file di Windows che il programma usa per compiere azioni (come aprire file o connettersi a internet).

Dall'analisi della cattura traffico, è stato rilevato il download di un software malevolo: Richiesta `GET` per il file `W32.Nimda.Amm.exe`.

Domanda Sfida: Nonostante il nome W32.Nimda.Amm.exe, questo eseguibile non è il famoso worm. Per motivi di sicurezza, questo è un altro file eseguibile che è stato rinominato come W32.Nimda.Amm.exe. Usando i frammenti di parole visualizzati dalla finestra Follow TCP Stream di Wireshark, puoi dire quale eseguibile sia realmente?

Nonostante il nome `W32.Nimda.Amm.exe`, l'analisi delle stringhe interne rivela una realtà diversa:

Vero contenuto: La presenza di librerie come `kernel32.dll` e `msvcrt.dll` in chiaro indica che il file è in realtà il **Prompt dei comandi** (`cmd.exe`) **di Windows** rinominato.

Scopo del camuffamento: Questa tecnica viene usata per evadere i controlli superficiali dei firewall o per ingannare l'utente, fornendo all'attaccante una riga di comando remota (backdoor) una volta eseguito.

Pertanto, Il nome del file è un'etichetta inaffidabile; l'analisi del contenuto (payload) è l'unico modo per confermare la natura di una minaccia.

Estrazione di File Scaricati dal PCAP

Perché W32.Nimda.Amm.exe è l'unico file nella cattura?

Perché in questa funzione Wireshark elenca esclusivamente i file trasferiti tramite protocollo HTTP e non ci sono altre richieste `GET` nel flusso.

salvato il file e cambiato il nome alla cartella con W32.Nimda

```
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 32
-rw-r--r-- 1 root    root    2184 Feb 17 13:02 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Jun 17  2025 Desktop
drwxr-xr-x 3 analyst analyst 4096 Jun 18  2025 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jun 18  2025 lab.support.files
drwxr-xr-x 3 analyst analyst 4096 Jun 18  2025 scripts
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst    0 Feb 19 09:38 space.txt
drwxr-xr-x 2 analyst analyst 4096 Feb 25 04:56 W32.Nimda
drwxr-xr-x 5 analyst analyst 4096 Jun 18  2025 yay
[analyst@secOps ~]$
```

nel processo di analisi del malware quale sarebbe un probabile passo successivo per un analista di sicurezza?

1. Analisi dell'Ambito (Scoping)

Bisogna capire quanto è grave la situazione.

- **Identificazione della vittima:** risalendo all'indirizzo IP interno e al nome del dispositivo.
- **Verifica della ripetitività:** Si controllano i log per vedere se lo stesso IP esterno ha interagito con altri computer della rete o se lo stesso file è stato scaricato più volte.

2. Analisi dell'Host (Post-Compromissione)

Una volta che il file è stato scaricato (e abbiamo visto che il server ha risposto `200 OK`), bisogna verificare se il sistema sia compromesso.

- **l'Esecuzione è avvenuta?** Si controllano i log del sistema operativo (Event Viewer su Windows o Syslog su Linux) per vedere se il file è stato effettivamente avviato.
- **Persistenza:** Si cerca se il malware ha creato chiavi di registro o "cron jobs" per riavviarsi da solo.

3. Contenimento (Isolamento)

Se il file è stato eseguito:

- **Isolamento della macchina:** scollegare il computer dalla rete per evitare che il malware si diffonda (movimento laterale).
- **Blocco degli Indicatori di Compromissione (IoC):** inserire l'IP del server malevolo (`209.165.202.133`) e l'hash del file nella "blacklist" del firewall e dell'antivirus aziendale.

4. Eradicazione e Recupero

- **Pulizia:** Rimozione del file e ripristino dei sistemi da un backup pulito.
- **REPORT:** Si scrive il report finale per spiegare come il malware è entrato e come evitare che accada di nuovo.
