S9-E2 **Umberto Valentini**

MALWARE ANALYSIS

Nel progetto odierno è stata richiesta l'analisi di un malware relativamente pericoloso chiamato **calcolatriceinnovativa.exe** (CALC.EXE), individuato all'interno di una VM con Windows 10 Pro. L'analisi del malware è stata condotta seguendo due approcci complementari: **Static Analysis** e **Dynamic Analysis**.

Static Analysis

L'analisi statica consente di esaminare il malware senza eseguirlo, attraverso strumenti specifici. Di seguito, i dettagli delle tecniche adottate:

VirusTotal

VirusTotal è un servizio di Alphabet che permette l'analisi di file sospetti confrontandoli con oltre 70 database antivirus.

+ **Procedura:** Il malware è stato caricato su VirusTotal per eseguire una scansione.
+ **Risultati:** Il file è stato segnalato come malevolo in 59 database, con classificazioni come:
    - **Trojan/CobaltStrike**
    - **Win32:SwPatch (wrm)**
    - **Backdoor con payload meterpreter**

VirusTotal ha anche mostrato che il malware:

+ Invita traffico tramite **TCP** verso IP pubblici sconosciuti (porte **443** e **80**).
+ Presenta un pattern di memoria collegato all'indirizzo **192.168.1.80:4444**, suggerendo una possibile **connessione reverse TCP**, tipica di una backdoor.

MalwareBazaar

MalwareBazaar è una piattaforma gestita da Abuse.ch per la raccolta e condivisione di campioni di malware.

+ **Procedura:** È stato fornito l'hash del file recuperato da VirusTotal.
+ **Risultati:** Conferma che il malware è un file eseguibile (.exe). Sono state recuperate informazioni aggiuntive, tra cui l'utilizzo di **Shikata_ga_nai**, un encoder avanzato per offuscare il codice.

CFF Explorer

CFF Explorer è uno strumento avanzato per l'analisi di file PE (Portable Executable) su Windows.

+ **Analisi:** Il file, identificato come eseguibile (firma **MZ**), è stato esaminato per verificare la presenza di dipendenze critiche tramite il **Dependency Walker**. Sono state individuate 7 librerie principali:
- **SHELL32.dll** (interazione con la shell Windows)
- **Msvcrt.dll** (funzioni runtime standard C/C++)
- **ADVAPI32.dll** (manipolazione della sicurezza)
- **KERNEL32.dll** (funzioni di base del sistema operativo)
- **GDI32.dll** (funzioni grafiche)
- **USER32.dll** (gestione di finestre e input utente)
+ **Conclusioni:** È stato verificato che il malware non possa eseguire operazioni critiche come la modifica dei registri di Windows o connessioni non autorizzate.

Dynamic Analysis

L'analisi dinamica è stata condotta eseguendo il malware in un ambiente controllato (sandbox) per osservare il suo comportamento.

Cuckoo Sandbox

Cuckoo è una sandbox open-source per l'analisi di malware.

+ **Procedura:** Il file è stato caricato su Cuckoo per l'osservazione del suo comportamento.
+ **Risultati:**
    - Confermata la presenza di attività sospette, come la tentata connessione TCP verso **192.168.1.80:4444**.
    - Identificata una possibile connessione Metasploit all'IP privato.

Analisi Avanzata con Procmon

+ **Configurazione:** Il malware è stato eseguito in una VM Windows 10 Pro isolata, senza connessione a Internet o comunicazione bidirezionale con altre macchine.
+ **Osservazioni:**
    - Il malware ha creato processi multipli identificati tramite **Procmon**.
    - Ha tentato connessioni agli IP e alle porte precedentemente individuati, incluse **192.168.1.80:4444**.
+ **Test con Metasploit:** Dopo aver riattivato l'accesso a Internet, tramite una macchina **Kali Linux**, è stato configurato Metasploit in ascolto sulla porta **4444**. La connessione è stata stabilita, confermando la natura backdoor del malware.

Conclusioni

L'analisi combinata ha permesso di individuare le seguenti caratteristiche del malware:

- **Tipologia:** Probabile backdoor con funzionalità Trojan.
- **Comportamento:** Tentativi di connessione TCP a IP pubblici e privati, creazione di processi multipli.
- **Tecniche avanzate:** Uso di encoder come **Shikata_ga_nai** per offuscare il codice.

- **Criticità:** Il malware utilizza dipendenze di sistema, ma non sono state individuate operazioni critiche sui registri di sistema o funzionalità di cancellazione/modifica dei file.

L'uso di strumenti come VirusTotal, MalwareBazaar, CFF Explorer, Cuckoo, e Procmon ha dimostrato l’efficacia di un approccio integrato nell’analisi di malware.