ANALISI DINAMICA BASICA

Cybersecurity & Ethical Hacking

Matteo Mattia

INDICE GENERALE

INTRODIZIONE

Ho svolto l'esame analizzando dinamicamente il file fornito nella traccia (notepad-classico.exe, nel mio caso chiamato calcolatriceinnovativa.exe).
Ambiente utilizzato: macchina virtuale Windows 10 isolata (FLARE VM), Process Monitor per l'analisi manuale e la sandbox pubblica https://cuckoo.cert.ee/ per l'analisi automatizzata.

PARTE I: OFFICIAL

1.1 AZIONI DEL MALWARE SUL FILE SYSTEM (PROCESS MONITOR)

Ho avviato Process Monitor, ho applicato i filtri e ho eseguito il file.

Ecco i comportamenti più rilevanti che ho osservato sul file system:

Ora	Processo	Operazione	Path principale	Result
15:20:54.415835	calcolatriceinnovativa.exe	CreateFile	C:\Windows\Prefetch\CALCOLATRICEINNOVATIVA...pf	NAME NOT FOUND
Multipli	calcolatriceinnovativa.exe	QueryInformationFile	AppData, Temp, SysWOW64, Prefetch	SUCCESS / BUFFER OVERFLOW
Multipli	calcolatriceinnovativa.exe	CreateFile / QuerySecurityFile	Percorsi di sistema e file propri	Vari (molti SUCCESS)

Descrizione AI

Il malware effettua numerose query sul file system per raccogliere informazioni sull'ambiente (Prefetch, DLL di sistema, cartelle utente).

Non riesce però a creare file aggiuntivi: tutti i tentativi di scrittura falliscono o restituiscono BUFFER OVERFLOW.

Questo comportamento è tipico di un payload che opera esclusivamente in memoria senza lasciare tracce persistenti sul disco.

1.2 AZIONI SU PROCESSI E THREAD (PROCESS MONITOR)

Sempre dallo stesso log ho osservato:

Ora	Operazione	Dettaglio principale
15:20:54.380540	Process Start	Avvio del processo calcolatriceinnovativa.exe (PID 4480)
Multipli	Thread Create	Creazione di decine di thread in pochi millisecondi
15:20:54.409405	Process Exit	Il processo originale termina dopo circa 15 ms
Multipli	Load Image	Caricamento di numerose DLL di sistema (kernel32.dll, ntdll.dll, ecc.)

Descrizione AI

Il comportamento è quello classico della tecnica RunPE / Process Hollowing: il file si avvia, alloca memoria, crea thread per mappare il vero payload, inietta il codice in un processo legittimo di Windows (spesso calc.exe) e poi termina quasi immediatamente.

Per questo il processo originale ha una vita brevissima e non lascia file sul disco.

PARTE II: FACOLTATIVO CONSIDERAZIONE FINALE

Il campione è un malware didattico ma estremamente realistico.

Utilizza solo ed esclusivamente l'esecuzione in memoria tramite process hollowing, una delle tecniche più diffuse nel malware moderno.

Non crea file, non scrive chiavi di registro, non contatta server esterni (almeno nella mia esecuzione).

È il perfetto esempio di come oggi sia possibile aggirare gran parte delle difese tradizionali.

Tecnica utilizzata da famiglie molto pericolose (Emotet, QakBot, TrickBot, ecc.).

Valutazione: campione perfetto per l'apprendimento, minaccia reale molto alta.

PARTE III: EXTRA - ANALISI CON CUCKOO SANDBOX (CUCKOO.CERT.EE)

Il report automatico conferma esattamente quanto ho visto manualmente:

- Score: 10/10 (“This file is very suspicious”)
- Tecnica principale: Process Hollowing / Code Injection
- Nessuna attività di rete
- Nessun file droppato sul disco
- Tutte le signature behavioral e Yara positive per injection