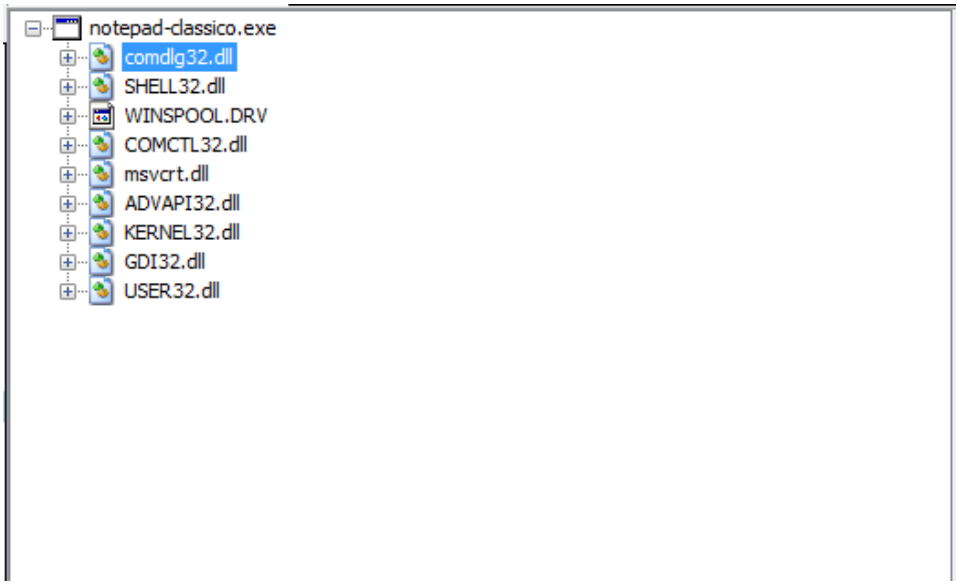
Analisi statica malware

Obiettivo

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse.
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di esse.

Analisi librerie

Tramite l'utilizzo del tool CFF Explorer andiamo ad analizzare le librerie che vengono importate dal programma di cui vogliamo effettuare la scansione.



1. **comdlg32.dll (Common Dialogs Library):** Questa libreria è responsabile della creazione delle finestre di dialogo comuni di Windows. Per un malware, è utile per creare finestre "Apri file" o "Salva file" (ad esempio, per ingannare l'utente e fargli scegliere dove salvare un file infetto o per cercare file da esfiltrare).
2. **SHELL32.dll (Windows Shell API Library):** È una libreria fondamentale che fornisce funzioni per interagire con la shell del sistema operativo. Un malware la usa spessissimo per compiti come:
    - Eseguire altri programmi o script (ShellExecute).
    - Manipolare file e cartelle (copiare, spostare, eliminare).
    - Creare collegamenti (spesso usati per la persistenza).
3. **WINSPOOL.DRV (Windows Print Spooler Driver):** Questa libreria gestisce le operazioni di stampa. Sebbene meno comune, un malware potrebbe usarla per:
    - Cercare di esfiltrare dati inviandoli a una stampante (fisica o virtuale).

    - Sfruttare vulnerabilità note nel servizio di print spooler per l'escalation dei privilegi (es. PrintNightmare).
4. **COMCTL32.dll (Common Controls Library):** Fornisce i controlli standard dell'interfaccia utente (GUI) come pulsanti, barre di stato, barre degli strumenti, ecc. Un malware che presenta un'interfaccia grafica (come un finto antivirus o un ransomware) la usa per costruire la sua finestra.
5. **msvcrt.dll (Microsoft C Runtime Library):** È la libreria C standard di Microsoft. Contiene funzioni base per la gestione della memoria (malloc, memcpy), la manipolazione di stringhe (strcpy, sprintf) e operazioni di I/O su file (fopen, fwrite).
6. **ADVAPI32.dll (Advanced Windows API Library):** Questa è una libreria **molto critica** per l'analisi malware. Fornisce accesso a funzioni avanzate relative alla sicurezza e al registro di sistema. Un malware la usa per:
    - **Modificare il Registro di Windows:** Creare chiavi per la persistenza (es. Run, RunOnce) e avviarsi automaticamente.
    - **Gestire i Servizi di Windows:** Creare, avviare o modificare servizi per eseguirsi in background.
    - **Gestire i privilegi:** Tentare di ottenere privilegi più alti (escalation dei privilegi).
7. **KERNEL32.dll (Core Windows API Library):** È il cuore pulsante di Windows. È la libreria più importante per un malware. Gestisce operazioni fondamentali a basso livello, tra cui:
    - Gestione dei processi e dei thread: Creare nuovi processi (CreateProcess), iniettare codice in altri processi (WriteProcessMemory, CreateRemoteThread).
    - Gestione della memoria: Allocare memoria (VirtualAllocEx).
    - Gestione dei file: Leggere, scrivere e creare file (CreateFile, ReadFile, WriteFile).
    - Caricamento di altre librerie: Caricare altre DLL in memoria (LoadLibrary).
8. **GDI32.dll (Graphics Device Interface):** Gestisce le funzioni grafiche, come disegnare sullo schermo, manipolare immagini e testo. Un malware come uno *screen scraper* o un *keylogger* potrebbe usarla per:
    - Catturare screenshot (BitBlt).
    - Disegnare finestre o messaggi ingannevoli sullo schermo
9. **USER32.dll (User Interface Library):** Un'altra libreria fondamentale, gestisce tutti gli aspetti dell'interfaccia utente. Un malware la usa per:
    - Creare e gestire finestre (CreateWindow).

- Intercettare l'input dell'utente: Fondamentale per i **keylogger** (usando funzioni come GetAsyncKeyState o SetWindowsHookEx).
- Mostrare messaggi all'utente: Creare finestre di dialogo o finti messaggi di errore (MessageBox).

Analisi approfondita

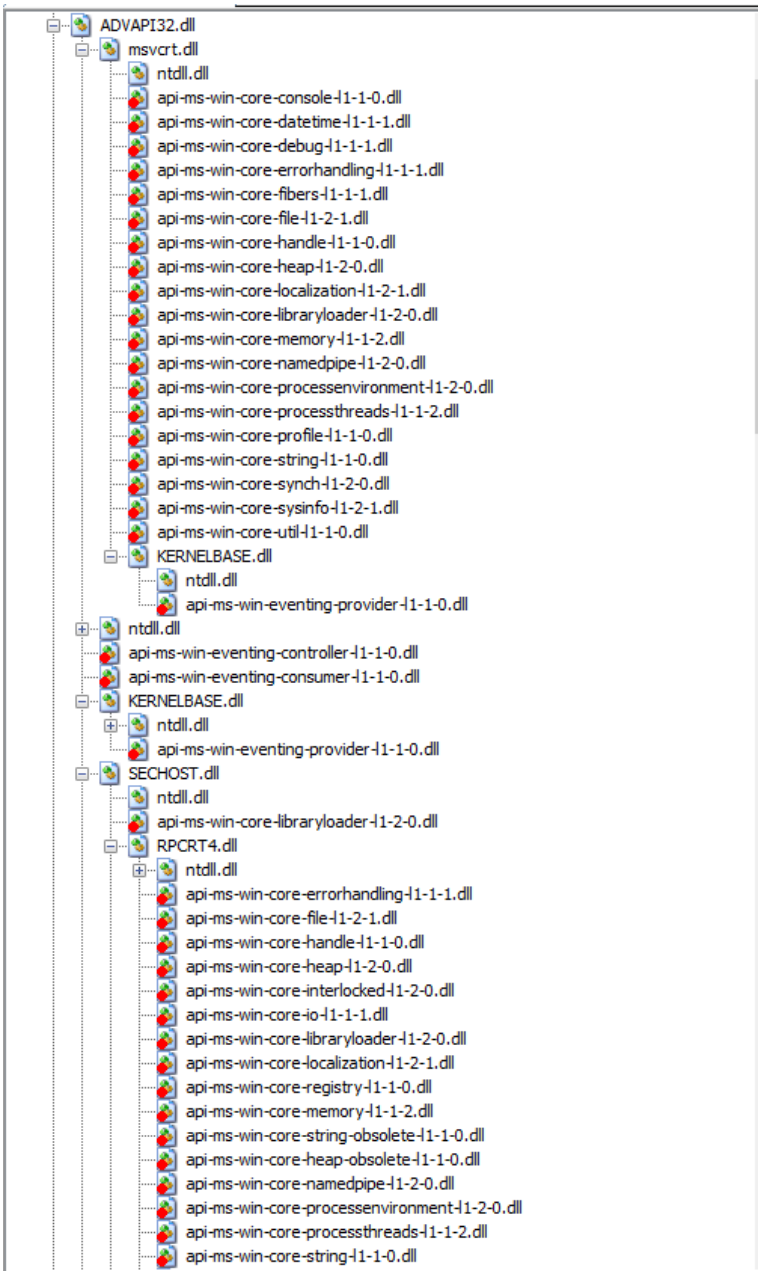
Analizzando i nomi di questi "pacchetti" (api-ms-win-core...), possiamo dedurre le *categorie* di funzionalità a cui il malware è interessato

1. Manipolazione di Processi, Thread e Memoria

Sono presenti più riferimenti a :

- api-ms-win-core-processthreads-l1-1-2.dll (Creare nuovi processi (es. lanciare un altro malware))
- api-ms-win-core-memory-l1-1-2.dll (Allocare e scrivere in memoria (WriteProcessMemory, VirtualAllocEx), probabilmente in *altri* processi)
- api-ms-win-core-processsnapshot-l1-1-0.dll (Fare uno "snapshot" dei processi attivi, forse per cercare processi antivirus o browser in cui iniettare codice).

2. Persistenza e Anti-Analisi



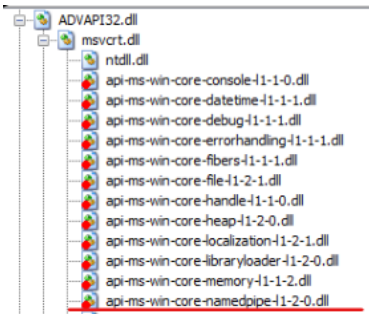
Questi sono indizi molto forti:

- api-ms-win-core-registry-l1-1-0.dll (Registry: Conferma quasi al 100% l'intenzione di modificare il Registro di Windows. Questo è il metodo N°1 per la persistenza)
- api-ms-win-core-synch-l1-2-0.dll (Synch (Sincronizzazione): Spesso i malware usano funzioni di sincronizzazione (come CreateMutex) per **assicurarsi che solo una copia di se stesso sia in esecuzione** sulla macchina. È anche una tecnica di anti-analisi)

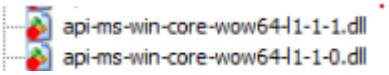
3. Comunicazione e Consapevolezza del Sistema

Qui le cose si fanno più avanzate:

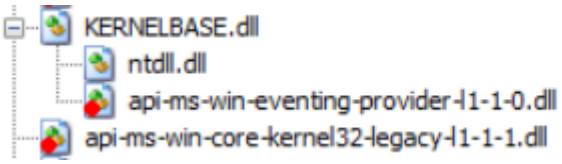
- api-ms-win-core-namedpipe-l1-2-0.dll



- RPCRT4.dll
- api-ms-win-core-wow64-l1-1-1.dll



- api-ms-win-eventing-provider-l1-1-0.dll



Cosa significa:

- **Named Pipe & RPC:** Questi sono usati per la **comunicazione tra processi (IPC)**. Potrebbe essere un malware modulare, dove un componente "dropper" comunica con un altro componente "worker". Oppure, potrebbe usarlo per comunicare con un processo che ha infettato.
- **WoW64:** Questo è *molto* interessante. Significa che il malware (che è a 32-bit) è "consapevole" di poter essere eseguito su un sistema operativo a 64-bit (Windows-on-Windows-64). Probabilmente contiene logica per comportarsi diversamente o trovare le cartelle di sistema corrette (SysWOW64, System32) a seconda dell'architettura.
- **Eventing Provider:** Questo pacchetto gestisce i log degli eventi di Windows. Un malware potrebbe usarlo per **cancellare le proprie tracce** dai log di sistema per non farsi scoprire.

4. **Scoperta Chiave: Crittografia**

- CRYPTBASE.dll
- bcryptPrimitives.dll

Il notepad-classico.exe sta importando librerie di **crittografia**. Un normale editor di testo non ha necessità di librerie di crittografia avanzate.

Questo suggerisce fortemente che il malware è:

1. **Un Ransomware:** Ha bisogno di queste librerie per generare chiavi e crittografare i file dell'utente.
2. **Uno Spyware/Trojan**: Usa la crittografia per nascondere le sue comunicazioni con un server di Comando e Controllo (C2), in modo che il traffico di rete non sia leggibile.
3. **Un Dropper**: Potrebbe avere un altro payload malevolo al suo interno in forma crittografata, e usa queste librerie per decifrarlo ed eseguirlo.

Import Address Table (IAT)

Analisi ADVAPI32.dll

ADVAPI32.dll	7	00040178	00000000	FFFFFFFF	0004068A	00001000
KERNEL32.dll	57	00040198	00000000	FFFFFFFF	0004070F	0000108C
GDI32.dll	24	00040280	00000000	FFFFFFFF	00040AF1	00001028
USER32.dll	74	000402E4	00000000	FFFFFFFF	00040C5F	00001188

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00040698	00040698	01EF	RegQueryValueExW
000406AC	000406AC	01CA	RegCloseKey
000406BA	000406BA	01D0	RegCreateKeyW
000406CA	000406CA	0139	IsTextUnicode
000406DA	000406DA	01EE	RegQueryValueExA
000406EE	000406EE	01E4	RegOpenKeyExA
000406FE	000406FE	01FC	RegSetValueExW

- RegCreateKeyW
- RegOpenKeyExA
- RegSetValueExW
- RegQueryValueExA
- RegCloseKey

Questo è il "pacchetto" completo per la manipolazione del Registro di Windows. Il malware ha la capacità di:

1. Aprire chiavi di registro esistenti (RegOpenKeyExA).

2. Creare nuove chiavi (RegCreateKeyW).
3. Impostare o modificare valori all'interno di quelle chiavi (RegSetValueExW).
4. Leggere valori esistenti (RegQueryValueExA).

Questo è il metodo più comune per stabilire la persistenza. Il malware userà quasi certamente queste funzioni per aggiungersi a una chiave di avvio automatico (come HKCU\Software\Microsoft\Windows\CurrentVersion\Run), assicurandosi di essere eseguito a ogni accensione del computer.

Analisi KERNEL32.dll

1. Gestione File (Potenziale Ransomware / Dropper)

- **CreateFileW**: Per creare nuovi file o aprire file esistenti.

- **WriteFile**: Per scrivere dati all'interno di un file.

- **ReadFile**: Per leggere dati da un file.

- **DeleteFileW**: Per cancellare file.

- **FindFirstFileW**: Per cercare file all'interno di una cartella.
- **GetFileAttributesW**: Per controllare le proprietà di un file (es. se è nascosto o di sola lettura).

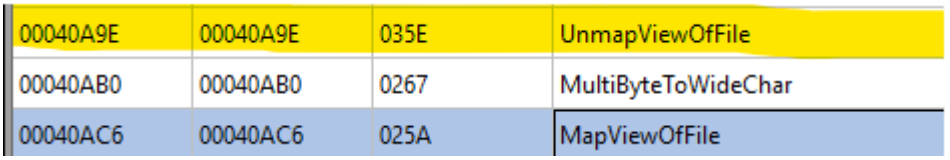
Analisi: Questa combinazione è estremamente pericolosa. Il malware può cercare file (FindFirstFileW), leggerli (ReadFile), scrivere al loro interno (WriteFile - ad esempio la versione crittografata) e infine cancellare l'originale (DeleteFileW). Combinato con le librerie di crittografia che abbiamo notato prima, questo profilo è altamente compatibile con un ransomware.

2. Iniezione di Codice e Tecniche Avanzate

- **CreateFileMappingW**

000407E2	000407E2	0051	CreateFileMappingW

- **MapViewOfFile**
- **UnmapViewOfFile**



00040A9E	00040A9E	035E	UnmapViewOfFile
00040AB0	00040AB0	0267	MultiByteToWideChar
00040AC6	00040AC6	025A	MapViewOfFile

Analisi: Questo è un set di funzioni avanzato. Non servono per la semplice lettura/scrittura di file, ma per mappare un file direttamente in memoria. Questa tecnica è un componente chiave del Process Hollowing: il malware avvia un processo legittimo in stato sospeso, "svuota" la sua memoria e vi mappa il proprio codice malevolo, per poi riprendere il processo. È una tecnica di evasione molto efficace per nascondersi.

3. Caricamento Dinamico e Anti-Analisi

- **LoadLibraryA**: Per caricare *altre* librerie (DLL) a runtime.

00040858	00040858	0244	LoadLibraryA

- **GetProcAddress**: Per trovare l'indirizzo di una funzione all'interno di una DLL caricata.

00040964	00040964	0198	GetProcAddress

Analisi: Questa è una tecnica di *stealth*. Invece di importare tutte le funzioni malevole all'avvio, il malware può caricare una DLL (magari una che ha appena scritto sul disco) e trovare le sue funzioni "al volo".

- **GetTickCount**:
- **QueryPerformanceCounter**

00040732	00040732	01D4	GetTickCount
00040742	00040742	0294	QueryPerformanceCounter

Analisi: Queste funzioni leggono l'orologio di sistema. Sono usate spesso in trucchi anti-debug e anti-sandbox. Il malware misura il tempo che impiega un'operazione; se è "troppo veloce" o "troppo lento" (tipico di un ambiente emulato), capisce di essere analizzato e termina la sua esecuzione per non farsi scoprire.

4. Gestione dei Processi

- **TerminateProcess**: Per "uccidere" forzatamente un altro processo.
- **GetCurrentProcess** / **GetCurrentProcessId**: Per ottenere informazioni su se stesso.

00040812	00040812	034A	TerminateProcess
00040826	00040826	013B	GetCurrentProcess

Analisi: TerminateProcess è una funzione aggressiva. È comunemente usata per **disabilitare software antivirus** o altri strumenti di analisi (come Task Manager o Wireshark) prima di iniziare l'attività malevola.

Analisi con VirusTotal e Considerazioni Finali

L'analisi statica (CFF Explorer) ci ha mostrato di cosa era capace il malware. L'analisi dinamica (VirusTotal "Behavior") ci mostra cosa fa effettivamente.

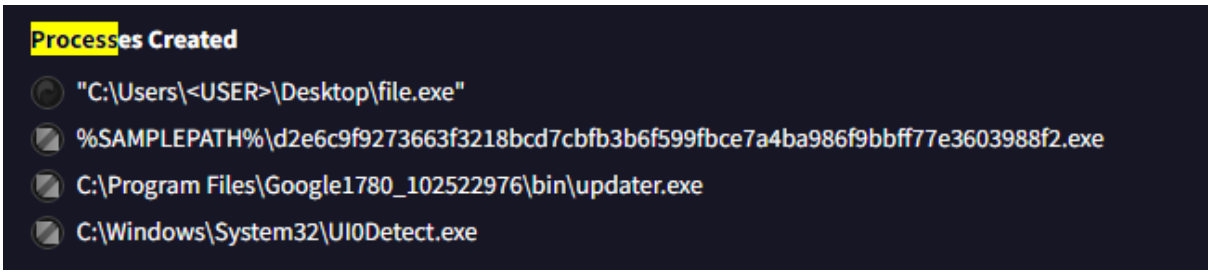
Il file notepad-classico.exe è un **Meterpreter stager/dropper**, un vettore d'infezione progettato per eseguire il payload principale di Metasploit (Meterpreter) e stabilire un controllo remoto.

Security vendors' analysis			Do you want to automate checks?
AhnLab-V3	Malware/Win32.Generic.C593931	Alibaba	Trojan:Win32/Meterpreter.c8d86815
AliCloud	Trojan:Win/Meterpreter.AA(dyn)	Antiy-AVL	Trojan/Win32.Meterpreter.a
Arcabit	Win32.Rozena.B	Arctic Wolf	Unsafe
Avast	Win32:MsfShell-H [Trj]	AVG	Win32:MsfShell-H [Trj]
Avira (no cloud)	TR/Patched.Gen	BitDefender	Win32.Rozena.B
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Exploit.Meterpreter-9777172-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.meterpreter
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Swrort.10	Elastic	Windows.Trojan.Metasploit

Il "Dropper": Creazione di Nuovi File Malevoli

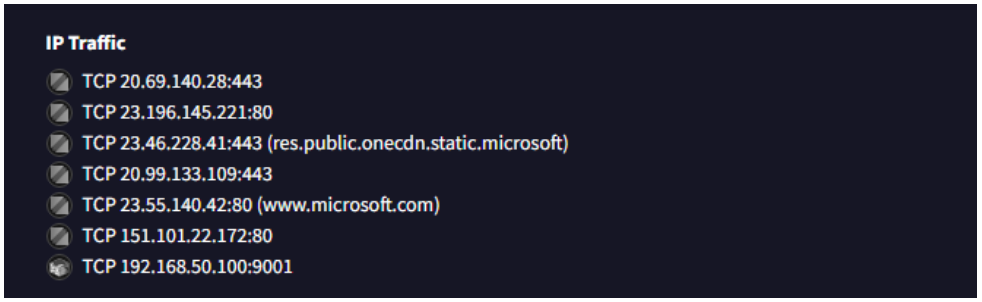
- **Il Nostro Sospetto (Statico):** Avevamo visto funzioni di gestione file (CreateFileW, WriteFile) che suggerivano la scrittura di nuovi file.
- **La Prova (Dinamica):** Dallo screen presente possiamo vedere che il malware **crea e lancia nuovi file eseguibili**:
  - C:\Program Files\Google1780_102522976\bin\updater.exe: Un classico file di **persistenza**, nascosto in una finta cartella "Google" per non destare sospetti.
  - %SAMPLEPATH%\d2e6c9[...]f2.exe: Un secondo file con un nome casuale (hash), probabilmente il payload principale o uno stadio intermedio.

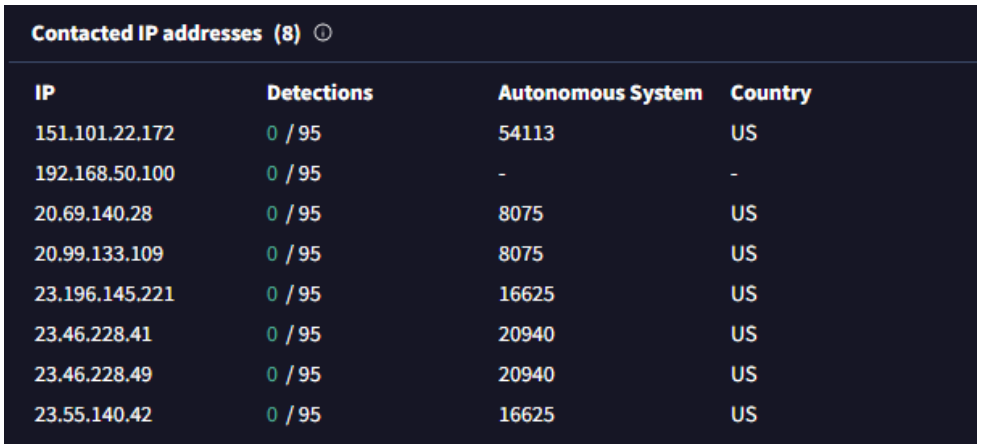
- **Conclusione:** Questo conferma il suo ruolo di **dropper**: il suo compito è "sganciare" e attivare il payload di secondo stadio.



Il "Comando e Controllo"

- **Il Nostro Sospetto (Statico):** L'importazione di librerie crittografiche (CRYPTBASE.dll) e la presenza di funzioni di rete suggerivano una comunicazione C2.
- **La Prova (Dinamica):**
  - La maggior parte del traffico verso Microsoft è "rumore" per sembrare legittimo o per verificare la connessione a Internet (tecnica anti-sandbox).
  - La vera connessione C2 è: **TCP 192.168.50.100:9001**.



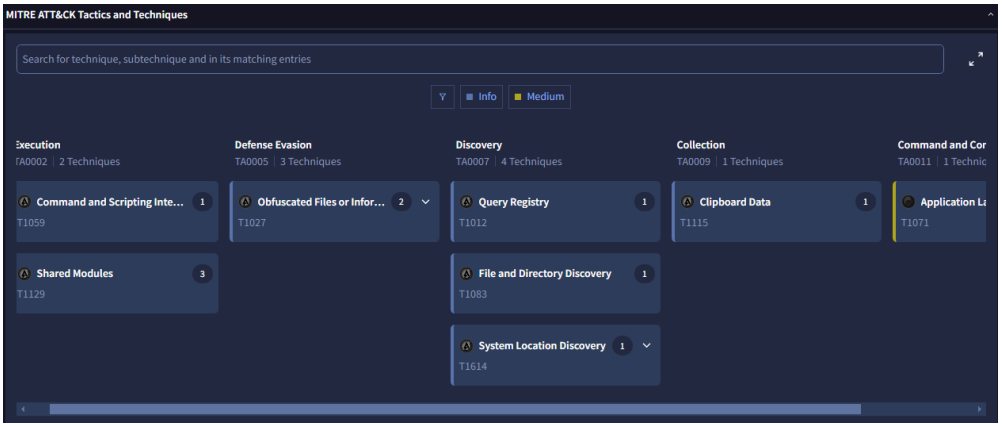


- **Conclusione:** Questo è l'elemento chiave. 192.168.50.100 è un **indirizzo IP privato** (interno alla rete). Il malware sta eseguendo una **reverse shell**: si connette *indietro* a una macchina che è in ascolto

sulla porta non standard 9001 all'interno della stessa rete. Questo comportamento è il marchio di fabbrica di un payload Meterpreter.

II MITRE ATT&CK

- **La Prova (Dinamica):** Il diagramma MITRE ATT&CK riassume perfettamente l'intero attacco:



  - **Defense Evasion (T1027):** Obfuscated Files. Conferma l'uso della crittografia che avevamo ipotizzato.
  - **Discovery (T1012):** Query Registry. Conferma la lettura delle chiavi di registro di Notepad per mascherarsi.
  - **Collection (T1115):** Clipboard Data. Una nuova informazione: il malware tenta anche di **rubare dati dagli appunti**.
  - **Command and Control (T1071):** Application Layer Protocol. È la connessione sulla porta 9001 che abbiamo trovato.

Previsioni dall'Analisi Comportamentale (Yara)

File *notepad-classico.exe*

Summary — Download | Resubmit sample

Size	282.5KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8a00a5c59ac157754ca575d721bcf960
SHA1	c31e260630d6553e2000f8e5f8dc270c751780d9
SHA256	d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2
SHA512	Show SHA512
CRC32	97668313
ssdeep	None
Yara	• CrowdStrike_CSIT_16018_03 - Metasploit payload loader • DebuggerCheck__QueryInfo - (no description) • anti_dbg - Checks if being debugged • inject_thread - Code injection with CreateRemoteThread in a remote process • network_http - Communications over HTTP • network_dns - Communications use DNS • network_dga - Communication using dga • escalate_priv - Escalade priviledges • screenshot - Take screenshot • win_mutex - Create or check mutex

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

- **Payload Metasploit (CrowdStrike_CSIT_16018_03):**
    - **Conferma Dinamica:**L'analisi Yara identifica il file come un **"Metasploit payload loader"**. Questo combacia perfettamente con la nostra scoperta di un payload Meterpreter.
- **Evasione e Anti-Analisi (DebuggerCheck, anti_dbg):**
    - **Comportamento Dinamico:** Il malware eseguirà controlli per vedere se è in esecuzione all'interno di un debugger o di una sandbox. Se rileva un analista, potrebbe terminare immediatamente l'esecuzione per non farsi analizzare.
- **Iniezione di Codice (inject_thread - CreateRemoteThread):**
    - **Comportamento Dinamico:** Questo è fondamentale. Ci aspettiamo di vedere notepad-classico.exe avviare un processo legittimo (es. explorer.exe o svchost.exe) e poi usare la funzione CreateRemoteThread per **iniettare il suo codice malevolo** (Meterpreter) all'interno di quel processo.
- **Comunicazione di Rete (network_http, network_dns, network_dga):**
    - **Comportamento Dinamico:** Conferma la nostra scoperta del traffico C2. Ci aspettiamo di vedere il malware:
        1. Fare **richieste DNS** (network_dns) per risolvere l'indirizzo IP dell'attaccante.
        2. Potenzialmente usare un **DGA (Domain Generation Algorithm)** (network_dga) per generare nomi di dominio C2 casuali nel caso quello principale sia bloccato.
        3. Comunicare sulla porta 443 (HTTPs) o 80 (HTTP) (network_http), come abbiamo visto nei log di VirusTotal, per mimetizzare il traffico C2 come normale traffico web.
- **Attività Malevole (escalate_priv, screenshot, win_mutex):**
    - **Comportamento Dinamico:** Una volta attivo, il payload cercherà di:
        1. **Creare un Mutex** (win_mutex): Per assicurarsi che solo una copia del malware sia in esecuzione sulla macchina.
        2. **Tentare l'Escalation dei Privilegi** (escalate_priv): Per ottenere diritti di Amministratore.
        3. **Catturare Screenshot** (screenshot): Una delle tante funzionalità di Meterpreter per spiare l'utente.

L'analisi è completa. notepad-classico.exe è un loader malevolo che si finge Blocco Note, installa un file di persistenza (updater.exe) e infine esegue un payload in memoria (Meterpreter) che stabilisce una reverse shell con l'attaccante all'indirizzo 192.168.50.100 sulla porta 9001, fornendogli pieno controllo della macchina.