Esercizio 1 Usare Windows PowerShell

Domande

Quali sono gli output del comando dir?

La powershell usa oggetti strutturati .Net
Powershell è più facile da filtrare e manipolare con Pipeline

Quali sono i risultati?

ping-> ovviamente non ce il collegamento perché non ho attivato una altra macchina però in entrambi i casi mi dicono i pacchetti che hanno inviato e quanti di questi sono stati ricevuti

cd-> in entrambi i casi mi sposta nella directory desiderata

ipconfig-> in entrambi e casi mi danno informazioni sugli indirizzi ipv6-4 subnetmask e Gateway

Qual è il comando PowerShell per dir?

Posso usare sia LS che DIR come alias del comando nativo, ovvero Get-ChildItem

Qual è il gateway IPv4?

192.168.64.254

Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Posso ottenere 1.informazioni generali come ultimo accesso, ultima modifica, percorso dei file,ecc,
2.Informazioni sugli utenti che hanno le autorizzazione per di scrittura e lettura
3.Dettagli come versione, nome,ecc

Cosa è successo ai file nel Cestino?

Tutti gli elementi sono stati eliminati

Domanda di Riflessione

Risultati della ricerca

2.1. Raccolta di Artefatti Critici e Live Forensics
Questi comandi sono cruciali per la fase di Risposta agli Incidenti (IR), permettendo la raccolta rapida di dati volatili da un sistema potenzialmente compromesso.

- Processi:
  - Cmdlet: Get-Process
  - Scopo: Elenca tutti i processi. L'uso con Select-Object -Property Path, CommandLine, StartTime è vitale per identificare eseguibili malevoli, percorsi insoliti o argomenti di riga di comando sospetti.
- Rete:
  - Cmdlet: Get-NetTCPConnection
  - Scopo: Mostra le connessioni TCP attive e i relativi processi (OwningProcess). Fondamentale per rilevare comunicazioni Command and Control (C2) o data exfiltration.
- Log di Sistema:
  - Cmdlet: Get-WinEvent
  - Scopo: Interroga in modo efficiente gli Event Log di Windows (e.g., Sicurezza, PowerShell/Operational). Essenziale per la ricerca di specifici ID Evento (e.g., Logon 4624, Process Creation 4688, PowerShell Script Block 4104).
- Persistenza (Servizi):
  - Cmdlet: Get-Service
  - Scopo: Elenca i servizi. Usato per identificare servizi non standard configurati per l'avvio automatico da parte di un attaccante.
- Persistenza (Attività):
  - Cmdlet: Get-ScheduledTask
  - Scopo: Elenca e ispeziona tutte le attività pianificate, un meccanismo di persistenza molto comune.
- Archiviazione:
  - Cmdlet: Start-Transcript -Path <Percorso>
  - Scopo: Registrazione di Audit obbligatoria. Cattura tutto l'input e l'output della sessione PowerShell, fornendo una traccia non ripudiabile delle azioni dell'analista forense.

2.2. Audit, Valutazione delle Vulnerabilità e Hardening
Questi comandi vengono utilizzati per la valutazione della configurazione di sicurezza e per automatizzare i controlli di compliance.

- Integrità File:
  - Cmdlet: Get-FileHash -Algorithm SHA256
  - Scopo: Calcola l'hash crittografico di un file per verificarne l'integrità e confrontarlo con database di Indicatori di Compromissione (IOC) o hash noti di sistema.
- Controlli di Accesso:
  - Cmdlet: Get-Acl -Path <Risorsa>
  - Scopo: Recupera l'Access Control List (ACL) di file, cartelle o chiavi di registro. Cruciale per verificare che le autorizzazioni su risorse critiche non siano state modificate.
- Politiche Esecutive:
  - Cmdlet: Get-ExecutionPolicy
  - Scopo: Verifica le restrizioni sull'esecuzione degli script. Deve essere impostata su un livello sicuro (e.g., RemoteSigned o AllSigned) per prevenire l'esecuzione non autorizzata di codice.
- Certificati:
  - Cmdlet: Get-ChildItem -Path Cert:
  - Scopo: Ispeziona i certificati installati. Utile per scovare certificati dannosi o non attendibili utilizzati per la firma di codice (o per la decrittazione di traffico intercettato).
- Account:
  - Cmdlet: Get-LocalUser / Get-ADUser
  - Scopo: Audit rapido per identificare account locali o di dominio non autorizzati, disabilitati o con privilegi eccessivi.
- Inventario:

    - Cmdlet: Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*
    - Scopo: Rileva il software installato per identificare applicazioni vulnerabili, non autorizzate o con licenze scadute.
3. Contromisure (Dal Punto di Vista dell'Attaccante)

È essenziale riconoscere che PowerShell è uno strumento molto utilizzato anche dagli attaccanti ("Living off the Land" - LoL). Gli attaccanti spesso sfruttano:

- Codice Offuscato: Utilizzo di -EncodedCommand o IEX (Invoke-Expression) per bypassare le difese basate sulla firma.
- Bypass AMSI: Tentativi di manipolare l'Antimalware Scan Interface (AMSI) per nascondere i payload in memoria.

4. Raccomandazioni per l'Hardening e il Blue Teaming

Per massimizzare l'efficacia di PowerShell come strumento di sicurezza, si raccomanda l'implementazione immediata delle seguenti policy in tutta l'organizzazione:

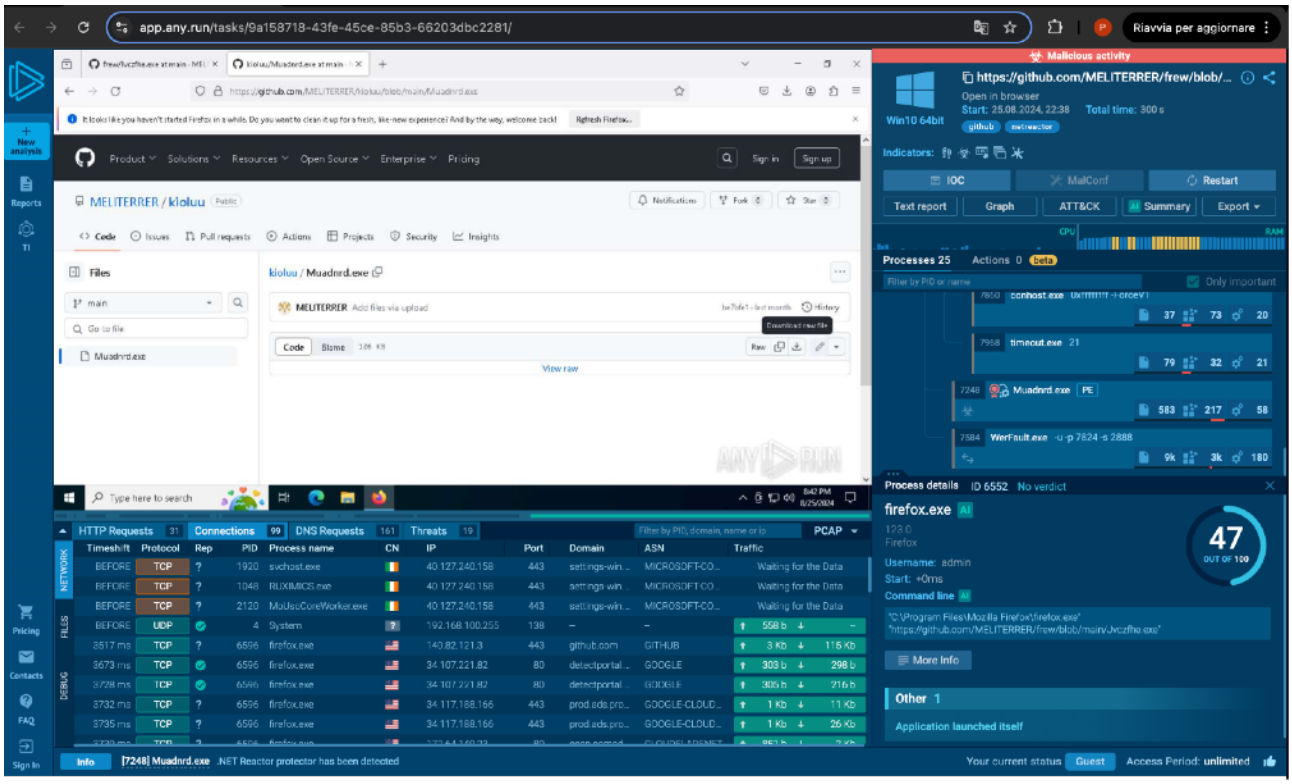
1. Abilitare il Script Block Logging (Event ID 4104): Questa funzionalità registra l'intero blocco di codice eseguito, catturando anche il codice de-offuscato e in memoria, vanificando la maggior parte delle tecniche di evasione degli attaccanti.
2. Centralizzare i Log: Configurare il Windows Event Forwarding (WEF) per inoltrare immediatamente tutti i log di PowerShell al SIEM.
3. Restrizioni Linguistiche: Per gli utenti non amministratori, valutare l'uso della Modalità Lingua Vincolata (Constrained Language Mode) per limitare l'accesso alle funzionalità più pericolose di PowerShell.

L'uso consapevole e l'abilitazione delle funzionalità di logging di PowerShell sono la base per una strategia di sicurezza Windows efficace.

Esercizio 2: Studio Ioc

Panoramica iniziale

Da questa analisi si possono ricavare molte informazioni utili come le richieste HTTP, le connessioni che sono avvenute, le richieste DNS, i THREATS.



Inizio ad analizzare le richieste HTTP ed riesco ad ricavare varie informazioni:

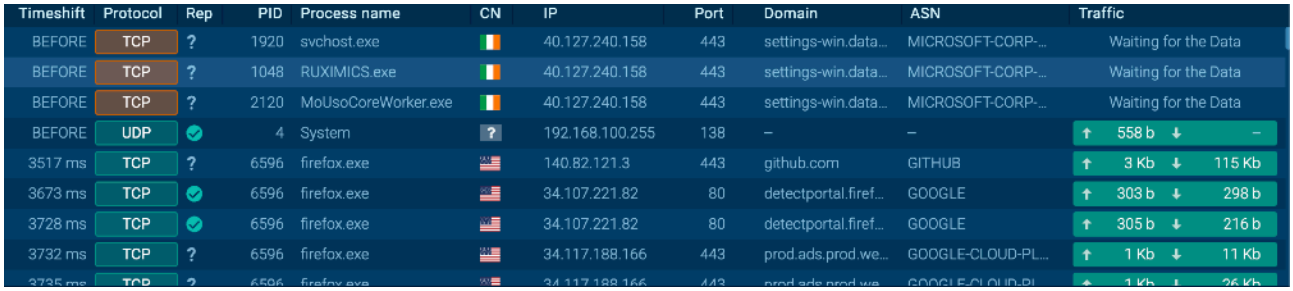
1. **Comunicazione con Domini Sospetti** Il processo **firefox.exe** (PID 6596) sta comunicando attivamente con domini che non sono tipici di una normale navigazione web. Le richieste **POST** a **http://r10.o.lencr.org/** e **http://r11.o.lencr.org/** sono particolarmente allarmanti. Il fatto che il processo stia scambiando dati binari in entrambe le direzioni suggerisce una potenziale connessione a un **server C2** (Command and Control) per ricevere istruzioni o scaricare ulteriori payload.

2. **Verifica Certificati come Attività di Copertura** Si vede che il browser sta contemporaneamente comunicando con domini legittimi come **ocsp.sectigo.com**, **ocsp.digicert.com** e **o.pki.goog/wr2**. Questi sono domini di server OCSP (Online Certificate Status Protocol) e PKI (Public Key Infrastructure) utilizzati per verificare la validità dei certificati SSL/TLS. Questo comportamento è una tecnica comune: l'attività sospetta si nasconde nel normale traffico del browser per sembrare meno anomalo e per sfuggire al rilevamento.

3. **Correlazione tra Processi e Attività** Il file **SIHClient.exe** (PID 7816) effettua una richiesta **GET** a un dominio Microsoft (http://www.microsoft.com/...). Questo suggerisce che l'eseguibile potrebbe essere legittimo o che il malware si sta fingendo un processo di aggiornamento o un componente Microsoft per scaricare ulteriori file o stabilire una connessione. La richiesta scarica un file binario di circa 400KB, che merita un'indagine approfondita.

4. **Download di un File Sospetto di Grandi Dimensioni** Una richiesta **GET** proveniente ancora da **firefox.exe** (PID 6596) scarica un file compresso di 480 KB da http://ciscobinary.openh264.org/openh264-win64.... Anche se **openh264** è un codec video legittimo, il fatto che il download avvenga in parallelo con le altre attività sospette e da un processo che si sta comportando in modo anomalo, solleva dubbi significativi sulla sua legittimità in questo contesto.

Analisi delle connessioni:



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	TCP	?	1920	svchost.exe		40.127.240.158	443	settings-win.data...	MICROSOFT-CORP-...	Waiting for the Data
BEFORE	TCP	?	1048	RUXIMICS.exe		40.127.240.158	443	settings-win.data...	MICROSOFT-CORP-...	Waiting for the Data
BEFORE	TCP	?	2120	MoUsoCoreWorker.exe		40.127.240.158	443	settings-win.data...	MICROSOFT-CORP-...	Waiting for the Data
BEFORE	UDP		4	System	?	192.168.100.255	138	–	–	↑ 558 b ↓ –
3517 ms	TCP	?	6596	firefox.exe		140.82.121.3	443	github.com	GITHUB	↑ 3 Kb ↓ 115 Kb
3673 ms	TCP		6596	firefox.exe		34.107.221.82	80	detectportal.firef...	GOOGLE	↑ 303 b ↓ 298 b
3728 ms	TCP		6596	firefox.exe		34.107.221.82	80	detectportal.firef...	GOOGLE	↑ 305 b ↓ 216 b
3732 ms	TCP	?	6596	firefox.exe		34.117.188.166	443	prod.ads.prod.we...	GOOGLE-CLOUD-PL...	↑ 1 Kb ↓ 11 Kb

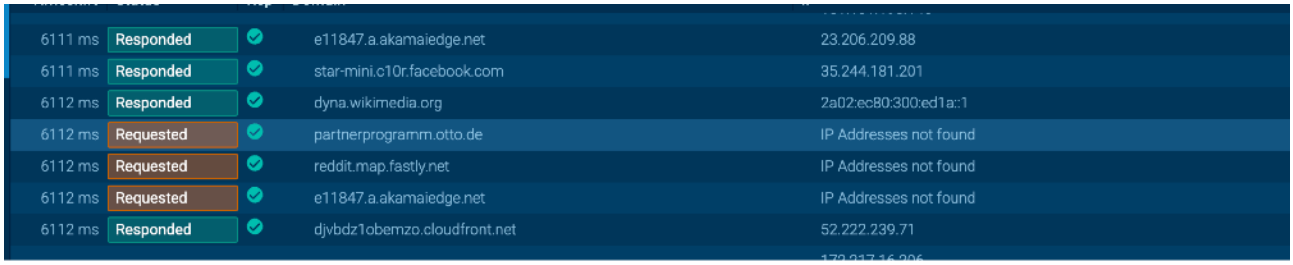
1.Conferma della comunicazione C2: L'attività con i **domini r10.o.lencr.org** e **r11.o.lencr.org** è confermata su protocollo **TCP** (porta 80) e **TCP** (porta 443). Il fatto che i dati scambiati siano di tipo **binario** (binary) e che il traffico in entrata e in uscita sia consistente (es. 2-3 KB in uscita e 1-3 KB in entrata) suggerisce una comunicazione attiva con un **server C2**.

2.Tecnica di esfiltrazione dati: Le connessioni a satebrowsing.google.com e pki-googl.google.com (con un notevole traffico di 2 KB in uscita e 8 MB in entrata) sono particolarmente interessanti. Un malware spesso usa domini legittimi e molto trafficati (come quelli di Google) per camuffare l'esfiltrazione di dati. Il traffico di 8 MB in entrata è insolitamente grande per una semplice verifica di certificato o un'attività di browsing, e potrebbe indicare il download di un secondo payload o di istruzioni complesse.

3.Download da fonti legittime ma insolite: La connessione a **raw.githubusercontent.com** è cruciale. Questo dominio è usato per servire file grezzi da GitHub, una tecnica molto comune per gli attaccanti per ospitare script malevoli (MuadDerd.exe) o altri strumenti. Il fatto che **MuadDerd.exe** si connetta a questo dominio conferma la sua natura di **"download and execute".**

4.Infezione di altri processi: Si nota che anche processi come **svcshost.exe** e **WerFault.exe** (entrambi processi di sistema legittimi di Windows) stanno effettuando connessioni a domini Microsoft, come **login.live.com** e **client.wns.windows.com**. Questo potrebbe indicare che il malware ha iniettato codice in questi processi per camuffarsi o che sta usando le loro funzioni per **scopi malevoli** (es. l'esfiltrazione dati o la compromissione delle credenziali).

Analisi delle connessioni DNS:



1. **Conferma della comunicazione con domini malevoli:** Le richieste per **r10.o.lencr.org** sono state **risolte in 184.24.77.48**, e un'altra richiesta per **github.com** è stata **risolta in 140.82.121.3.** Queste risoluzioni **DNS** confermano che il sistema ha tentato di stabilire un contatto con domini noti per ospitare contenuti dannosi (come visto nelle richieste HTTP) o che sono comunemente usati dagli attaccanti (come GitHub).

2. **Tecnica di Domain Generation Algorithm (DGA):** Richieste **DNS fallite** per domini come **partnerprogramm.otto.de**, **reddit.map.fastly.net** e altre stringhe complesse che non sono state risolte (IP Addresses not found). Questo comportamento è tipico di un **DGA**, un algoritmo usato dai malware per **generare** centinaia di **domini casuali**. L'attaccante registra uno di questi domini per ogni "campagna" di attacco, rendendo molto **difficile** per i sistemi di sicurezza **bloccare** tutti i potenziali **server C2**. La presenza di richieste non risolte è un fortissimo segnale di un'infezione da malware.

3. **Abuso di servizi legittimi per l'infiltrazione:** I domini **detectportal.firefox.com**, **firefox.settings.services.mozilla.com** e **safebrowsing.googleapis.com** sono legittimi. Il fatto che il sistema stia comunicando con questi server è normale. Tuttavia, in un contesto di attacco, **il malware** può **sfruttare** queste **connessioni legittime** per camuffare le sue comunicazioni, rendendo più difficile per i sistemi di sicurezza distinguere il traffico buono da quello cattivo. L'analisi **DNS** di questi domini, in combinazione con l'analisi **HTTP**, può rivelare se i dati scambiati sono anomali (ad esempio, di grandi dimensioni o con un contenuto inaspettato).

Analisi dei THREADS:

1. **Tentativi di accesso sospetti:** L'avviso **"Attempting to access raw user content on GitHub**" è un chiaro **segnale** di **allarme**. Questo significa che il processo **svchost.exe** (PID 2256), un processo di sistema legittimo, ha cercato di accedere a un file "grezzo" su GitHub.
    - Come l'ho capito: Gli **attaccanti** usano spesso i file **grezzi di GitHub** (raw.githubusercontent.com) per ospitare **script** o eseguibili **malevoli**. Se un processo di sistema come **svchost.exe** cerca di accedere a un contenuto del genere, è un'indicazione molto forte di iniezione di **codice malevolo** o di un abuso di un processo legittimo.

2. **Attività di DNS Dinamico (Dynamic DNS - DDNS):** L'avviso "ET INFO DYNAMIC_DNS Query to a *.duckdns.org Domain" è estremamente sospetto.
    - Come l'ho capito: I servizi di **DDNS** come **duckdns.org** permettono di associare un nome di dominio a un indirizzo IP che cambia frequentemente. Gli attaccanti usano questi servizi per nascondere i loro **server C2**. Questo rende molto più **difficile** per le difese **bloccarli**, poiché **l'indirizzo IP cambia di continuo**. Le query **DNS** a questi domini sono un forte indicatore di **compromissione** (IOC) e suggeriscono che il **malware** sta cercando di mettersi in contatto con il suo **server** di controllo.

3. **Coinvolgimento di un processo legittimo:** Tutte le minacce sono associate a svchost.exe.
    - Come l'ho capito: I **malware** spesso **iniettano** codice in **processi legittimi** per mascherare le loro attività e sfuggire ai sistemi di difesa. L'iniezione di **codice** in **svchost.exe** è una tecnica comune e pericolosa.

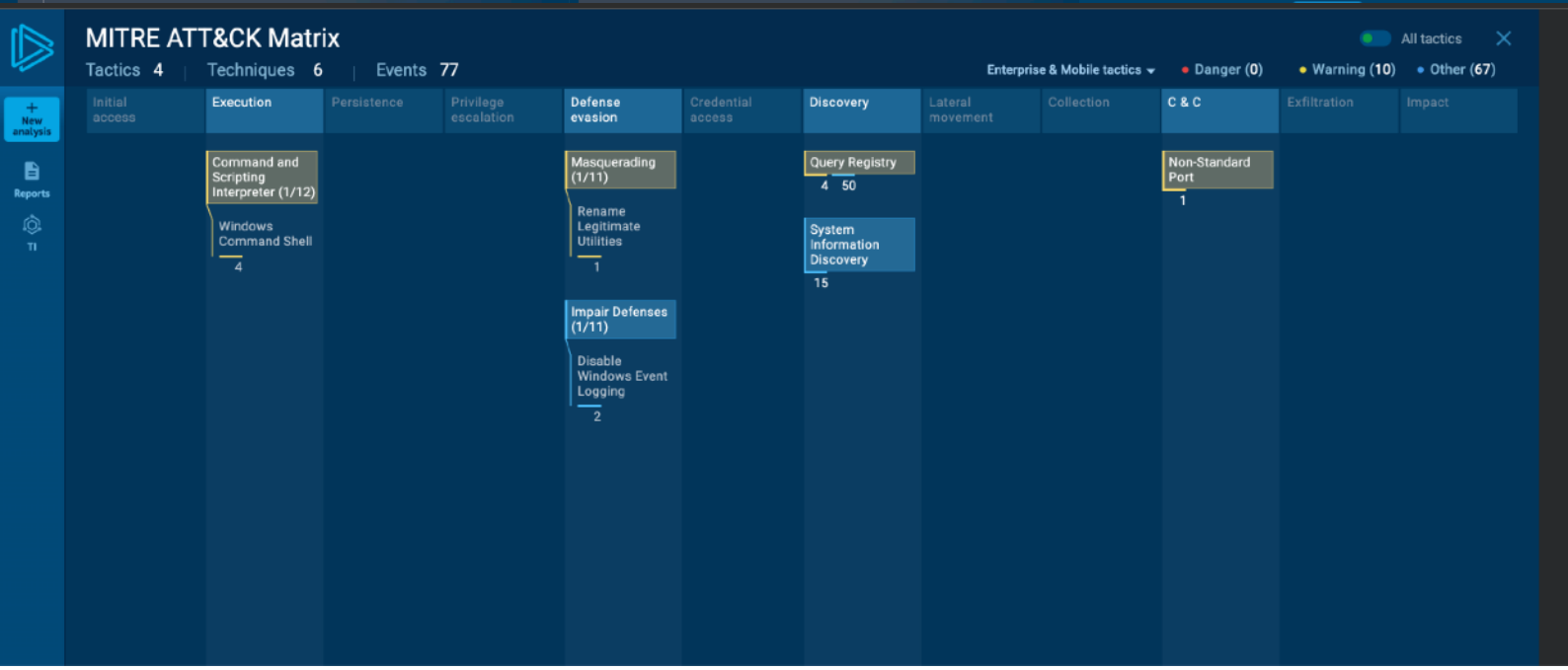
Correlazione con le analisi precedenti

Le informazioni sui "threads" confermano e collegano i dati delle analisi precedenti:

- **L'accesso** a contenuti grezzi su **GitHub** (raw.githubusercontent.com) visto nelle richieste **DNS/HTTP** è ora **confermato** come un'attività potenzialmente malevola dal sistema di sicurezza.
- Il coinvolgimento di **svchost.exe** in attività sospette **suggerisce** che il **malware** (probabilmente scaricato da Firefox) ha iniettato **codice** in un processo di sistema per **mantenere** la **persistenza** e **camuffarsi**.
- Le query a **duckdns.org** confermano che il **malware** sta usando un servizio di **DDNS** per la sua comunicazione **C2**, un'ulteriore prova della sua natura di minaccia avanzata.

In sintesi, l'analisi dei "threads" fornisce una classificazione e un'interpretazione degli eventi di rete, trasformando semplici dati di connessione in allarmi specifici che un analista di sicurezza può usare per capire e contrastare la minaccia.

Ultime analisi:



1. **Correlazione dei processi:** Si vede che il processo **firefox.exe** (ID 6552) è il punto di ingresso che ha **lanciato Jvczfhe.exe**. Successivamente, **firefox.exe** ha **lanciato Muadnrd.exe**. Questo conferma che il malware non è stato lanciato direttamente dall'utente, ma è **un'esecuzione** a **catena**, in cui un eseguibile (Muadnrd.exe) lancia un altro (Jvczfhe.exe). Questo è un comportamento comune per i "**loader**" o "**downloader**" di malware.

2. **Tecniche di attacco MITRE ATT&CK:** Il report MITRE è la parte più importante di questa analisi, poiché traduce le attività in categorie di attacco riconosciute.
    - **Execution**: "Command and Scripting Interpreter" e "Windows Command Shell" indicano che il malware ha usato il prompt dei comandi di Windows (cmd.exe) per eseguire i suoi comandi. Questo è un metodo comune per aggirare le restrizioni.
    - **Defense Evasion:**
        - "Masquerading: Rename Legitimate Utilities" è un segnale di allarme. Questo significa che il malware ha rinominato un file eseguibile come Jvczfhe.exe e Muadnrd.exe per camuffarsi. Spesso i malware si travestono da processi legittimi per non insospettire l'utente e i sistemi di sicurezza.
        - "Impair Defenses: Disable Windows Event Logging" è una tecnica molto pericolosa. Questo indica un tentativo del malware di disabilitare la registrazione degli eventi di Windows per non lasciare tracce delle sue attività. Questo è un forte segnale di una minaccia avanzata e stealth.
    - **Discovery**: "Query Registry" e "System Information Discovery" mostrano che il malware sta esplorando il sistema per raccogliere informazioni (es. configurazione del sistema, software installato, etc.).
    - **C & C (Command and Control):** "Non-Standard Port" conferma che il malware ha usato una porta non convenzionale per comunicare con il suo server di controllo, una tattica per sfuggire ai firewall basati su regole standard.

Conclusione: Spiegazione dell’attacco

1. Il Punto di Ingresso: Firefox

Tutto è iniziato quando un utente, identificato come "**admin**", ha usato il browser **Firefox**. Dal repository **GitHub** di un utente chiamato "**brob**", un file eseguibile **malevolo**, chiamato **MuadDerd.exe**, è stato **scaricato**. Questo è stato il punto di partenza dell'intera infezione.

2. Esecuzione e Camuffamento

Una volta scaricato, **MuadDerd.exe** non si è limitato a fare i suoi danni. Ha **avviato** un altro eseguibile chiamato **Jvczfhe.exe**, usando il prompt dei comandi (**cmd.exe**). Questo comportamento è tipico dei malware **TROJAN** che usano un "**loader**" o "**dropper**" per scaricare ed eseguire il payload principale. Il nome strano dei file (Jvczfhe.exe e MuadDerd.exe) è un tentativo di mascheramento, una tecnica usata per sembrare un file di sistema casuale e non attirare l'attenzione.

3. Esplorazione e Evasione delle Difese

Dopo essere stato eseguito, il **malware** ha iniziato a muoversi con cautela. Ha **compiuto** due **azioni fondamentali** per non essere scoperto:

- **Ha esplorato il sistema**: Ha eseguito una "discovery", cercando informazioni sul sistema e nel registro di Windows. Questo serve per capire il tipo di macchina su cui si trova e adattare il suo comportamento.
- **Ha cercato di disabilitare le difese**: La minaccia ha provato a disabilitare la registrazione degli eventi di Windows, un'azione estremamente pericolosa. Se fosse riuscita, avrebbe cancellato le sue tracce, rendendo l'indagine forense quasi impossibile.

4. Comunicazione Nascosta

La parte più **critica** dell'attacco è la sua **comunicazione con l'esterno**. Il malware ha usato una serie di tecniche avanzate:

- **Ha abusato di processi legittimi:** Ha iniettato del codice in svchost.exe, un processo di sistema fondamentale, per inviare richieste di rete e nascondere la sua attività malevola nel traffico di rete normale.
- **Ha usato domini legittimi per nascondersi:** Ha comunicato con server legittimi di Google e Microsoft, probabilmente per camuffare i suoi scambi di dati. Il grande traffico in uscita e in entrata su questi domini (come pki-googl.google.com) suggerisce un tentativo di esfiltrazione dati o il download di un secondo payload.
- **Ha usato un server di controllo camuffato**: La minaccia ha comunicato con un servizio di DNS dinamico (duckdns.org) e altri domini sconosciuti (lencr.org). Questa è una tattica classica per i server di "comando e controllo" (C2), in quanto permette all'attaccante di cambiare rapidamente l'indirizzo IP del suo server per evitare che venga bloccato.

BONUS 1

Domande

1.Cos'è Nmap?

map, acronimo di Network Mapper, è un strumento open-source utilizzato per la scansione e la mappatura delle reti.

2.Per cosa viene usato nmap?

Il suo scopo principale è quello di scoprire host e servizi su una rete inviando pacchetti di dati e analizzando le risposte.

3.Qual è il comando nmap usato?

nmap -A -T4 **scanner.nmap.org**

4.Cosa fa -A

Fa una scansione di tutto porte, servizi, ecc

5.Cosa fa l'opzione -T4

Fa una scansione agressiva e veloce senza preoccuparsi della discrezione

6.Quali porte e servizi sono aperti?

21/tcp FTP vsftpdz 2.0.8 or later
22/tcp SSH openSSH 7.7

7.A quale rete appartiene la tua VM?

127.0.0.1/8

8. Quanti host sono attivi?

2 Host sono attivi

9.Quali porte e servizi sono attivi?

10.Quali porte e servizi sono filtrati?

11.Quale l’indirizzo ip del server?

12.Qual è il sistema operativo?

13.Nmap puo essere usato sia in maniera per rinforzare la propria rete oppure in maniera malevola, con le scansioni si possono ottenere molte informazioni utili e cercare vulnerabilità nella rete.

Bonus 2.