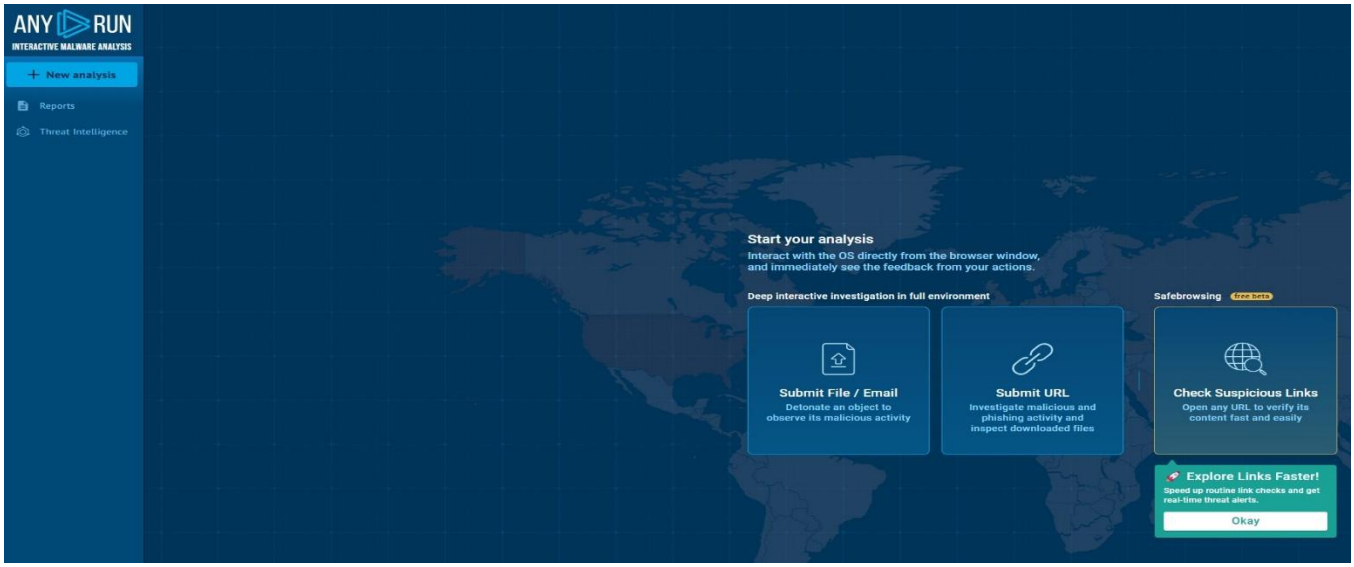
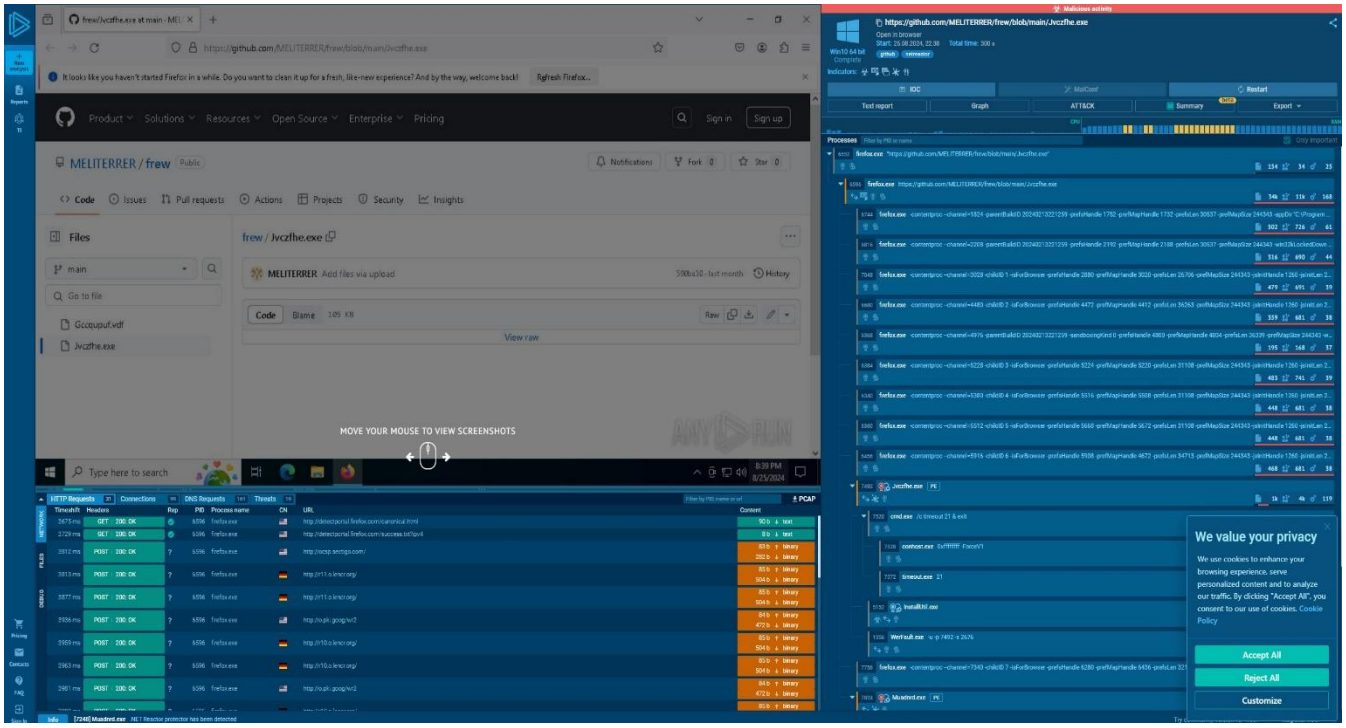
Report Malware – Persistenza e Comunicazione C2

Nella prima e seguente immagine avvio il tool interattivo **ANY RUN** per analizzare il Malware:



Nella seguente immagine, dopo aver caricato il file malevolo **Jvczfhe.exe**, posso notare che ho vari dati estrapolati dal tool **ANY RUN**, come descritto ed illustrato di seguito:

https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/



Nella seguente immagine possiamo vedere, che l'inizio del processo si avvia, con l'esecuzione di **firefox.exe**, e che la propagazione e la distribuzione del Malware all'interno del Sistema Operativo, avviene tramite i processi di Firefox, e quindi utilizzando Internet

- Possiamo osservare e notare che la ramificazione ed estensione di vari **firefox.exe**, con molta probabilità, indicano dei comportamenti anomali, creando svariati processi, così da mascherare il codice sorgente ed evitare, che il Malware venga rilevato.

- **svchost.exe:** è utilizzato dai Malware per offuscare il codice, essendo un processo nella maggior parte delle volte legittimo, può ingannare, il sistema.
- **installUtil.exe:** è un processo legittimo di **Microsoft.NET** ed è utilizzata per installare e configurare le applicazioni .NET, ma viene anche sfruttata per caricare ed eseguire Malware con la tecnica conosciuta con l'acronimo **LOLBAS** (**Living of the Land Binaries and Scripts**), con il quale gli strumenti utilizzati dal Malware, evitano il rilevamento da parte dei Sistemi di Sicurezza.
- **muadRnd.exe:** è un file dannoso e quindi una minaccia per il Sistema, utilizzando tecniche di offuscamento ed utilizzo di processi legittimi, per evitare di essere rilevato dai Sistemi di Sicurezza.
- **cmd.exe**
  - File exe dal Prompt dei Comandi di Windows, con il quale lo User può eseguire gli script e file batch.
  - **Utilizzo legittimo (User)**: utilizzato per eseguire la gestione dei file, configurare la rete ed altre attività con **Privilege Administrator**
  - **Utilizzo illegale (Attacker):** un attaccante può utilizzare il cmd.exe per scopi malevoli, e quindi eseguire accessi da remoto, far partire uno script tramite PowerShell, lanciare Payload o anche eseguire altri Malware, che vanno a modificare la configurazione del Sistema.
- **conhost.exe** (**Console Windows Host**): migliora la l'utilizzo della riga di comando, con l'aggiunta di funzioni, come il drag-and-drop dei file, nel Prompt dei comandi.
  - **Utilizzo legittimo (User):** fa si che la console della **GUI** (**Graphical User Interface**), funzioni correttamente e che ci sia sicurezza e compatibilità.
  - **Utilizzo illegale (Attacker):** un attaccante può sfruttare questi eseguibili per offuscare le attività dannose, così da far sembrare i processi, eseguiti, o in esecuzione, legittimi.
- **timeout.exe:** viene utilizzato per immettere un ritardo o mettere in pausa file batch o script, ma anche di interrompere il processo di uno script.
  - **Utilizzo legittimo (User):** il timeout.exe crea gli intervalli tra i comandi e processi, permettendo il completamento degli stessi, per determinare varie condizioni, prima di procedere all'esecuzione del processo successivo.
  - **Utilizzo illegittimo (Attacker):** un attaccante può utilizzare il timeout.exe per ritardare l'esecuzione del processo, tramite i comandi, mascherandosi e non facendosi rilevare durante l'esecuzione, ed inoltre può programmare l'attacco e sincronizzarsi con la rete Internet.


start
firefox.exe
no specs
firefox.exe
svchost.exe
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
firefox.exe
no specs
jvczfhe.exe
firefox.exe
no specs
muadnrd.exe
cmd.exe
no specs
conhost.exe
no specs
timeout.exe
no specs
THREAT
installutil.exe
werfault.exe
cmd.exe
no specs
conhost.exe
no specs
timeout.exe
no specs
THREAT
muadnrd.exe
no specs
werfault.exe

Possiamo notare che il file malevolo **Jvczthe.exe** ha un comportamento tipico delle infrastrutture di **Comando e Controllo** (**C2**), stabilendo connessioni verso i domini sospetti come:

detectorportal.firefox.com: analizzando il dominio possiamo notare da subito che non si tratta di un dominio ufficiale, di Firefox, e quindi con alta probabilità è un sito sospetto e dannoso.

- Firefox utilizza domini ufficiali come **firefox.com**, nel caso analizzato non utilizza tale dominio di origine, e quindi è sospetto, in tal caso è altamente probabile che sia un sito web clonato o un sito che utilizza la tecnica di phishing.
- Se durante un'analisi del Malware è stato rilevato tale dominio (detectorportal.firefox.com), potrebbe essere stato utilizzato da attori malevoli per attacchi di **Phishing**, **Command and Control**, o per la distribuzione **payload dannosi**.

Command and Control (C2)

- è un termine utilizzato e conosciuto nell'ambito della Cybersecurity per descrivere l'infrastruttura utilizzata dagli attaccanti per il controllo remoto, persistente su un sistema. Il Server di C2 permette all'attaccante di poter comunicare con il malware installato sui dispositivi infetti ed eseguire, comandi, estrarre dati, e di eseguire operazioni malevole.

ocsp.sectigo.com: dominio legittimo utilizzato da Sectigo, una delle principali autorità di certificazione (CA) che emette certificati digitali per siti web, applicazioni e dispositivi.
Il dominio è associato al servizio OCSP (**Online Certificate Status Protocol**), che può verificare in tempo reale lo stato della validità dei certificati digitali emessi da Sectigo.

Misure di Sicurezza (Remediation e Mitigation)

- Segmentazione della Rete
- Monitoraggio del Traffico e dei Log di Rete
- Hardening dei Sistemi e delle Applicazioni
- Controllare gli Accessi e la Gestione delle Identità
- Analisi dei Comportamenti e del Threat Intelligence
- Bloccare e Monitorare il Traffico in uscita
- Esecuzione di Scansioni Anti-Malware e Ripristino del Sistema
- Formazione e Consapevolezza sulla Sicurezza al personale
- Backup e Piano di Risposta agli Incidenti

Conclusioni

L'analisi del file malevolo **Jvczthe.exe** ha evidenziato una minaccia altamente sofisticata che utilizza in modo malevolo ed illecito i processi legittimi di del Sistema Operativo Windows, come **firefox.exe**, **svchost.exe** e **InstallUtil.exe**, per mascherarsi ed offuscare, una connessione ad un Server di **Comando e Controllo (C2)**, descritto in precedenza, in grado di ricevere istruzioni e di trasmettere dati.
L'analisi del Malware **Jvczthe.exe** indica un elevato rischio di esfiltrazione di informazioni, controllo remoto, con l'intenzione di persistere all'interno del sistema compromesso.
Dop un'attenta e profonda analisi del Malware **Jvczthe.exe**, possiamo confermare che si tratta di una minaccia reale

Non è un Falso Positivo ma una MINACCIA REALE!!!!

Per evitare che tale evento si presenti e che possa causare danni ingenti all'infrastruttura aziendale, è altamente consigliato attuare le misure di **Mitigation** e **Remediation**, descritte in precedenza.

31/10/2024 **Christian Vagnoni**