Esercizio 2: Studio Ioc

Link del report Anyrun:
https://app.any.run/tasks/9a15871843fe-45ce-85b366203dbc2281/

Il report fornito da **Anyrun**, presenta un'analisi approfondita di due file caricati su **GitHub.**
I file in questione risulterebbero danneggiati, tuttavia, è possibile dimostrare quanto essi possano essere dannosi, in quanto sono stati offuscati per eseguire attività sospette.
I file sono degli eseguibili **.exe** chiamati rispettivamente:
Jvczfhe.exe e **Muadnrd.exe**.

Presentano entrambi gli stessi processi figli:

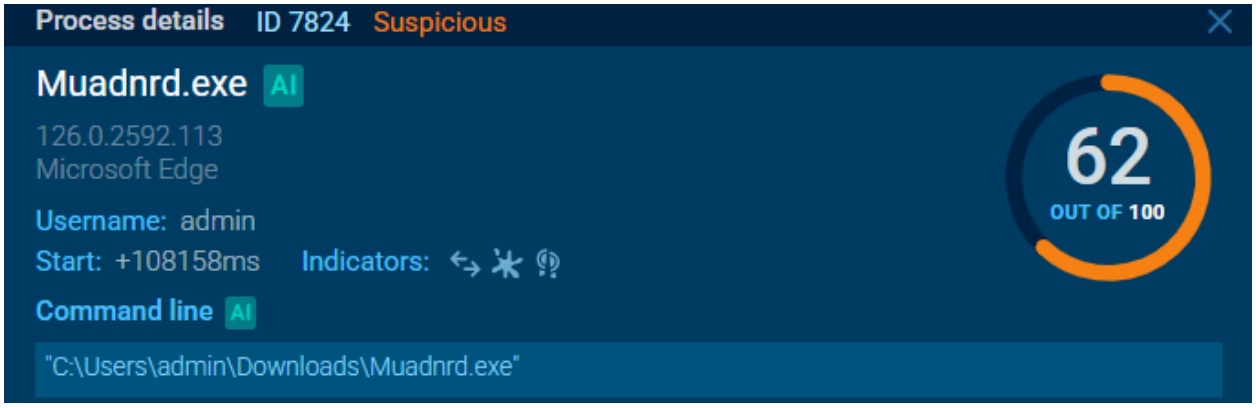
I processi figli in questo caso sono: **cmd.exe, conhost.exe e timeout.exe**.

Cmd è il prompt dei comandi di Windows, potrebbe essere usato per eseguire comandi batch, script o comunque comandi singoli sospetti. **Conhost.exe** è il processo figlio di cmd, il suo supporto grafico. **Timeout.exe** è un comando impostato per ritardare l'esecuzione di altri comandi, potrebbe essere impostato per offuscare il **malware** stesso lanciando i comandi con degli intervalli di tempo.

Il grafico di quanto detto sopra è stato fornito direttamente da **anyrun**.

Qui si può vedere come essi siano collegati con i loro processi figli, creando sottoprocessi molto sospetti, come quelli descritti sopra.

Cliccando sui dettagli dei processi, si può notare il risultato di **VirusTotal**, un servizio gratuito che analizza file e URL sospetti per rilevare virus, worm, trojan, e altri tipi di malware.



In questo caso 62 Antivirus su 100, hanno identificato **Muadnrd.exe** come eseguibile malevolo.

Sempre sulla stessa pagina, si trovano maggiori informazioni di quello che sta succedendo.
In particolare sono presenti le seguenti voci:

Executes application which crashes: Il programma prova ad avviare un altro programma, ma questo va in errore o si chiude improvvisamente.

Application launched itself: Indica che il programma si è auto-avviato.

Starts cmd.exe for commands executions: attività sospetta, che come descritto sopra, utilizza il prompt dei comandi per eseguire script o comandi stessi.

Il malware guarda nelle impostazioni interne di Windows per raccogliere informazioni utili in quanto sono presenti informazioni di lettura come:

Checks Windows Trust Settings, ciò visualizzerebbe i certificati e la sicurezza.

Reads security settings of Internet Explorer, simile a quanto sopra, ma legge principalmente le impostazioni del Browser specifico **Internet Explorer**.

Reads the software policy settings, legge i permessi del sistema ed eventuali restrizioni.

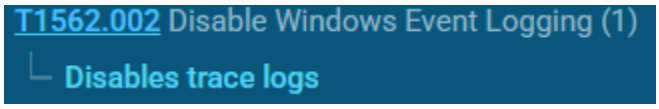
Checks proxy server information, controlla se il Computer utilizza un Proxy.

Reads Environment values, guarda le informazioni generali del sistema, come nome utente, percorso delle cartelle, ecc.

Reads the machine GUID from the registry, legge un codice identificativo unico del computer.

Reads the computer name & Checks supported languages, leggono rispettivamente il nome del Computer e la Lingua utilizzata.

Il malware inoltre, disattiva i Log del Sistema.



Disattiva i registri di sistema: un'altra tecnica di offuscamento, serve per nascondere le sue attività nel sistema e rendere più difficile la rilevazione da parte degli antivirus.

Traffico sospetto rilevato

Durante l'esecuzione, Firefox ha mostrato reindirizzamenti sospetti verso:

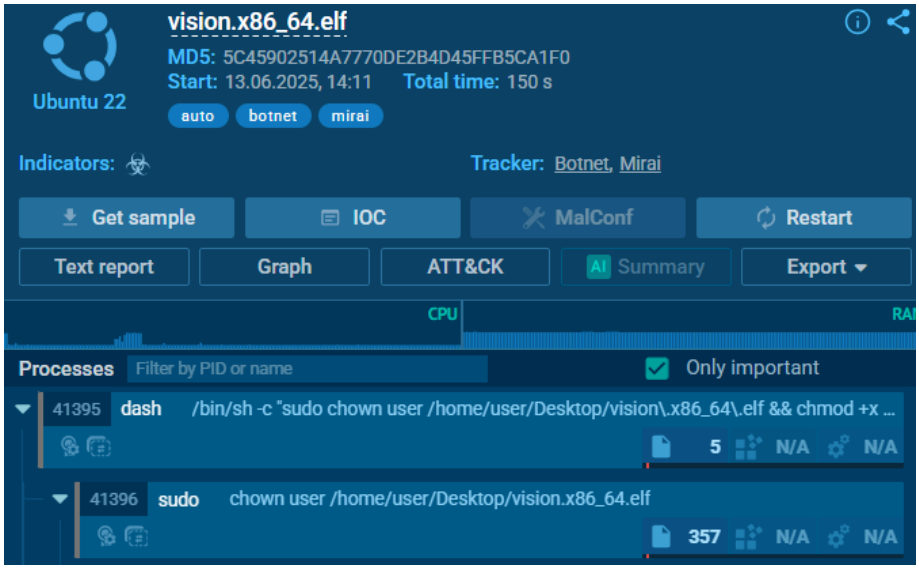
draport digitals
dweb.link/ipfs (relativo alla rete IPFS)

Questo suggerisce un possibile tentativo di comunicare con un server di comando.

Il malware infatti interagisce con la rete, creando diversi sotto-reindirizzamenti.

E’ inoltre classificato come **Phishing**.

E’ stato rilevato inoltre un file chiamato **vision.x86_64.elf**.



Il file in questione sta cercando di fare una **privilege escalation**.

Si possono vedere infatti i comandi compresi di script nello screenshot, con l’utilizzo di **chown**, che modificherebbe il proprietario del file.

Conclusioni

Nonostante il file principale appaia danneggiato, l’analisi dimostra chiaramente che il malware è capace di eseguire azioni dannose. Sfrutta processi di sistema come cmd.exe, conhost.exe e timeout.exe per nascondere le sue operazioni e rallentare l’esecuzione dei comandi, rendendo difficile la sua individuazione. Il malware raccoglie informazioni dal sistema, disabilita i log per evitare di essere tracciato e mostra caratteristiche di offuscamento.