Report Analisi Any.Run – Esercizio 2

1. Introduzione

In questo esercizio abbiamo analizzato un file sospetto usando Any.Run, un ambiente di analisi automatizzata che permette di osservare il comportamento di un file dannoso in un sistema Windows virtuale. L'obiettivo era comprendere se il file fosse pericoloso e raccogliere Indicatori di Compromissione (IoC).

2. Informazioni sul file

- **Nome del file:** Muadrnd.exe
- **Estensione:** .exe
- **Origine:** repository GitHub
- **Tipo di minaccia:** sospetta attività malware con tecniche di evasione e connessioni sospette

3. Cosa fa il file (comportamento)

Appena eseguito, il file lancia una catena di comandi:

- Avvia `cmd.exe` per eseguire comandi silenziosi
- Usa `InstallUtil.exe`, uno strumento spesso abusato dai malware per aggirare gli antivirus
- Viene aperto il browser `firefox.exe`, che fa numerose connessioni verso Internet
- Si esegue una seconda istanza dello stesso file, seguita da altri comandi

Il comportamento è tipico di un file **dropper** o **infostealer** che cerca di nascondersi e connettersi a server esterni per scaricare ulteriori payload o esfiltrare dati.

4. Connessioni sospette (rete)

Il malware apre connessioni a diversi indirizzi IP e domini, tra cui:

- 34.160.144.191 (Google Cloud)
- 104.107.240.43 (Mozilla Push Services)

- 184.24.77.81 (Akamai Technologies)
- prod.westservices.mozcgp.net (dominio sospetto)

Vengono usati protocolli **HTTP**, **UDP**, **TCP** e **DNS**. Il traffico su porte 80 e 443 è indice di tentativi di comunicazione con server esterni, probabilmente per ricevere istruzioni o scaricare altri file.

5. Indicatori di Compromissione (IoC)

- **File sospetto:** Muadrnd.exe
- **Processi:** InstallUtil.exe, cmd.exe, timeout.exe
- **Domini:** *.mozillapush.net, mozcgp.net, outbound CDN
- **Tecniche MITRE ATT&CK rilevate:**
    - Execution: uso di interpreti di comandi
    - Defense Evasion: masquerading, disabilitazione dei log
    - Discovery: interrogazione del registro e informazioni sul sistema
    - Command & Control: uso di porte non standard

6. Conclusione

Il comportamento del file analizzato è tipico di un malware che tenta di sfuggire al rilevamento e comunicare con l'esterno. L'utilizzo di InstallUtil, l'esecuzione silenziosa di comandi e le molteplici connessioni indicano che il file ha finalità potenzialmente dannose. Va trattato come una **minaccia confermata** e isolato da ogni rete di produzione.