S11 L5
Studio Ioc
Esercizio 2

1. Informazioni Generali sul File

- **Nome del file:** Jvczfhe.exe.
- **Verdetto:** Attività malevola.
- **Data analisi:** 25 agosto 2024.
- **Hash SHA256:** 0307EE805DF8B94733598D5C3D62828678EAEADBF1CA3689FA678A3780DD3DF0.
- **Ambiente di test:** Windows 10 Professional a 64 bit.

2. Introduzione all'Analisi

L'oggetto dell'analisi è un file eseguibile denominato **Jvczfhe.exe**.
Il report descrive un'analisi dinamica interattiva eseguita il **25 agosto 2024** in un ambiente controllato con **Windows 10 Professional**.
L'obiettivo è identificare le capacità del software, che è stato classificato con un verdetto di **attività malevola**.

3. Analisi comportamento malware

3.1. Evasione e Anti-Analisi (Fase di "Self-Protection")

Prima di palesare la sua natura malevola, il file cerca di rendersi invisibile ai sistemi di sicurezza:

- **Offuscamento:** Il file è protetto con **.NET Reactor**, un software che cripta e offusca il codice sorgente per impedire agli analisti di capire cosa faccia l'eseguibile.
- **Tecnica del Delay (Sleep):** Il malware avvia `cmd.exe` per eseguire il comando `timeout 21`. Questo ritardo di 21 secondi serve a bypassare le sandbox automatiche che spesso analizzano i file solo per pochi istanti.
- **Disabilitazione dei Log:** Il processo tenta di disabilitare i log di tracciamento del sistema (trace logs) per non lasciare impronte digitali delle sue attività nel registro di Windows.

3.2. Ricognizione del Sistema (Fase di "Fingerprinting")

Una volta attivo, il malware raccoglie informazioni per identificare la vittima e verificare se si trova in un ambiente virtuale (sandbox):

- **Identificazione Univoca:** Legge il **Computer Name** e il **Machine GUID** dal registro di sistema per distinguere il PC infetto da altri.
- **Analisi della Sicurezza:** Controlla le impostazioni di attendibilità di Windows (Trust Settings) e le zone di sicurezza di Internet Explorer.
- **Configurazione di Rete:** Verifica la presenza di server proxy per capire come instradare la connessione verso l'esterno.

3.3. Esecuzione e Iniezione (Fase di "Payload Delivery")

Invece di agire direttamente, il malware preferisce "nascondersi" dietro processi legittimi:

- **Utilizzo di InstallUtil.exe:** Il malware sfrutta `InstallUtil.exe`, uno strumento legittimo di Microsoft .NET, per caricare ed eseguire il codice malevolo. Questo processo è quello che effettivamente apre la connessione verso l'attaccante.
- **Processo Secondario (Muadnrd.exe):** Viene creato o scaricato un secondo eseguibile chiamato `Muadnrd.exe` (identificato come minaccia) che replica i comportamenti del primo, garantendo ridondanza in caso il file principale venga rimosso.

3.4. Connessione Reverse Shell / C2

I dati di rete sono la prova definitiva del tentativo di controllo remoto:

- **Dominio Dinamico:** Il malware contatta `egehgdehjbhitre.duckdns.org`. DuckDNS è un servizio di DNS dinamico molto usato dai criminali informatici perché permette di cambiare rapidamente l'indirizzo IP del server di controllo senza cambiare il nome dominio.
- **Porta Insolita:** La connessione avviene sulla **porta 7702** (non standard), un segnale tipico di una comunicazione tra un malware e il suo server C2.
- **Esecuzione di Comandi:** Il report segnala l'avvio di `CMD.EXE` per l'esecuzione di comandi impartiti dall'esterno. Questo conferma che l'attaccante può inviare

istruzioni testuali che vengono eseguite direttamente sulla macchina vittima, definendo appunto una **reverse shell**.

4. Riassunto delle Attività Rilevate

Il malware si comporta come un **Remote Access Trojan (RAT)** con capacità di stabilire una **reverse shell**. Ecco i punti chiave del suo funzionamento:

- **Evasione e Persistenza**: Utilizza il comando `TIMEOUT.EXE` per sospendere l'esecuzione e ingannare i sistemi di rilevamento automatico. Inoltre, avvia processi che poi vanno in crash per manipolare i log di sistema.
- **Mascheramento**: Sfrutta processi legittimi di Windows, in particolare **InstallUtil.exe** (un'utility di .NET Framework), per eseguire il proprio codice e stabilire connessioni di rete.
- **Infiltrazione nei Browser**: Accede estensivamente ai profili di **Mozilla Firefox**, leggendo database SQLite contenenti cookie, cronologia e impostazioni di sicurezza.
- **Comando e Controllo (C2)**: Tenta di connettersi al dominio dinamico **egehgdehjbhjtre.duckdns.org** sulla porta insolita **7702**.
- **Manipolazione del Registro**: Ha generato oltre **35.000 eventi**, modificando chiavi relative alla privacy, alle impostazioni di rete e ai log di tracciamento.

5. Conclusioni e Mitigazione

In sintesi, il file è un malware sofisticato progettato per il furto di informazioni (Infostealer) e il controllo remoto (RAT). La sua capacità di iniettarsi in processi fidati e comunicare tramite DNS dinamico lo rende una minaccia persistente.

Strategie di Mitigazione

Per proteggere i sistemi e bonificare un'eventuale infezione, si consigliano i seguenti passaggi:

1. **Isolamento della Rete**: Bloccare immediatamente a livello di firewall l'IP **91.92.253.47** e il dominio **duckdns.org** (se non necessario per scopi aziendali).
2. **Terminazione Processi**: Monitorare e terminare istanze anomale di `InstallUtil.exe`, `Jvczfhe.exe` e `Muadnrd.exe`.
3. **Bonifica dei Browser**: Resettare o eliminare i profili browser Firefox compromessi, poiché il malware ha avuto accesso ai dati sensibili memorizzati.
4. **Ripristino Registro**: Rimuovere le chiavi di tracciamento e le modifiche alle zone di sicurezza di Internet Explorer create dal malware.