Report su uno studio loc

Analisi Malware: Jvczfhe.exe

L'analisi identifica il file `Jvczfhe.exe` come una minaccia ad alto rischio (punteggio 100/100), classificata come Malicious Activity. Si tratta di un Trojan di Accesso Remoto (RAT) progettato per compromettere totalmente il sistema della vittima.

1. Obiettivo della Minaccia

L'obiettivo principale di questo malware è stabilire una presenza persistente nel sistema per:

- Esfiltrare dati sensibili: Monitoraggio di tasti premuti (keylogging) e furto di credenziali dai browser.
- Controllo Remoto: Permettere all'attaccante di eseguire comandi a distanza o scaricare ulteriori payload malevoli.
- Sorveglianza: Monitorare l'attività dell'utente senza che questi se ne accorga.

---

2. Analisi del Comportamento (Execution Flow)

L'analisi mostra una catena di esecuzione studiata per eludere i controlli di sicurezza:

- Vettore di Infezione: Il file viene scaricato tramite un browser (`firefox.exe`) da un repository pubblico di GitHub (`MELITERRER/frew`), sfruttando la reputazione del dominio per evitare blocchi preventivi.

- Esecuzione Iniziale: Una volta avviato, `Jvczfhe.exe` (PID 7544) genera processi figli per eseguire script di sistema tramite `cmd.exe`.
- Iniezione di Codice (Process Hollowing): Il malware abusa di `InstallUtil.exe` (PID 1152), un componente legittimo di Windows .NET, per iniettare il proprio codice malevolo e girare "sotto copertura".
- Ingegneria Sociale: Durante l'esecuzione, il malware mostra un pop-up di "Fatal Error". Questo serve a ingannare l'utente, facendogli credere che il programma abbia smesso di funzionare, mentre in realtà continua a operare in background.

---

3. Tecniche di Evasione e Rete

- Protezione del Codice: È stata rilevata la presenza di .NET Reactor, un software di offuscamento utilizzato per impedire il reverse engineering e nascondere le stringhe di comando agli antivirus.
- Attività di Rete: Il malware effettua query DNS e connessioni HTTP verso server remoti (es. `pki-goog.l.google.com` e IP localizzati in Germania) per verificare la connettività e comunicare con il server di Comando e Controllo (C2).

Conclusione

Il malware è estremamente efficace nel nascondersi grazie all'uso di strumenti di sistema legittimi e a tecniche di offuscamento professionale. La distribuzione tramite GitHub indica una campagna mirata a utenti che scaricano software da fonti di sviluppo.