ANALISI MALWARE TRAMITE ANY.RUN

Introduzione

Il presente report riguarda l'analisi di un file sospetto condotta tramite la piattaforma di sandbox interattiva **ANY.RUN**.
L'analisi è stata effettuata il **25 agosto 2024 alle ore 16:11:02**, su un sistema operativo **Windows 10 Pro**.
Link anyrun:
https://app.any.run/tasks/371957e1-d9604b8a-8c68241ff918517d/
Link report anyrun:
https://any.run/report/325396d5ffca8546730b9a56c2d0ed99238d48b5e1c3c49e7d027505ea13b8d1/371957e1-d960-4b8a-8c68-241ff918517d

Il file analizzato, denominato **66bdfcb52736_vidar.exe**, si è rivelato essere associato a una **famiglia di malware** multipla, comprendente:

- **Loader**
- **Lumma Stealer**
- **Vidar Stealer**

Durante l'analisi sono stati rilevati hash che confermano l'unicità e potenziale pericolosità del file:

- **MD5**: `fedb687ed23f77925b35623027f799bb`
- **SHA1**: `7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81`
- **SHA256**: `325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1`

Svolgimento

1. Analisi del Malware per Tipologia

Loader

- **Scopo**: Funziona come punto di accesso iniziale, scaricando ed eseguendo malware aggiuntivo da server remoti.

- **Funzionalità**: Veicola payload dannosi come ransomware, trojan o infostealer, stabilendo comunicazioni con server C2.

Lumma Stealer

- **Scopo**: Infostealer specializzato nel furto di dati sensibili.

- **Funzionalità**:

    - Credenziali (e-mail, social, banking)

    - Dati di carte di credito e wallet

    - Cookie, cronologia browser

    - Informazioni di sistema

Vidar Stealer

- **Scopo**: Malware di tipo infostealer, erede del trojan Arkei.

- **Funzionalità**:

    - Raccolta di credenziali, dati finanziari, cronologia e cookie

    - Informazioni sull’OS e wallet di criptovalute

2. Strategia di Remediation

L’attività di bonifica è stata strutturata in **sei fasi principali**, mirate alla rimozione completa del malware e alla prevenzione di future compromissioni:

Fase 1: Isolamento e Contenimento

- Disconnessione immediata dalla rete per prevenire la propagazione e l’esfiltrazione di dati.

Fase 2: Identificazione e Analisi

- Scansione con strumenti antivirus multipli.
- Analisi dei log, processi e traffico per tracciare payload, C2 e comportamenti anomali.

Fase 3: Rimozione del Malware

- Eliminazione completa dei file infetti, chiavi di registro e processi attivi, anche tramite modalità provvisoria.

Fase 4: Recupero dei Dati

- Ripristino da backup sicuri **antecedenti all’infezione** per evitare reintroduzione del malware.

Fase 5: Bonifica e Ripristino

- Aggiornamento di sistema e software.
- Cambio password e verifica account compromessi.
- Patch delle vulnerabilità sfruttate.
- Rimozione di avvii automatici sospetti.

Fase 6: Monitoraggio e Prevenzione Futura

- Implementazione di soluzioni di sicurezza robuste.
- Autenticazione a più fattori (MFA).
- Formazione degli utenti e monitoraggio continuo del traffico di rete.

---

3. Considerazioni Specifiche per i Malware Coinvolti

- **Loader**: Deve essere rimosso per impedire download futuri di altri malware. Va identificato anche il **vettore d'ingresso iniziale**.
- **Lumma e Vidar Stealer**: Essendo malware da furto di dati, si richiede il cambio urgente delle **credenziali** e il **monitoraggio di eventuali attività fraudolente**.

Conclusione

L'analisi condotta ha confermato la presenza di un file malevolo classificabile come **Loader con payload Stealer**, identificato nei ceppi **Lumma** e **Vidar**.
Questi malware sono specializzati nel **furto di informazioni sensibili** e nella **compromissione dell'integrità del sistema**.

La strategia di remediation proposta si basa su un approccio metodico e articolato che include:

- **Isolamento immediato**
- **Rimozione completa**
- **Recupero sicuro dei dati**
- **Ripristino delle condizioni ottimali**
- **Prevenzione attiva per il futuro**

È essenziale che ogni fase venga implementata correttamente per garantire la **totale eradicazione della minaccia** e la **protezione continua** del sistema e dei dati in esso contenuti.