Report Dettagliato - Analisi Malware

Nome File: 66bddfcb52736_vidar.exe

Tipologia: Loader + Stealer (Vidar, Lumma)

Piattaforma Target: Windows 10 Professional (64 bit)

Data Analisi: 25 Agosto 2024

Analisi Completa

https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d

Verdetto: ATTIVITÀ MALEVOLE RILEVATA

Il file analizzato ha mostrato un comportamento dannoso, con capacità di:

- **Rubare credenziali** da browser, wallet di criptovalute e altri software.
- **Scaricare ed eseguire ulteriori payload malevoli**.
- **Eludere i controlli antivirus** e altre misure di sicurezza.

Analisi Dettagliata

1. Tipologie di Minaccia

- **Vidar Stealer**: Malware attivo dal 2018, noto per il furto di dati di login e criptovalute.
- **Lumma Stealer**: Malware venduto come Malware-as-a-Service (MaaS), continuamente aggiornato.
- **Loader**: Funziona come porta d'ingresso per altri malware.

2. Indicatori di Compromissione (IoCs)

Hash del File Malevolo

- **MD5**: FEDB687ED23F77925B35623027F799BB
- **SHA1**: 7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81

- **SHA256**: 325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1

Attività di Rete

- **Connessioni a server C2 (Command & Control)** per esfiltrare dati rubati.
- **Domini sospetti:**
  - t.me/pech0nk (Possibile Telegram C2)
  - steamcommunity.com/profiles/76561199751190313
  - t.me/jamelwt

File Modificati o Creati

- Creazione di file nascosti nei dati utente (**AppData\Local\Temp\...**)
- Droppati eseguibili sospetti (**RegAsm.exe, HCAEHJJKFC.exe**)

Modifiche al Registro di Windows

- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**
- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**

3. Comportamento del Malware

- Ruba credenziali da browser e account vari.
- Legge impostazioni di sicurezza per eludere il rilevamento.
- Connessioni a server C2 per inviare dati rubati.
- Modifica file di sistema per mantenere l'infezione.

Cosa Abbiamo Fatto?

Dopo aver individuato la minaccia, abbiamo agito prontamente per limitare i danni e garantire la sicurezza del sistema. Inizialmente, abbiamo isolato il file per evitare che potesse causare ulteriori danni. Una volta preso il controllo della situazione, abbiamo eliminato il file dannoso dal sistema e bloccato i server sospetti, impedendo così qualsiasi connessione malevola. Abbiamo continuato a monitorare attentamente la rete e i log di sistema per identificare segni di persistenza della minaccia e, parallelamente, abbiamo effettuato un controllo sulle credenziali per verificare se fossero state compromesse, consigliando il cambio delle password ove necessario. Per garantire un ambiente sicuro, abbiamo anche valutato la possibilità di un ripristino

da backup. Infine, per un'analisi più approfondita, abbiamo inviato il campione al vendor di sicurezza.

Scelte di Remediation e Motivazioni

Opzione	Descrizione	Quando Applicarla
Mettere in quarantena	Spostare il file sospetto in un ambiente sicuro senza eliminarlo subito.	Quando non siamo sicuri al 100% che sia un malware o vogliamo fare ulteriori analisi.
Eliminare il file	Rimuovere definitivamente il file malevolo.	Quando il file è chiaramente dannoso e confermato come minaccia.
Bloccare IP / URL sospetti	Impedire connessioni ai server di comando e controllo (C2).	Quando il malware comunica con server esterni per rubare dati.
Chiedere al vendor	Inviare il file sospetto all'antivirus o a un esperto per un'analisi più approfondita.	Quando il malware è nuovo o poco conosciuto.
Verificare falso positivo / negativo	Controllare se un file segnalato è davvero dannoso o è stato rilevato erroneamente.	Quando un software legittimo viene bloccato per errore o un malware non viene rilevato.
Ripristino da backup	Ripristinare i sistemi a una versione precedente pulita.	Quando il malware ha compromesso file critici o causato danni gravi.
Cambiare credenziali	Forzare il reset di password compromesse.	Quando il malware è uno stealer (come Vidar o Lumma) che ruba login e dati sensibili.
Monitorare il sistema	Tenere sotto controllo i log di sistema per segni di persistenza del malware.	Dopo la rimozione, per assicurarsi che la minaccia non torni.

Come Proteggersi dai Malware?

- **Evitare link sospetti** → Non aprire email e allegati sconosciuti.
- **Aggiornare l'antivirus** → Abilitare la protezione in tempo reale.
- **Monitorare la rete** → Bloccare connessioni sospette.
- **Formare il personale** → Sensibilizzare i dipendenti con corsi di sicurezza.
- **Implementare backup regolari** → Ripristinare in caso di attacco.

Conclusione

Il malware **Vidar/Lumma Stealer** rappresenta una grave minaccia alla sicurezza informatica, in grado di sottrarre dati sensibili e compromettere intere reti aziendali. Abbiamo adottato tutte le misure necessarie per neutralizzare la minaccia e prevenire futuri attacchi. Si consiglia di mantenere alta l’attenzione e applicare le best practice di sicurezza.

Link all'analisi completa