ANALISI DEI LINK ANYRUN

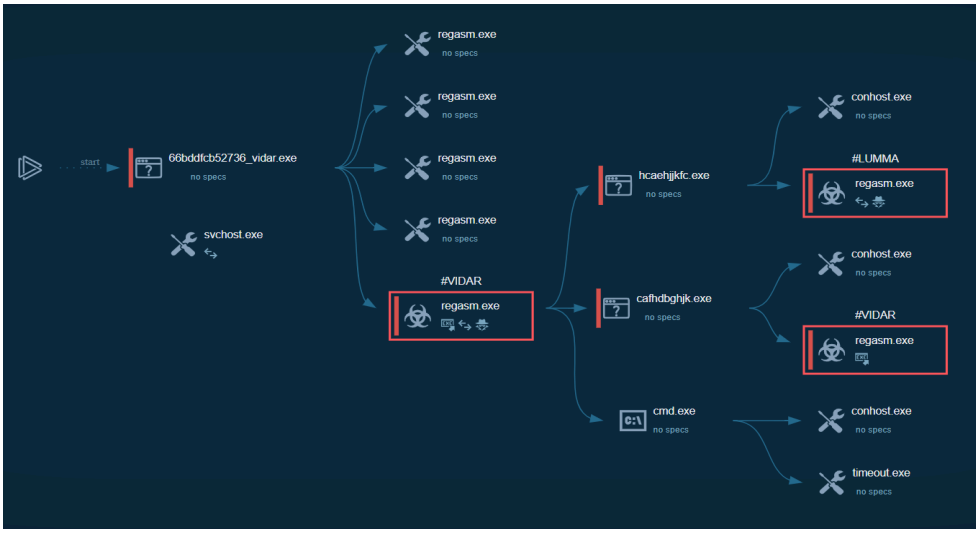
Esercizio 1:

ID Analisi:`66bddfcb52736_vidar.exe`

MD5: fedb687ed23f77925b35623027f799bb

---

1. Spiegazione per il Manager / Cliente



Il file analizzato non è un semplice virus, ma una vera e propria "squadra d'attacco" composta da tre elementi distinti:

- **Il Loader (Il Trasportatore):** è un software dannoso che si infiltra nei dispositivi per distribuire payload malevoli. In particolare questo loader è in grado di infettare i computer delle vittime, analizzare le informazioni del loro sistema e installare altri tipi di minacce. Gli hacker solitamente distribuiscono questi virus tramite email di phishing o tattiche di social engineering, per di più, una volta scaricato, il loader è difficile rilevarlo perché si nasconde come programma legittimo all'interno del sistema infettato.

- **Lumma & Vidar (I Ladri):** sono information stealers sviluppati in C. Vengono messi in vendita come malware as a service, con diversi piani disponibili. solitamente prendono di mira portafogli di criptovalute e credenziali di accesso. In merito al furto delle credenziali, nei sistemi window le password

crittografate possono essere ottenute dai registri di google chrome nel file **App/Data/Local/Google/Chrome/User/Data/Default/Login Data** ed eseguendo una query SQL: **SELECT action_url, username_value,password_value FROM logins;** successivamente la password in chiaro può essere ottenuta utilizzando la API di **Window CryptUnprotectData**.

In parole semplici:

Un finto programma ha aperto la porta a due ladri professionisti che hanno il compito di svuotare le casseforti digitali (le password) dell'azienda.

---

2. Scelte di Remediation e Motivazioni

In base alle evidenze tecniche, ecco le azioni da intraprendere:

- **Classificazione: Vero Positivo.**
  - *Motivazione:* L'attività rilevata è inequivocabilmente malevola (furto di dati e installazione di minacce aggiuntive).

- **Scelta: Quarantena ed Eliminazione immediata.**

  - ***Motivazione**:* Trattandosi di un "Loader", il file potrebbe continuare a scaricare nuovi virus se lasciato nel sistema.

- **Scelta: Blacklist.**

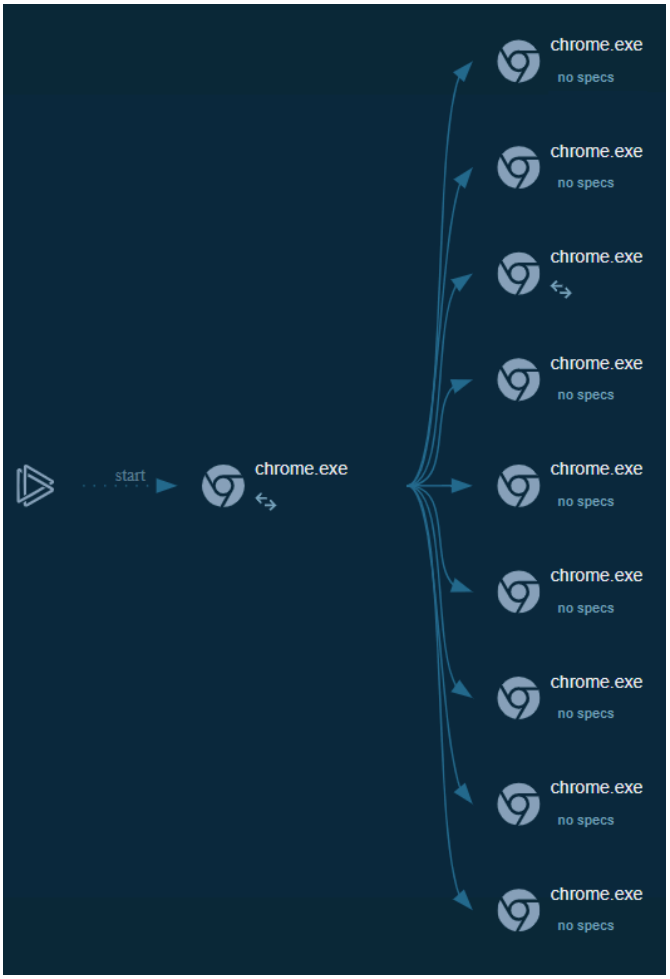
  - ***Motivazione**:* È necessario bloccare a livello di rete tutti i server esterni (C2) contattati dal malware per impedire che i dati rubati vengano spediti ai criminali.

- **Scelta: Reset Forzato delle Credenziali.**

- ***Motivazione**:* Poiché Vidar e Lumma sono "Stealer", dobbiamo dare per scontato che ogni password presente su quel computer sia stata già compromessa.

Esercizio 2:

Analisi della Minaccia



- **Identificazione**: Il sistema ha analizzato un indirizzo web (URL) e il verdetto è **"No threats detected"** (Nessuna minaccia rilevata).

- **Spiegazione per il Management**: Il collegamento analizzato appartiene a una piattaforma di email marketing ampiamente utilizzata (ConvertKit). Viene spesso usato per tracciare i clic nelle newsletter aziendali legittime. Durante l'analisi, il link non ha mostrato comportamenti sospetti, come il download automatico di file o il reindirizzamento verso siti fraudolenti.

- **Rischio Aziendale**: **Assente**. Si tratta di una normale attività di comunicazione digitale.

2. Scelte di Remediation e Motivazioni

- **Classificazione: Vero Negativo**.
    - **Motivazione**: Il sistema ha correttamente analizzato l'elemento e ha confermato che non rappresenta un pericolo.
- **Azione**: **Nessun intervento richiesto**.
    - **Motivazione**: Non essendoci minacce, non è necessario mettere in quarantena o bloccare il dominio. L'utente può procedere con la navigazione.
- **Nota di sicurezza**: Nonostante l'esito negativo, è sempre buona norma non cliccare su link provenienti da email di cui non si conosce il mittente, poiché un sito sicuro oggi potrebbe essere compromesso domani.
