Esercizio 5: Anyrun

Studiare questi link di anyrun e spiegare queste minacce in un piccolo report.

https://app.any.run/tasks/371957e1-d960¾4b8a-8c68¾241ff918517d/ https://app.any.run/tasks/f1f20828¾2222¾46fb-a886¾09f77581e67b/

Analisi del primo link

Riepilogo: Cosa è Successo

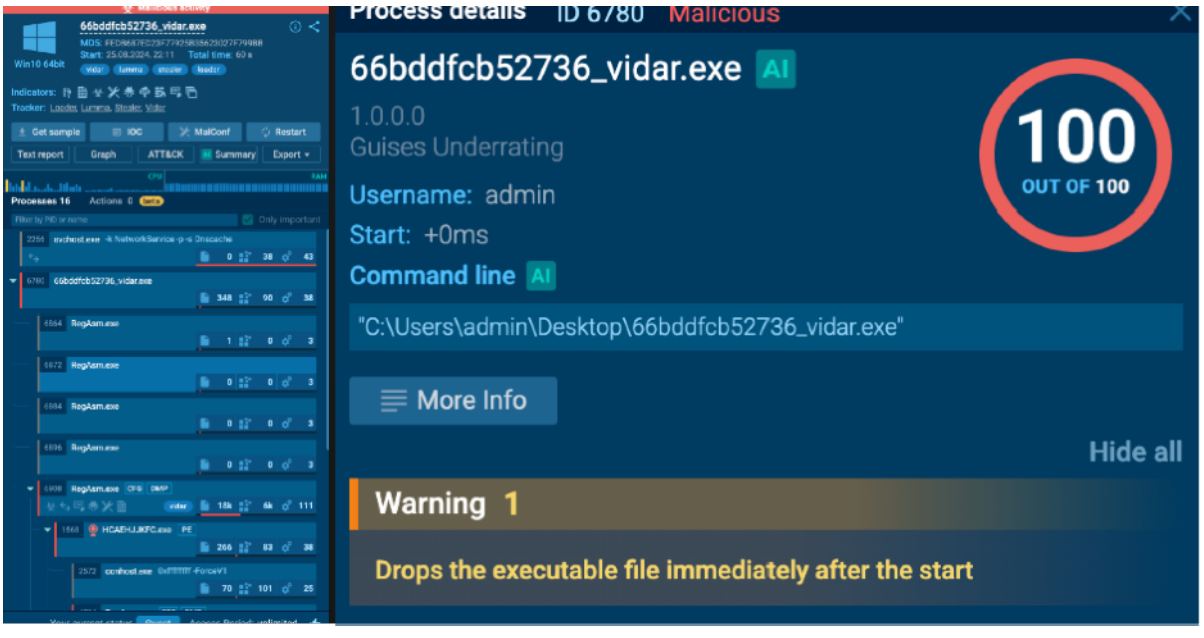
Il file che è stato eseguito, identificato come **`66bddfcb52736_vidar.exe`**, è un malware estremamente pericoloso, classificato come un **InfoStealer** (ladro di informazioni) di tipo **Vidar**, ma mostra anche comportamenti tipici di **Lumma** e funge da **Loader** per altro codice malevolo.

In termini semplici: **il tuo computer è stato infettato da un software spia che cerca di rubare i tuoi dati e le tue password, e ha cercato anche di scaricare altri programmi dannosi.**

Analisi Dettagliata delle Attività Maligne

1. L'Infezione Iniziale (Il "Paziente Zero")

- **File Principale: `66bddfcb52736_vidar.exe`** (ID 6780).
- **Comportamento:** Ha un punteggio di pericolo di **100/100** e viene rilevato immediatamente come **Vidar**. Il file **"Drops the executable file immediately after the start"** (rilascia l'eseguibile immediatamente dopo l'avvio). Questo significa che il primo file ha subito iniettato/creato altri file malevoli per iniziare le sue operazioni e mascherarsi.

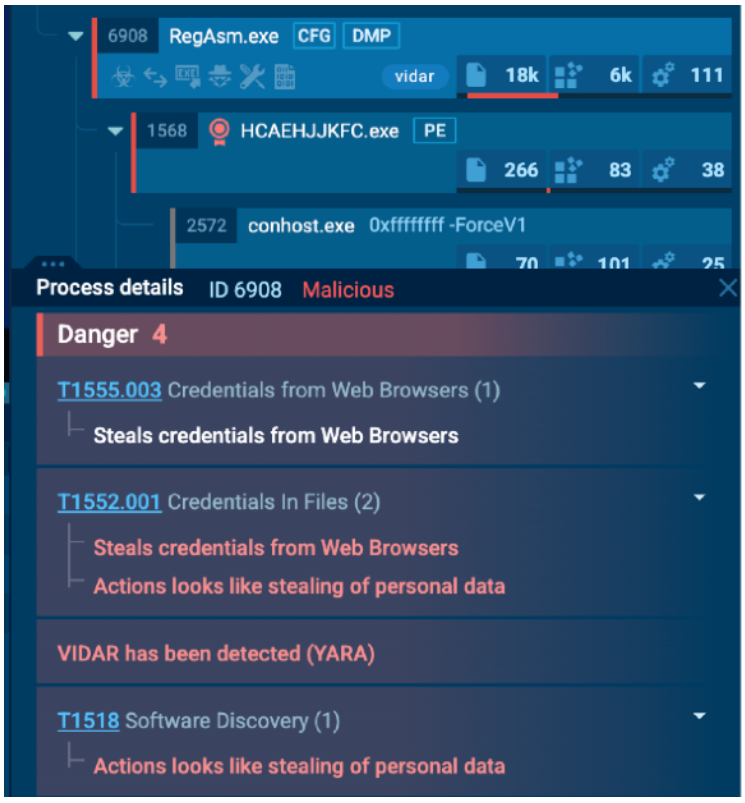


2. Il

Camuffamento e l'Azione Principale

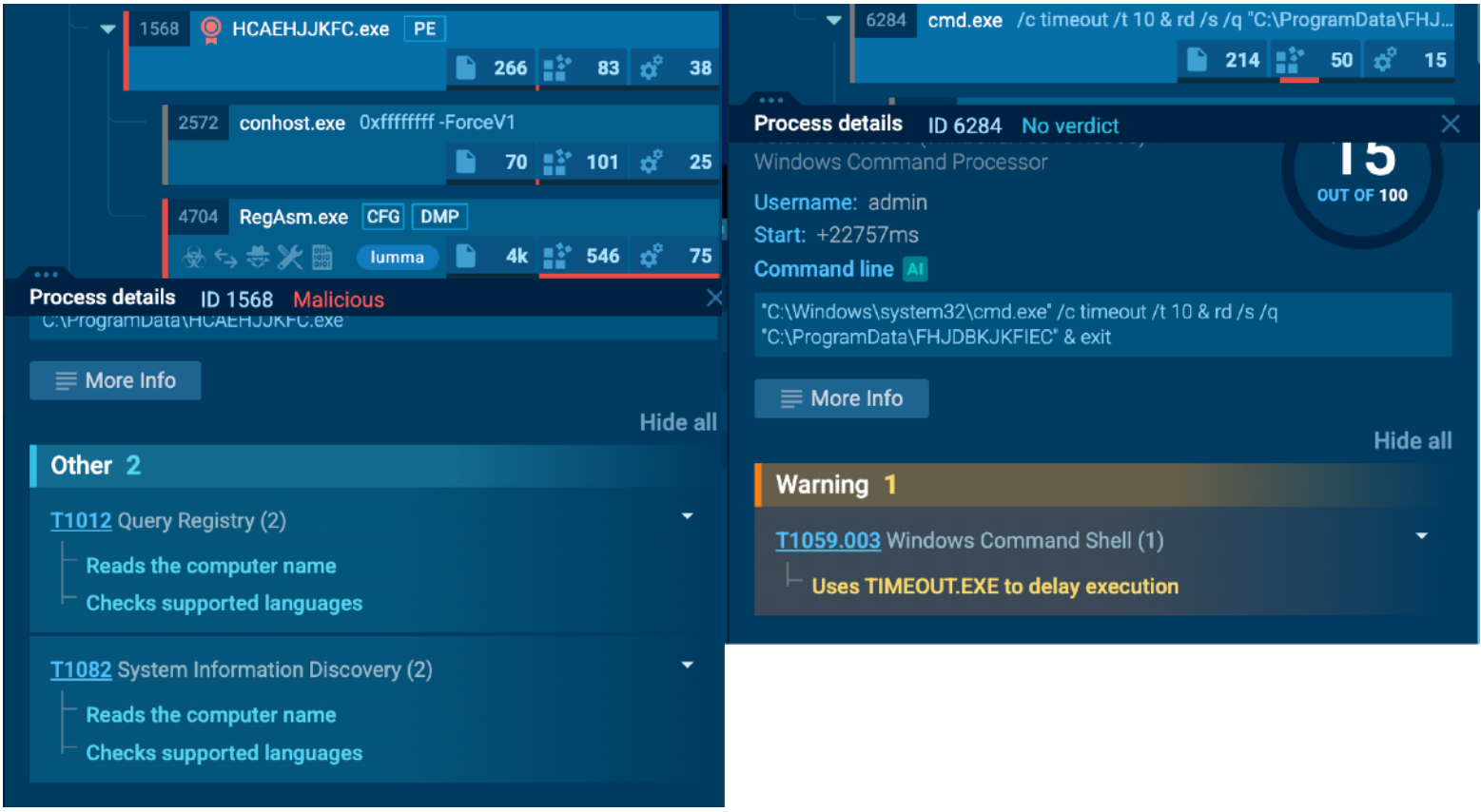
Il malware usa processi legittimi di Windows per nascondere le sue attività:

- **Processo Fittizio:** Vengono eseguiti più istanze del file **`RegAsm.exe`** (Microsoft .NET Assembly Registration Utility), che è un programma legittimo di sistema, ma in questo caso viene abusato dal malware.
    - **`RegAsm.exe` (ID 6908):** Questo è il cuore dell'attività di furto. L'analisi rileva chiaramente: **"Steals credentials from Web Browsers" (Ruba le credenziali dai browser web)**, un chiaro segnale di un InfoStealer (ladro di informazioni).
- **Download di Altro Malware (Loader):** Lo stesso processo `RegAsm.exe` (ID 6908) è stato visto eseguire **richieste HTTP** (con IP russo) che portavano a scaricare **"executable"** (file eseguibili/programmi) e traffico classificato come **"Potentially Bad Traffic"** e **"INFO Executable Download"**. Questo conferma che il malware principale sta agendo anche da **Loader**, scaricando altri componenti o altri malware.



3. Attività di Esecuzione e Persistenza

- **Esecuzione Nascosta:** Viene notato un altro processo, **`HCAEHJJJKFC.exe`** (ID 1568), eseguito da una cartella **`C:\ProgramData\`**. Questo è un nome casuale per un file, tipico di malware che cerca di nascondersi in cartelle di sistema.
- **Spionaggio:** Questo processo (ID 1568) **"Reads the computer name" (Legge il nome del computer)** e altri dati di sistema (**"Query Registry"**), tipico di InfoStealer che raccolgono informazioni di base sul sistema prima di esfiltrare i dati.
- **Comando Sospetto:** Il malware utilizza il comando **`cmd.exe /c timeout t 10 & rd /s /q ...`** (ID 6284). Questo è un comando che spesso viene usato per **eliminare i file lasciati dall'infezione** ("pulizia delle tracce") o per eseguire altre azioni di sistema in modo automatizzato.



4. Le Minacce Rilevate (I Nomi in Codice)

Il malware è etichettato con vari nomi, il che è comune perché un file può combinare le funzionalità di diversi tipi di minaccia:

- **Vidar:** Un noto InfoStealer che prende credenziali, portafogli di criptovalute e altri dati sensibili.
- **Lumma:** Un altro InfoStealer molto diffuso e pericoloso, confermato dalla minaccia **"STEALER (ANY.RUN) Lumma Stealer TLS Connection"** (ID 4704).
- **Loader:** La capacità di scaricare e installare altro software malevolo.

Linee Guida di Prevenzione e Sicurezza

1. Protezione Immediata dei Dati

- **Cambia tutte le Password: Il malware ha rubato le credenziali dai tuoi browser.**
- **Abilita l'Autenticazione a Due Fattori (2FA)**
- **Controlla i Conti Bancari/Finanziari:** Verifica se ci sono state transazioni sospette.

2. Pulizia del Sistema

- **Scollega la Macchina da Internet:** Impedisci al malware di inviare i dati rubati.
- **Esegui un'Analisi Approfondita:** Usa un software antivirus per una scansione completa in **Modalità Provvisoria** o con un "Rescue Disk".

3. Consigli per il Futuro / Prevenzione

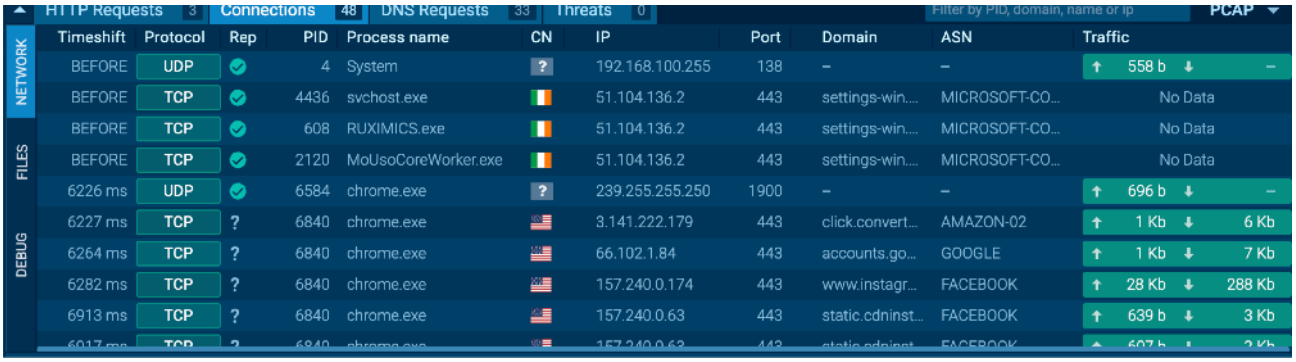
- **Sii Sospettoso dei File Sconosciuti:** Non scaricare ed eseguire mai allegati email o file (specialmente archivi ZIP/RAR) provenienti da mittenti non verificati o siti web pirata. Gli InfoStealer come Vidar e Lumma sono spesso distribuiti tramite email di phishing o download illegali.
- **Mantieni il Sistema Aggiornato:** Assicurati che il tuo sistema operativo e il tuo browser siano sempre aggiornati. Gli aggiornamenti contengono spesso correzioni di sicurezza essenziali.
- **Usa un Password Manager:** Usa strumenti come 1Password, LastPass, o Bitwarden. Questi salvano le password in una cassaforte crittografata e le inseriscono automaticamente, riducendo il rischio che un malware le trovi nei file non crittografati dei browser.
- **Installa un Antivirus/Endpoint Protection:** Un buon software di sicurezza può bloccare queste minacce prima che vengano eseguite.

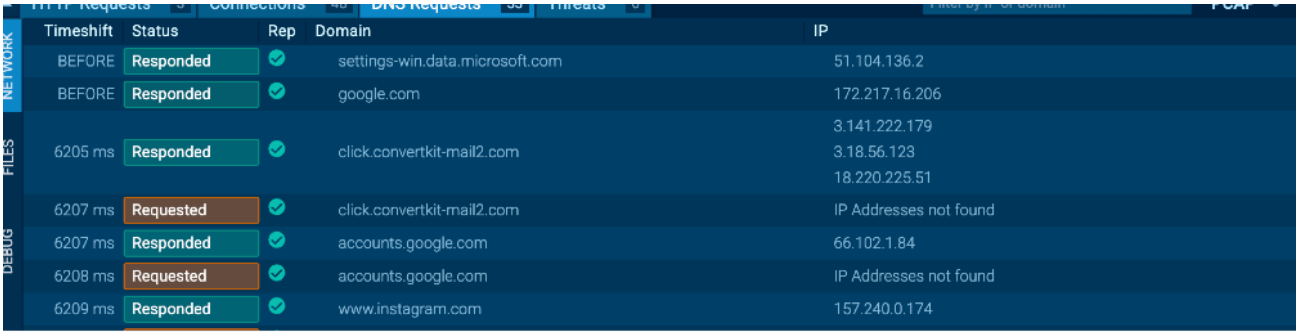
In sintesi, l'analisi ha confermato una grave infezione da InfoStealer multifunzione. La priorità assoluta è il cambio di password e l'attivazione della 2FA.

Analisi del secondo link

Analisi dei dati

In base ai dati possiamo vedere che non ci sono minacce evidenti e sembrerebbe tutto in regola.





L'analisi del traffico di rete non ha rilevato download di malware, ma gli URL di login mostrati negli screenshot (**Instagram e Facebook**) indicano un'attività di navigazione non standard e altamente sospetta.

Il problema principale non è l'indirizzo base (`instagram.com` o `facebook.com`), ma i **parametri aggiuntivi** che manipolano il flusso di accesso.

1. Anomalie nell'URL di Instagram

?next= Indica la pagina a cui l'utente deve essere reindirizzato *dopo* un login riuscito

Problema

L'URL di destinazione è un profilo specifico (`aussienurserecruiters`) e non la homepage dell'utente o la pagina di feed.

Un attaccante potrebbe aver manipolato il browser per aggiungere questo parametro. Lo scopo è forzare l'utente, subito dopo il login (e il potenziale furto di credenziali), ad atterrare su un profilo specifico o una pagina controllata per ulteriori azioni.

2. Anomalie nell'URL di Facebook

api_key=... e app_id= = Questi parametri sono usati per gli accessi tramite applicazioni esterne o servizi di terze parti (I valori specifici delle chiavi API e degli ID app sono sospetti)

Problema

La presenza di un **`api_key`** e **`app_id`** sconosciuti suggerisce che l'utente non è stato semplicemente sul sito di Facebook, ma è stato **reindirizzato** da un'applicazione o un link esterno **mascherato** che tenta di ottenere le **credenziali di accesso**. Se l'utente si logga, non sta solo accedendo a Facebook, ma sta concedendo l'autorizzazione a una specifica (e potenzialmente malevola) **applicazione** di **terze parti**.

Conclusione Vero Negativo

Dopo un'analisi più approfondita, abbiamo confermato che l'azione avvenuta **non è malevola**, classificandola come **Vero Negativo (TN)**. L'attività è risultata provenire da un servizio legittimo di email marketing.

Prevenzione

1. Concentrati sul Dominio Principale (La Radice)
2. Diffida dei Sottodomini Sospetti
3. Controlla il "Lucchetto" (HTTPS)
4. Analisi dei Parametri (`?next=`, `&app_id=`)