TRACCIA 2

□ Report di Analisi delle Minacce Anyrun

Data: 03/02/2025
Piattaforma di Analisi: AnyRun

---

1. Introduzione

Questo report sintetizza l'analisi di due campioni sospetti esaminati tramite AnyRun. Le evidenze raccolte indicano comportamenti tipici di malware attivi, con implicazioni potenzialmente gravi per l'infrastruttura aziendale. Le misure di remediation consigliate sono finalizzate a isolare e neutralizzare le minacce, nonché a rafforzare la sicurezza complessiva.

---

2. Analisi Tecnica Dettagliata

Campione 1

Report di Analisi del Malware Vidar

Analisi tramite Any.Run

Data dell'analisi: 25 agosto 2024
Sistema operativo analizzato: Windows 10 64-bit
Tempo totale di esecuzione: 6 secondi
Hash del file eseguibile: `66dbdfcb52736`
Nome del file malevolo: `vidar.exe`
Indicatori rilevati: **Attività malevola confermata**

---

1. Descrizione del Malware

Vidar è un malware infostealer avanzato progettato per sottrarre dati sensibili dai sistemi infetti. Può esfiltrare credenziali salvate nei browser, cookie, informazioni su criptovalute, dati di carte di credito e altre informazioni sensibili.

---

2. Processi Identificati

Durante l'analisi, sono stati osservati i seguenti processi malevoli:

- `vidar.exe` **(PID: 348)** → Processo principale del malware, responsabile della raccolta dei dati.
- `RegAsm.exe` **(PID: 69, 470, 474, 476)** → Multipli istanze di questo processo suggeriscono tecniche di persistenza o evasione.
- `conhost.exe` **(PID: 156, 192)** → Associato a Vidar, potrebbe essere usato per eseguire comandi senza essere visibile all'utente.
- `cmd.exe` **(PID: 63)** → Utilizzato per eseguire comandi di sistema con timeout.
- `svchost.exe` **(PID: 2226)** → Utilizzato per comunicazioni di rete, potrebbe indicare esfiltrazione dei dati.

---

3. Attività di Rete

Durante l'esecuzione del malware, sono state osservate diverse richieste HTTP. Alcuni URL di interesse includono:

Timestamp	Metodo	Codice	Processo	URL
1057 ms	GET	200 OK	svchost.exe	`hxxp://nscq.digicert.com/...` (Potenziale comando C2)
2815 ms	GET	200 OK	RegAsm.exe	`hxxp://47.45.14.144/blog/update64bitdeb8.exe`
2815 ms	GET	200 OK	SHClient.exe	`hxxp://47.45.14.144/blog/6a6c6f4a1d_volkerx.exe`
2815 ms	GET	200 OK	SHClient.exe	`hxxp://www.microsoft.com/pkiops/...`

I domini **`47.45.14.144`** e **`nscq.digicert.com`** sono sospetti e possono essere server di comando e controllo (C2) utilizzati dal malware per ricevere istruzioni e trasmettere i dati rubati.

---

4. Indicatori di Compromissione (IoC)

Tipo	Valore
Hash MD5	`66dbdfcb52736`
IP Sospetto	`47.45.14.144`
Dominio sospetto	`nscq.digicert.com`
File sospetto	`vidar.exe`
Processi anomali	`RegAsm.exe`, `conhost.exe`, `svchost.exe`

---

5. Mitigazione e Contromisure

✅Passaggi immediati

1. **Isolare il sistema infetto** → Disconnettere il dispositivo da Internet per impedire l'esfiltrazione dei dati.
2. **Terminare i processi malevoli** → Utilizzare **Process Explorer** o **Task Manager** per terminare `vidar.exe`, `RegAsm.exe` e `conhost.exe`.
3. **Bloccare i domini sospetti** → Implementare regole firewall per impedire comunicazioni con `47.45.14.144` e `nscq.digicert.com`.
4. **Scansionare il sistema** → Usare software anti-malware avanzati (es. **Malwarebytes, Kaspersky, Windows Defender ATP**) per rimuovere Vidar.
5. **Cambiare tutte le credenziali** → Se il malware ha sottratto password, cambiare immediatamente le credenziali di account sensibili.

□ Protezione a lungo termine

- **Abilitare Windows Defender ATP** e strumenti EDR per il monitoraggio delle attività sospette.

- **Bloccare esecuzione di script non firmati** tramite policy di sistema (`gpedit.msc` → `Computer Configuration` → `Administrative Templates` → `System`).
- **Usare l'Autenticazione a Due Fattori (2FA)** per proteggere gli account compromessi.

---

6. Conclusioni

Il malware **Vidar** è stato confermato attivo sul sistema analizzato, mostrando una tipica catena di infezione con esecuzione di eseguibili secondari, comunicazione con server C2 e possibile furto di dati sensibili. È **necessario intervenire immediatamente** con misure di sicurezza per evitare ulteriori compromissioni.

Campione 2

Report di Analisi – Attività Sospetta su Browser (Phishing & Redirect)

Analisi tramite Any.Run

Data dell'analisi: 25 agosto 2024
Sistema operativo analizzato: Windows 10 64-bit
Tempo totale di esecuzione: 47 secondi
Stato della minaccia: Attività sospetta rilevata
Indicatori di compromissione: Possibile phishing o attività malevola tramite redirect

---

1. Descrizione dell'Attività Malevola

Questa analisi mostra un comportamento sospetto all'interno del browser Google Chrome, con un tentativo di accesso a un **falso sito di login di Instagram**. Il malware o un attore malevolo potrebbe aver aperto automaticamente il browser per eseguire il furto di credenziali.

L'URL sospetto presente nella barra degli indirizzi sembra essere un link manipolato che reindirizza gli utenti a un'eventuale pagina di **phishing**.

---

2. Processi Osservati

Diversi processi legati a **Google Chrome** sono stati avviati, probabilmente per eseguire lo script malevolo:

- **`chrome.exe` (PID: 6504)** → Ha letto chiavi di registro di Microsoft Office (possibile abuso per raccolta di informazioni).
- **Multipli `chrome.exe` renderer** → Usati per gestire il caricamento della pagina e possibili attività di background.
- **`svchost.exe` (PID: 2226)** → Ha effettuato richieste HTTP verso un dominio sospetto.
- **`SHClient.exe` (PID: 6296, 6346)** → Comunicazioni sospette con server esterni.

---

3. Attività di Rete

Sono state rilevate più richieste HTTP verso URL sospetti:

Timestamp	Metodo	Codice	Processo	URL
8047 ms	GET	200 OK	`svchost.exe`	`hxxp://nscq.digicert.com/...`
2815 ms	GET	200 OK	`SHClient.exe`	`hxxp://www.microsoft.com/pkiops/...`

Inoltre, l'URL principale analizzato è:

- **`hxxps://click.convertkit-mail2.com/wvuqgqrvwagh50ndd6c7hxxl...`** → Possibile link di phishing o C2 server.

---

4. Indicatori di Compromissione (IoC)

Tipo	Valore
URL sospetto	`hxxps://click.convertkit-mail2.com/...`
Processo malevolo	`chrome.exe` con attività anomala
Dominio sospetto	`nscq.digicert.com`
Richieste di rete	`svchost.exe` e `SHClient.exe` con connessioni non riconosciute

---

5. Mitigazione e Contromisure

✅Azioni immediate

1. **Non inserire alcuna credenziale** sulla pagina di login di Instagram finché il sistema non è stato verificato.
2. **Chiudere immediatamente tutte le finestre del browser** e terminare i processi sospetti (`chrome.exe` e `SHClient.exe`).
3. **Bloccare l'URL sospetto** nei filtri del firewall aziendale o di rete personale.
4. **Effettuare una scansione del sistema** con un **antivirus avanzato** come **Windows Defender ATP, Malwarebytes o Kaspersky**.
5. **Cambiare tutte le password salvate nel browser**, nel caso in cui il malware abbia già raccolto credenziali.

🔒 Protezione a lungo termine

- **Utilizzare un'estensione di sicurezza per il browser**, come **uBlock Origin o Malwarebytes Browser Guard**, per prevenire il caricamento di pagine di phishing.
- **Abilitare l'autenticazione a due fattori (2FA)** su Instagram e altri servizi sensibili.
- **Verificare la configurazione del DNS e il file `hosts`** (`C:\Windows\System32\drivers\etc\hosts`) per assicurarsi che il sistema non stia reindirizzando verso server malevoli.
- **Monitorare i log di rete** con strumenti come **Wireshark o Splunk** per verificare eventuali esfiltrazioni di dati.

---

6. Conclusioni

L'analisi suggerisce che il sistema sia stato esposto a un **tentativo di phishing avanzato**. Il malware potrebbe aver aperto il browser automaticamente per portare la vittima su una **pagina di login falsa di Instagram**, con l'obiettivo di rubare credenziali. È altamente consigliato **non interagire con il sito** e **eseguire una bonifica immediata del sistema**.

---

4. Conclusioni e Raccomandazioni Generali

- **Valutazione Complessiva:**
  Entrambi i campioni sono confermati come **Vero Positivo**, con comportamenti malevoli che richiedono interventi tempestivi.
- **Azioni Immediati:**
  - **Isolamento/Quarantena:** Bloccare immediatamente i sistemi e i file interessati.

    - **Pulizia e Scansione:** Eseguire scansioni complete per identificare eventuali altre minacce o componenti residui.
    - **Aggiornamento Sicurezza:** Rafforzare le regole del firewall e aggiornare le blacklist per prevenire comunicazioni con server C2.
    - **Coordinamento con il Vendor:** Inviare il report completo agli sviluppatori per migliorare le difese e aggiornare le definizioni delle minacce.
- **Raccomandazioni per il Management:**
    - **Investimento in Cyber Security:** Considerare il potenziamento degli strumenti di protezione (IDS/IPS, endpoint security, etc.).
    - **Piano di Contingenza:** Verificare l'efficacia dei backup e aggiornare il piano di risposta agli incidenti.
    - **Formazione Continua:** Promuovere sessioni di aggiornamento per tutto il personale in modo da migliorare la consapevolezza sulle minacce informatiche.