Report Esercizio 5 (PT.1): Malware Vidar (Infostealer)

A cura di Iris Canole, Federico Giannini, Daniele Castello, Luca Pani, Rosario Papa, Yari Olmi, Alessandro Salerno

#buildweek

1.0 Panoramica Gestionale (Management Overview)

Questo report ha lo scopo di fornire un'analisi chiara e non tecnica della minaccia malware nota come "Vidar". Il documento illustra il potenziale impatto di questa minaccia sulle operazioni aziendali e delinea un piano d'azione strategico per la risposta e la prevenzione. È stato redatto specificamente per i decisori aziendali, al fine di supportare una comprensione completa del rischio e delle contromisure necessarie.

I risultati chiave della nostra analisi possono essere riassunti come segue:

- **La Minaccia:** Abbiamo identificato un malware di tipo "infostealer" chiamato Vidar. Questo software dannoso è specificamente progettato per infiltrarsi nei sistemi informatici e rubare un'ampia gamma di dati sensibili, tra cui credenziali di accesso, informazioni bancarie, cookie di sessione e portafogli di criptovalute.
- **L'Impatto:** L'infezione da Vidar rappresenta un rischio concreto e immediato per l'azienda. Le conseguenze possono includere la compromissione di account aziendali critici, perdite finanziarie dirette dovute al furto di dati bancari o asset digitali, e significative violazioni della privacy dei dati che possono comportare danni reputazionali e sanzioni normative.
- **La Soluzione:** È stato definito un piano di risposta strutturato, suddiviso in fasi, per contenere immediatamente il danno, eradicare completamente la minaccia dai sistemi colpiti e, soprattutto, rafforzare le nostre difese per prevenire incidenti futuri di questa natura.

Per affrontare efficacemente questo rischio, è essenziale comprendere in dettaglio la natura del malware che stiamo fronteggiando.

2.0 Identificazione della Minaccia: Conoscere il Nemico

Identificare con precisione una minaccia informatica è il primo, fondamentale passo per combatterla efficacemente. Comprendere le caratteristiche specifiche, le capacità e le firme digitali di un malware

ci permette di calibrare la nostra risposta, scegliere gli strumenti giusti e implementare le difese più adeguate.

Il malware analizzato è **Vidar**, un software specializzato nel furto di informazioni (noto come *infostealer*). Il suo nome deriva dal dio della vendetta della mitologia scandinava, un'analogia che ben rappresenta la sua natura aggressiva e dannosa. Le sue principali capacità, tradotte in rischi di business, includono:

- **Furto di credenziali:** Sottrazione di nomi utente, password e dati di sessione salvati nei principali browser (incluso il browser per la navigazione anonima TOR), che possono dare agli aggressori accesso diretto a servizi cloud aziendali, email, VPN e portali clienti.
- **Furto di cookie di sessione:** Acquisizione dei cookie di sessione del browser, che possono consentire a un aggressore di bypassare l'autenticazione (inclusa l'MFA) e accedere a sessioni web già attive, come quelle della posta elettronica o dei portali aziendali.
- **Sottrazione di dati finanziari:** Acquisizione mirata dei dati di compilazione automatica dei browser, che spesso includono numeri di carte di credito, date di scadenza, indirizzi di fatturazione e dettagli di conti bancari.
- **Furto di asset digitali:** Ricerca attiva e furto di file relativi a portafogli di criptovalute, inclusi quelli conservati offline, con conseguente perdita irreversibile di fondi.
- **Spionaggio:** Acquisizione di screenshot dello schermo della vittima per monitorare le attività e registrazione di messaggi da software di comunicazione, esponendo conversazioni private e dati aziendali riservati.
- **Furto di file:** Sottrazione di documenti specifici, come file di testo, che potrebbero contenere ulteriori informazioni sensibili.

Identificatori Tecnici Univoci (Hashes)

Questi valori funzionano come impronte digitali uniche. I nostri team di sicurezza utilizzano questi "Indicatori di Compromissione" (IOC) per dare la caccia a questa specifica minaccia attraverso la nostra rete e configurare le nostre difese per bloccarla automaticamente. Le seguenti firme digitali identificano in modo univoco il campione di malware analizzato.

Tipo di Hash	Valore
MD5	`FEDB687ED23F77925B35623027F799BB`
SHA1	`7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81`

SHA256	`325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1`

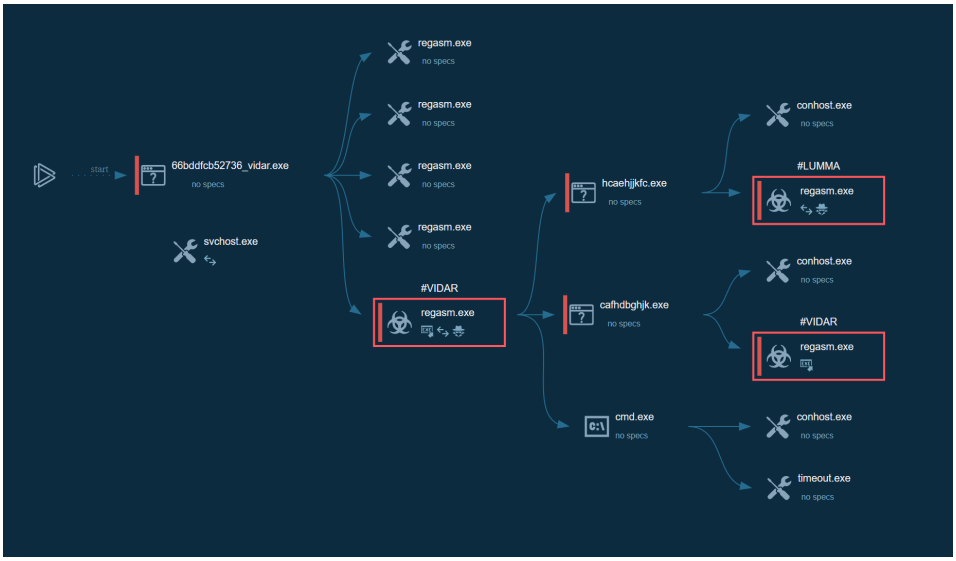
Ora che abbiamo identificato il nemico, è cruciale analizzare come agisce concretamente una volta che ha infettato un sistema.

3.0 Anatomia dell'Attacco: Come Opera Vidar

Comprendere le tattiche operative di un aggressore non è un mero esercizio tecnico; è un'esigenza strategica per un manager. Questa conoscenza permette di apprezzare la sofisticazione della minaccia, giustifica la necessità di difese a più livelli e chiarisce perché una semplice soluzione antivirus potrebbe non essere sufficiente.

3.1 Catena di Esecuzione e Tattiche di Evasione

Vidar non opera da solo, ma agisce come un **loader** attraverso una **catena di esecuzione a cascata**. Ciò significa che il file iniziale, `vidar.exe`, non solo esegue le proprie attività di furto di dati, ma funge anche da "porta d'ingresso" per installare altre minacce. La nostra analisi ha rivelato che Vidar ha scaricato un secondo infostealer, **Lumma**, sul sistema compromesso. L'impatto aziendale è quindi doppio: non stiamo affrontando una singola infezione, ma un potenziale gateway per attacchi multipli e simultanei, dove Vidar potrebbe rubare le credenziali mentre Lumma si concentra sui portafogli di criptovalute.



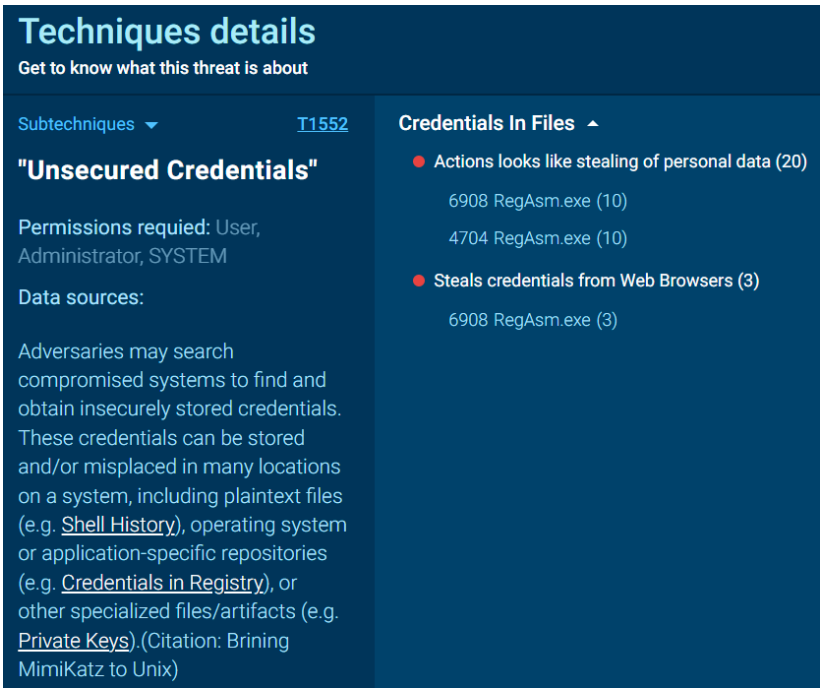
L'analisi del flusso dei processi rivela come Vidar sfrutti strumenti di sistema per i propri scopi:

- `RegAsm.exe`: Dal punto di vista della risposta agli incidenti, l'esecuzione ripetuta di `RegAsm.exe` da parte di un processo non firmato è un indicatore definitivo di attività dannosa. Si tratta di una tecnica nota utilizzata dagli avversari per iniettare codice e rubare credenziali mascherandosi da strumento di sistema legittimo di Microsoft `.NET` Framework.
- `svchost.exe`: Questo è un processo di sistema critico di Windows. Vidar ne abusa per "mimetizzarsi" con le normali attività del sistema operativo. Questa tecnica gli permette di eludere il rilevamento e di comunicare con i server di comando e controllo degli aggressori senza destare sospetti.

3.2 Tecniche di Furto delle Credenziali

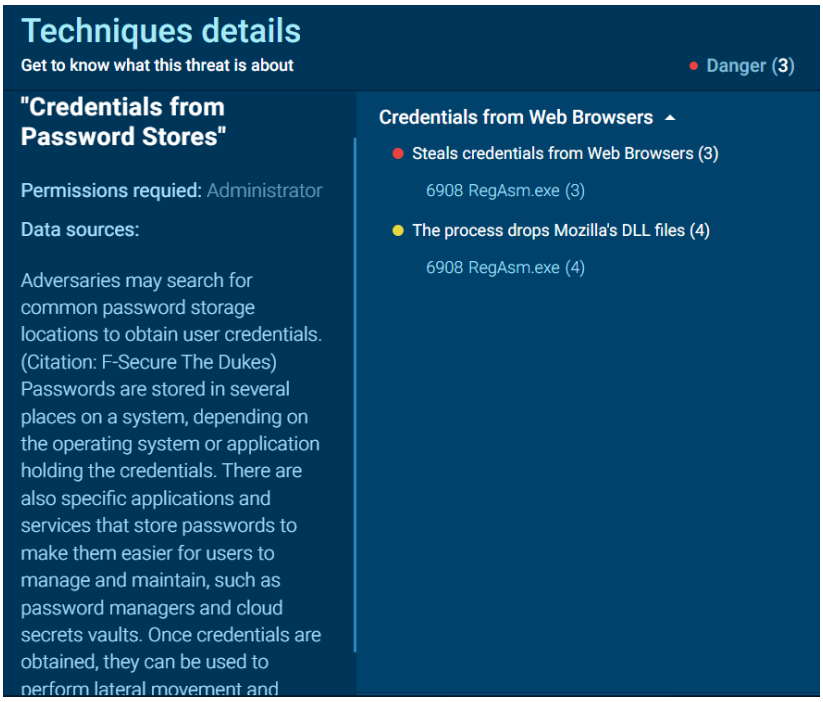
L'obiettivo primario di Vidar è localizzare ed estrarre credenziali in ogni forma possibile. Per farlo, utilizza tecniche specifiche.

Tecnica: "Unsecured Credentials" Il malware ricerca attivamente credenziali salvate in modo non sicuro all'interno del sistema. Queste possono trovarsi in file di testo semplici, nella cronologia dei comandi della shell o in aree del registro di sistema. Questa tattica sfrutta le cattive abitudini degli utenti di salvare le password in luoghi non protetti.



Tecnica: "Credentials from Password Stores" Questa è la tecnica più pericolosa. Vidar prende di mira specificamente i database di credenziali salvate all'interno dei browser web. Per un aggressore, questa è una vera e propria miniera d'oro, poiché contiene gli accessi a innumerevoli servizi online, sia personali che aziendali. L'analisi tecnica mostra che Vidar è altamente specializzato, arrivando a

rilasciare file DLL specifici di Mozilla per estrarre con successo le credenziali dal browser Firefox. Il processo `RegAsm.exe` è direttamente coinvolto in questa attività.



Comprendere come Vidar agisce è fondamentale, ma è altrettanto importante sapere come riesce a entrare nei nostri sistemi in primo luogo.

4.0 Vettori di Infezione e Misure di Prevenzione

La prevenzione è la nostra prima, e più importante, linea di difesa. Comprendere come le minacce entrano in azienda è essenziale per costruire barriere efficaci e per formare il nostro personale, che rappresenta l'elemento umano cruciale nella catena della sicurezza.

4.1 Come si Diffonde Vidar

Vidar utilizza metodi di distribuzione comuni ma efficaci, che fanno leva sull'ingegneria sociale e sulla disattenzione dell'utente. Un dettaglio di threat intelligence rilevante è che le campagne di Vidar prendono di mira utenti in tutto il mondo, ad eccezione di alcuni paesi dell'ex Unione Sovietica, inclusa la Russia.

1. **Campagne di Phishing via Email:** Il metodo di infezione più comune. Gli aggressori inviano email di spam che sembrano legittime, contenenti allegati dannosi (es. finti documenti, fatture). Una volta che l'utente apre l'allegato, il malware si attiva e infetta il sistema.
2. **Software Illegittimo:** Il download di software "craccato", attivatori illegali o programmi da fonti

non ufficiali rappresenta un rischio altissimo. Spesso questi pacchetti contengono malware come Vidar, nascosto all'interno dell'installer.

3. **Client di Hacking per Giochi:** Questo vettore dimostra come anche attività non strettamente lavorative possano introdurre rischi in azienda. I "cheat" e gli "hack" per videogiochi sono un veicolo di infezione molto diffuso per questo tipo di malware.

4.2 Strategie di Difesa Proattiva

Per prevenire infezioni come Vidar, è necessario applicare e far rispettare una serie di policy di sicurezza informatica a tutti i livelli dell'organizzazione.

- **Policy di Tolleranza Zero per Allegati Sospetti:** Deve essere applicata la regola inderogabile di non scaricare né aprire mai allegati provenienti da mittenti sconosciuti, inattesi o sospetti.
- **Utilizzo Esclusivo di Software Ufficiale:** È imperativo che tutto il software sia scaricato e installato solo da fonti ufficiali e affidabili, utilizzando licenze legittime.
- **Mantenimento Continuo degli Aggiornamenti:** Assicurarsi che sistema operativo, browser e software di sicurezza siano sempre aggiornati all'ultima versione disponibile è una policy critica, non un'opzione. Gli aggiornamenti chiudono le vulnerabilità di sicurezza che i malware sfruttano.
- **Implementazione Obbligatoria dell'Autenticazione a Più Fattori (MFA):** L'MFA deve essere abilitata su tutti i servizi aziendali. Agisce come una "seconda chiave" di sicurezza: anche se una password viene rubata, l'accesso è bloccato senza il secondo fattore di verifica.
- **Obbligo di Utilizzo di un Password Manager Approvato:** Salvare le password nel browser è intrinsecamente rischioso. Deve essere applicata una policy che vieti questa pratica e imponga l'uso di gestori di password aziendali approvati (es. 1Password, KeePass), che isolano le credenziali da questo tipo di attacco.
- **Formazione Continua e Obbligatoria:** La difesa più importante è un utente consapevole. Sessioni di formazione regolari per riconoscere i tentativi di phishing e comprendere i rischi associati al download di file non sicuri devono essere obbligatorie per tutto il personale.

Nonostante le migliori pratiche di prevenzione, è cruciale disporre di un piano d'azione robusto per quando, inevitabilmente, un incidente si verifica.

5.0 Piano di Risposta e Remediation

Un piano di risposta rapido, strutturato e ben definito è cruciale per minimizzare i danni finanziari, operativi e reputazionali derivanti da un'infezione malware. Le azioni proposte di seguito sono suddivise in tre fasi logiche: contenimento, bonifica e prevenzione futura.

Fase 1: Contenimento Immediato (Fermare l'Emorragia)

Questa fase è il "pronto soccorso" dell'incidente, finalizzata a "fermare l'emorragia". Le azioni devono essere intraprese immediatamente per limitare l'estensione del danno.

- **Isolare immediatamente l'host:** Disconnettere il sistema infetto dalla rete aziendale (sia WiFi che cavo LAN). Questa azione impedisce al malware di comunicare con i server degli aggressori e previene la sua diffusione laterale ad altri sistemi.
- **Procedere al reset globale delle credenziali:** Considerare compromesse tutte le password e i token di sessione presenti sul sistema. Eseguire il reset immediato delle password per tutti i servizi critici a cui l'utente aveva accesso (email, VPN, portali aziendali, account cloud, servizi bancari).
- **Congelare immediatamente i cripto-wallet:** Se applicabile, l'utente deve trasferire subito eventuali fondi rimanenti da portafogli compromessi a un nuovo indirizzo sicuro e non collegato al sistema infetto.

Fase 2: Bonifica del Sistema (Eliminazione della Minaccia)

Questa fase consiste nell'eliminare completamente ogni traccia della minaccia, ripartendo da una base sicura.

- **Eseguire il re-imaging totale del sistema:** Una semplice scansione antivirus non è sufficiente. L'unica via sicura per garantire l'integrità del sistema è la **formattazione completa del disco** ("ricominciare da zero") e la reinstallazione del sistema operativo e delle applicazioni da fonti pulite e verificate.
- **Eseguire una scansione approfondita delle periferiche:** Tutti i dischi esterni, le chiavette USB e le condivisioni di rete con cui il sistema infetto è entrato in contatto devono essere sottoposti a una scansione completa con un software di sicurezza professionale aggiornato, come una soluzione EDR (Endpoint Detection and Response), che offre una visibilità e una capacità di risposta superiori rispetto a un antivirus tradizionale.

Fase 3: Prevenzione Futura (Rafforzare le Difese)

Questa fase è l'opportunità per "imparare la lezione" dall'incidente e migliorare la postura di sicurezza complessiva dell'organizzazione. È fondamentale rafforzare le strategie di difesa proattiva:

- **Implementazione Sistematica dell'MFA** su tutti i servizi critici.
- Applicazione di **Politiche di Patching Rigorose** per garantire che tutti i sistemi siano costantemente aggiornati.
- Definizione di una **Policy di Gestione Password** che vieti esplicitamente il salvataggio delle credenziali nei browser e imponga l'uso di password manager approvati.
- Organizzazione di **Sessioni di Formazione Obbligatoria sul Phishing** per tutto il personale, con test periodici.

Queste fasi costituiscono un ciclo virtuoso che non solo risolve l'incidente attuale, ma rende l'intera organizzazione più resiliente agli attacchi futuri.

6.0 Conclusioni e Raccomandazioni Finali

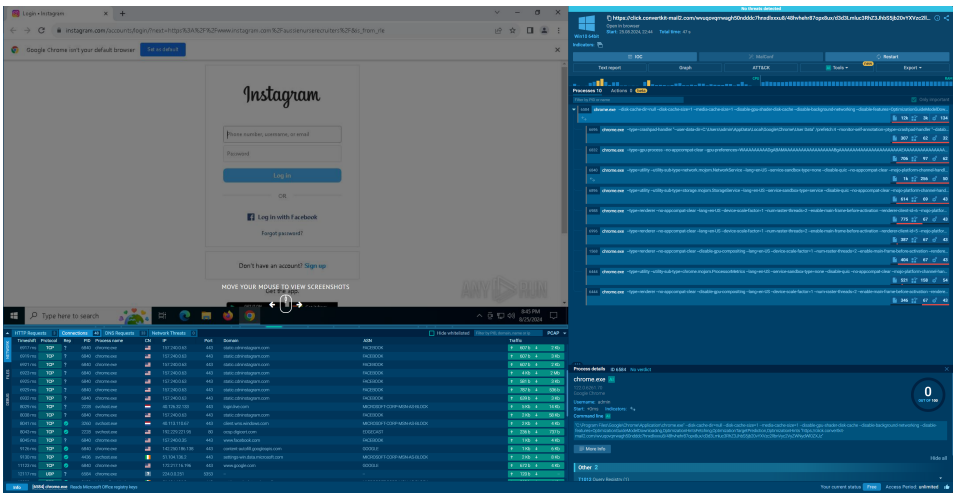
L'analisi ha confermato che il malware Vidar è una minaccia sofisticata e pericolosa. Non si tratta di un virus generico, ma di uno strumento specializzato nel furto di dati sensibili che, agendo anche come loader per altre minacce, rappresenta un rischio concreto e diffuso per la sicurezza delle informazioni aziendali, la stabilità finanziaria e la reputazione del nostro brand.
Raccomandiamo la formalizzazione immediata del piano di risposta qui delineato come protocollo standard per la gestione di incidenti di tipo *infostealer*. Inoltre, chiediamo l'allocazione di risorse per una campagna di sensibilizzazione sul phishing obbligatoria e a livello aziendale da completarsi entro il prossimo trimestre. La difesa proattiva non è una spesa, ma un investimento essenziale per proteggere i nostri asset principali da un panorama di minacce persistente e in continua evoluzione.

Report Esercizio 5 (PT.2): Analisi Malware 2

1. Sintesi Esecutiva (Executive Summary)

L'analisi approfondita delle comunicazioni di rete conferma che l'incidente è un tentativo mirato di Phishing volto al furto di credenziali (Credential Harvesting), mascherato da comunicazione legittima. Nonostante i sistemi di sicurezza automatizzati non abbiano rilevato "file" infetti (esito "No threats detected"), l'analisi manuale del traffico ha isolato un comportamento malevolo attivo: l'utente viene reindirizzato verso una pagina fraudolenta che replica l'interfaccia di Instagram.

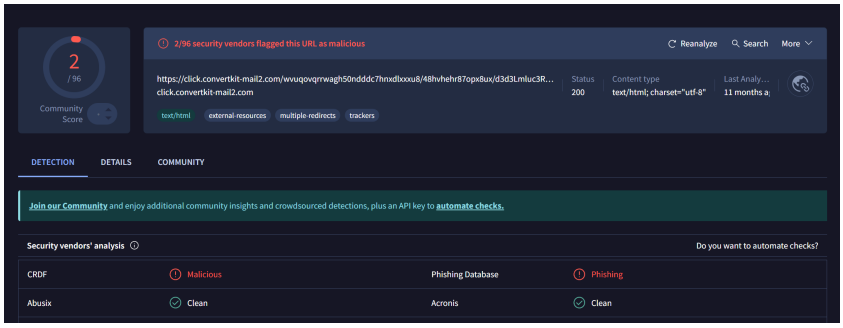
- **Verdetto Finale**: potenzialmente MALEVOLO (Phishing & Social Engineering).
- **Livello di Criticità**: potenzialmente ALTO (Rischio immediato di compromissione account).
- **Stato**: Attacco basato sul web (nessun malware persistente rilevato su disco).



2. Scenario dell'Attacco (Ricostruzione dell'Evento)

Ecco come si svolge l'attacco, basato sulla ricostruzione della navigazione dell'utente e delle "tracce" lasciate sulla rete:

1. **L'Esca (The Hook)**: L'attacco inizia con un link che sfrutta un'infrastruttura lecita di email marketing (`click.convertkit-mail2.com`). Questo serve a bypassare i filtri antispam, che riconoscono il dominio come "affidabile".



2. **Il Reindirizzamento Silenzioso**: Una volta cliccato, il browser non scarica nulla di pesante. I log di rete mostrano uno scambio dati minimo (pochi Kilobyte), indicando che non c'è un download di virus, ma un semplice comando di "invio" verso una nuova destinazione.
3. **La Trappola Visiva**: La vittima atterra su una pagina di login contraffatta. A differenza di un virus che agisce di nascosto, qui è richiesta la collaborazione involontaria dell'utente: l'inserimento manuale di username e password.

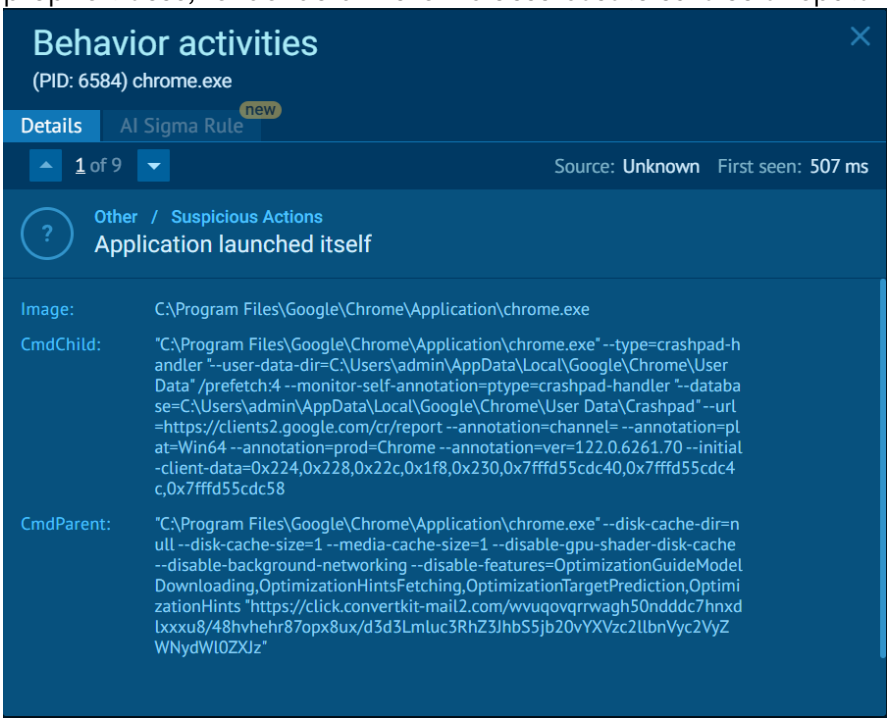
3. Analisi Tecnica Approfondita (Network & Behavior)

Questa sezione dettaglia le evidenze tecniche che supportano il verdetto, distinguendo tra minacce reali e "rumore di fondo":

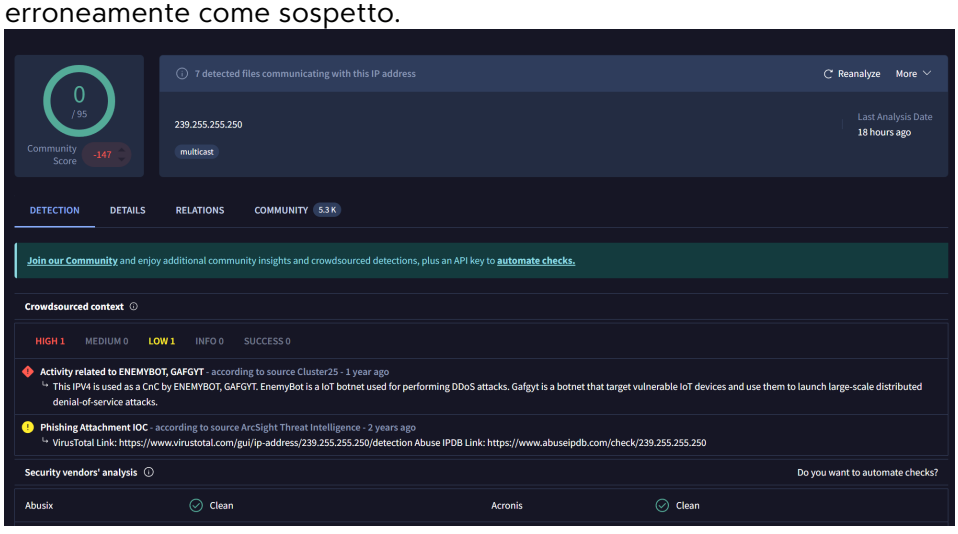
1. **Il Vettore di Attacco (HTTPS/443) →** Il traffico malevolo principale viaggia su canale cifrato (Porta TCP 443).

- **Osservazione**: Abbiamo isolato connessioni verso l'indirizzo IP `3.141.222.179`.

- **Significato**: Questo IP appartiene a servizi cloud (AWS) usati dalla piattaforma di marketing citata sopra. L'attaccante sta "abusando" di server legittimi per nascondere le proprie tracce, rendendo difficile il blocco basato sulla sola reputazione dell'IP.



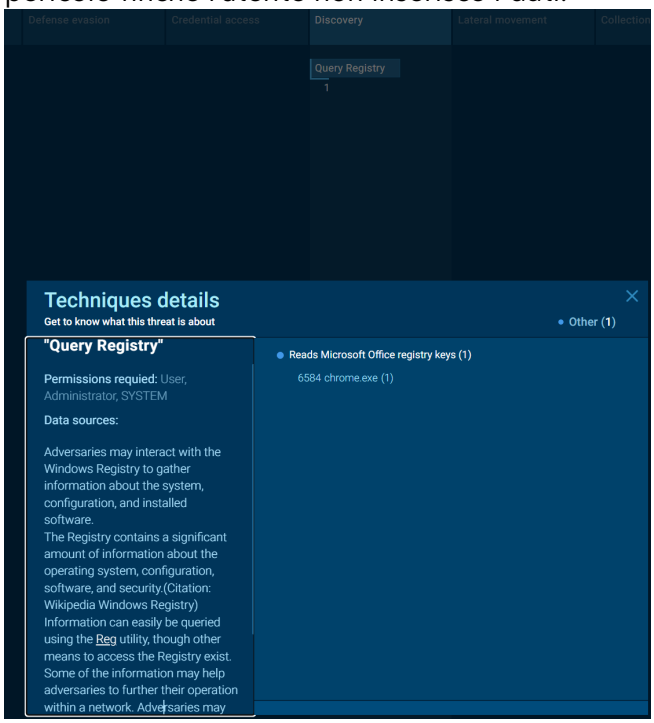
2. **Analisi del "Falso Positivo" (Il caso dell'IP 239.255.255.250)** ➜ Durante l'analisi è emerso un volume di traffico UDP verso l'IP `239.255.255.250` (Porta `1900`), spesso segnalato erroneamente come sospetto.



- **Valutazione Tecnica**: Confermiamo che questo non è parte dell'attacco. Si tratta di traffico SSDP (Simple Service Discovery Protocol) generato automaticamente da Google Chrome per cercare dispositivi "cast" (come smart TV) nella rete locale.
- **Decisione**: Questo traffico va classificato come "rumore di fondo" (benigno) e non richiede azioni di blocco, permettendoci di focalizzare le difese sul vero vettore di phishing.

3. **Evasione dei Controlli** ➜ Il malware non scrive file su disco e non modifica chiavi di registro

critiche (nessuna "persistenza"). Questo spiega perché l'analisi automatica (Sandbox) ha dato esito verde: se non c'è un file `.exe` da analizzare, molti antivirus tradizionali non vedono il pericolo finché l'utente non inserisce i dati.



Il processo tenta di leggere le chiavi di registro per raccogliere informazioni sul sistema ospite

---

4. Impatto di Business e Rischi

- **Furto di Identità Aziendale**: Se un dipendente inserisce le credenziali, l'attaccante potrebbe accedere non solo a Instagram, ma tentare le stesse password su Office 365 o VPN aziendali (fenomeno del Password Reuse).
- **Danno Reputazionale**: Un account social aziendale compromesso può essere usato per truffare i clienti o pubblicare contenuti dannosi a nome dell'azienda.

---

5. Raccomandazioni Operative

Azioni Immediate (Network Security):

1. **Blacklist URL**: Bloccare l'accesso al dominio `click.convertkit-mail2.com` e monitorare le richieste verso l'IP `3.141.222.179` se non strettamente necessario per il business.
2. **Verifica Accessi**: Se qualche utente ha segnalato di aver cliccato il link, forzare immediatamente il cambio password (e attivare la MFA se non presente).

Miglioramenti Strategici:

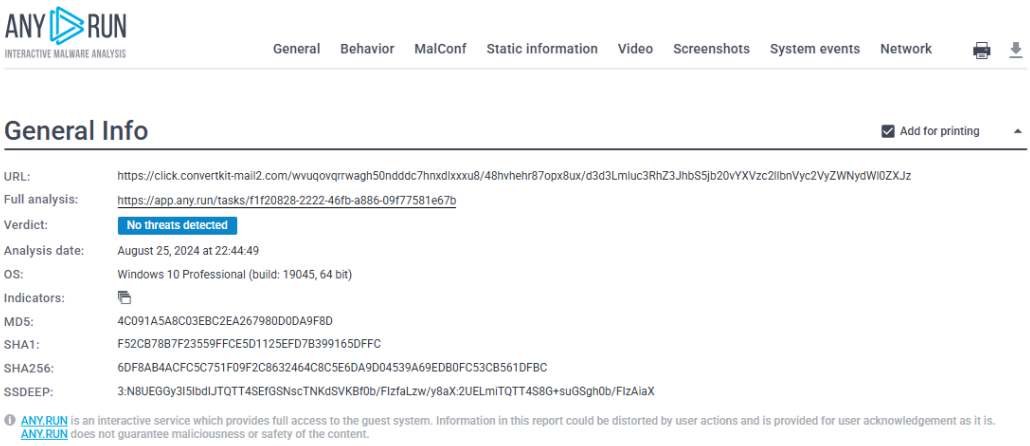
- Implementare soluzioni di sicurezza che analizzino la **reputazione dei link** in tempo reale, non solo gli allegati.

- Formazione utenti: "Nessun servizio legittimo chiede di rifare il login subito dopo un click da email”.

Appendice: Indicatori di Compromissione (IOCs)

Dati tecnici per configurazione Firewall/Proxy

- **Dominio Phishing**: `click.convertkit-mail2.com` - Redirect iniziale
- **Indirizzo IP**: `3.141.222.179` - Hosting del redirect (AWS)
- **Protocollo**: TCP / 443 (HTTPS) - Traffico cifrato
- **Traffico Benigno**: `239.255.255.250` (UDP/1900) - SSDP/Multicast (Ignorare)



Conclusioni

L'analisi di questo incidente evidenzia come le moderne minacce di phishing si siano evolute per aggirare i controlli di sicurezza tradizionali.

Il fatto che i sistemi automatici non abbiano rilevato minacce ("No threats detected") dimostra che la sicurezza non può basarsi solo sul software, ma richiede un monitoraggio costante e un'analisi critica.

Sebbene non sia stato rilevato alcun virus in grado di distruggere dati, il rischio di furto di credenziali (Instagram e potenzialmente accessi aziendali) rappresenta una minaccia critica.

L'applicazione immediata dei blocchi di rete suggeriti e una rinnovata sensibilizzazione degli utenti sono le difese più efficaci per mitigare questo rischio.