Report Analisi Malware Vidar

Identificazione della Minaccia:

La presenza del malware "Vidar" è stata rilevata tramite strumenti di monitoraggio come Any.Run e YARA, che hanno identificato un eseguibile sospetto ("vidar.exe") in esecuzione sul sistema. Vidar è noto per la sua capacità di sottrarre informazioni sensibili come credenziali e dati finanziari.

Modalità di Infezione:

Il dispositivo potrebbe essere stato infettato tramite allegati e-mail sospetti, download di file da fonti non affidabili o exploit di vulnerabilità nel sistema operativo. Una volta eseguito, Vidar instaura connessioni con server di comando e controllo (C2) per esfiltrare i dati.

Vidar è un infostealer avanzato, progettato per infiltrarsi nei sistemi e sottrarre informazioni personali. Ecco come si muove in dettaglio:

1. Infezione: Vidar si diffonde attraverso tecniche di social engineering, spesso utilizzando campagne di phishing o file eseguibili mascherati come allegati o download legittimi.

2. Esfiltrazione di Dati: Una volta installato, raccoglie una vasta gamma di dati: credenziali di accesso, dettagli di carte di credito, cronologia del browser, cookie, informazioni sul sistema e file specifici che potrebbero contenere dati sensibili. Utilizza comandi specifici per accedere a tali informazioni, incluso l'uso di API per recuperare password memorizzate e altre credenziali.

3. Connessione a Server C2: Vidar stabilisce una connessione con un server di comando e controllo (C2) utilizzando protocolli HTTP o HTTPS, tramite indirizzi IP o domini predefiniti. Questo permette agli attaccanti di ricevere i dati raccolti e inviare ulteriori comandi per modificare il comportamento del malware in tempo reale.

4. Comportamenti di Offuscamento e Cancellazione delle Tracce: Vidar può utilizzare diversi metodi per rimanere nascosto e persistente nel sistema. Può cancellare file temporanei e alterare il registro di sistema per evitare il rilevamento. A volte, dopo aver completato la raccolta dei dati, può disinstallarsi o eliminare le proprie tracce per ridurre la possibilità di essere rilevato da un antivirus.

5. Distribuzione di Payload Aggiuntivi: In alcuni casi, Vidar agisce come dropper, scaricando e installando ulteriori malware come ransomware o altri tipi di trojan sul sistema infetto.

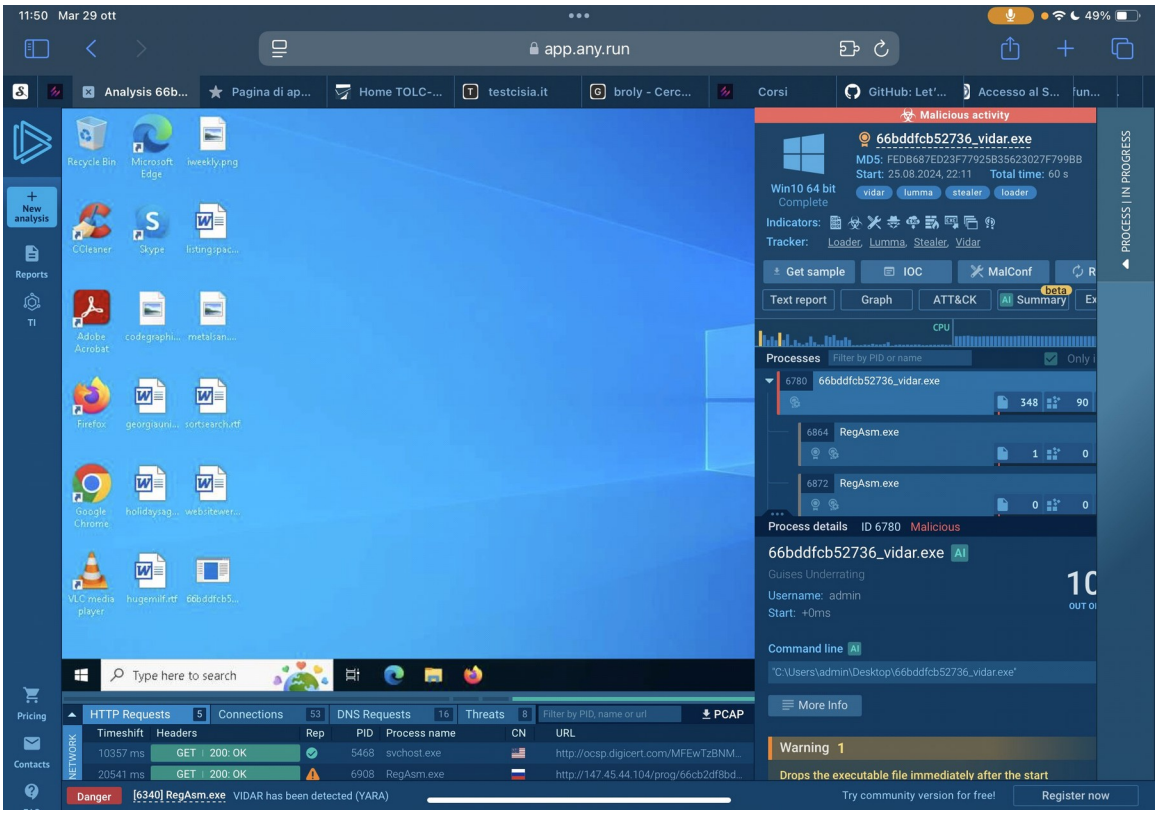
Programmi Utilizzati nell'Analisi:

- Any.Run: è una sandbox interattiva per l'analisi di malware in tempo reale. A differenza delle sandbox tradizionali che generano solo rapporti statici, Any.Run permette agli analisti di interagire con il malware (eseguire clic, aprire finestre) e osservare il comportamento in tempo reale. Questo è particolarmente utile per capire come un malware come Vidar interagisce con il sistema, quali processi

attiva, quali connessioni di rete stabilisce e quali file modifica o crea. Grazie alla sua interfaccia visiva, Any.Run è utile per analisi rapide e per rilevare comportamenti dinamici che altri strumenti potrebbero non individuare. Scegliere Any.Run consente di ridurre i falsi negativi perché gli analisti possono scoprire dettagli comportamentali complessi.

- YARA: è un framework di regole che aiuta a identificare file o pattern dannosi attraverso l'uso di firme specifiche. Le regole YARA sono particolarmente utili per l'identificazione di malware conosciuti o per la creazione di pattern personalizzati in base a indicatori di compromissione (IOC) rilevati in precedenza. Nel caso di Vidar, YARA può essere configurato con pattern che identificano librerie, stringhe di testo, o funzioni specifiche che il malware potrebbe utilizzare. L'uso di YARA consente una rilevazione accurata basata su caratteristiche peculiari, minimizzando il rischio di falsi positivi poiché le regole sono precise e personalizzabili.

- Combinazione di Statico e Dinamico: Mentre Any.Run fornisce una visione comportamentale dinamica, YARA aggiunge una capacità di rilevamento basata su firme. Questa combinazione permette di coprire sia malware che mostrano azioni evidenti sia quelli che operano in modo più nascosto o silenzioso.



Nella sezione **"Threats" di Any.Run**, possiamo osservare in dettaglio le minacce rilevate:

1. "Potentially Bad Traffic": Questo alert segnala traffico di rete considerato sospetto o malevolo, che potrebbe puntare a server di comando e controllo (C2). È indicativo di tentativi di esfiltrazione di dati o di ricezione di istruzioni da parte del malware.

2. "Network Trojan Detected": Indica la presenza di una connessione trojan verso un server esterno, utilizzata per sottrarre informazioni o ricevere comandi. Questo conferma che Vidar sta cercando di inviare dati sensibili o di eseguire comandi remoti.

3. "ET POLICY PE EXE or DLL Windows file download HTTP": Segnala che il malware sta tentando di scaricare file eseguibili o librerie aggiuntive tramite HTTP. Questo comportamento è spesso associato all'installazione di componenti aggiuntivi o payload secondari che possono ampliare le funzionalità del malware (come keylogger o moduli per rubare credenziali).

4. "Misc Attack": Categoria generica per attività che violano le policy di sicurezza o comportamenti anomali. Questa categorizzazione spesso include azioni che non rientrano nelle tipiche categorie di attacco ma che sono comunque ritenute potenzialmente pericolose, come tentativi di evasione o di alterazione dei registri.

5. "STealer TLS Connection": Questo avviso è specifico per connessioni cifrate stabilite da strumenti di furto dati come Vidar. In questo caso, la connessione sicura (TLS) viene utilizzata per inviare i dati sottratti al server remoto in modo che non possano essere intercettati facilmente.

Interpretazione Generale

Questi avvisi evidenziano un comportamento classico dei malware infostealer come Vidar, con tentativi di:

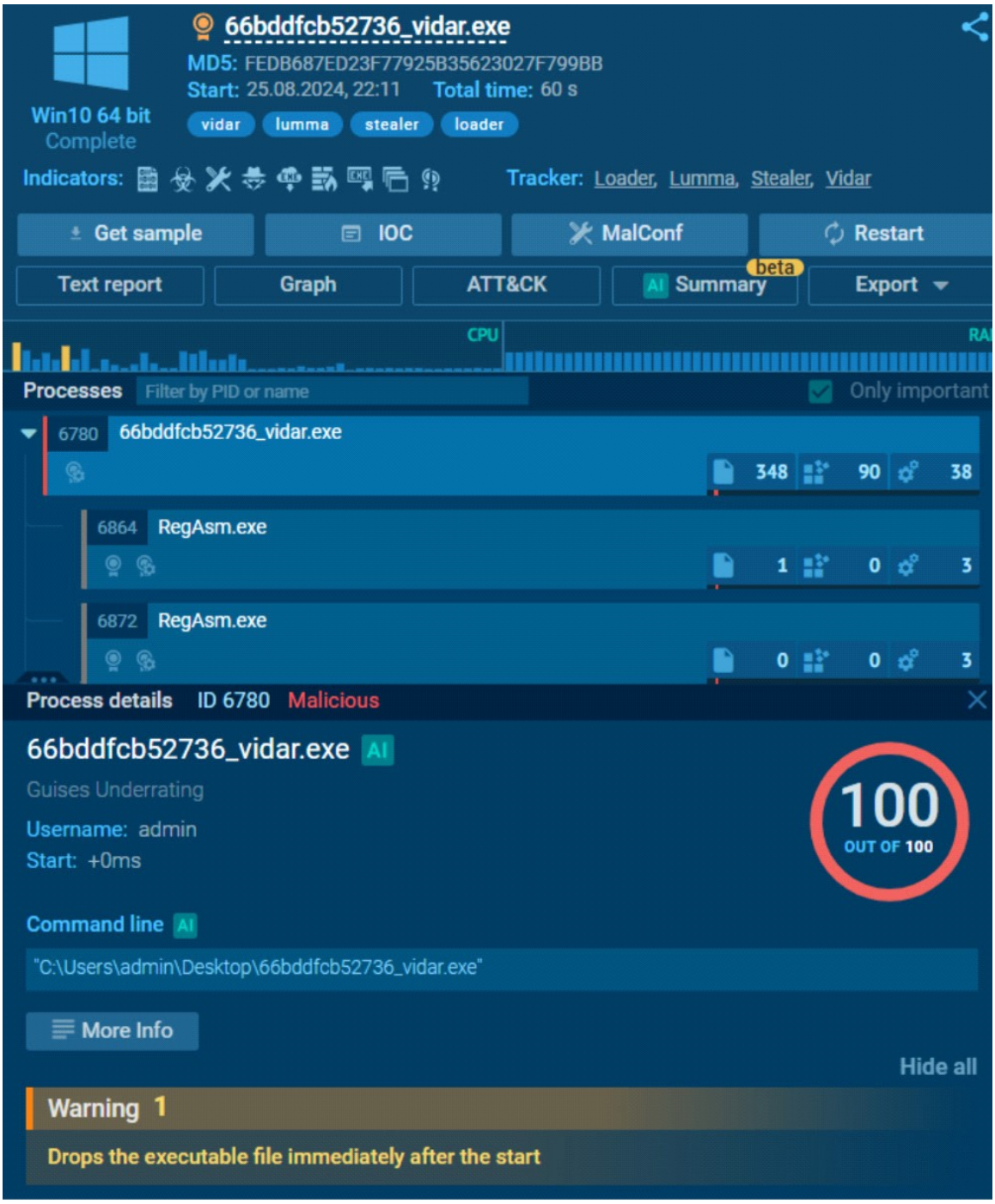
- Esfiltrare dati tramite connessioni non autorizzate e sicure (C2).

- Scaricare ed eseguire moduli aggiuntivi per estendere le proprie funzionalità malevole.

- Mascherare il traffico malevolo tramite l'uso di protocolli cifrati, rendendo più difficile il rilevamento.

Emergono altri dettagli importanti sui processi correlati e sull’interazione tra Vidar e altri file eseguibili:

1. Vidar (66bddfcb52736_vidar.exe): Identificato come il principale infostealer, Vidar esegue comandi per sottrarre informazioni e stabilisce connessioni con server esterni per esfiltrare i dati. Appena eseguito, Vidar attiva immediatamente altri processi, confermando la sua natura di “loader” per ulteriori componenti dannosi.

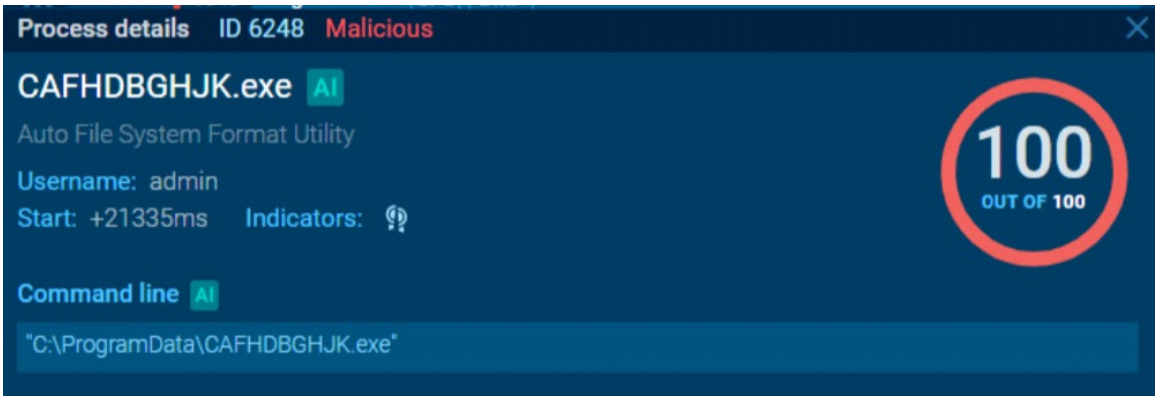


2. RegAsm.exe: Questo processo, solitamente legittimo per la registrazione di assembly .NET, viene abusato da Vidar per mascherare la sua attività. Nel contesto di un'infezione, Vidar utilizza RegAsm.exe come processo "figlio" per evitare il

rilevamento e comunicare con server esterni. Vari tentativi di connessione a URL sospetti e IP esterni confermano l’esfiltrazione di dati.

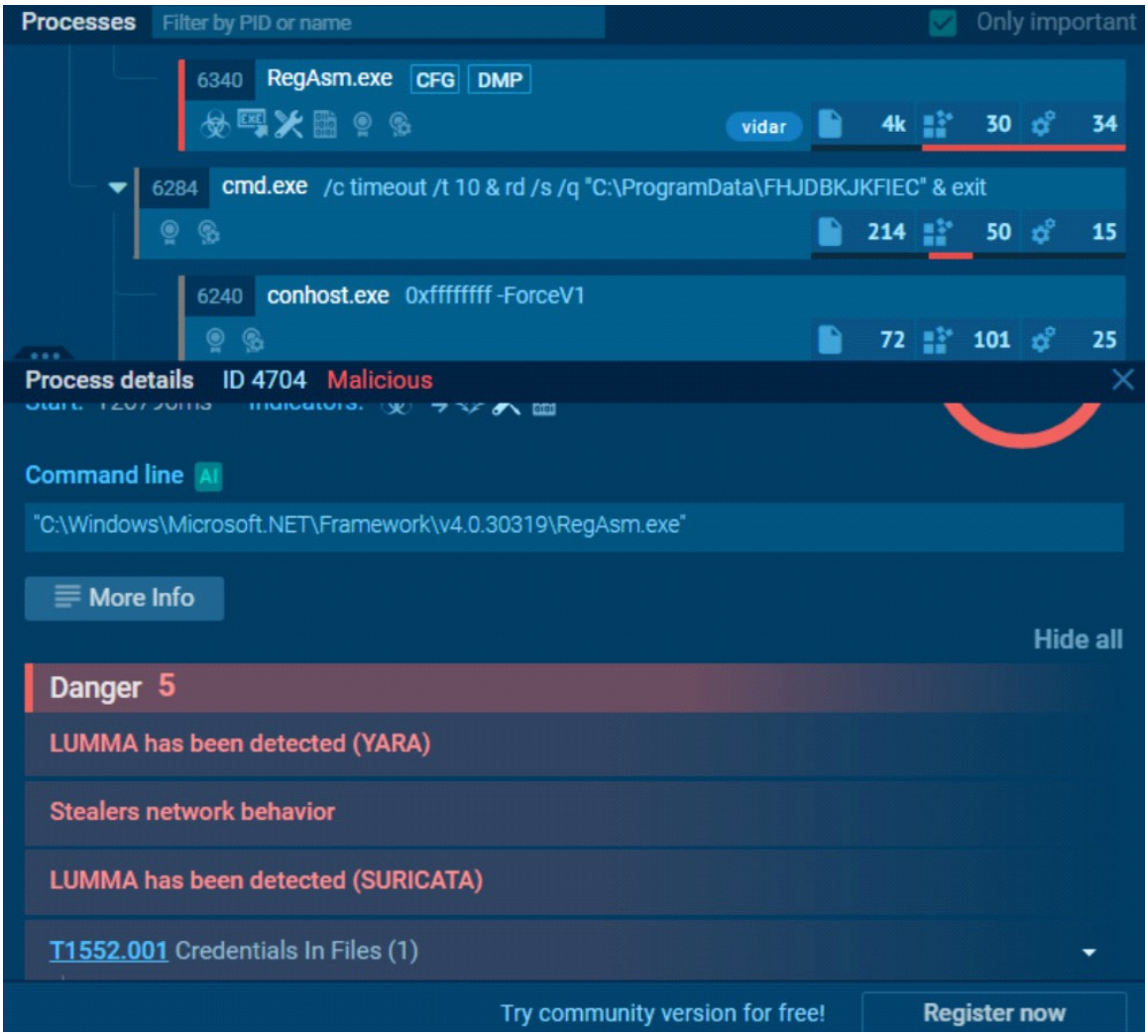
3. CAFHDBGJK.exe: Questo eseguibile è probabilmente un payload secondario distribuito da Vidar. In genere utilizzato per attività di persistenza e offuscamento, CAFHDBGJK.exe contribuisce all'infezione, mantenendo il controllo e,

potenzialmente, scaricando ulteriori malware. Viene eseguito in una directory non standard (ProgramData), indice di comportamento malevolo.



4. Altri Indicatori di Minaccia (T1555.003, T1552.001, T1518): Questi ID MITRE ATT&CK indicano le tecniche usate da Vidar per rubare credenziali dal browser, dai file locali e per scoprire informazioni sul sistema ospite (software discovery). Ciò conferma l'intento di Vidar di raccogliere quante più informazioni possibili.

5. In seguito emerge che **"Lumma"** è stato identificato insieme a Vidar. Lumma, come Vidar, è uno stealer, progettato per sottrarre informazioni sensibili dal sistema. Gli alert mostrano che Lumma è stato rilevato tramite regole YARA e SURICATA, strumenti di rilevamento usati rispettivamente per pattern di firme e analisi del traffico di rete.



Collegamenti tra i Processi:

Vidar funge da malware primario che:

- Avvia processi secondari come RegAsm.exe per operazioni malevole (esfiltrazione, comunicazione con C2).

- Distribuisce ulteriori componenti come CAFHDBGJK.exe, che possono operare

autonomamente per mantenere l’infezione e rinforz

are le attività di persistenza e furto di dati.

- La presenza di Lumma e Vidar insieme è comune in infezioni complesse, dove vari stealer collaborano per massimizzare la raccolta di dati. La conferma tramite YARA e SURICATA evidenzia l’uso di tecniche di rilevamento complementari: YARA identifica i file pericolosi basandosi su pattern, mentre SURICATA rileva attività di rete sospette.

Importanza degli Alert

Ciascuno di questi alert aiuta a costruire un quadro dettagliato delle capacità e delle intenzioni del malware, confermando che Vidar è attivamente impegnato in attività dannose e richiede interventi immediati di remediation.

Remediation Consigliata:

1. Isolamento del File (Quarantena): Mettere in quarantena l’eseguibile "vidar.exe" per impedirne ulteriori attività sul dispositivo e valutarne l'estensione.

2. Eliminazione del Malware: Se l'analisi conferma la minaccia, rimuovere completamente il file dal sistema per evitare riattivazioni.

3. Blacklist degli Indirizzi IP e Domini Sospetti: Bloccare gli IP e domini di rete utilizzati dal malware per comunicare con i server di controllo, evitando così ulteriori esfiltrazioni di dati.

4. Aggiornamenti e Patch di Sicurezza: Assicurarsi che il sistema e i programmi siano aggiornati per mitigare il rischio di exploit.

5. Implementazione di Endpoint Detection and Response (EDR): L'uso di soluzioni EDR permette di monitorare e rispondere a minacce in tempo reale, identificando e isolando comportamenti sospetti futuri.

Motivazione della Remediation: Questa strategia di remediation è necessaria per prevenire ulteriori danni e furti di dati. L'isolamento e la successiva eliminazione del file garantiscono che il malware non possa essere riattivato, mentre la blacklist degli IP interrompe eventuali comunicazioni malevole. L'uso di EDR e le patch rafforzano la sicurezza per minimizzare il rischio di nuove infezioni.

Report Analisi 2

Identificazione della Minaccia:

L'analisi ha individuato un possibile rischio di phishing legato a un link ricevuto

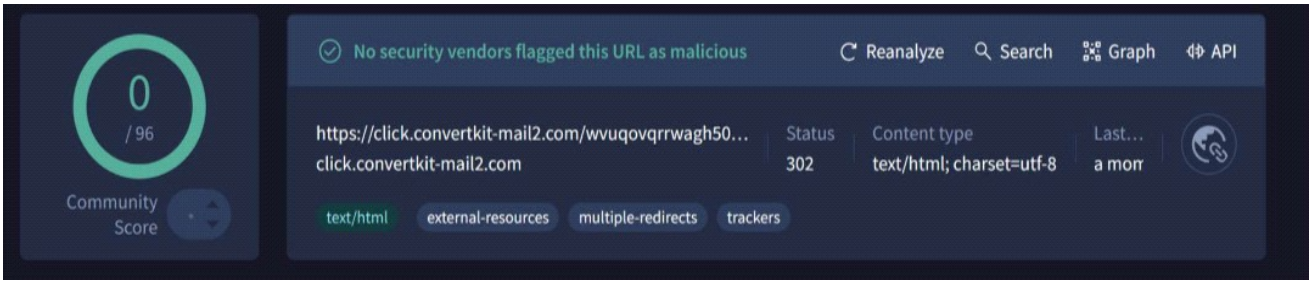
tramite e-mail ("https://click.convertkit-mail2.com/..."), che ha attivato una serie di redirect portando l'utente a pagine come Instagram, tramite accesso con account Facebook. Il traffico generato da questi reindirizzamenti non ha rilevato comportamenti direttamente malevoli, ma evidenzia potenziali rischi legati all'uso di meccanismi di redirezione non autorizzati.

Modalità di Infezione:

L'infezione potrebbe avvenire sfruttando tecniche di phishing, mediante messaggi di posta elettronica con collegamenti che portano l'utente a pagine di accesso per account di social media (es. Instagram/Facebook), potenzialmente per raccogliere credenziali.

Analisi dei Programmi Utilizzati

- Any.Run: Utilizzato per verificare i comportamenti del link durante l'accesso e visualizzare eventuali alert di traffico sospetto. In questo caso, Any.Run non ha rilevato processi sospetti o malevoli, ma ha mostrato reindirizzamenti tipici di campagne di marketing che potrebbero ingannare l'utente.



- VirusTotal: Utilizzato per un controllo aggiuntivo, non ha rilevato minacce nei

link analizzati, suggerendo che i reindirizzamenti siano stati causati da campagne promozionali non dannose. VirusTotal ha confermato l'assenza di alert di pericolosità legati al link.

Alert e Attività Rilevati

Durante l’analisi del traffico, sono emerse diverse richieste indirizzate a server di Instagram, Facebook, e Windows per aggiornamenti, oltre a interazioni con le chiavi di registro, come "HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\OFFICE\16.0\ACCESS\CAPABILITIES\URLASSOCIATIONS", causate dall’integrazione di Office nei browser. Questi comportamenti sono stati identificati come normali attività di sistema senza alcuna componente malevola.

1. Redirect a Pagine Social: La serie di reindirizzamenti ha portato a una pagina di accesso a Instagram, senza processi sospetti generati sul dispositivo.

2. Richieste a Server di Aggiornamento Windows: Generate come attività standard del sistema, non presentano criticità in termini di sicurezza.

3. Accesso a Chiavi di Registro Microsoft Office: Tentativo di gestione di link tramite applicazioni del pacchetto Office, tipico nelle integrazioni con i browser.

Interpretazione Generale

L’assenza di alert di pericolosità e processi sospetti suggerisce che i reindirizzamenti osservati derivino da campagne di marketing via e-mail piuttosto che da malware. Tuttavia, il rischio potenziale risiede nella possibilità che simili tecniche di redirezione vengano sfruttate in attacchi di phishing mirati, soprattutto se portano l’utente a concedere accessi o informazioni sensibili.

Remediation Consigliata

1. Monitoraggio degli Accessi: Educare l’utente sull’importanza di accedere solo a link da fonti verificate e riconosciute, specialmente se si tratta di reindirizzamenti multipli.

2. Controllo della Validità dei Link: Utilizzare strumenti come VirusTotal per una scansione preventiva dei link sospetti in e-mail.

3. Aggiornamenti e Protezione del Browser: Assicurarsi che browser e applicazioni siano aggiornati per ridurre vulnerabilità sfruttabili nei reindirizzamenti.

4. Filtro delle E-mail di Phishing: Implementare un filtro anti-phishing per bloccare messaggi che utilizzano link di redirezione sospetti.

Motivazione della Remediation:

L’educazione e il monitoraggio degli accessi ai link, associati a una protezione del browser e filtri e-mail, prevengono i rischi di phishing e accessi a pagine non sicure. Questa strategia di mitigazione riduce la possibilità che l’utente esponga le proprie credenziali o acceda a pagine compromesse.