BuildWeek_III_Analisi_Anyrun

Consegna

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

https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d/
https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b/

Come output vorrei la spiegazione in italiano per un eventuale cliente / manager (che è poco preparato sulla materia) di questi malware (o presunti tali). Indicare le vostre scelte di remediation (mettere in quarantena, eliminare, blacklist, falso positivo, falso negativo, vero positivo, vero negativo, chiedo al vendor, ecc.) motivandole.

Svolgimento

Analisi primo link

Una volta aperto il link e spostatomi all'interno della sezione dei processi avviati dal presunto malware possiamo notare diversi dettagli sospetti:

Il sample iniziale è 66bddfcb52736_vidar.exe: il nome vidar fa riferimento ad un **malware** infostealer che può raccogliere un'ampia gamma di dati sensibili dai browser e dai portafogli digitali.

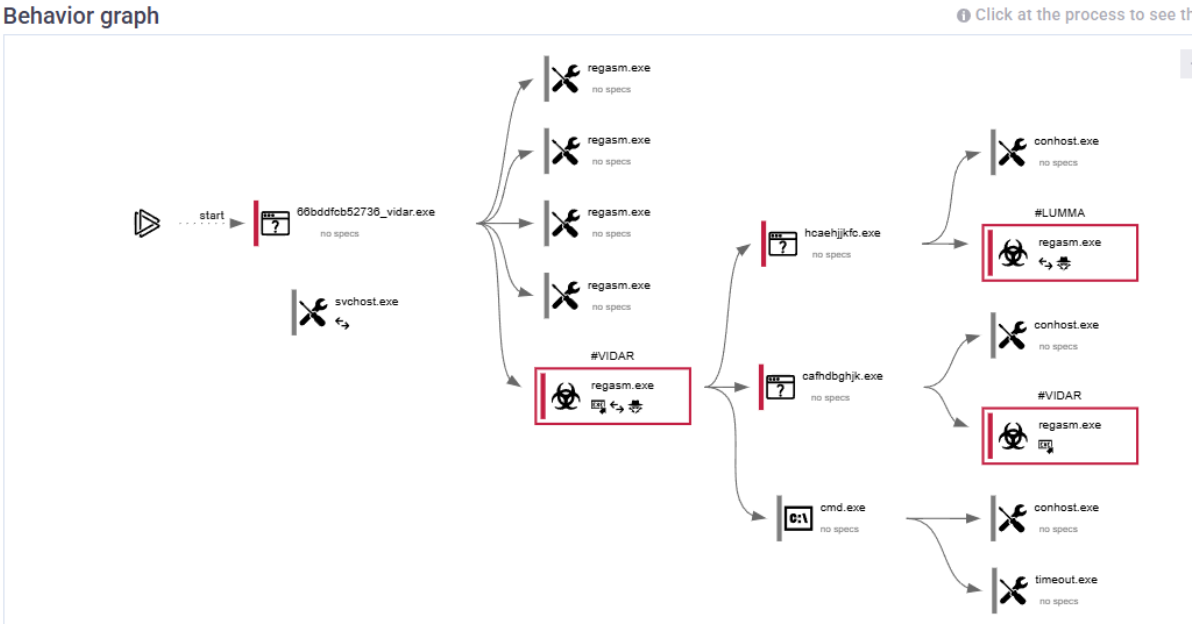
L'eseguibile iniziale lancia poi diversi processi regasm.exe, Assembly Registration Tool, un applicativo usato dagli sviluppatori .NET per registrare un assembly (file .dll scritto in .NET) come oggetto **COM (Component Object Model)**, in modo che possa essere richiamato da altre applicazioni Windows.

In pratica, regasm.exe permette a librerie .NET di essere visibili e utilizzabili dal sistema operativo o da altri programmi che non sono scritti in .NET.

Da uno di questi processi regasm, si ramificano altri processi ("HCAEHJJKFC.exe", "CAFHDBGHJK.exe") che a loro volta generano cmd.exe e

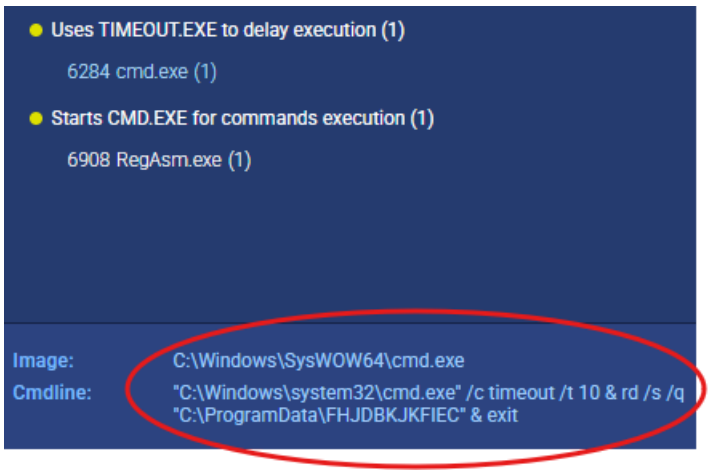
altri comandi (timeout.exe) e processi di supporto (conhost.exe).

C'è anche il tag **#LUMMA** accanto ad un regasm.exe, il che suggerisce che il comportamento osservato ha caratteristiche miste attribuite sia a Vidar che a Lumma (o che il sistema di detection ha rilevato elementi compatibili con entrambe le famiglie).



Spostandoci all'interno della sezione MITRE&ATTACK possiamo analizzare ulteriori dettagli.

Sotto alla voce Execution troviamo infatti specifiche interessanti circa i prompt utilizzati dal presunto malware:



Nel primo screenshot notiamo l'uso di timeout.exe, il comando utilizzato è: timeout /t 10.

Tramite tale input il malware avvia il processo con un ritardo di 10 secondi.

Questo serve a rendere più difficile l'analisi automatica (sandbox evasion), perché molte sandbox hanno un tempo limitato e potrebbero non osservare le attività successive.

Nel secondo screenshot notiamo invece l'esecuzione di cmd.exe con eliminazione file tramite:

"C:\Windows\system32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit

Qui il malware compie due operazioni:

Aspetta 10 secondi (timeout /t 10).

Cancella in maniera ricorsiva e forzata (rd /s /q) la cartella C:\ProgramData\FHJDBKJKFIEC.

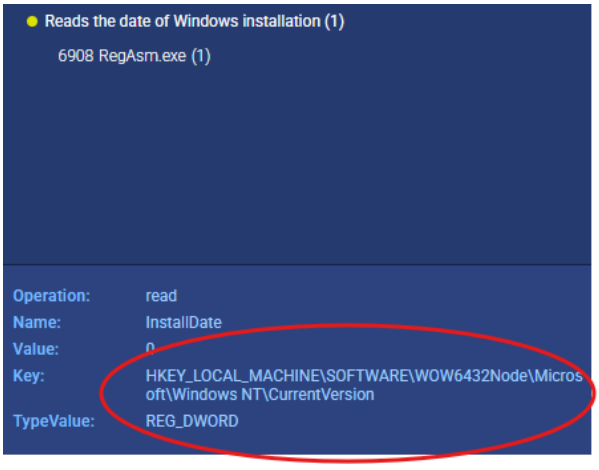
Infine chiude la shell con exit.

Con buona probabilità quella cartella era una directory temporanea usata per il drop iniziale o per contenere un modulo del malware. Dopo aver eseguito il payload principale, il malware la elimina per cancellare le tracce e ridurre la possibilità che venga analizzata.

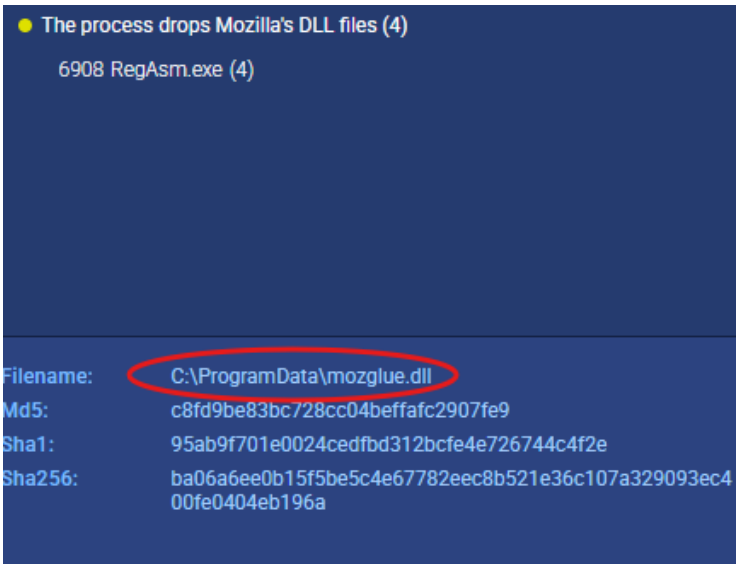
All'interno della sezione Defense Evasion notiamo che il programma va a leggere la chiave di registro relativa alla data di installazione del sistema operativo su cui sta venendo eseguito:

HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\InstallDate

Questo comportamento è probabile sia pensato per identificare ambienti "recenti" (tipici di sandbox) o VM appena create; se l'InstallDate è troppo recente, il malware può scegliere di non eseguire la sua logica malevola.



Dettagli più interessanti emergono dall'analisi della sezione Credential Access dove, tra le varie criticità, possiamo riscontrare un drop da parte di RegAsm.exe di 4 diverse dll (mozglue.dll, nss3.dll, softokn3.dll e freebl3.dll) all'interno del percorso C:\ProgramData\.



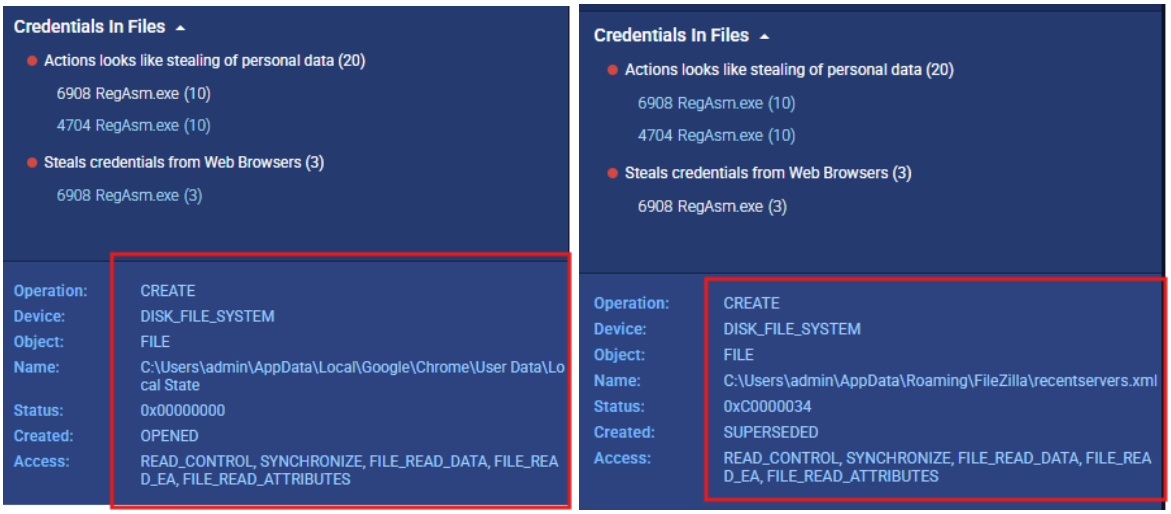
La loro presenza rafforza l'ipotesi che il malware sia progettato per interagire con/agganciare i browser e manipolare dati sensibili (tipico comportamento di un infostealer come Vidar/Lumma).

La parte più interessante e malevola la troviamo però all'interno dai tentativi di lettura dei vari cookies, configurazioni e credenziali di numerosi browser da parte del Malware.

Di seguito la lista dei principali percorsi ricercati dall'eseguibile:

- C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State
- C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
- C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\History
- C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Login Data
- C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Web Data
- C:\Users\admin\AppData\Local\Chromium\User Data\Local State

- C:\Users\admin\AppData\Local\Google\Chrome SxS\User Data\Local State
- C:\Users\admin\AppData\Local\Amigo\User Data\Local State
- C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Version
- C:\Users\admin\AppData\Roaming\Opera Software\Opera Stable\Last Version
- C:\Users\admin\AppData\Roaming\FileZilla\recentservers.xml
- C:\Users\admin\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini
- C:\Users\admin\AppData\Roaming\Thunderbird\profiles.ini
- C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account



I percorsi elencati sono **i punti chiave** dove gli infostealer cercano dati sensibili: configurazioni e chiavi (Local State), database SQLite dei browser (Login Data, Web Data, History, Cookies), profili di client (**Thunderbird**, **FileZilla**) e vari fork/derivate di **Chromium**. Questi file contengono credenziali salvate, cookie, cronologia, cookie di sessione e talvolta chiavi/indizi per decifrare le password (es. la key DPAPI in Local State per Chrome/Chromium).

Tutto ciò indica chiaramente che il campione effettua una ricognizione mirata ai browser e ai client di rete, con intento di furto di credenziali e cookie (exfiltration).

All'interno della sezione Discovery otteniamo poi la conferma che il software esegue numerose operazioni di analisi di varie chiavi per rilevare quanti più dettagli possibili circa il sistema:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software
- PublishingHKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player PPAPI
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security

IOC

File info

PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Hash

MD5: FEDB687ED23F77925B35623027F799BB

SHA1: 7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81

SHA256:
325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1

Sample iniziale

66bddfcb52736_vidar.exe.

File e percorsi drop dll

- C:\ProgramData\mozglue.dll

- C:\ProgramData\nss3.dll
- C:\ProgramData\softokn3.dll
- C:\ProgramData\freebl3.dll
- Cartella temporanea rimossa: C:\ProgramData\FHJDBKJKFIEC\

Percorsi target letti (furto credenziali / info browser & client)

- Chrome / Chromium / Edge / Opera:
    - C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Local State
    - C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
    - C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\History
    - C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Login Data
    - C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Web Data
    - C:\Users\<user>\AppData\Local\Chromium\User Data\Local State
    - C:\Users\<user>\AppData\Local\Google\Chrome SxS\User Data\Local State
    - C:\Users\<user>\AppData\Local\Amigo\User Data\Local State
    - C:\Users\<user>\AppData\Local\Microsoft\Edge\User Data\Last Version
    - C:\Users\<user>\AppData\Roaming\Opera Software\Opera Stable\Last Version

- Client & altri software:
    - C:\Users\<user>\AppData\Roaming\FileZilla\recentservers.xml
    - C:\Users\<user>\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini
    - C:\Users\<user>\AppData\Roaming\Thunderbird\profiles.ini
    - C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account

Chiavi di registro osservate

- Persistenza / fingerprinting / discovery:
    - HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\InstallDate
    - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
    - HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
    - HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player PPAPI
    - HKCU\SOFTWARE\Microsoft\Internet Explorer\Security

Processi / tecniche osservate

- regasm.exe → abusato per eseguire codice malevolo.
- cmd.exe → usato con comandi di pulizia:
    - cmd.exe /c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit
- timeout.exe → ritardo esecuzione (anti-sandbox).
- conhost.exe → processi di supporto.

Executive summary

E' stato analizzato il comportamento di un campione eseguito su Any.Run, risultato riconducibile a un infostealer (famiglie note come *Vidar/Lumma-like*). Un infostealer è un tipo di malware il cui scopo principale è rubare dati sensibili salvati sul dispositivo — in particolare credenziali e cookie presenti nei browser e nei client di rete.

Cosa ha fatto il malware

Il programma ha mostrato queste azioni principali:

- si è installato e ha avviato diversi sotto-processi;
- ha scritto componenti che servono per agganciare i browser (librerie tipo mozglue.dll, nss3.dll, ecc.);
- ha cercato e letto file dei profili dei browser e client (Chrome, Edge, Opera, Thunderbird, FileZilla) dove sono solitamente conservati password, cookie e configurazioni;
- ha usato strumenti di sistema legittimi per eseguire i suoi compiti in modo nascosto (tecnica di "mascheramento");
- ha adottato semplici contromisure anti-analisi (es. attese prima dell'esecuzione e cancellazione di cartelle temporanee).

Perché è pericoloso

- **Rischio immediato**: furto di credenziali salvate (account web, servizi, FTP, client di posta), cookie di sessione e altre impostazioni che permettono accessi non autorizzati.
- **Impatto operativo**: possibile compromissione di account aziendali e servizi, necessità di reset password e potenziali attività di riciclaggio di accessi.
- **Probabilità di esfiltrazione**: alta — il codice raccoglie artefatti destinati all'esfiltrazione.

Raccomandazione sintetica e priorità

1. **Isolare la macchina** (massima priorità) — scollegare la postazione dalla rete.
2. **Conservare prove** — acquisire snapshot/immagine e salvare i file indicati (browser DB, DLL droppate, esportazioni registro).
3. **Quarantena del campione e dei file droppati** — mettere in quarantena il file malevolo e le librerie droppate. (Classificazione: **Vero positivo**).
4. **Reset credenziali sensibili** — forzare cambio password per gli account potenzialmente memorizzati nei browser; revocare token e sessioni.
5. **Bloccare i domini osservati** a livello DNS/proxy/firewall e generare regole per EDR/SIEM con gli IOC.
6. **Hunting laterale** — cercare gli stessi IOC su altri endpoint per valutare diffusione.
7. **Forensic & follow-up** — se host critico, eseguire analisi forense completa; segnalare al CERT/Vendor se necessario.

Decisione su classificazione e azione

- **Classificazione:** VERO POSITIVO (infostealer).
- **Azioni consigliate:** quarantena + rimozione controllata + reset credenziali + blocco rete + ricerca laterale.

Analisi secondo link

Analizzando il secondo link, anyrun ci anticipa di non aver trovato alcuna attività malevola all'interno della sandbox.

La sessione rappresenta quello che sembra essere un redirect che passa per il dominio click.convertkit-mail2.com prima di condurre l'utente alla pagina di login di Instagram:

instagram.com/accounts/login/ → è la **pagina ufficiale di login** di Instagram.

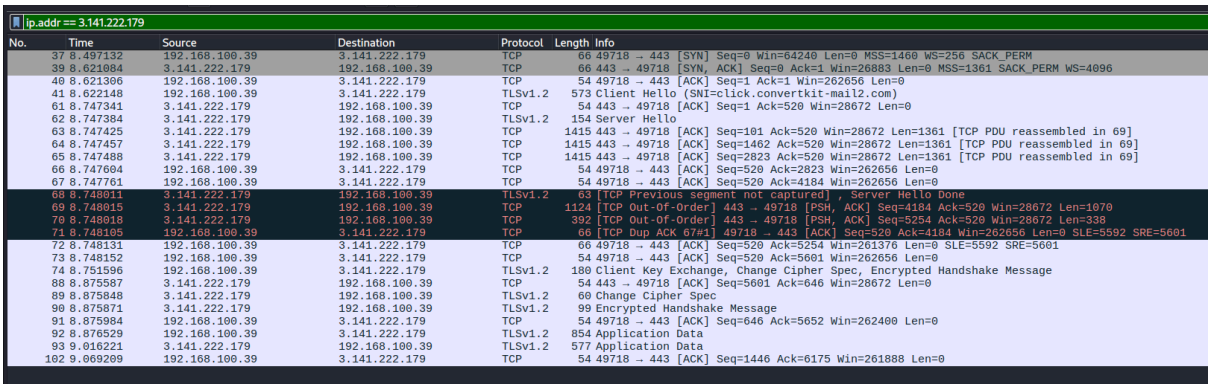
Il parametro next= all'interno del link ci comunica però che, dopo l'avvenuta autenticazione dell'utente, il browser provvederà a reindirizzarlo verso una nuova pagina".

In questo caso, traducendo l'istruzione da Base64 otteniamo che la pagina in oggetto è la seguente:

https://www.instagram.com/aussienurserecruiters/

Analisi Pcap

Per indagare ulteriormente ho provveduto a scaricare il pcap di anyrun ed analizzato il traffico relativo all'indirizzo ip sospetto:



ip.addr == 3.141.222.179

No.	Time	Source	Destination	Protocol	Length	Info
37	8.497132	192.168.100.39	3.141.222.179	TCP	66	49718 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
39	8.621084	3.141.222.179	192.168.100.39	TCP	66	443 → 49718 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1361 SACK_PERM WS=4096
40	8.621306	192.168.100.39	3.141.222.179	TCP	54	49718 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
41	8.622148	192.168.100.39	3.141.222.179	TLSv1.2	573	Client Hello (SNI=click.convertkit-mail2.com)
61	8.747341	3.141.222.179	192.168.100.39	TCP	54	443 → 49718 [ACK] Seq=1 Ack=520 Win=28672 Len=0
62	8.747384	3.141.222.179	192.168.100.39	TLSv1.2	154	Server Hello
63	8.747425	3.141.222.179	192.168.100.39	TCP	1415	443 → 49718 [ACK] Seq=101 Ack=520 Win=28672 Len=1361 [TCP PDU reassembled in 69]
64	8.747457	3.141.222.179	192.168.100.39	TCP	1415	443 → 49718 [ACK] Seq=1462 Ack=520 Win=28672 Len=1361 [TCP PDU reassembled in 69]
65	8.747488	3.141.222.179	192.168.100.39	TCP	1415	443 → 49718 [ACK] Seq=2823 Ack=520 Win=28672 Len=1361 [TCP PDU reassembled in 69]
66	8.747604	192.168.100.39	3.141.222.179	TCP	54	49718 → 443 [ACK] Seq=520 Ack=2823 Win=262656 Len=0
67	8.747761	192.168.100.39	3.141.222.179	TCP	54	49718 → 443 [ACK] Seq=520 Ack=4184 Win=262656 Len=0
68	8.748011	3.141.222.179	192.168.100.39	TLSv1.2	63	[TCP Previous segment not captured] , Server Hello Done
69	8.748015	3.141.222.179	192.168.100.39	TCP	1124	[TCP Out-Of-Order] 443 → 49718 [PSH, ACK] Seq=4184 Ack=520 Win=28672 Len=1070
70	8.748018	3.141.222.179	192.168.100.39	TCP	392	[TCP Out-Of-Order] 443 → 49718 [PSH, ACK] Seq=5254 Ack=520 Win=28672 Len=338
71	8.748105	192.168.100.39	3.141.222.179	TCP	66	[TCP Dup ACK 67#1] 49718 → 443 [ACK] Seq=520 Ack=4184 Win=262656 Len=0 SLE=5592 SRE=5601
72	8.748131	192.168.100.39	3.141.222.179	TCP	66	49718 → 443 [ACK] Seq=520 Ack=5254 Win=261376 Len=0 SLE=5592 SRE=5601
73	8.748152	192.168.100.39	3.141.222.179	TCP	54	49718 → 443 [ACK] Seq=520 Ack=5601 Win=262656 Len=0
74	8.751596	192.168.100.39	3.141.222.179	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
88	8.875587	3.141.222.179	192.168.100.39	TCP	54	443 → 49718 [ACK] Seq=5601 Ack=646 Win=28672 Len=0
89	8.875848	3.141.222.179	192.168.100.39	TLSv1.2	60	Change Cipher Spec
90	8.875871	3.141.222.179	192.168.100.39	TLSv1.2	99	Encrypted Handshake Message
91	8.875984	192.168.100.39	3.141.222.179	TCP	54	49718 → 443 [ACK] Seq=646 Ack=5652 Win=262400 Len=0
92	8.876529	192.168.100.39	3.141.222.179	TLSv1.2	854	Application Data
93	9.016221	3.141.222.179	192.168.100.39	TLSv1.2	577	Application Data
102	9.069209	192.168.100.39	3.141.222.179	TCP	54	49718 → 443 [ACK] Seq=1446 Ack=6175 Win=261888 Len=0

Il Flusso TCP/TLS verso click.convertkit-mail2.com avviene tramite **Handshake TLSv1.2** con SNI esplicito: click.convertkit-mail2.com.

L'IP di destinazione è 3.141.222.179 (AWS / Amazon ASN-02).

Subito dopo l'handshake il traffico diventa **TLS cifrato (Application Data)** → quindi non è possibile vedere il contenuto senza chiavi di sessione.

Interpretazione: la comunicazione è una normale connessione HTTPS a un dominio di tracking marketing (ConvertKit), senza evidenze dirette di exploit o payload.

Sono presenti altri flussi TLS nel PCAP con handshake verso accounts.google.com (TLSv1.3) e www.instagram.com (TLSv1.3).

- Tutti i certificati sono validi, domini coerenti e con SNI corretto.
- Anche qui, tutto il traffico dopo l'handshake è cifrato e appare come **Application Data**.

Da quanto si può apprendere, il redirect appare legittimo. Prima passa dal dominio ConvertKit per il tracciamento del click, poi l'utente viene inviato al

login ufficiale di Instagram e interagisce con Google (probabilmente per federated login).

Anche da questa analisi non è però emersa alcuna apparente criticità.

Osservando le richieste DNS risultano richieste verso:

- **settings-win.data.microsoft.com** → Telemetria/aggiornamenti Microsoft (legittimo).
- **google.com** e **accounts.google.com** → login/servizi Google (legittimo).
- **click.convertkit-mail2.com** → dominio di tracciamento/campaign tracking usato da ConvertKit (non intrinsecamente malevolo, ma spesso sfruttato in catene di phishing).
- **instagram.com** e **static.cdninstagram.com** → accesso al login e contenuti Instagram (legittimo).
- **login.live.com** e **client.wns.windows.com** → autenticazione Microsoft e notifiche Windows Push (legittimo).
- **ocsp.digicert.com** → verifica certificati SSL (legittimo).
- **facebook.com** e sotto-domini (fbcdn.net, star-mini.c10r.facebook.com, ecc.) → tipici del login e caricamento asset di Facebook/Meta (legittimo).
- **googleapis.com** → API di Google per autocompletamento/autenticazione (legittimo).
- **facer.delivery.mp.microsoft.com** → aggiornamenti di Windows (legittimo).

L'unico dominio "anomalo" nel flusso è **click.convertkit-mail2.com**

Ed il redirect/track da email marketing porta l'utente a instagram.com/aussienurserecruiters.

Criticità: **non è di per sé malware**, ma rappresenta un punto tipico di phishing/social engineering, perché l'utente pensa di cliccare su un link "sicuro" (Instagram), mentre in realtà passa da un redirect tracciato. Questo rende difficile distinguere se il flusso fosse legittimo (newsletter) o parte di una campagna malevola.

In conclusione non ci sono richieste DNS a host sconosciuti, offuscati o a TLD strani (tipo .ru, .top, .xyz) che di solito emergono in malware o phishing più grezzi.

Non è presente nessun tentativo di connessione a server C2 noti o a domini generati casualmente (DGA), nessun tunneling DNS (tutte le query sono standard A/CNAME, non ci sono payload dati all'interno), nessun traffico DNS anomalo in quantità (il volume è coerente con un redirect web + caricamento di risorse social).

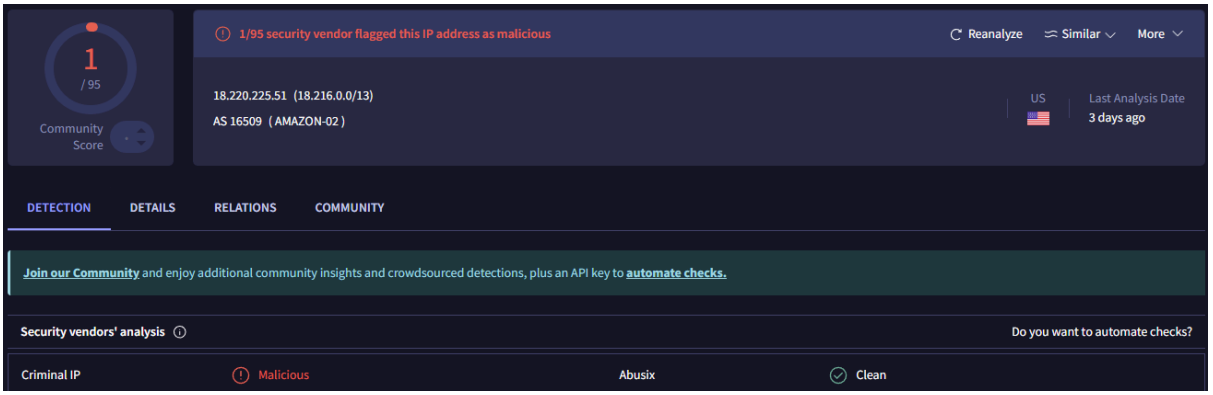
IOC

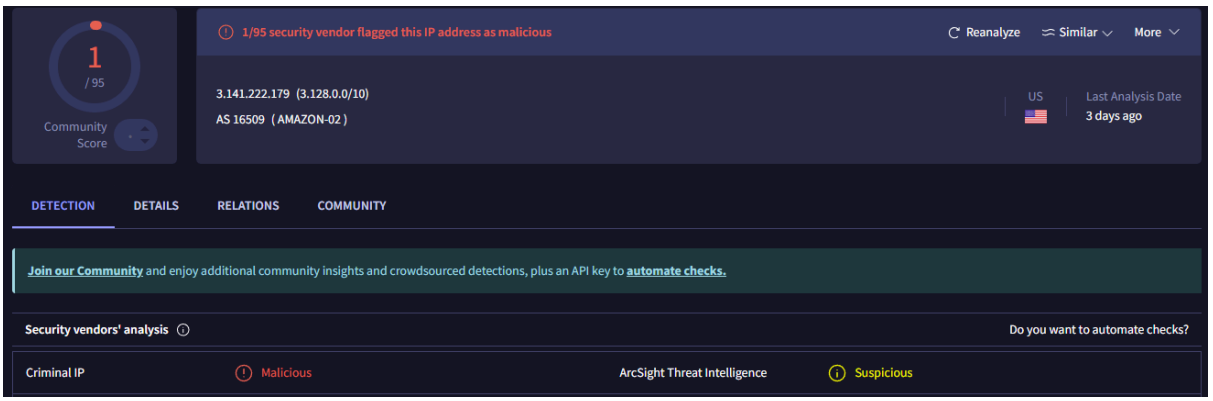
Hash task/oggetto aperto in Any.Run

- SHA256: 6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC
- SHA1: F52CB78B7F23559FFCE5D1125EFD7B399165DFFC
- MD5: 4C091A5A8C03EBC2EA267980D0DA9F8D

Domini / IP osservati

- click.convertkit-mail2.com → 3.141.222.179, 3.18.56.123, 18.220.225.51 (AWS)
- www.instagram.com → 157.240.0.174 (Meta)
- static.cdninstagram.com → 157.240.0.63 (Meta)
- accounts.google.com → 66.102.1.84 (Google)
- (di servizio) ocsp.digicert.com, www.microsoft.com (CRL), settings-win.data.microsoft.com, login.live.com, client.wns.windows.com





Executive Summary

Dall'analisi del secondo campione non emergono attività malware "classiche" (installazione di software malevolo, furto di credenziali automatico o comunicazioni verso Command&Control).
Quello che abbiamo osservato è un **redirect web**: cliccando un link, il traffico passa attraverso il dominio click.convertkit-mail2.com (**piattaforma di marketing/automazione email**) e porta poi alla pagina ufficiale di login di Instagram.

Di per sé questo comportamento è **legittimo** (normale tracciamento di click nelle newsletter), ma è anche una tecnica spesso sfruttata in **phishing**: l'utente pensa di cliccare un link sicuro (es. "Instagram"), ma in realtà prima passa per un servizio esterno che può essere usato per offuscare o mascherare la destinazione reale.

Rischi possibili

Per dare un giudizio più determinante riguardo all'analisi sarebbe però importante conoscere alcune dinamiche extra-analisi:

- E' opportuno capire se il link è stato ricevuto via email e cliccato da un dipendente, in questo caso significa che la persona in oggetto è vulnerabile a campagne di **phishing/social engineering**.

- Se il browser (Chrome) è stato aperto senza interazione diretta (ad esempio al boot del sistema), si potrebbe ipotizzare un automatismo o un comportamento sospetto, ma questo non è confermato dal campione.

Azioni consigliate

Alcune operazioni sono però fortemente raccomandate per prevenire qualsivoglia problematica in merito alla situazione analizzata:

1. **Formazione utenti in merito al phishing**: ricordare l'importanza di non cliccare link non verificati nelle email.
2. **Monitoraggio DNS e Proxy**: aggiungere controlli su domini "di tracciamento" come click.convertkit-mail2.com per distinguerne l'uso legittimo da quello sospetto.
3. **Policy di sicurezza email**: rafforzare i filtri antispam e phishing per intercettare link con redirect sospetti.
4. **Verifica endpoint**: controllare se Chrome è stato avviato da un utente o in background (es. all'avvio del sistema). Questo dettaglio aiuta a capire se c'è stata interazione o meno.

Classificazione

- **Non malware attivo**, ma **potenziale vettore di phishing**.
- Decisione: **vero positivo in contesto di phishing/social engineering**, non come infezione malware.
- Remediation: nessuna quarantena necessaria, ma **monitoraggio e formazione utenti**.

Conclusioni generali

Dalle analisi condotte su due campioni diversi emergono due scenari distinti:

1. Primo campione **(vero malware – infostealer Vidar/Lumma-like):**

   Abbiamo confermato la presenza di un software malevolo progettato per **rubare credenziali, cookie e informazioni sensibili dai browser e da alcuni client di rete**. Questo tipo di minaccia è pericolosa perché può portare al **furto di account aziendali**, accesso non autorizzato ai sistemi e possibili violazioni di dati. La classificazione è **vero positivo**: il file è realmente malevolo e richiede **quarantena immediata**, rimozione controllata e reset delle credenziali.

2. Secondo campione **(redirect web – rischio phishing/social engineering):**

   Non abbiamo trovato indicatori di malware attivo o comunicazioni verso server di comando e controllo. Si tratta invece di un **link di tracciamento marketing** che reindirizza al login ufficiale di Instagram. Di per sé non è dannoso, ma rappresenta una tipica tecnica sfruttata in campagne di **phishing**, in cui l'utente potrebbe essere indotto a cliccare su link dall'aspetto legittimo ma controllati da terze parti. La classificazione è **non malware attivo quindi vero negativo**, ma si potrebbe considerare un **vero positivo se visto in ottica phishing/social engineering**.

Implicazioni per l'organizzazione

- Nel primo caso siamo di fronte a una **minaccia concreta** che richiede risposta tecnica immediata.
- Nel secondo caso la criticità non è tecnica, ma **comportamentale**: se un dipendente ha cliccato il link senza verifiche, questo segnala la necessità di **formazione anti-phishing**.

Azioni prioritarie

- **Rimozione/quarantena immediata del primo malware e reset delle credenziali compromesse.**
- **Formazione del personale** su phishing e gestione sicura delle email.
- **Rafforzamento dei controlli di rete ed email** per intercettare redirect sospetti.
- **Monitoraggio degli endpoint e dei log DNS/proxy** per individuare tentativi simili in futuro.