Rapporto Ufficiale di Analisi di Sicurezza

A cura del team: SecureSentinels

Data di redazione: 24 Febbraio 2026

Oggetto: Verifica di potenziale tentativo di Phishing / Infezione Malware tramite link sospetto.

1. Sintesi per il Management (Executive Summary)

Il team **SecureSentinels** ha condotto un'indagine tecnica approfondita su un indirizzo web (URL) segnalato come potenziale minaccia. L'obiettivo era accertare se il link fosse un tentativo di rubare credenziali (phishing) o di installare virus sul computer.

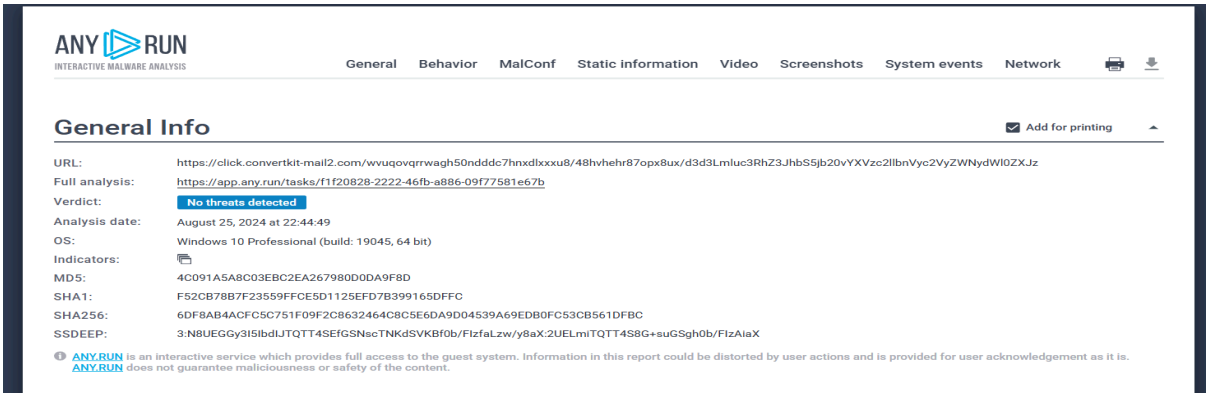
Esito Finale: Il link analizzato è **SICURO**. Si tratta di un normale link di reindirizzamento gestito da una piattaforma di email marketing (ConvertKit) che porta l'utente verso una pagina legittima di Instagram. Non sono state rilevate minacce per i dati aziendali o personali.

---

2. Esito dell'Analisi di Laboratorio (ANY.RUN)

Il primo passaggio ha previsto l'apertura del link in "ANY.RUN", una vera e propria camera blindata digitale (sandbox) che ci permette di far esplodere eventuali minacce senza alcun rischio.

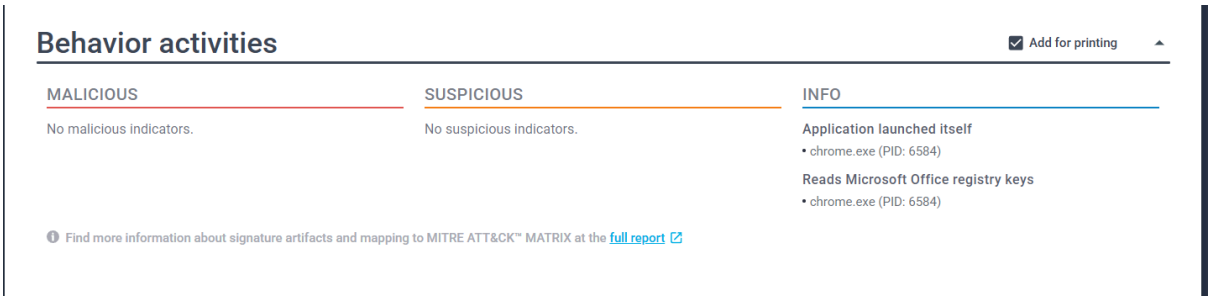
- **Verdetto Ufficiale:** Il sistema ha restituito l'esito verde **"No threats detected"** (Nessuna minaccia rilevata).
- **Impronte Digitali (Hash):** Sono stati calcolati i codici identificativi univoci dell'analisi (es. MD5: 4C091A5A8C03EBC2EA26798000DA9F8D) per garantire la tracciabilità e l'integrità del test.



3. Comportamento nel Computer (Cosa è successo realmente?)

Abbiamo analizzato come si è comportato il computer quando ha cliccato sul link, cercando qualsiasi azione sospetta (es. programmi nascosti che si avviano da soli).

- **Indicatori di Pericolo:** Le categorie "Malicious" (Malevolo) e "Suspicious" (Sospetto) sono risultate completamente pulite, registrando "0 indicatori".
- **Attività di Routine:** L'unica attività segnalata è stata la normale apertura del browser web ("chrome.exe") e la lettura di alcune chiavi di sistema legate a Microsoft Office. Si tratta di un comportamento standard dei moderni browser.

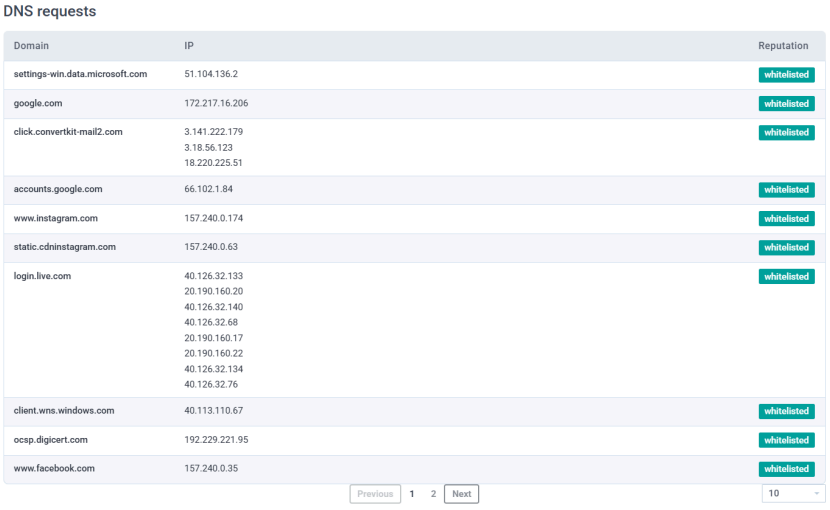


- **Albero dei Processi:** La rappresentazione visiva di come i programmi si sono attivati nel computer mostra esclusivamente il flusso naturale del browser Google Chrome che apre le sue schede di navigazione, senza che nessun programma estraneo o virus abbia tentato di inserirsi.

4. Analisi delle Comunicazioni (Chi ha contattato il link?)

Per smascherare un eventuale sito di phishing, dobbiamo guardare con chi "parla" il link su internet. Un sito truffaldino comunicherebbe con server sconosciuti in paesi a rischio.

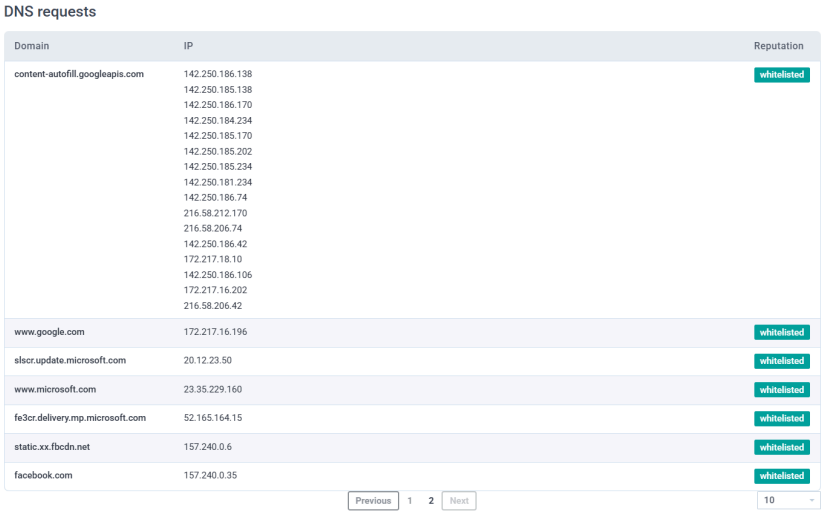
- **Elenco dei Siti Contattati (DNS):** Tutte le chiamate effettuate dal browser sono state rivolte a domini di aziende globali certificate. Nel dettaglio, il sistema ha assegnato l'etichetta verde **"whitelisted"** (sito affidabile e autorizzato) a tutti i domini contattati, tra cui:
    - I servizi Microsoft (es. `settings-win.data.microsoft.com`).
    - I server di reindirizzamento delle email (`click.convertkit-mail2.com`).
    - I servizi di Google (`accounts.google.com`, `google.com`).
    - Le piattaforme Meta/Facebook (`www.instagram.com`, `www.facebook.com`).



DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	51.104.136.2	whitelisted
google.com	172.217.16.206	whitelisted
click.convertkit-mail2.com	3.141.222.179 3.18.56.123 18.220.225.51	whitelisted
accounts.google.com	66.102.1.84	whitelisted
www.instagram.com	157.240.0.174	whitelisted
static.cdninstagram.com	157.240.0.63	whitelisted
login.live.com	40.126.32.133 20.190.160.20 40.126.32.140 40.126.32.68 20.190.160.17 20.190.160.22 40.126.32.134 40.126.32.76	whitelisted
client.wns.windows.com	40.113.110.67	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
www.facebook.com	157.240.0.35	whitelisted

Previous 1 2 Next 10



DNS requests

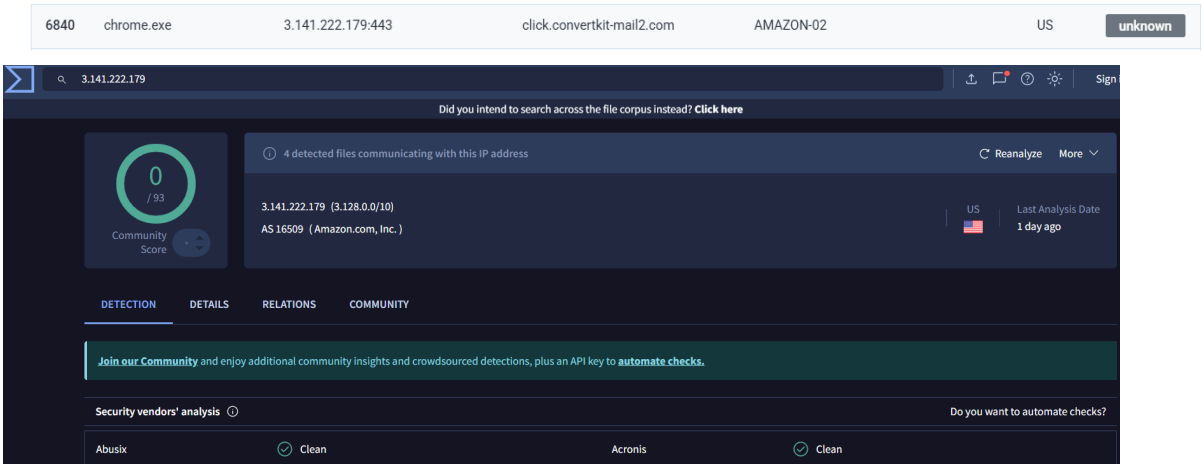
Domain	IP	Reputation
content-autofill.googleapis.com	142.250.186.138 142.250.185.138 142.250.186.170 142.250.184.234 142.250.185.170 142.250.185.202 142.250.185.234 142.250.181.234 142.250.186.74 216.58.212.170 216.58.206.74 142.250.186.42 172.217.18.10 142.250.186.106 172.217.16.202 216.58.206.42	whitelisted
www.google.com	172.217.16.196	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
www.microsoft.com	23.35.229.160	whitelisted
fe3cr.delivery.mp.microsoft.com	52.165.164.15	whitelisted
static.xx.fbcdn.net	157.240.0.6	whitelisted
facebook.com	157.240.0.35	whitelisted

Previous 1 2 Next 10

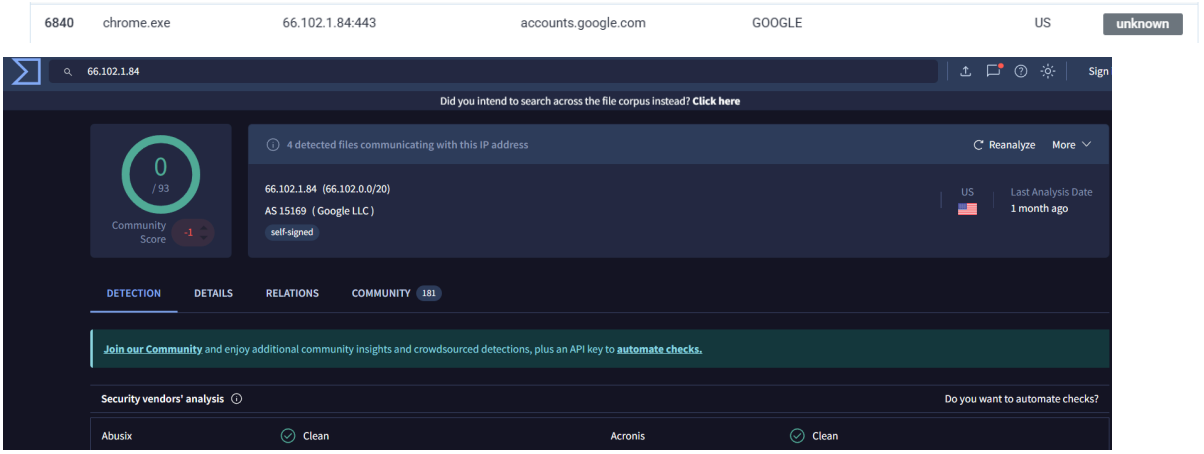
5. Controllo Incrociato Globale (VirusTotal)

Per fornire una sicurezza totale, il team **SecureSentinels** ha estratto gli indirizzi "fisici" (Indirizzi IP) dei server contattati ed ha interrogato **VirusTotal**, una piattaforma che aggrega oltre 90 dei migliori antivirus e sistemi di sicurezza al mondo.

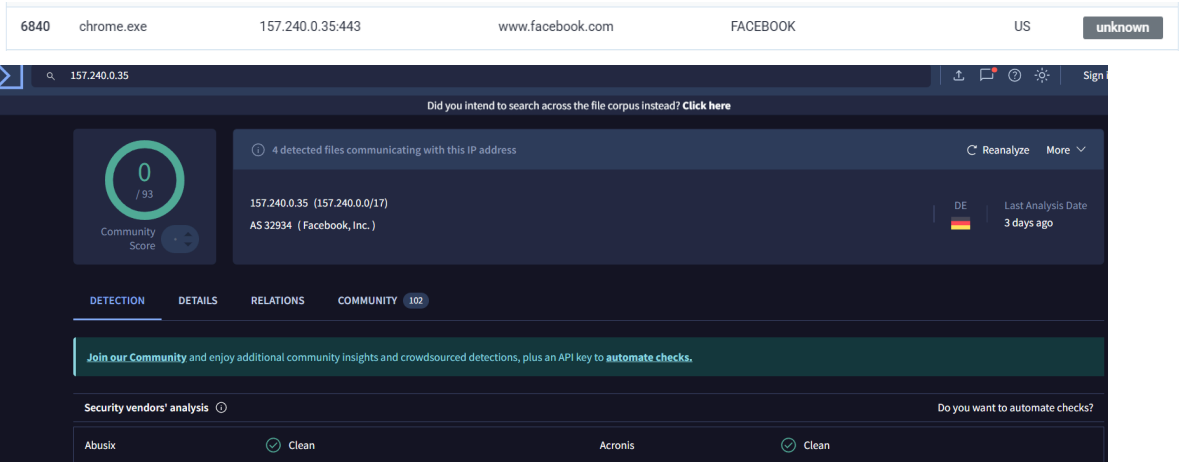
- **Server di Smistamento (Email):** L'indirizzo `3.141.222.179` (appartenente ad Amazon e usato da ConvertKit) è risultato **pulito al 100%** (0 motori su 93 hanno rilevato minacce).



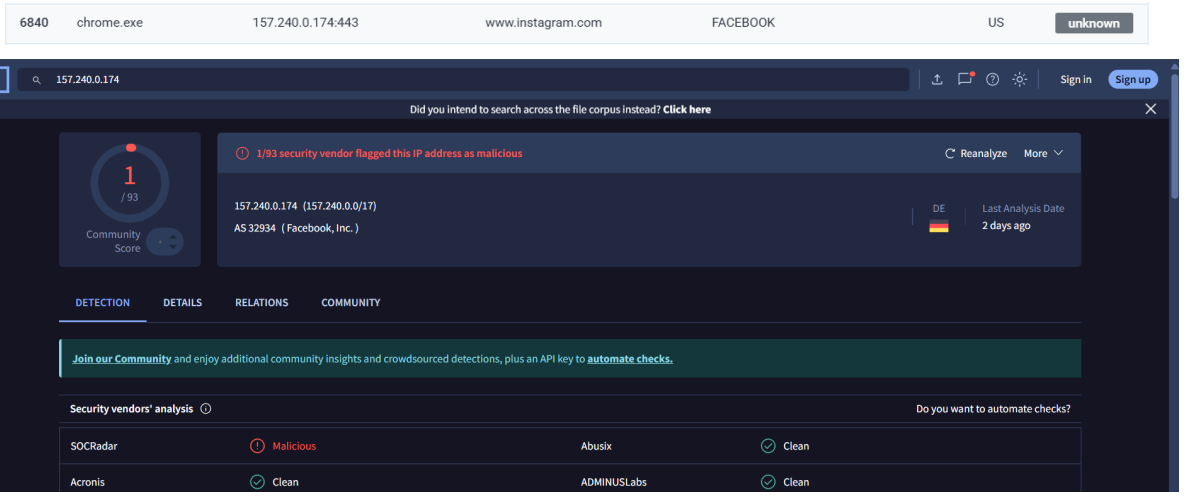
- **Server di Google:** L'indirizzo `66.102.1.84` (Google LLC) è risultato **pulito al 100%** (0 motori su 93 hanno rilevato minacce).



- **Server di Facebook/Instagram (1):** L'indirizzo `157.240.0.35` (Facebook, Inc.) è risultato **pulito al 100%** (0 motori su 93 hanno rilevato minacce).



- **Server di Facebook/Instagram (2):** L'indirizzo `157.240.0.174` (Facebook, Inc.) ha riportato un punteggio di **1/93** (un solo fornitore minore, SOCRadar, lo ha etichettato).
    - *Nota tecnica del team:* Questo singolo rilevamento su 93 è quello che in gergo si chiama "falso positivo" (un falso allarme). Essendo l'indirizzo parte dell'infrastruttura ufficiale e globale di Facebook, è impossibile che si tratti di un server malevolo gestito da hacker.



---

6. Conclusioni

Tutte le prove raccolte (analisi del comportamento, verifica del traffico e controllo incrociato globale) portano a un'unica e solida conclusione: l'utente che clicca su questo link non corre alcun rischio informatico.

Il team **SecureSentinels** archivia la segnalazione come **Falso Allarme**.