

BW III - Anyrun 1

Rapporto di analisi malware

Data: 03/02/2025

Compagnia: Security Griffins

- **Introduzione**

Questo rapporto descrive l'infezione da malware identificata all'interno dell'infrastruttura IT della compagnia. Verranno analizzati i dettagli tecnici dell'infezione, l'impatto sui sistemi e le possibili strategie di rimozione della minaccia.

- **Dettagli del malware**

Nome: Vidar

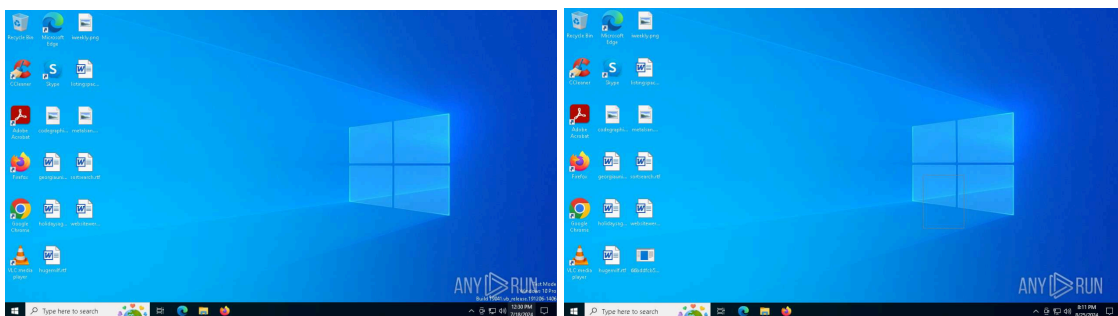
Categoria: Loader, Stealer

Vettori di infezione: Email di phishing, siti web compromessi.

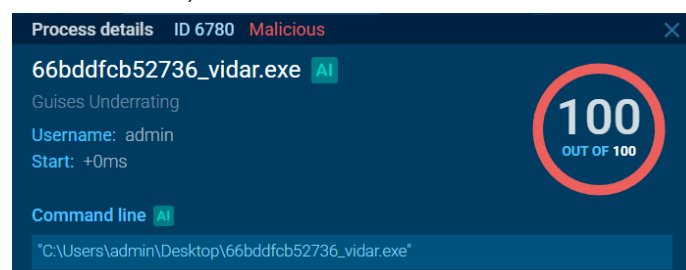
Obiettivi: Furto di credenziali, esfiltrazione dati, installazione di payload aggiuntivi.

- **Metodologia di infezione**

Attraverso un'analisi preliminare degli screenshot del sistema infetto pre e post infezione, possiamo notare la comparsa di uno strano file eseguibile.



Da un'analisi approfondita del file, esso viene riconosciuto come malevolo.



Tramite il report effettuato con Anyrun, veniamo a conoscenza del fatto che si tratta di un malware con in grado di svolgere due funzioni principali:

1. **Loader:** software malevolo progettato per infiltrarsi nei dispositivi e scaricare, installare o eseguire altri malware sul sistema infetto.
2. **Stealer:** software progettato per rubare informazioni sensibili da un dispositivo infetto e inviarle agli attaccanti.

Molto probabilmente si tratta di un file scaricato inconsapevolmente da un dipendente dell'azienda dopo essersi collegato al sito steamcommunity.com, un sito web compromesso. Ciò può essere visto sia nel report redatto da Anyrun, che analizzando il traffico di rete.

Malware configuration

Vidar

Vidar

(PID) Process

(6908) RegAsm.exe

C2

https://t.me/pech0nk

URL

https://steamcommunity.com/profiles/76561199751190313

Strings (310)

INSERT_KEY_HERE

HTTP Requests

5

Connections

53

DNS Requests

16



Threats

8

Filter by PID, domain, name or ip

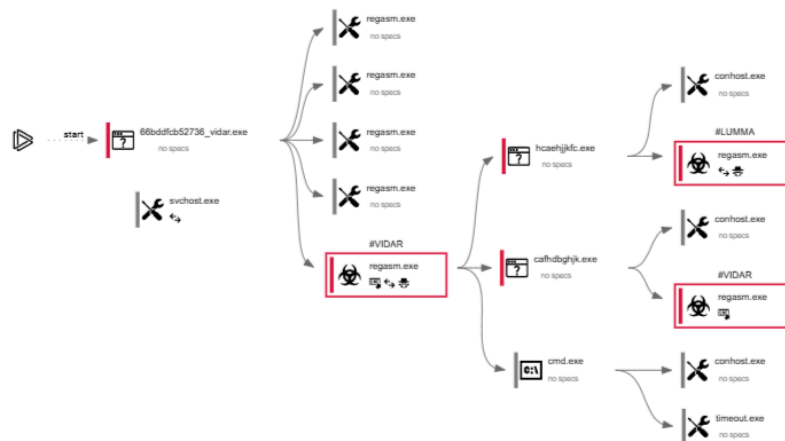
PCAP

Download

PID	Process name	CN	IP	Port	Domain	ASN	Traffic
—	—		4.231.128.59	443	settings-win....	MICROSOFT-CO...	<div>↑</div> <div>2 Kb</div> <div>↓</div> <div>8 Kb</div>
6908	RegAsm.exe		23.212.216.106	443	steamcomm...	AKAMAI-AS	<div>↑</div> <div>459 b</div> <div>↓</div> <div>40 Kb</div>

- **Analisi malware**

Passiamo ora ad un'analisi del malware per capire come funziona nel dettaglio e quali sono i possibili rischi per l'azienda di nostro interesse.



Analizzando lo schema soprastante, possiamo vedere che l'eseguibile **66bddfcb52736_vidar.exe** ha una serie di eseguibili ad esso associati, tutti con il nome **regasm.exe**, molto probabilmente per cercare di evadere sistemi di sicurezza.

Uno di questi in particolare, è riconosciuto da Anyrun come malevolo.

A sua volta infatti, quest'ultimo, avvia due applicazioni:

- ## 1. hcaehjjkfc.exe:

Process details

ID 1568

Malicious

✕

HCAEHJJKFC.exe

AI

100
OUT OF 100

Auto File System Format Utility

Username: admin

Start: +20553ms

Indicators: 🚩

Command line

AI

"C:\ProgramData\HCAEHJJKFC.exe"

More Info

More Info

Hide all

Other 2

T1012 Query Registry (2)

- Reads the computer name
- Checks supported languages

T1082 System Information Discovery (2)

- Reads the computer name
- Checks supported languages

- ## 2. **cafhdbghjk.exe:**

Process details ID 6248 Malicious

CAFHDBGHJK.exe AI

Auto File System Format Utility

Username: admin

Start: +21335ms Indicators:

Command line AI

"C:\ProgramData\CAFHDBGHJK.exe"

100 OUT OF 100

Other 2

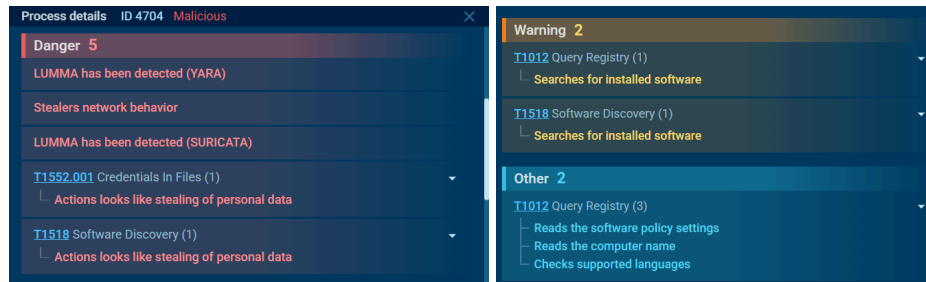
T1012 Query Registry (2)

- Checks supported languages
- Reads the computer name

T1082 System Information Discovery (2)

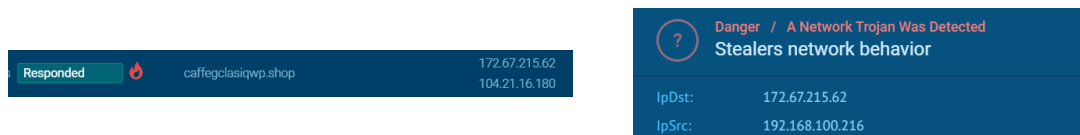
- Checks supported languages
- Reads the computer name

Entrambi i file sono in grado di leggere informazioni dal registro di sistema. Inoltre essi sono responsabili dell'avvio di un altro applicativo **RegAsm.exe** (processo differente rispetto al processo padre **regasm** precedente):



Qui risiedono le attività più pericolose:

1. **Lumma has been detected:**
LUMMA è un malware as-a-service, utilizzato per “rubare” informazioni dal sistema target.
2. **Stealers network behavior:**
Indica che il programma in grado di leggere informazioni sul nostro sistema sta cercando di comunicare su internet. Questo è tipico dell'esfiltrazione dati. Tali comunicazioni sono visibili anche tramite un'analisi di rete attraverso cui vengono riconosciute richieste DNS e connessioni TCP sospette.



3. **Actions looks like stealing of personal data:**
Il malware ha accesso a file in cui sono salvate credenziali.
4. **Searches for installed software:**
Ricerca software installati sul sistema.
5. **Reads the software policy settings:**
E' in grado di prendere informazioni dal registro tra cui informazioni critiche come le policy di sicurezza.

Inoltre **regasm.exe** è in grado di avviare in autonomia **cmd.exe** e quindi eseguire comandi da terminale con cui potrebbe apportare pesanti modifiche al sistema. Nel fare ciò, esso utilizza delle tecniche di evasione come il **timeout.exe**, con cui è in grado di ritardare le sue azioni sfuggendo ai controlli.

Le azioni malevole del file sono poi confermate anche da altri elementi presenti nel report Anyrun, come modifiche al registro ad opera del file **RegAsm** e richieste **GET** sospette.

Modification events

(PID) Process:	(6908) RegAsm.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation:	write	Name:	CachePrefix
Value:			
(PID) Process:	(6908) RegAsm.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation:	write	Name:	CachePrefix
Value:	Cookie:		
(PID) Process:	(6908) RegAsm.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation:	write	Name:	CachePrefix
Value:	Visited:		

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6908	RegAsm.exe	GET	200	147.45.44.104:80	http://147.45.44.104/prog/66cb2dfb8d84_jawmg.exe	unknown	--	--	suspicious
6908	RegAsm.exe	GET	200	147.45.44.104:80	http://147.45.44.104/prog/66cb2df1d4a01_vakerk.exe	unknown	--	--	suspicious

Infine, come ultima analisi per capire a fondo il comportamento del malware in esame, passiamo all'analisi degli avvisi prodotti dal nostro **IDS**:

HTTP Requests	5	Connections	53	DNS Requests	16	Threats	8	Filter by message	PCAP
Timeshift	Class	PID	Process name	Message					
20421 ms	Potentially Bad Traffic	6908	RegAsm.exe	ET HUNTING SUSPICIOUS Dotted Quad Ho...					
20417 ms	Potential Corporate Privacy Violation	6908	RegAsm.exe	ET POLICY PE EXE or DLL Windows file dow...					
20409 ms	Potentially Bad Traffic	6908	RegAsm.exe	ET INFO Executable Download from dotted...					
20424 ms	Misc Attack	6908	RegAsm.exe	ET DROP Spamhaus DROP Listed Traffic In...					
21446 ms	Potentially Bad Traffic	6908	RegAsm.exe	ET INFO Executable Download from dotted...					
21449 ms	A Network Trojan was detected	4704	RegAsm.exe	STEALER [ANY.RUN] Lumma Stealer TLS C...					
22978 ms	Potentially Bad Traffic	2256	svchost.exe	ET POLICY DNS Query to DynDNS Domain *					
89388 ms	Potentially Bad Traffic	6908	RegAsm.exe	ET HUNTING SUSPICIOUS Dotted Quad Ho...					

1. **ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response:**
Indica una risposta HTTP sospetta contenente un header MZ (tipico dei file eseguibili Windows, .exe).
2. **ET POLICY PE EXE or DLL Windows file download HTTP:**
Indica che un file eseguibile (.exe) o una libreria (.dll) è stato scaricato tramite HTTP. In questo caso, il file viene scaricato dall'indirizzo IP 147.45.44.104 (malevolo).
3. **ET DROP Spamhaus DROP Listed Traffic Inbound group 23:**
Indica che del traffico in entrata proviene da un indirizzo IP elencato nella Spamhaus DROP List, che include IP noti per attività malevola.
4. **STEALER [ANY.RUN] Lumma Stealer TLS Connection:**
Indica che il malware Lumma Stealer è stato rilevato mentre stabiliva una connessione TLS criptata con un server remoto.
5. **ET POLICY DNS Query to DynDNS Domain .zapro.org:**
Indica che è stata effettuata una query DNS verso un dominio zapro.org, che è un servizio offerto da DynDNS. Tali domini possono essere utilizzati da cybercriminali per controllare malware o creare infrastrutture di attacco.

● Conclusione analisi

Un dipendente aziendale ha scaricato inconsapevolmente un file malevolo da una pagina steamcommunity.com modificata.

Una volta avviato, tale file compie molteplici funzioni:

1. Si collega ad internet e tramite richieste HTTP scarica altri payload malevoli.
2. Legge informazioni chiave presenti sul sistema.
3. Es filtra queste informazioni tramite internet verso IP malevoli.
4. Interviene sul registro di sistema per garantire persistenza e operabilità.

● Remediation

1. Considerando che il file malevolo es filtra i dati sensibili, dobbiamo impedire qualsiasi comunicazione con gli attaccanti **isolando** immediatamente il file ed il dispositivo infetto:

- Scollegare immediatamente il dispositivo infetto da internet e dalla rete aziendale .
- Mettere in quarantena il file malevolo per evitare che venga eseguito accidentalmente (utilizzando un software antivirus o manualmente).
- Bloccare l'esecuzione di programmi sospetti sul dispositivo compromesso.

Così facendo preveniamo la sottrazione di informazioni e blocchiamo la diffusione del malware.

2. Avendo la certezza che il file sia un **vero positivo** dobbiamo procedere all'**eliminazione** completa del malware:
 - Facciamo una scansione antivirus/EDR su tutto il dispositivo.
 - Controlliamo se il malware ha creato file aggiuntivi in cartelle di sistema o temporanee.
 - Rimuoviamo completamente il file **66bddfcb52736_vidar.exe** e i suoi file correlati.Così facendo eliminiamo il malware e garantiamo che non possa essere riattivato.
3. Per **evitare** che il file venga scaricato nuovamente in futuro:
 - Aggiungiamo l'hash SHA256 del file alla blacklist aziendale.
 - Configuriamo firewall, antivirus ed EDR per rilevare e bloccare file con lo stesso hash.Così facendo preveniamo future infezioni dello stesso malware.
4. Purtroppo, il malware potrebbe aver già inviato i dati rubati agli attaccanti. Dobbiamo **controllare** i log di sistema e di rete per identificare:
 - Connessioni a indirizzi IP sospetti.
 - Trasferimenti di dati insoliti.
 - Tentativi di contattare server C2 (sono i server utilizzati per controllare e gestire i botnet).
 - Dobbiamo bloccare indirizzi IP e domini sospetti identificati nei log e monitorare il traffico per eventuali nuove connessioni anomale.Così facendo capiamo se i dati sono già stati sottratti e impediamo future comunicazioni con gli attaccanti.
5. Considerando che il malware legge e ruba le password salvate nei browser dobbiamo:
 - Obbligare il **cambio password** per tutti gli utenti che hanno usato il dispositivo infetto.
 - Invalidare eventuali sessioni attive (logout forzato dagli account aziendali: per Google, Microsoft, Facebook, ecc., esistono opzioni per disconnettere tutti i dispositivi).
 - Verificare accessi sospetti su account aziendali e personali.Così facendo preveniamo l'uso delle credenziali rubate da parte degli attaccanti e cerchiamo di limitare i danni.
6. Dal momento in cui il malware ha modificato file o configurazioni di sistema, la soluzione più sicura è effettuare una **formattazione completa** e ripristinare tutto da un **backup sicuro**:
 - Formattare completamente il dispositivo infetto (cancellando tutte le partizioni e reinstallando il sistema operativo da zero).
 - Ripristinare il backup pulito (dopo aver reinstallato il sistema, ripristiniamo il backup solo se è stato creato prima dell'infezione).Così facendo rimuoviamo ogni traccia del malware e garantiamo un ritorno a uno stato sicuro.

7. Considerando che il malware sfrutta vulnerabilità nei sistemi per infettare i dispositivi, è fondamentale **applicare patch e aggiornamenti di sicurezza** per ridurre il rischio di nuove infezioni:

- Aggiornare il sistema operativo e tutti i software installati per correggere eventuali falle di sicurezza.
- Verificare la presenza di patch di sicurezza per eventuali vulnerabilità note ed applicarle tempestivamente.
- Limitare i privilegi amministrativi agli utenti per evitare l'esecuzione non autorizzata di file sospetti.

Così facendo, riduciamo il rischio di nuove infezioni attraverso vulnerabilità non messe in sicurezza

8. Visto che questo malware si diffonde spesso tramite e-mail di phishing, allegati malevoli e siti infetti, è fondamentale **formare e sensibilizzare gli utenti** per prevenire future infezioni:

- Informare i dipendenti sui rischi legati all'apertura di allegati sospetti e link non verificati.
- Implementare un programma di formazione sulla sicurezza informatica per migliorare la consapevolezza sulle minacce informatiche.

Così facendo, riduciamo il rischio di nuove infezioni migliorando la consapevolezza e i comportamenti di sicurezza degli utenti.

9. Se l'infezione ha coinvolto dati sensibili, potrebbe essere necessario **segnalare** il caso ai vendor di sicurezza e alle autorità competenti per mitigare i rischi e prevenire ulteriori attacchi:

- Inviare il file sospetto ai vendor di sicurezza per migliorare il rilevamento e la protezione contro minacce simili.
- Se l'infezione ha causato una fuga di dati personali, valutare la segnalazione al Garante della Privacy (GDPR) per adempiere agli obblighi di protezione dei dati.
- Se l'infezione riguarda un'azienda pubblica o servizi critici, segnalare il caso alla Polizia Postale o ad altri enti di cybersecurity competenti.

Così facendo, proteggiamo l'azienda da conseguenze legali e contribuiamo a prevenire futuri attacchi informatici.

Anyrun 2

The screenshot displays the Anyrun 2 web interface, which is used for analyzing and monitoring system processes. The interface is divided into several sections:

- Top Section:** Shows the target application (Instagram) and its login page. It includes fields for "Phone number, username, or email" and "Password", and a "Log in" button.
- Bottom Section:** Contains a table of HTTP requests, a table of connections, a table of DNS requests, and a table of threats. The threats table shows three entries for "chrome.exe" with various threat indicators.
- Right Side:** Features a "No threats detected" message and a "Click to open in browser" button. Below this, there's a "Processes" section showing a list of running processes with their PIDs, names, and threat indicators.
- Bottom Right:** Includes a "Try community version for free!" button and a "Register now" button.

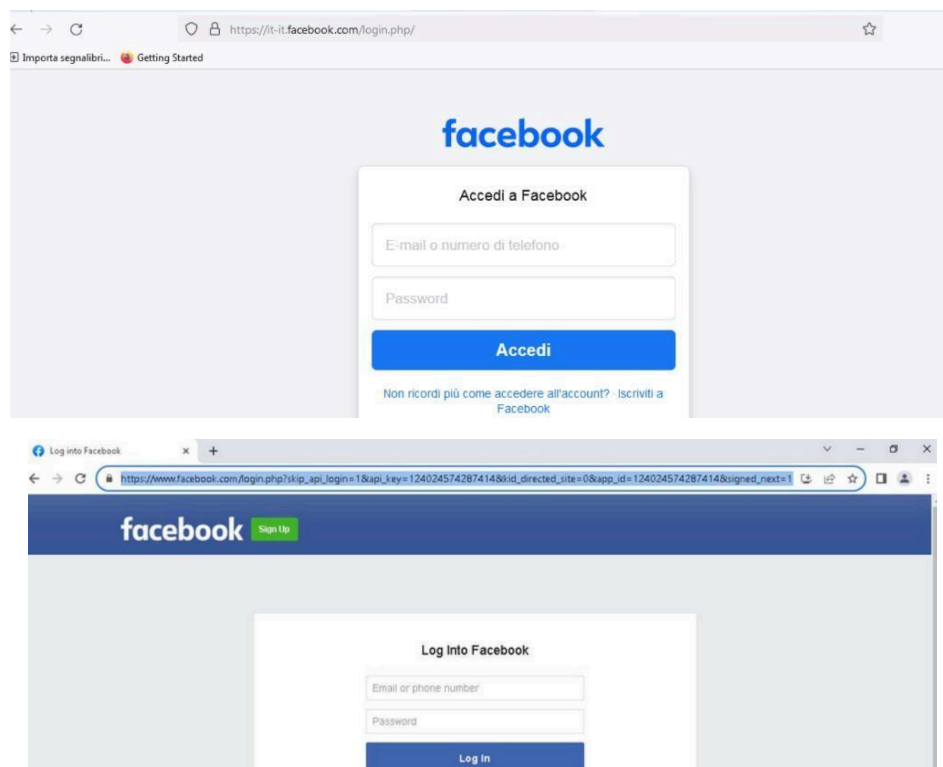
Abbiamo aperto il link e, da una prima analisi, non sembra avere intenzioni sospette. Non compare nessuna flag che possa indicare che l'obiettivo sia malevolo e analizzando le varie sezioni non sembrano esserci parti sospette. Tuttavia, per avere la conferma che questo link fosse innocuo, abbiamo deciso di utilizzare VirusTotal e accertarci che l'analisi con Anyrun fosse valida.

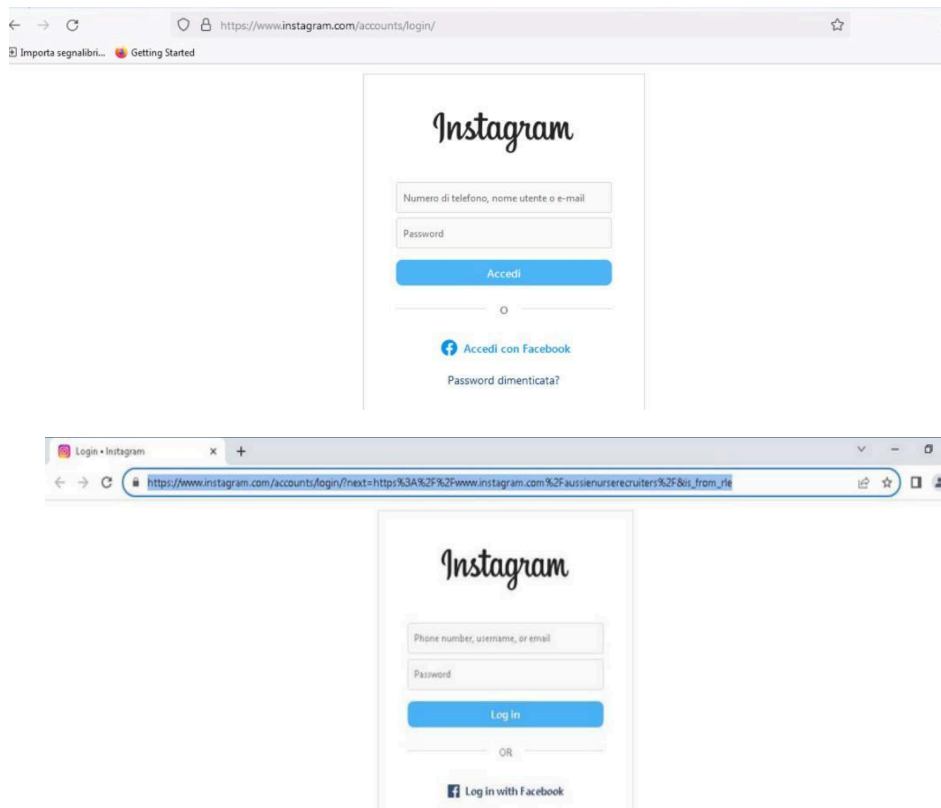
The screenshot shows the VirusTotal interface for the URL `https://click.convertkit-mail2.com/vwqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vVXVzc2llbnVyc2VyZWYdWl0ZXJz`. The Community Score is 2/96. A warning states: "2/96 security vendors flagged this URL as malicious". The status is 200, and the content type is text/html. The analysis was performed 1 month ago. The detection section shows the following results:

Security vendors' analysis	CRDF	Abusix	Phishing Database	Acronis
Malicious	Malicious	Clean	Phishing	Clean

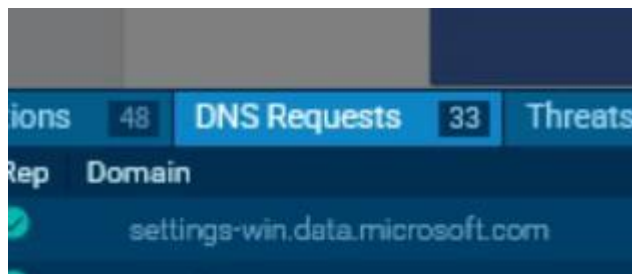
L'analisi su VirusTotal riconosce il link come malevolo e sospetto. Infatti, da questi risultati, abbiamo dedotto che la mail convertkit-mail2.com potrebbe essere una mail di phishing in grado di mostrarsi come una mail valida che porta al login di Instagram e Facebook.

Infatti, considerando le immagini recuperate su Anyrun e facendo un confronto con le pagine di login ufficiali di Instagram e Facebook abbiamo notato che queste non combaciano con le prime. Inoltre è comune che gli URL di phishing spesso usino parametri lunghi per confondere l'utente.





Inoltre abbiamo notato l'alto numero di richieste DNS.



Le 33 richieste DNS potrebbero essere dovute a diversi fattori:

1. Il sito caricato ha risorse esterne

- o Il sito visitato potrebbe caricare contenuti da più domini (es. immagini, script, pubblicità, tracker).
Esempio: Visitando un sito fasullo di Facebook, il sistema potrebbe risolvere DNS per facebook.com, ma anche per tracking-ads.com, malicious-script.net, ecc.

2. Redirezioni o caricamento di più pagine

- o Se il sito ha reindirizzamenti, ogni passaggio potrebbe generare nuove richieste DNS.
- o Una pagina di phishing può reindirizzare l'utente a più server per offuscare la truffa.

3. Tentativi di connessione con server sospetti

- o Alcuni malware o pagine malevole effettuano richieste DNS multiple per connettersi a server di comando e controllo (C2) o per esfiltrare dati.

Analizzando gli ip delle richieste DNS su VirusTotal, molti appaiono sospetti e malevoli.

This screenshot shows the VirusTotal report for the IP address 142.250.185.170. The interface includes a search bar at the top with the IP entered. On the left, a circular 'Community Score' widget shows a score of 1 out of 94. The main header area displays the IP, its range (142.250.0.0/15), and the AS (AS 15169 - GOOGLE). A red warning icon indicates that 1/94 security vendors flagged this IP as malicious. Below this, a 'Security vendors' analysis' table is partially visible, showing results from MalwareURL, Acronis, and others. The 'DETECTION' tab is selected, and a 'Join our Community' banner is present.

This screenshot shows the VirusTotal report for the IP address 142.250.186.42. Similar to the first report, it shows a 'Community Score' of 3 out of 94. The header indicates that 3/94 security vendors flagged this IP as malicious. The 'Security vendors' analysis' table shows more results, including 'Antly-AVL' (Malicious), 'MalwareURL' (Malware), 'Abusix' (Clean), 'Criminal IP' (Malicious), 'Gridinsoft' (Suspicious), and 'Acronis' (Clean). The 'DETECTION' tab is selected, and a 'Join our Community' banner is present.

DNS requests		
Domain	IP	Reputation
content-autofill.googleapis.com	142.250.186.138	whitelisted
	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	

fe3cr.delivery.mp.microsoft.com	52.165.164.15
static.xx.fbcdn.net	157.240.0.6
facebook.com	157.240.0.35

157.240.0.35

2 / 94
Community Score

2/94 security vendors flagged this IP address as malicious

157.240.0.35 (157.240.0.0/17)
AS 32934 (FACEBOOK)

DE

DETECTION DETAILS RELATIONS COMMUNITY 10+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

MalwareURL Malware SOCRadar Malicious

157.240.0.6

1 / 94
Community Score

1/94 security vendor flagged this IP address as malicious

157.240.0.6 (157.240.0.0/17)
AS 32934 (FACEBOOK)

DETECTION DETAILS RELATIONS COMMUNITY 10+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

SOCRadar Malicious

facebook.com	157.240.0.35
--------------	--------------

Abbiamo perciò ipotizzato che il risultato fosse un falso positivo in quanto Anyrun non mostra sezioni sospette ma facendo un'analisi più approfondita abbiamo riscontrato che fosse malevolo.

Mitigazione:

Le email di phishing possono essere pericolose, ma si possono adottare diverse strategie per mitigarne il rischio e proteggere i dati.

1. Educazione e Consapevolezza

- Verificare l'URL prima di cliccare: passare il mouse sopra i link per vedere l'URL reale prima di cliccare.
- Controllare l'indirizzo del mittente: se l'email proviene da un dominio strano (es. "support- facebook.com" invece di "facebook.com"), potrebbe essere un tentativo di phishing.
- Fare attenzione agli errori grammaticali: le email di phishing spesso contengono errori ortografici o di formattazione.

2. Strumenti di Sicurezza

- Usare un filtro antispam
- Abilitare l'autenticazione a due fattori (2FA)
- Aggiornare regolarmente browser e software di sicurezza
- Usare un password manager

3. Mitigazione Tecnica per Aziende

- Implementare SPF, DKIM e DMARC: questi protocolli aiutano a prevenire lo spoofing delle email.
- Bloccare gli URL sospetti a livello di rete: i firewall e i proxy web aziendali possono filtrare i siti dannosi.
- Formazione periodica per i dipendenti: organizza simulazioni di phishing per educare il personale a riconoscere le minacce.

4. Cosa Fare in Caso di Phishing

- Non inserire mai le credenziali in siti sospetti.
- Segnalare il phishing a Facebook o al servizio interessato.
- Se si ha inserito la password, cambiarla immediatamente e controllare eventuali accessi non autorizzati.
- Eseguire una scansione antivirus nel caso siano stati scaricati file sospetti.