



...

Analisi del file sospetto

66bddfcb52736_vidar.exe

Cos'è una minaccia Vidar?

- Tipo di malware: Infostealer (ruba informazioni).

Obiettivi:

- Sottrarre credenziali, dati finanziari e file sensibili.
- Comunicare con server remoti controllati dagli attaccanti.
- Tecniche usate:
- Mascheramento tramite processi legittimi (es. RegAsm.exe).
- Connessioni a server esterni per esfiltrazione dati.





Comportamento osservato

Esecuzione iniziale:

- Il file avvia processi legittimi (es. RegAsm.exe, cmd.exe, svchost.exe).
- Utilizza file con nomi casuali (es. HCAEHJJKFC.exe).
- Accesso a directory e file:
- Scrive in percorsi di sistema come C:\ProgramData.
- File generati: mozglue.dll, nss3.dll.
- Connessioni di rete:
- Tenta di comunicare con domini remoti:
 - condedqpwqm.shop
 - traineiwnqo.shop

Catena di processi malevoli

6780	66bddfcb52736_vidar.exe			348	90	38
6864	RegAsm.exe			1	0	3
6872	RegAsm.exe			0	0	3
6884	RegAsm.exe			0	0	3
6896	RegAsm.exe			0	0	3
6908	RegAsm.exe	CFG	DMP			
				vidar	18k	6k 111
1568	HCAEHJJKFC.exe	PE				
					266	83 38
2572	conhost.exe	0xffffffff -ForceV1			70	101 25
4704	RegAsm.exe	CFG	DMP			
				lumma	4k	546 75
6248	CAFHDBGHJK.exe	PE				
					264	83 37
1292	conhost.exe	0xffffffff -ForceV1			69	101 25
6340	RegAsm.exe	CFG	DMP			
				vidar	4k	30 34
6284	cmd.exe	/c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit			214	50 15
6240	conhost.exe	0xffffffff -ForceV1			72	101 25
6372	timeout.exe	/t 10			80	32 21
2256	svchost.exe	-k NetworkService -p -s Dnscache			0	38 43

Indicatori di Compromissione (IoC)

Cos'è un Indicatore di Compromissione (IoC)?

Gli IoC sono segnali che aiutano a identificare se un sistema è stato compromesso. In questo caso, gli IoC includono file, processi, hash, e connessioni sospette legate al file analizzato



Hash del file sospetto

Un hash è una "impronta digitale" del file, che lo identifica in modo univoco. Può essere usato per confrontarlo con database di malware conosciuti.

SHA256:325396D5FFCA8546730B9A56C2D0ED9923
8D48B5E1C3C49E7D027505EA13B8D1.

Perché è importante?

Questo hash consente di riconoscere il file su altri sistemi e segnalarlo come pericoloso.



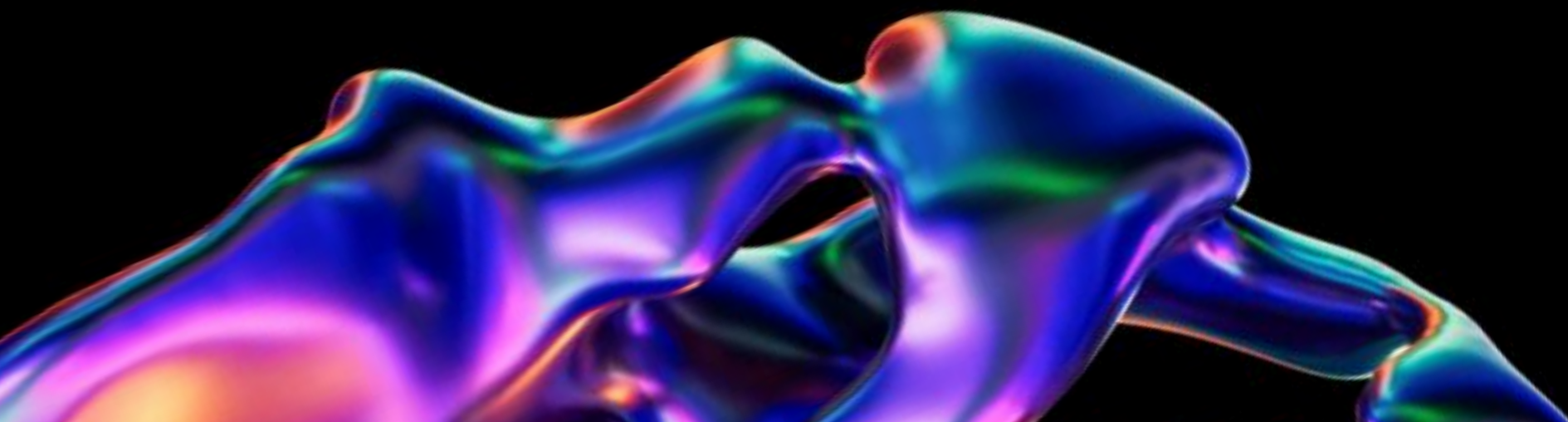
File e processi generati dal malwa

Il malware crea file e processi durante la sua esecuzione per compiere attività sospette o dannose.

File generati:

- HCAEHJJKFC.exe
- CAFHDBGHJK.exe
- Librerie DLL:
- mozglue.dll
- nss3.dll
- softokn3.dll

Sono file chiave per identificare e rimuovere l'infezione



Connessioni di rete

Il malware tenta di comunicare con server di comando e controllo (C2) per esfiltrare dati o ricevere istruzioni.

Domini sospetti rilevati:

- condedqpwqm.shop
- traineiwnqo.shop
- caffegclasiqwp.shop
- millyscroqwp.shop
-

Questi domini non sono legittimi e devono essere bloccati immediatamente nel firewall aziendale per prevenire comunicazioni con gli hacker.



Comportamenti osservati nei processi

Il malware sfrutta processi legittimi di Windows per mascherare le sue attività:

Processi coinvolti:

- RegAsm.exe → Utilizzato per eseguire comandi malevoli.
- cmd.exe, timeout.exe, svchost.exe → Usati per nascondere l'attività del malware

Questi processi non sono malevoli di per sé, ma il loro utilizzo anomalo è un segnale chiave di compromissione.



File e processi generati dal malwa

Il malware crea file e processi durante la sua esecuzione per compiere attività sospette o dannose.

File generati:

- HCAEHJJKFC.exe
- CAFHDBGHJK.exe
- Librerie DLL:
- mozglue.dll
- nss3.dll
- softokn3.dll

Sono file chiave per identificare e rimuovere l'infezione



Rischi per l'organizzazione

- Furto di dati sensibili: Credenziali, documenti e dati finanziari.
- Esfiltrazione verso domini non affidabili.
- Potenziale accesso ad altri sistemi aziendali.

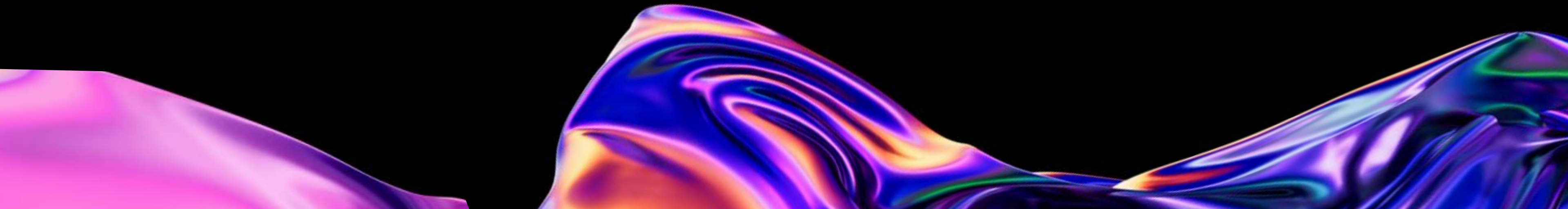


Rischi per l'organizzazione

- Mettere in quarantena: Isolare immediatamente il file e i processi associati.
- Bloccare domini sospetti come:
 - `condedqpwm.shop`, `traineiwnqo.shop`.
- Eseguire una scansione completa: Analizzare tutti i dispositivi aziendali.
- Rimuovere i file malevoli: Eliminare file come `mozglue.dll`, `HCAEHJJKFC.exe`.
- Cambiare le credenziali: Reimpostare password salvate nei browser

STAY SAFE

Il file è un vero positivo e rappresenta una minaccia concreta.
Le azioni di remediation suggerite aiuteranno a contenere il rischio.
Controllare la rete per identificare eventuali altre infezioni.





Chrome.exe: Minaccia o falso positivo?

Cos'è il file Chrome.exe?



Si tratta di un file eseguibile che avvia il browser Google Chrome, uno strumento di navigazione web ampiamente utilizzato.

L'hash di questo file è:

- 6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC.
- Questo ci permette di confrontarlo con database di malware conosciuti per verificare se sia pericoloso.

Scrittura e accesso a file

- Il file ha scritto e modificato dati nella cartella locale di Google Chrome:
- Percorso: C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default.
- Questa cartella è utilizzata dal browser per memorizzare informazioni come preferenze, cronologia e cache. È un comportamento normale per un browser.
- Esempi di file scritti:
- File temporanei (.tmp):
- Questi file vengono creati per conservare dati momentanei, come informazioni su una pagina web che si sta caricando.
- LOG.old:
- È un file di registro usato per tenere traccia delle attività del browser (es. accesso ai siti).
- Preferences:
- È un file che memorizza le preferenze dell'utente, come le impostazioni di navigazione.

Connessioni di rete

Il file ha stabilito connessioni con i seguenti indirizzi:

- accounts.google.com (IP: 66.102.1.84):
- Usato per autenticare gli accessi e sincronizzare dati.

6840	chrome.exe	66.102.1.84:443	accounts.google.com	GOOGLE
------	------------	-----------------	---------------------	--------

- www.instagram.com (IP: 157.240.0.174):
- Caricamento del sito web Instagram.

6840	chrome.exe	157.240.0.174:443	www.instagram.com	FACEBOOK
------	------------	-------------------	-------------------	----------

- www.facebook.com (IP: 157.240.0.35):
- Caricamento del sito web facebook.

6840	chrome.exe	157.240.0.35:443	www.facebook.com	FACEBOOK
------	------------	------------------	------------------	----------

- click.convertkit-mail2.com (IP: 3.141.222.179):
- Dominio associato a servizi di tracciamento email,
- non malevolo ma da monitorare.

6840	chrome.exe	3.141.222.179:443	click.convertkit-mail2.com	AMAZON-02
------	------------	-------------------	----------------------------	-----------



Cosa significa?

Google, Instagram e facebook: Questi sono domini legittimi e tipici per un browser come Chrome.

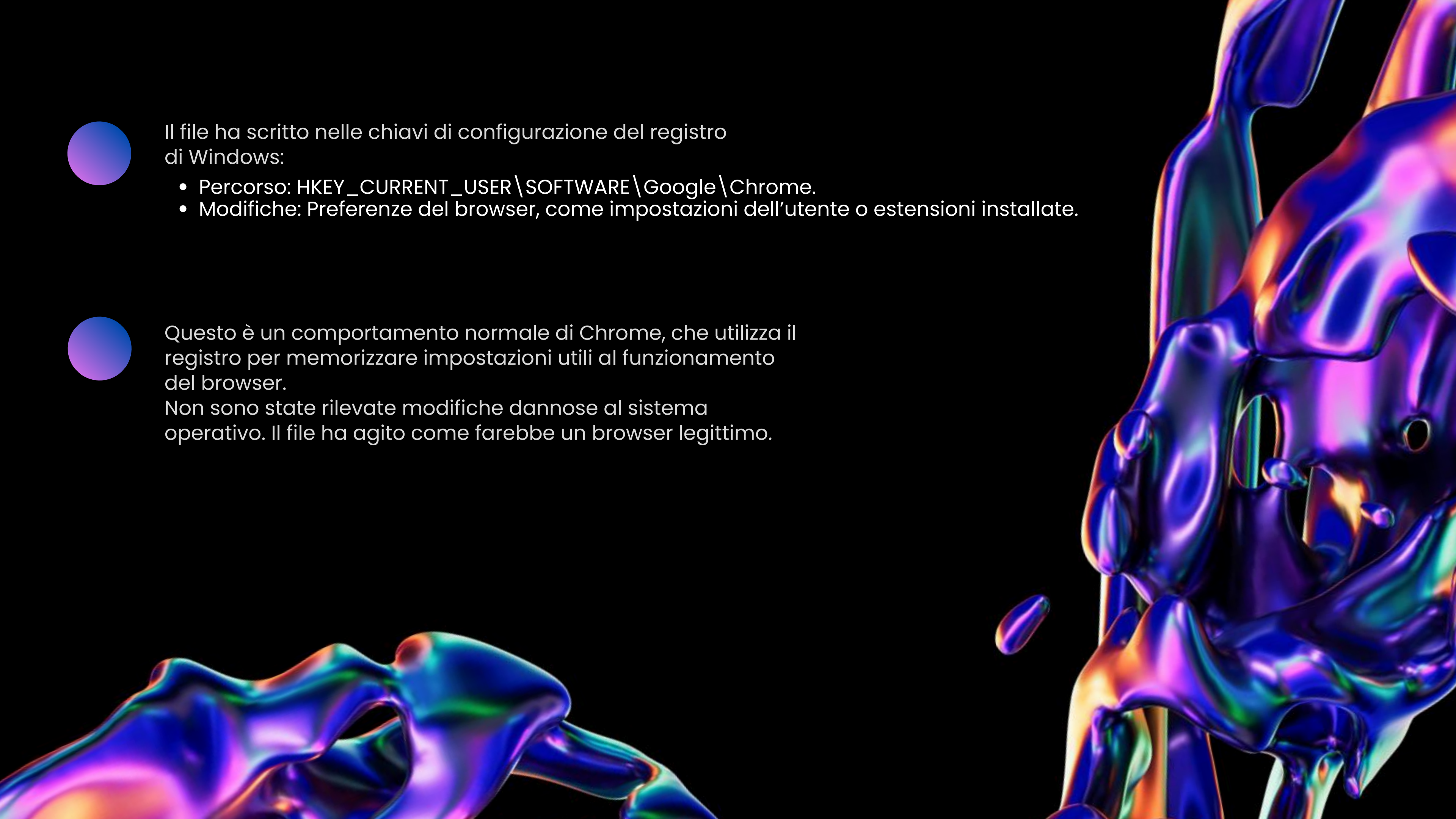
ConvertKit

Potrebbe essere utilizzato per monitorare link cliccati in email o campagne di marketing. Anche se non è direttamente pericoloso, merita attenzione.

- ConvertKit è una piattaforma legittima usata per campagne email e tracciamento dei clic, ma i suoi link possono essere sfruttati per scopi fraudolenti, come phishing o distribuzione di malware.

Potenziiali abusi:

- Anche se il dominio `click.convertkit-mail2.com` è sicuro, attori malevoli potrebbero utilizzarlo per mascherare link dannosi.



Il file ha scritto nelle chiavi di configurazione del registro di Windows:

- Percorso: HKEY_CURRENT_USER\SOFTWARE\Google\Chrome.
- Modifiche: Preferenze del browser, come impostazioni dell'utente o estensioni installate.

Questo è un comportamento normale di Chrome, che utilizza il registro per memorizzare impostazioni utili al funzionamento del browser.

Non sono state rilevate modifiche dannose al sistema operativo. Il file ha agito come farebbe un browser legittimo.



Remediation e Conclusione

Classificazione del file:

Questo è un falso positivo. Non sono richieste azioni correttive immediate.

Monitoraggio:

- Anche se non ci sono rischi evidenti, è consigliabile tenere sotto controllo eventuali attività future legate al dominio `click.convertkit-mail2.com`, che potrebbe essere utilizzato per scopi di tracciamento.

Nessuna quarantena necessaria:

- Non è richiesto isolare o eliminare il file.

Comunicazione chiara:

- Informare gli utenti che il file è sicuro e che non ci sono rischi per i sistemi aziendali.



Esito dell'analisi:

Il file "Chrome.exe" non è una minaccia.

- Azioni richieste: Nessuna azione necessaria oltre al monitoraggio del dominio ConvertKit.
- Raccomandazioni: Assicurarsi che i sistemi di sicurezza siano aggiornati per evitare falsi positivi futuri.

