



Analisi del file sospetto

66bddfcb52736_vidar.exe

Cos'è una minaccia Vidar e Lumma?

- 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 estrarre i dati.



Catena di processi malevoli





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.
- Connessioni di rete:
- Tenta di comunicare con domini remoti esempio:
 - condedqpwqm.shop
 - traineiwnqo.shop

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.



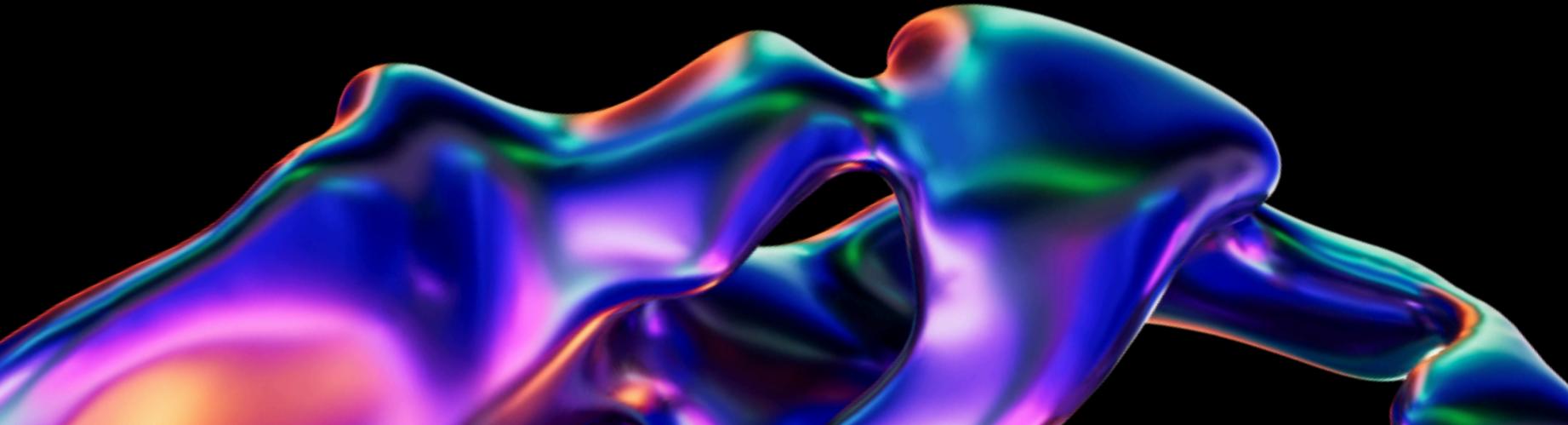
File e processi generati dal malware

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

File generati come:

- HCAEHJJKFC.exe
- CAFHDBGHJK.exe

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:

- condedqpwm.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, timeout, svchost → 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.



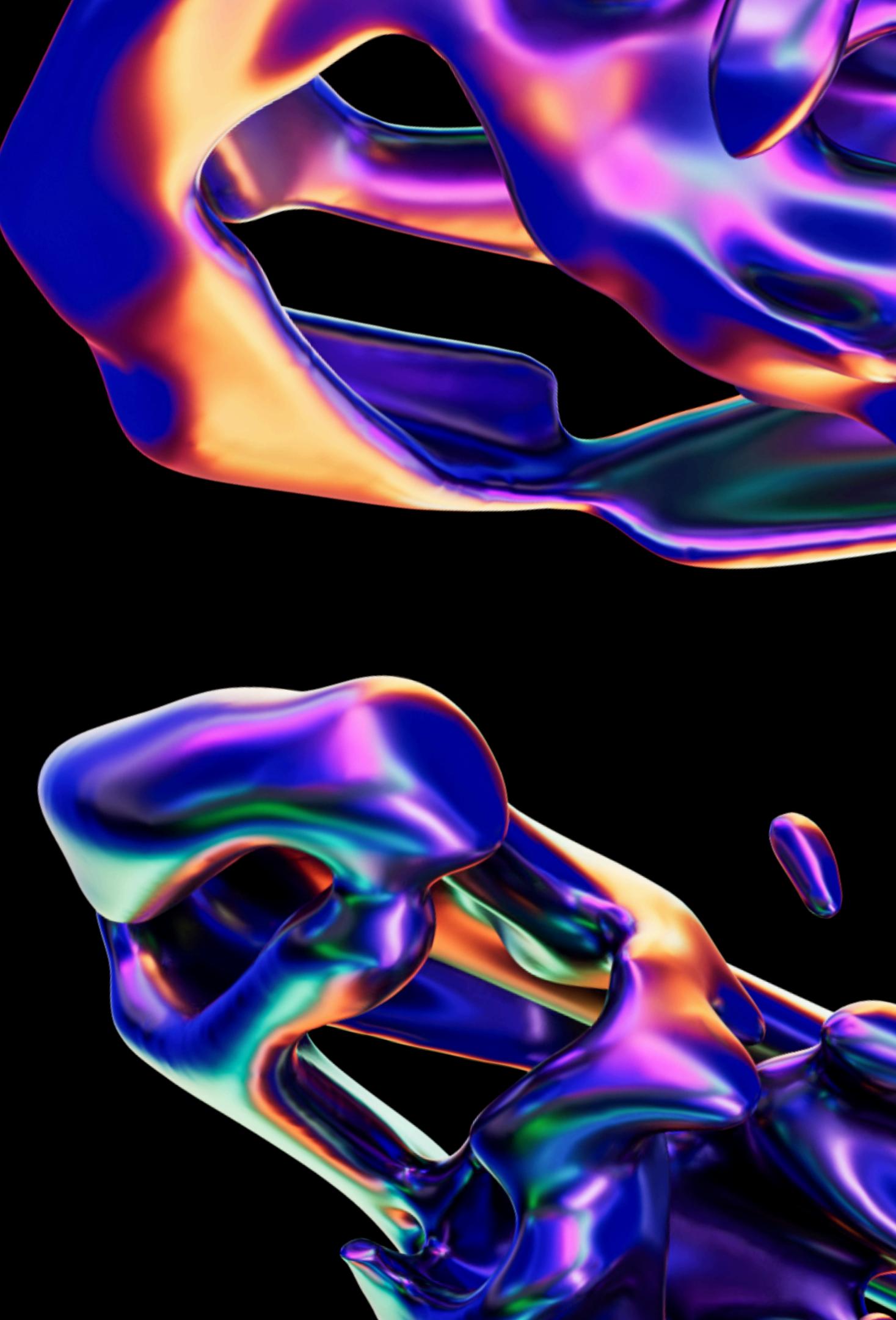
Rischi per l'organizzazione

- 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 , HCAEHJJJKFC.exe.
- Cambiare le credenziali: Reimpostare password salvate nei browser



Comportamenti del browser

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 utente che usa Chrome.

ConvertKit

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

- i suoi link possono essere sfruttati per scopi fraudolenti, come phishing o distribuzione di malware.

Potenziali abusi:

- Anche se il dominio click.convertkit-mail2.com è sicuro, i malintenzionati potrebbero utilizzarlo per mascherare link dannosi.



Remediation e Conclusioni

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:

- 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.