Build Week 3 - ES 5 - PARTE 1
Analisi Malware: Vidar/Lumma Stealer

Executive Summary

L’analisi dinamica del campione sospetto ha evidenziato un’infezione multi-stadio riconducibile alle famiglie di infostealer Vidar e Lumma Stealer. Il file iniziale agisce come *loader*, sfruttando tecniche di process injection su un processo legittimo di Windows (RegAsm.exe) per eludere i controlli di sicurezza (Living off the Land).

Una volta stabilita l’esecuzione occulta, il malware scarica payload secondari da server remoti, instaura comunicazioni cifrate su HTTPS verso infrastrutture di Command & Control (C2) e avvia attività di raccolta ed esfiltrazione di credenziali (browser, FTP, wallet crypto).

Sono state osservate tecniche avanzate di evasione, tra cui:

- Uso di CDN (Cloudflare) per mascherare l’infrastruttura C2
- Domini Dynamic DNS come fallback
- Creazione massiva di file temporanei per ritardare l’analisi sandbox
- Decrittazione locale dei database browser tramite librerie Mozilla droppate sul sistema

Gli Indicatori di Compromissione (IoC) estratti includono indirizzi IP, domini, hash file e artefatti locali, utili per il rafforzamento delle difese perimetrali ed endpoint.

1. Introduzione

In questa sessione di laboratorio, ho condotto un'analisi su un campione eseguibile sospetto al fine di comprenderne il comportamento, identificare le tecniche di evasione e mappare gli Indicatori di Compromissione (IOC). L'obiettivo di questa relazione è documentare passo dopo passo l'esecuzione del malware e le sue interazioni con il sistema operativo e la rete, argomentando le motivazioni tecniche alla base delle azioni rilevate.

2. Strumenti Utilizzati

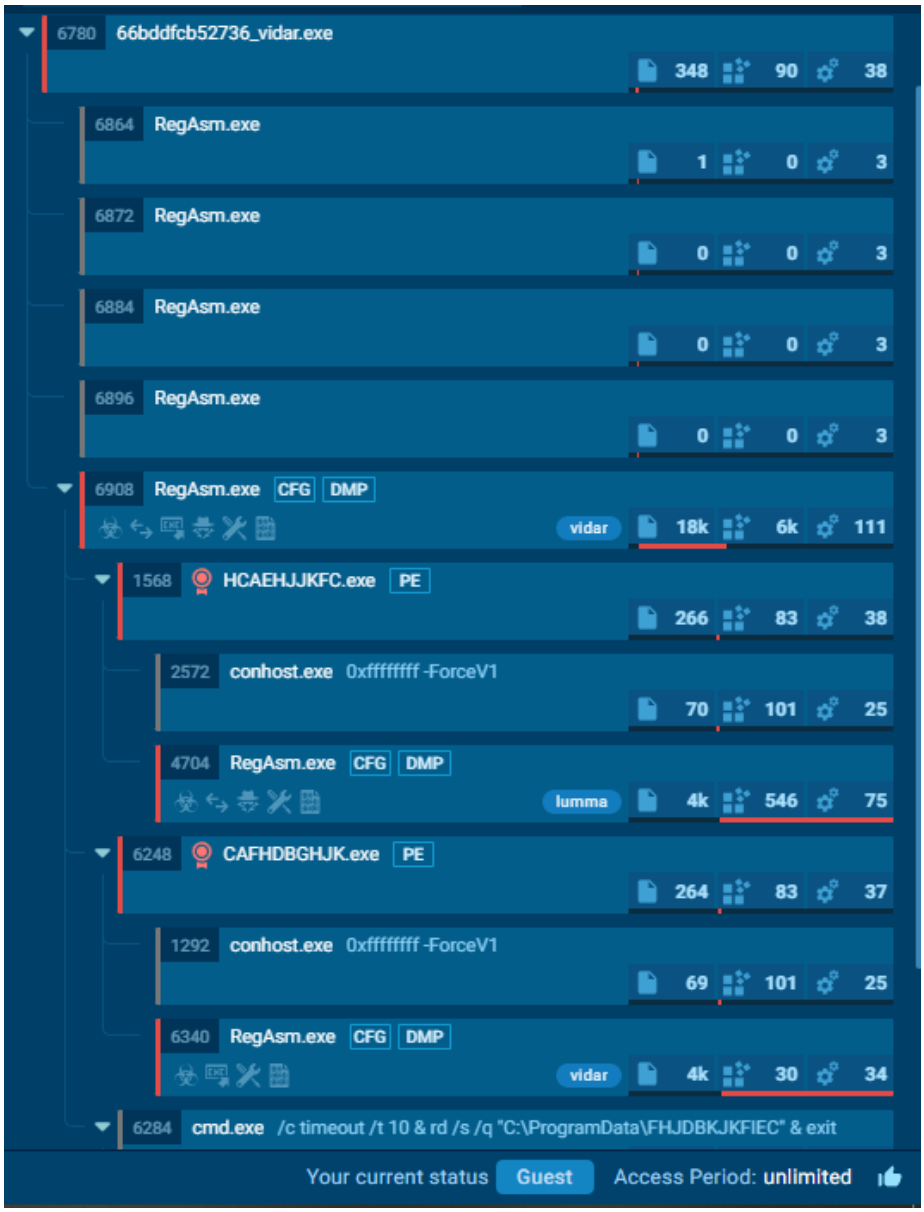
Per garantire l'isolamento e la sicurezza durante l'analisi, tutte le operazioni sono state condotte in un ambiente Sandbox. Nello specifico, ho impiegato:

- **ANY.RUN (Interactive Malware Sandbox):** Utilizzato per l'analisi dinamica del campione in un ambiente Windows 10 a 64-bit controllato, che mi ha permesso di monitorare processi, traffico di rete e modifiche al registro in tempo reale.

3. Analisi

Fase 1: Esecuzione iniziale e analisi dei processi

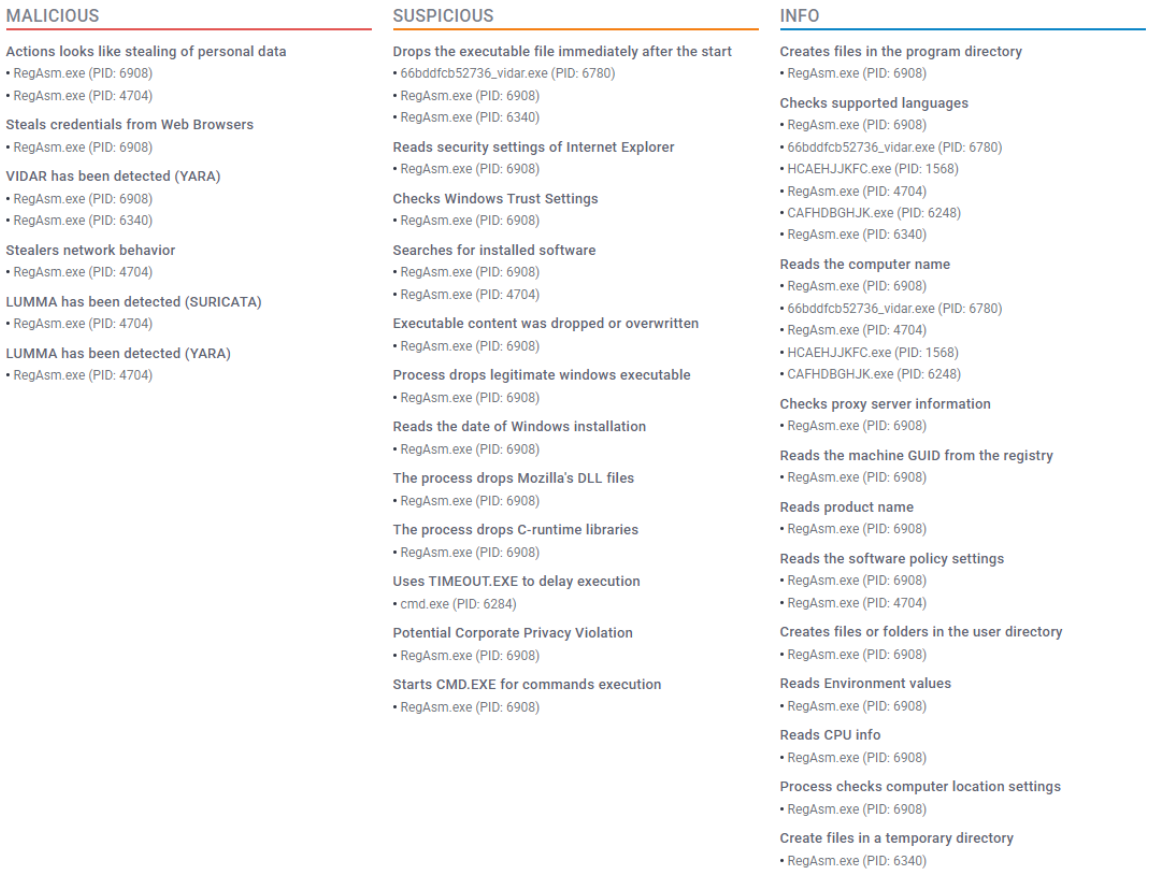
Ho iniziato l'analisi del file sospetto nominato 66bddfcb52736_vidar.exe all'interno della sandbox.



Osservando il pannello laterale destro (l'albero dei processi), ho notato immediatamente un comportamento anomalo. Dopo l'avvio del processo principale (PID 6780), il malware ha avviato istanze multiple di RegAsm.exe (es. PID 6864, PID 6872, PID 6908).

RegAsm.exe (Assembly Registration Tool) è un'utility legittima del framework .NET di Microsoft. Il fatto che il malware lo stia richiamando ripetutamente è un chiaro indicatore di una tecnica nota come **"Process Hollowing"** o in generale di tecniche Living off the Land (LotL). Il malware avvia un processo legittimo in stato di sospensione, svuota la sua memoria e vi inietta il proprio codice maligno (payload). In questo modo, il codice malevolo viene eseguito sotto le spoglie di un processo fidato di Windows, nel tentativo di eludere i controlli degli antivirus (EDR/AV).

Il sistema di analisi ha infatti taggato questa attività associandola a noti "stealer" (Lumma, Vidar), confermando l'intento malevolo.



MALICIOUS

Actions looks like stealing of personal data
• RegAsm.exe (PID: 6908)
• RegAsm.exe (PID: 4704)

Steals credentials from Web Browsers
• RegAsm.exe (PID: 6908)

VIDAR has been detected (YARA)
• RegAsm.exe (PID: 6908)
• RegAsm.exe (PID: 6340)

Stealers network behavior
• RegAsm.exe (PID: 4704)

LUMMA has been detected (SURICATA)
• RegAsm.exe (PID: 4704)

LUMMA has been detected (YARA)
• RegAsm.exe (PID: 4704)

SUSPICIOUS

Drops the executable file immediately after the start
• 66bddfcb52736_vidar.exe (PID: 6780)
• RegAsm.exe (PID: 6908)
• RegAsm.exe (PID: 6340)

Reads security settings of Internet Explorer
• RegAsm.exe (PID: 6908)

Checks Windows Trust Settings
• RegAsm.exe (PID: 6908)

Searches for installed software
• RegAsm.exe (PID: 6908)
• RegAsm.exe (PID: 4704)

Executable content was dropped or overwritten
• RegAsm.exe (PID: 6908)

Process drops legitimate windows executable
• RegAsm.exe (PID: 6908)

Reads the date of Windows installation
• RegAsm.exe (PID: 6908)

The process drops Mozilla's DLL files
• RegAsm.exe (PID: 6908)

The process drops C-runtime libraries
• RegAsm.exe (PID: 6908)

Uses TIMEOUT.EXE to delay execution
• cmd.exe (PID: 6284)

Potential Corporate Privacy Violation
• RegAsm.exe (PID: 6908)

Starts CMD.EXE for commands execution
• RegAsm.exe (PID: 6908)

INFO

Creates files in the program directory
• RegAsm.exe (PID: 6908)

Checks supported languages
• RegAsm.exe (PID: 6908)
• 66bddfcb52736_vidar.exe (PID: 6780)
• HCAEHJJKFC.exe (PID: 1568)
• RegAsm.exe (PID: 4704)
• CAFHDBGHJK.exe (PID: 6248)
• RegAsm.exe (PID: 6340)

Reads the computer name
• RegAsm.exe (PID: 6908)
• 66bddfcb52736_vidar.exe (PID: 6780)
• RegAsm.exe (PID: 4704)
• HCAEHJJKFC.exe (PID: 1568)
• CAFHDBGHJK.exe (PID: 6248)

Checks proxy server information
• RegAsm.exe (PID: 6908)

Reads the machine GUID from the registry
• RegAsm.exe (PID: 6908)

Reads product name
• RegAsm.exe (PID: 6908)

Reads the software policy settings
• RegAsm.exe (PID: 6908)
• RegAsm.exe (PID: 4704)

Creates files or folders in the user directory
• RegAsm.exe (PID: 6908)

Reads Environment values
• RegAsm.exe (PID: 6908)

Reads CPU info
• RegAsm.exe (PID: 6908)

Process checks computer location settings
• RegAsm.exe (PID: 6908)

Create files in a temporary directory
• RegAsm.exe (PID: 6340)

Approfondimento: Analisi del comportamento del Trojan (Text Report)

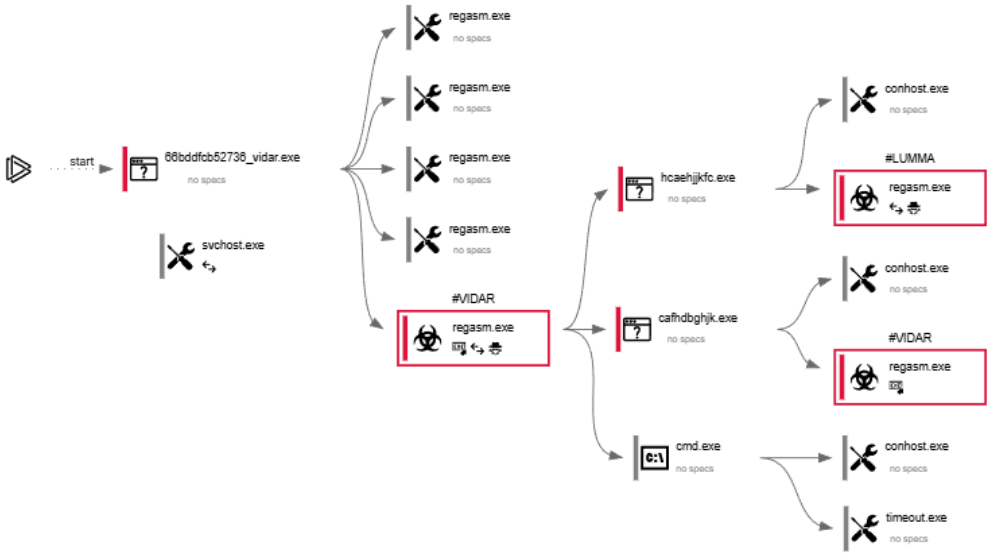
Prima di analizzare il traffico di rete, ho consultato il report testuale dettagliato (Text Report) per comprendere a fondo la natura della minaccia che stavo affrontando.

Dall'analisi del report emerge chiaramente che non ci troviamo di fronte a una singola minaccia lineare, ma a un attacco multi-stadio complessa. Il file iniziale agisce principalmente come **Loader**, il cui scopo è preparare il terreno e scaricare payload secondari altamente specializzati. Le firme YARA e le regole Suricata hanno classificato l'infezione associandola a due note famiglie di malware: **Vidar** e **Lumma Stealer**.

In base alle attività registrate a livello di sistema operativo, il comportamento primario del Trojan si divide nelle seguenti macro-attività:

1. **Furto di Credenziali (Information Stealing):** Il malware mira attivamente ai dati sensibili salvati in locale. Ricerca e tenta di estrarre:
    a. Credenziali salvate nei browser web (es. password di login, cookie di sessione, cronologia).
    b. File di configurazione e password di client FTP (come FileZilla).
    c. Portafogli di criptovalute (Cryptocurrency Wallets), scansionando directory specifiche alla ricerca dei file wallet.dat.
2. **Raccolta di Informazioni sul Sistema (Fingerprinting):** Prima di esfiltrare i dati, il Trojan raccoglie dettagli sull'ambiente in cui viene eseguito (nome del computer, versione dell'OS, software installati) per identificare le vittime di maggior valore e, possibilmente, per capire se si trova all'interno di un ambiente di analisi (tecnica anti-VM).
3. **Modifica del Sistema (Persistency/Defense Evasion):** Il report evidenzia che il malware ha droppato e avviato ulteriori file eseguibili con nomi offuscati (es. HCAHLLHKFC.exe e CAFHD0GHUK.exe), associati specificamente al modulo Lumma Stealer. Questo indica la volontà di ramificare l'infezione e stabilire un controllo più profondo sulla macchina compromessa.

Successivamente ho analizzato il grafico fornito da anyrun:



Il processo iniziale 66bddfcb52736_vidar.exe genera contemporaneamente ben quattro istanze di RegAsm.exe (strumento legittimo di Windows).

1. **Primo stadio (VIDAR):** Una di queste istanze di RegAsm.exe viene esplicitamente etichettata dal motore di analisi come #VIDAR, presentando icone che indicano traffico di rete malevolo. Questo dimostra l'uso di una tecnica di **Process Injection**: il malware ha iniettato il suo codice malevolo in un processo legittimo per nascondersi (LOLBin abuse). Questo specifico processo funge da perno centrale dell'infezione.

2. **Tecniche di Evasione:** Dal processo #VIDAR principale viene lanciato cmd.exe, il quale a sua volta esegue timeout.exe. Come argomentato in precedenza, questa è una tecnica di "sleep" mirata a ritardare l'esecuzione per eludere le sandbox automatizzate, sperando che il tempo di analisi scada prima che vengano eseguite le azioni critiche.

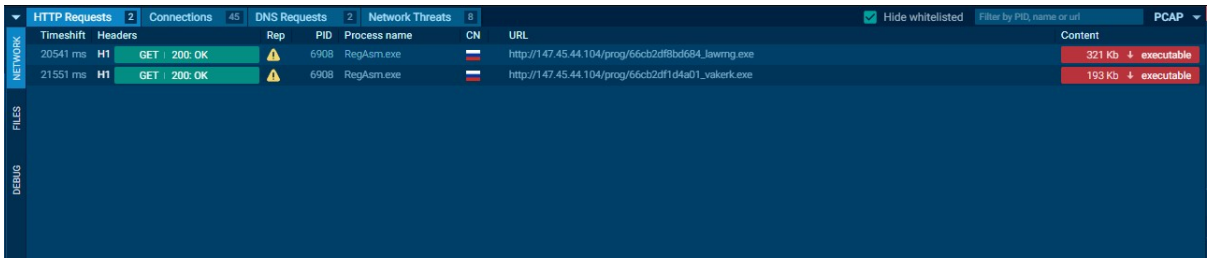
3. **Secondo stadio (Drop e Multi-Family):** L'aspetto più interessante è che il processo #VIDAR agisce anche da "Dropper". Genera due nuovi eseguibili dai nomi palesemente casuali e quindi sospetti: hcaehjjkfc.exe e cafhdbghjk.exe.

4. **Terzo stadio (LUMMA e furto dati):** Questi due nuovi eseguibili ripetono la tecnica di iniezione, lanciando ulteriori istanze di RegAsm.exe. Una viene etichettata come #LUMMA (con attività di rete) e l'altra nuovamente come #VIDAR (con un'icona esplicita indicante il furto di dati/credenziali).

Questo mi porta a concludere che ci troviamo di fronte a un'infezione complessa che scarica o estrae payload secondari, coinvolgendo potenzialmente due diverse famiglie di Infostealer (Vidar e Lumma) per massimizzare la probabilità di successo nell'esfiltrazione dei dati.

Fase 2: Analisi del Traffico di Rete (Network Activity)

A questo punto, avendo compreso che l'obiettivo del malware è rubare dati e scaricare ulteriori moduli, ho focalizzato la mia attenzione sul pannello inferiore relativo alle richieste HTTP.



Come visibile, i processi RegAsm.exe infetti hanno generato traffico di rete verso indirizzi IP esterni. In particolare, ho evidenziato due connessioni HTTP (porta 80) di tipo GET verso l'indirizzo IP 147.45.44.104. Le richieste puntano a risorse specifiche per scaricare i payload menzionati in precedenza:

- http://147.45.44.104/prog/66cb2df8bd684_lawmg.exe (scaricati 321 KB)
- http://147.45.44.104/prog/66cb2df1d4a01_vakerk.exe (scaricati 193 KB)

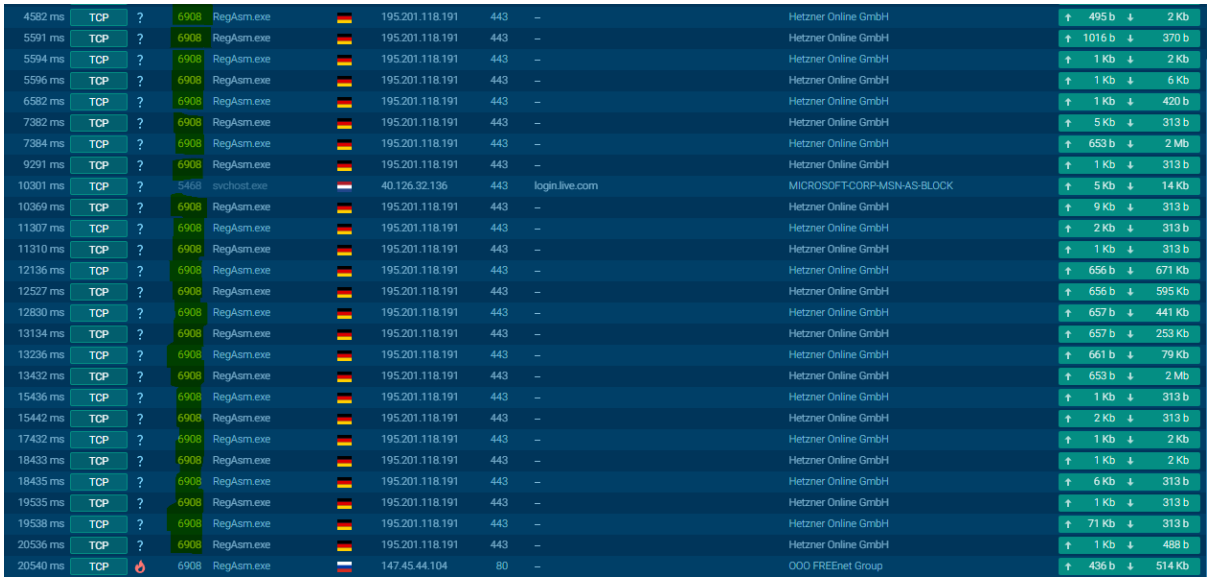
Questa è la fase operativa del Loader. Avendo stabilito un punto di appoggio nel sistema iniettandosi in RegAsm.exe, il malware contatta il server di Comando e Controllo (C2) per recuperare le armi vere e proprie dell'attacco (probabilmente i moduli stealer Lumma/Vidar veri e propri). La comunicazione avviene in chiaro su protocollo HTTP, facilitando la nostra analisi ma evidenziando come l'infrastruttura dell'attaccante sia attiva e pronta a distribuire payload aggiuntivi.

Fase 3: Analisi delle Connessioni TCP, Identificazione C2 ed Esfiltrazione

Per completare l'analisi di rete ed estrapolare gli Indicatori di Compromissione (IoC) definitivi, ho esaminato la tabella delle connessioni TCP globali generate durante l'esecuzione in sandbox.

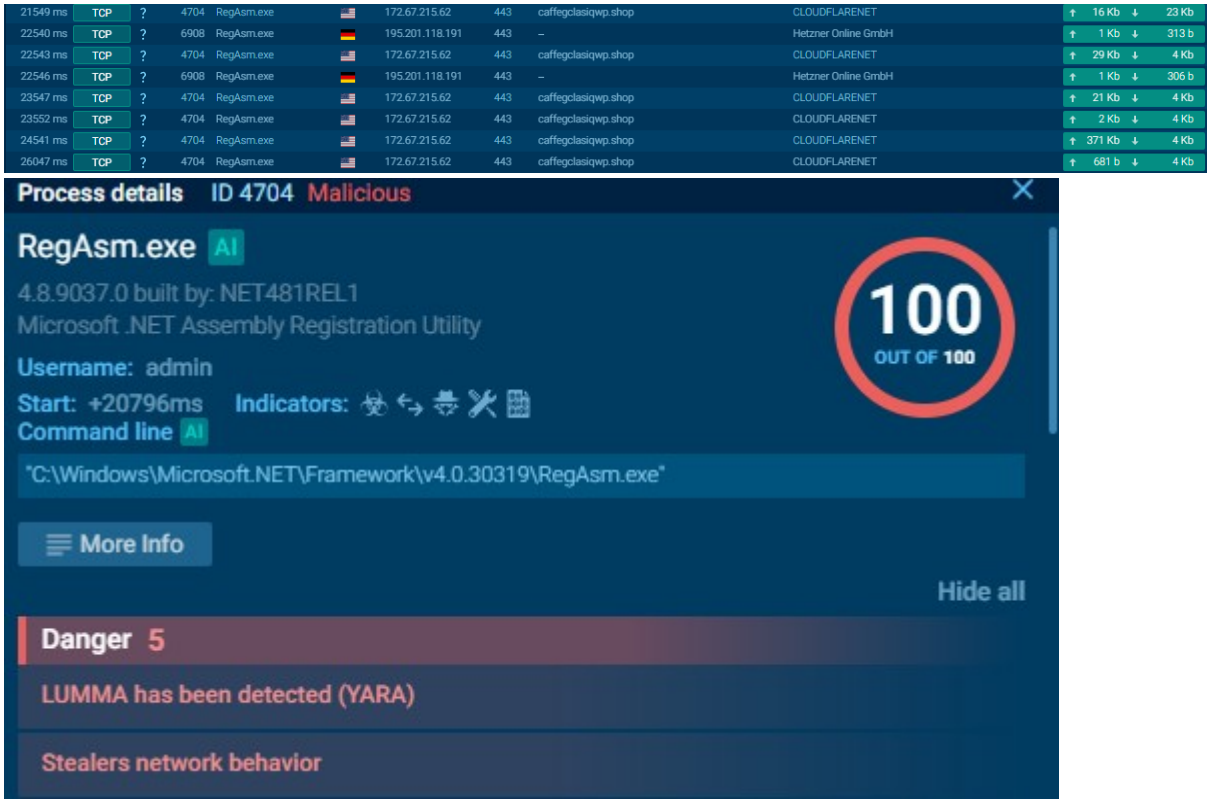
L'analisi del traffico di rete rivela una chiara distinzione tra le connessioni legittime del sistema operativo come le chiamate di svchost.exe o SIHClient.exe verso i domini Microsoft per la telemetria e le comunicazioni malevole orchestrate dalle istanze iniettate di RegAsm.exe. Nello specifico, ho isolato tre flussi di traffico critici:

1. **Conferma del Server di Staging (Porta 80):** Il processo con PID 6908 (identificato come #VIDAR) ha effettuato una connessione in chiaro (porta 80) verso l'IP russo 147.45.44.104 (ASN: OOO FREEnet Group). Come analizzato al punto 3 del grafico questa connessione è stata utilizzata come "Dropper" per scaricare i payload secondari. La piattaforma etichetta correttamente questa connessione con l'icona del fuoco (minaccia accertata).



4582 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 495 b	↓ 2 Kb
5591 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1016 b	↓ 370 b
5594 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 2 Kb
5596 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 6 Kb
6582 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 420 b
7382 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 5 Kb	↓ 313 b
7384 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 653 b	↓ 2 Mb
9291 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 313 b
10301 ms	TCP	?	5468	svchost.exe		40.126.32.136	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 5 Kb	↓ 14 Kb
10369 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 9 Kb	↓ 313 b
11307 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 2 Kb	↓ 313 b
11310 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 313 b
12136 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 656 b	↓ 671 Kb
12527 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 656 b	↓ 595 Kb
12830 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 657 b	↓ 441 Kb
13134 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 657 b	↓ 253 Kb
13236 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 661 b	↓ 79 Kb
13432 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 653 b	↓ 2 Mb
15436 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 313 b
15442 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 2 Kb	↓ 313 b
17432 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 2 Kb
18433 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 2 Kb
18435 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 6 Kb	↓ 313 b
19535 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 313 b
19538 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 71 Kb	↓ 313 b
20536 ms	TCP	?	6908	RegAsm.exe		195.201.118.191	443	–	Hetzner Online GmbH	↑ 1 Kb	↓ 488 b
20540 ms	TCP		6908	RegAsm.exe		147.45.44.104	80	–	OOO FREEnet Group	↑ 436 b	↓ 514 Kb

2. **Comunicazione C2 Primaria - VIDAR (Porta 443):** Lo stesso processo PID 6908 ha stabilito molteplici connessioni TCP criptate (porta 443) verso l'indirizzo IP 195.201.118.191, geolocalizzato in Germania e ospitato sui server di Hetzner Online GmbH (Hetzner è un'azienda tedesca assolutamente legittima e molto famosa nel mondo IT e il suo lavoro è affittare server). Questa persistenza di connessioni brevi e ravvicinate è tipica delle comunicazioni Command and Control (C2), utilizzate dal malware per segnalare il proprio stato di operatività o ricevere istruzioni. È estremamente anomalo e sospetto che un processo come RegAsm.exe (che non ha motivo di navigare su Internet in quel modo) invii continui pacchetti dati a un IP intestato a un provider commerciale di server a noleggio in Germania (Hetzner).



3. **Esfiltrazione Dati - Modulo LUMMA (Porta 443):**
   L'evidenza più critica dell'intera analisi emerge dallo studio del traffico generato dal processo con PID 4704, precedentemente identificato nel grafo di esecuzione come l'iniezione del payload secondario associato alla famiglia LUMMA Stealer. Come documentato nei log di rete, questo processo instaura comunicazioni HTTPS verso il dominio caffegclasiqwp.shop, risolto sull'IP 172.67.215.62. È importante sottolineare due aspetti tattici:

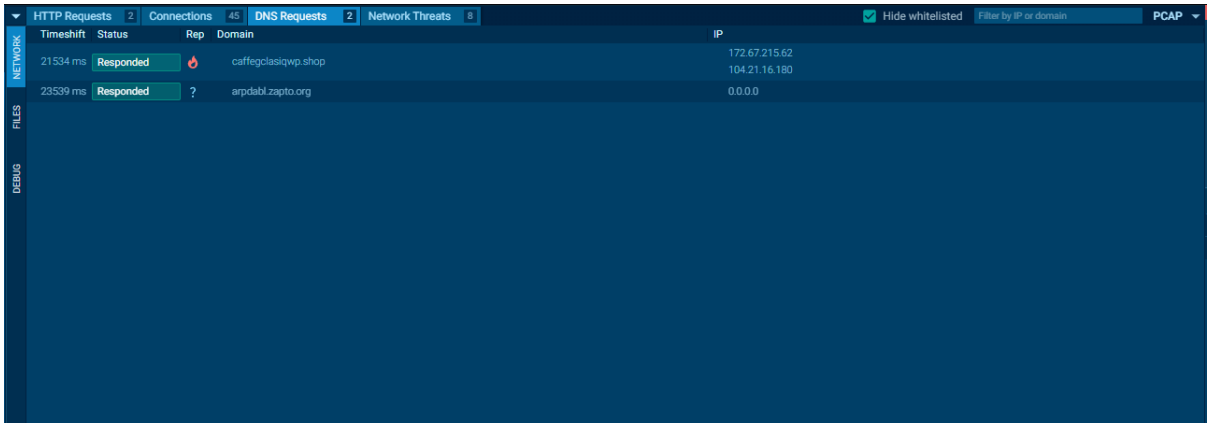
   a. **Uso tattico di CDN:** L'IP di destinazione appartiene all'ASN CLOUDFLARENET. L'attaccante sta abusando di questa rete di distribuzione dei contenuti (CDN) legittima per fungere da reverse proxy, celando il vero indirizzo IP del server C2 finale e complicando le operazioni di takedown dell'infrastruttura.

   b. **La prova dell'esfiltrazione:** Osservando il volume di traffico della connessione verso questo dominio, si nota un picco anomalo di 371 Kb di traffico in uscita (Upload) a fronte di soli 4 Kb in entrata. Questo volume di dati corrisponde esattamente al momento in cui l'Infostealer ha impacchettato le credenziali rubate dai

browser locali e le ha trasmesse (esfiltrate) al server remoto dell'attaccante.

Fase 4: Analisi delle Richieste DNS e Mappatura dell'Infrastruttura

Per avere un quadro completo delle comunicazioni esterne tentate dal malware prima dell'instaurazione delle connessioni TCP, ho esaminato i log di risoluzione DNS (Domain Name System).



L'analisi di questo pannello rivela due query DNS distinte, entrambe altamente indicative del comportamento di un bot o di un Infostealer:

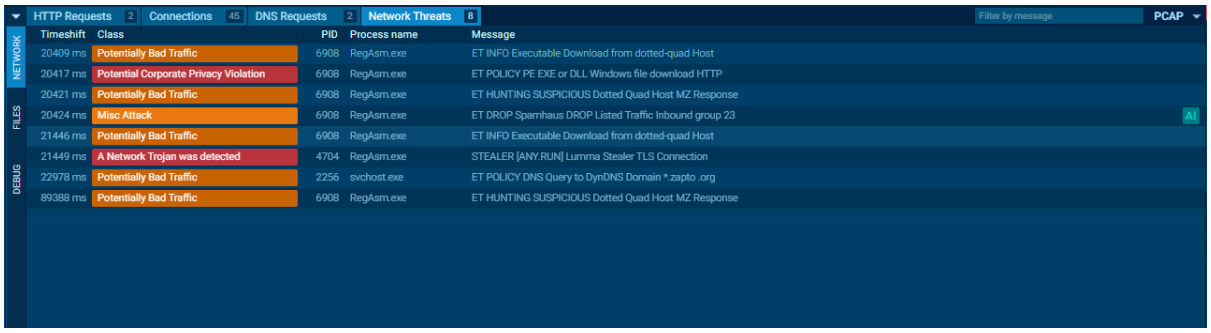
1. **La risoluzione del C2 Primario (LUMMA):** La prima richiesta, effettuata al millisecondo 21534, cerca di risolvere il dominio caffegclasiqwp.shop. Questo è il dominio che abbiamo precedentemente associato all'esfiltrazione dei dati. Il server DNS risponde fornendo due indirizzi IP: 172.67.215.62 e 104.21.16.180.
    a. Come accennato, questi IP appartengono alla rete Cloudflare. L'uso di un dominio.shop generato casualmente e mascherato dietro una CDN commerciale è un chiaro tentativo di blindare l'infrastruttura di Comando e Controllo contro le analisi e i blocchi degli analisti di sicurezza. La sandbox etichetta giustamente questa richiesta con un indicatore di minaccia rosso.
2. **Il Dominio di Fallback / Dinamico (DDNS):** La seconda richiesta DNS, effettuata al millisecondo 23539, cerca di risolvere un nuovo dominio: arpdabl.zapto.org.

a. Il dominio.zapto.org è un noto servizio di Dynamic DNS (DDNS) fornito da No-IP. Gli attaccanti abusano sistematicamente dei servizi DDNS perché permettono loro di registrare domini gratuitamente e di puntarli verso IP che cambiano continuamente, rendendo inefficaci i blocchi basati su singoli indirizzi IP.

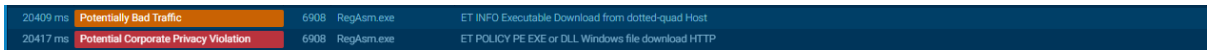
b. L'Anomalia (0.0.0.0): È interessante che la risposta a questa query DNS è 0.0.0.0. Questo significa che la risoluzione è fallita intenzionalmente. Le ragioni possono essere due: o il dominio è stato identificato come malevolo e disattivato (sinkholed) dal provider stesso, oppure il DNS della sandbox ha bloccato la richiesta. In ogni caso, questo dimostra che il malware possiede un meccanismo di fallback: cerca di contattare server C2 di riserva nel caso in cui le comunicazioni principali non vadano a buon fine.

Fase 5: Rilevamenti IDS e Firme del Traffico di Rete

Per validare formalmente le anomalie riscontrate durante l'analisi manuale delle connessioni e delle richieste HTTP/DNS, ho consultato i log dell'Intrusion Detection System (IDS) integrato nella piattaforma, esaminando la scheda "Network Threats".



L'output dell'IDS rafforza le deduzioni precedenti, innescando diverse regole di sicurezza (Emerging Threats) che categorizzano il comportamento del malware in tre filoni principali:



1. **Fase di Dropper/Staging (PID 6908):** Diverse allerte arancioni (Potentially Bad Traffic) colpiscono il processo RegAsm.exe primario. Le firme ET INFO Executable Download from dotted-quad Host e ET

POLICY PE EXE or DLL Windows file download HTTP identificano il download dei payload secondari. Nel gergo della sicurezza, un download HTTP diretto da un indirizzo IP nudo (ovvero 147.45.44.104) senza un dominio associato è un indicatore di compromissione classico, tipico degli script di staging dei malware. Viene inoltre segnalato che parte del traffico coinvolge un IP presente nelle liste di blocco globali (regola Spamhaus DROP).

2. **Fingerprinting Definitivo di LUMMA Stealer (PID 4704):** L'evidenza più schiacciante è l'allerta critica in rosso (A Network Trojan was detected). L'IDS ha ispezionato l'handshake crittografico della connessione HTTPS verso il dominio su Cloudflare. La regola STEALER [ANY.RUN] Lumma Stealer TLS Connection dimostra che il motore di sicurezza ha riconosciuto la specifica impronta digitale usata dalla famiglia LUMMA per cifrare le comunicazioni di esfiltrazione.

3. **Rilevamento Abuso DDNS:** Infine, l'allerta ET POLICY DNS Query to DynDNS Domain *.zapto .org conferma l'anomalia rilevata in precedenza, segnalando che il semplice tentativo di risoluzione verso un provider di Dynamic DNS gratuito è sufficiente a innescare i sistemi di monitoraggio aziendali, confermando la natura di fallback della comunicazione.

Fase 6: Analisi degli Artefatti (Filesystem e Modifiche Locali)

Per comprendere le azioni compiute dal malware a livello locale e isolare ulteriori indicatori (Host-based IoC), ho analizzato il pannello "Files", che traccia tutti i file creati, modificati o rilasciati (dropped) dai processi infetti.

Files modification 107

Only important | Filter by filename

NETWORK | FILES | DEBUG

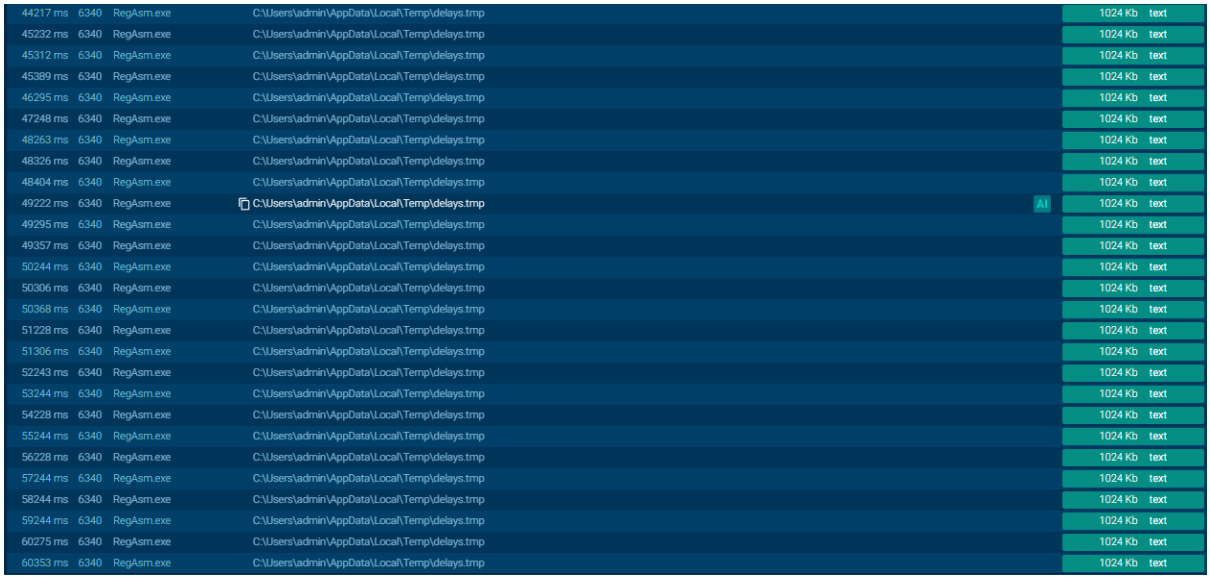
Timeshift	PID	Process name	Filename	Content
3462 ms	6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\RR3E01RZ\76561199751190313[1].htm	34 Kb html
8384 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\EBAKFI	24 Kb binary
8509 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\IECFIE	192 Kb binary
8525 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\FLJJKE	46 Kb binary
9118 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\EGIJEB	128 Kb binary
9165 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CBAFID	40 Kb binary
10118 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KJJECG	192 Kb binary
10700 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\GCBGCG	56 Kb binary
11368 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CGHCGI	224 Kb binary
14166 ms	6908	RegAsm.exe	C:\ProgramData\freebl3.dll	669 Kb executable
14166 ms	6908	RegAsm.exe	C:\ProgramData\mozglue.dll	594 Kb executable
14182 ms	6908	RegAsm.exe	C:\ProgramData\msvcp140.dll	439 Kb executable
14197 ms	6908	RegAsm.exe	C:\ProgramData\softokn3.dll	252 Kb executable
14197 ms	6908	RegAsm.exe	C:\ProgramData\vcruntime140.dll	79 Kb executable
14244 ms	6908	RegAsm.exe	C:\ProgramData\nss3.dll	2 Mb executable
14307 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JECBGC	96 Kb binary
14307 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JECBGC-shm	32 Kb binary
14338 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\AFBKKF	256 Kb sqlite
15057 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KKECFI	5 Mb Oversized
15634 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KKECFI-shm	32 Kb binary
16853 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CFHILJ	17 Kb text
17682 ms	6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JEGDGI	4 Kb image
20270 ms	6908	RegAsm.exe	C:\ProgramData\HCAEHJJKFC.exe	321 Kb executable
20285 ms	6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\E4DJRUXW\66cb2df8bd684_lawrng[1].exe	321 Kb executable
21301 ms	6908	RegAsm.exe	C:\ProgramData\CAFHDBGHJK.exe	193 Kb executable
21301 ms	6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\E4DJRUXW\66cb2df1d4a01_vakerk[1].exe	193 Kb executable
21613 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
21629 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
21644 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
22145 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
22160 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
22192 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
23160 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
23176 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
23207 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
23223 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
23238 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
24160 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
24176 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
24207 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text

Files modification 107

Only important | Filter by filename

NETWORK | FILES | DEBUG

Timeshift	PID	Process name	Filename	Content
24223 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25145 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25160 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25192 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25207 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25254 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25270 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25285 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
25317 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
26270 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
26332 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
26442 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
27254 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
28207 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
28285 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
28363 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
30539 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	AI 1024 Kb image
31258 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
32211 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
32274 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
33211 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
34274 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
34336 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
35227 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb fli
36211 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
37227 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
37289 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
38211 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
38289 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
38367 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
39196 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb binary
40211 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
41217 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
41295 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
41357 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
42217 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
42279 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
43201 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
43279 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text
43342 ms	6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp	1024 Kb text



L'analisi di questi log evidenzia tre comportamenti distinti e altamente sospetti:

1. **Drop dei Payload Secondari:** Sotto la directory C:\ProgramData\, il processo primario RegAsm.exe (PID 6908) ha salvato i due eseguibili HCAEHJJKFC.exe (321 Kb) e CAFHDBCJHJK.exe (193 Kb). Questo coincide perfettamente sia con le dimensioni dei file scaricati via HTTP, sia con i nomi dei processi visti nel grafo di esecuzione. Il malware usa ProgramData come cartella di appoggio perché di solito è nascosta all'utente e non richiede privilegi di amministratore per scriverci.

2. **Preparazione al Furto (Credential Access):** L'evidenza più interessante è il rilascio di una serie di librerie legittime nella stessa cartella: freebl3.dll, mozglue.dll, msvcp140.dll, softokn3.dll, vcruntime140.dll, e nss3.dll. Queste specifiche DLL appartengono al motore di Mozilla/Firefox. Gli Infostealer come Vidar e Lumma portano con sé queste librerie e le estraggono sul disco per un motivo preciso: servono a decifrare localmente i database SQLite in cui i browser basati su Mozilla salvano le password degli utenti. Invece di inviare il database

cifrato, il malware lo decifra sul PC della vittima e invia all'attaccante le credenziali in chiaro.

3. **Tecnica di Evasione (I/O Flooding):** Gli screenshot mostrano un'anomala e massiccia creazione di file denominati delays.tmp (esattamente da 1024 Kb, ovvero 1 MB ciascuno) all'interno della cartella C:\Users\admin\AppData\Local\Temp\. Questa operazione è eseguita da un'altra istanza di RegAsm.exe (PID 6340). La generazione continua di file "spazzatura" (Junk data) è una nota tecnica di evasione: il malware esegue pesanti operazioni di scrittura sul disco per consumare cicli CPU, rallentare il sistema e, soprattutto far scadere il tempo massimo a disposizione della sandbox per l'analisi (Time-out evasion), sperando che il sistema virtuale si spenga prima che le azioni malevole principali vengano rilevate.

Conclusione dell'Analisi

L'analisi del campione ha rivelato una complessa catena di infezione multi-stadio, mirata al furto massivo di credenziali e dati sensibili (Infostealer).

L'attacco prende il via tramite l'esecuzione del file iniziale (66bddfcb52736_vidar.exe), il quale elude i controlli di sicurezza iniettando il proprio codice maligno all'interno di un processo legittimo di Windows (RegAsm.exe, tecnica di Process Hollowing/LOLBin). Una volta ottenuto l'accesso occulto, il malware agisce come Dropper, scaricando ed eseguendo ulteriori moduli dalla famiglia **VIDAR** e **LUMMA Stealer**.

Le tecniche di evasione ed esecuzione osservate sono avanzate:

- **Decrittazione locale:** Il malware rilascia sul disco librerie legittime di Mozilla (nss3.dll, freebl3.dll, ecc.) per estrarre in chiaro le password dai database dei browser direttamente sulla macchina della vittima.

- **Offuscamento di Rete:** L'esfiltrazione dei dati rubati avviene verso domini generati casualmente (.shop) e mascherati dietro la rete CDN di Cloudflare, rendendo difficile l'identificazione del vero server attaccante.

- **Resilienza:** L'uso di domini Dynamic DNS (.zapto.org) come fallback garantisce agli attaccanti un canale di riserva nel caso l'infrastruttura primaria venga abbattuta.

- **Time-out:** La creazione massiva di file temporanei spazzatura (delays.tmp) serve a rallentare i sistemi di analisi automatizzata.

Di seguito le informazioni estratte verranno inserite nella tabella riassuntiva degli **Indicatori di Compromissione (IoC)**, per essere implementati nei sistemi di difesa perimetrale (Firewall, IDS/IPS, Proxy) ed endpoint (EDR/Antivirus).

1. Indicatori di Rete (Network IoC)

Tipo	Valore	Descrizione / Contesto
Indirizzo IP	`147.45.44.104`	IP Staging Server (Russia). Utilizzato in chiaro (porta 80) per il download dei payload secondari.
Indirizzo IP	`195.201.118.191`	IP Server C&C Primario (Hetzner, Germania). Comunicazione HTTPS (porta 443) con pattern di *beaconing* (VIDAR).
Dominio	`caffegclasiqwp.shop`	Dominio di esfiltrazione dati (LUMMA Stealer).
Indirizzo IP	`172.67.215.62`	IP di risoluzione del dominio `.shop` (Cloudflare CDN).
Indirizzo IP	`104.21.16.180`	IP secondario di risoluzione del dominio `.shop` (Cloudflare CDN).
Dominio	`arpdabl.zapto.org`	Dominio DDNS di Fallback / Riserva.
URL HTTP	`http://147.45.44.104/prog/66cb2df8bd684_lawrng.exe`	URL di download del primo modulo secondario.
URL HTTP	`http://147.45.44.104/prog/66cb2df1d4a01_vakerk.exe`	URL di download del secondo modulo secondario.

2. Indicatori di Host e File (Endpoint IoC)

Tipo	Valore / Percorso	Descrizione
Nome File	`66bddfcb52736_vidar.exe`	File eseguibile malevolo originale.
Processo Abusato	`RegAsm.exe`	*Living off the Land Binary* (LOLBin) abusato per mascherare i processi infetti.
File Droppato	`C:\ProgramData\HCAEHJJKFC.exe`	Modulo eseguibile secondario rilasciato sul disco (321 Kb).
File Droppato	`C:\ProgramData\CAFHDBCJHJK.exe`	Modulo eseguibile secondario rilasciato sul disco (193 Kb).
Artefatto DLL	`C:\ProgramData\nss3.dll` (e simili: `freebl3.dll`, `mozglue.dll`, `softokn3.dll`)	Librerie legittime di Mozilla rilasciate abusivamente dal malware per il cracking locale dei database di password.
File Evasione	`C:\Users\admin\AppData\Local\Temp\delays.tmp`	File spazzatura (1024 Kb) generati in massa per saturare l'I/O del disco e ritardare l'analisi (Time-out evasion).