



MALWARE ANALYSIS

W W W . Z E R O D A Y K N I G H T S . C O M

INDICE

01

Analisi AdwCleaner

- 1.1 Analisi Statica (p.3)
- 1.2 Analisi dinamica (p.4)
- 1.3 Malware behavior (p.5)
- 1.4 Considerazioni e remediation (p.5)

02

AnyRun

- 2.1 Analisi Vidar.exe (p.7-11)
- 2.2 Analisi Chrome.exe (p.12-16)

03

Descrizione File System Linux

- 3.1 File System (p.20)
- 3.2 Comandi **lsblk** e **mount** (p.21)
- 3.3 Utilizzo di **mount** e **umount** (p.22)
- 3.4 Comandi **chmod** e **chown** (p.23)
- 3.5 Comandi **ls -l** e **ln -s** (p.24)

04

Estrazione File .PCAP

- 3.6 Analisi HTTP Stream
- 3.7 Individuazione ed estrazione
- 3.8 Classificazione file

ANALISI ADWCLEANER



Security vendor	Analysis result	Notes
AhnLab-V3	! Dropper/Win32.Dapato.R137988	Alibaba Hoax:MSIL/Porcupine.e66e0e97
Antiy-AVL	! HackTool[Hoax]/MSIL.Agent	Arcabit Trojan.Mint.Porcupine.ED5D10
Avast	! Win32:FakeAV-FLW [Trj]	AVG Win32:FakeAV-FLW [Trj]
Avira (no cloud)	! JOKE/Agent.rlham	BitDefender Gen:Heur.Mint.Porcupine.luZ@bOy2NApig

CFF Explorer VIII - [AdwereCleaner.exe]

File Settings ?

AdwereCleaner.exe

- File: AdwereCleaner.exe
 - Dos Header
 - Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
 - Import Directory
 - Resource Directory
 - Address Converter
 - Dependency Walker
 - Hex Editor
 - Identifier
 - Import Adder
 - Quick Disassembler
 - Rebuilder
 - Resource Editor
 - UPX Utility

Property Value

File Name	C:\Users\user\Desktop\AdwereCleaner.exe
File Type	Portable Executable 32
File Info	Nullsoft PiMP Stub -> SFX
File Size	190.82 KB (195400 bytes)
PE Size	75.50 KB (77312 bytes)
Created	Monday 16 December 2024, 14.26.54
Modified	Monday 16 December 2024, 14.54.24
Accessed	Monday 16 December 2024, 14.26.54
MD5	248AADD395FFA7FFB1670392A9398454
SHA-1	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5

Property Value

Empty	No additional info available
-------	------------------------------

ANALISI STATICÀ

Dopo aver ricevuto il software sospetto, la nostra prima attività è stata condurre un'analisi statica. **L'analisi statica** consiste nell'esaminare il file senza eseguirlo, analizzandone la struttura, il codice e i metadati per identificare potenziali comportamenti dannosi o anomalie. Utilizzando strumenti specializzati come **VirusTotal** e **CFF Explorer**, siamo riusciti a determinare la natura malevola del software.

VirusTotal ci ha fornito una valutazione basata sull'aggregazione di numerosi motori antivirus, mentre CFF Explorer ci ha permesso di analizzare in dettaglio i **PE headers** (Portable Executable) e altre informazioni strutturali del file, confermando la sua effettiva pericolosità.



ANALISI DINAMICA

La seconda fase del nostro processo di indagine ha coinvolto un'analisi dinamica. Questo tipo di analisi consiste nell'osservare il comportamento del software in esecuzione all'interno di un ambiente controllato, noto come sandbox, per comprendere le sue azioni in tempo reale. A differenza dell'analisi statica, che si concentra sulla struttura del file, l'analisi dinamica permette di rilevare attività che si manifestano solo durante l'esecuzione, come connessioni di rete, modifiche al sistema e interazioni con altri processi.

Per questa analisi, abbiamo utilizzato strumenti avanzati come Cuckoo Sandbox, una piattaforma automatizzata per il monitoraggio del comportamento del malware. Grazie alla sandbox, siamo riusciti a eseguire il software in un ambiente isolato, evitando qualsiasi rischio per il sistema reale. Durante l'esecuzione, abbiamo monitorato le sue azioni, tra cui le connessioni verso l'esterno e il traffico di rete. Inoltre, tramite l'uso di Procmon (Process Monitor), abbiamo analizzato nel dettaglio le attività sui processi, come la creazione di thread, modifiche ai registri di sistema e accessi ai file. Queste osservazioni ci hanno fornito ulteriori prove della natura malevola del software, evidenziando il suo intento dannoso e il suo potenziale impatto.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path

15:59... lsass.exe 560 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\Names\WmsControl

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\Names\WmsControl\(Default)

15:59... lsass.exe 560 RegCloseKey HKLM\SAM\SAM\DOMAINS\Account\Users\Names\WmsControl

15:59... lsass.exe 560 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\000003EB

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000003EB\F

15:59... lsass.exe 560 RegCloseKey HKLM\SAM\SAM\DOMAINS\Account\Users\000003EB\InternetSID

15:59... lsass.exe 560 RegCloseKey HKLM\SAM\SAM\DOMAINS\Account\Users\000003EB

15:59... lsass.exe 560 RegEnumKey HKLM\SAM\SAM\DOMAINS\Account\Users\Names

15:59... lsass.exe 560 RegCloseKey HKLM\SAM\SAM\DOMAINS\Account\Users\Names

15:59... lsass.exe 560 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\000001F7

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4

15:59... lsass.exe 560 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4\V

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4

15:59... lsass.exe 560 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4\V

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4\F

15:59... lsass.exe 560 RegQueryKey HKLM

15:59... lsass.exe 560 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegOpenKey HKLM\System\CurrentControlSet\Control\EAS\Policies

15:59... lsass.exe 560 RegQueryKey HKLM

15:59... lsass.exe 560 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegOpenKey HKLM\System\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegQueryKey HKLM

15:59... lsass.exe 560 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegOpenKey HKLM\System\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4\ForcePasswordReset

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4\ForcePasswordReset

15:59... svchost.exe 348 ReadFile C:\Windows\System32\winevt\Logs\HardwareEvents.evtb

15:59... lsass.exe 560 RegQueryValue HKLM\SAM\SAM\DOMAINS\Account\Users\000001F4\F

15:59... lsass.exe 560 RegQueryKey HKLM

15:59... lsass.exe 560 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegOpenKey HKLM\System\CurrentControlSet\Control\EAS\Policies

15:59... svchost.exe 348 ReadFile C:\Windows\System32\winevt\Logs\HardwareEvents.evtb

15:59... lsass.exe 560 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Control\NEAS\Policies

15:59... lsass.exe 560 RegQueryKey HKLM

15:59... lsass.exe 560 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Control\NEAS\Policies

Showing 953,923 of 1,116,826 events (85%) Backed by virtual memory

AdwCleaner - Your one stop solution for Adware

AdwCleaner

All done, please review results below

Threat Name	Malware Type	Danger Level	Location
Start page Changer Win.32	Browser Hijacker	Very High	adb_updater.exe - Running process
MediaTraffic Feed	Popup Advertising	High	HKEY_LOCAL_USERS\Boot
VombaSavers	Advertising	Medium	HKEY_LOCAL_USERS\Microsoft\Wind
Win32 Stealer Trojan	Spyware	Very High	Updater.exe - Running process
Win32.cc Loader	Sworm	Very High	adhoeh.exe - Running process

Infections Found: 13

Infections Cleanable: 13

Your PC is heavily infected! Clean now! ---->

Done

LOG Report

Clean

REPARSE Desired Access: Read
NAME NOT F... Desired Access: Read
BUFFER TOO... Length: 0
SUCCESS Type: REG_BINARY, Length: 4, Data: 00 00 00 00
SUCCESS Type: REG_BINARY, Length: 664, Data: 00 00 00 00 F4 00 00 00 ...
SUCCESS Offset: 4.096, Length: 128
SUCCESS Type: REG_BINARY, Length: 80, Data: 02 00 01 00 00 00 00 00 7...
SUCCESS Query: HandleTags, HandleTags: 0x0
REPARSE Desired Access: Read
NAME NOT F... Desired Access: Read
SUCCESS Query: HandleTags, HandleTags: 0x0
REPARSE Desired Access: Read
SUCCESS Offset: 4.096, Length: 128
NAME NOT F... Desired Access: Read
SUCCESS Query: HandleTags, HandleTags: 0x0
REPARSE Desired Access: Read
SUCCESS Offset: 4.096, Length: 128

MALWARE BEHAVIOR

01

Creazione ed esecuzione del file

Il malware genera un file chiamato 6AWDCLEANER e lo esegue immediatamente, dando il via all'attacco. In questo modo, il file funge da trigger per avviare le azioni malevoli.

02

Reset della Password

Il malware forza il reset delle password per ottenere l'accesso al dispositivo e individuare informazioni riservate. Questa tecnica permette di eludere le protezioni esistenti e accedere a dati sensibili dell'utente.

03

Modifica dei Registri di Windows

Il malware interviene sulle voci del Registro di sistema di Windows per alterare il comportamento del sistema operativo. Queste modifiche possono disabilitare funzionalità di sicurezza, garantire l'avvio automatico del malware all'accensione del dispositivo o nascondere la sua presenza, compromettendo così le prestazioni e la stabilità del sistema.

04

Escalation dei Privilegi

Il malware sfrutta vulnerabilità del sistema per ottenere privilegi più elevati, come quelli di amministratore. In questo modo, acquisisce un maggiore controllo sul dispositivo, permettendo l'esecuzione di operazioni che normalmente sarebbero vietate, come l'accesso a file protetti, la modifica di impostazioni di sistema critiche o l'installazione di altri malware.

05

Screenshot

Il malware può catturare screenshot del dispositivo infetto per raccogliere informazioni sensibili. Questi screenshot possono includere dati riservati, credenziali di accesso o dettagli su attività bancarie e altre informazioni personali, che vengono poi inviate a un server remoto controllato dall'attaccante.

06

Modifica impostazioni utente

Il malware sta modificando, accedendo o influenzando alcune impostazioni o dati privati associati al profilo utente del sistema.

07

Esfiltrazione dati

Esfiltrazione dei dati è il processo attraverso il quale un malware raccoglie e trasferisce informazioni sensibili da un dispositivo compromesso a un server remoto controllato dall'attaccante. Questi dati possono includere credenziali di accesso, informazioni bancarie, file personali, e dettagli riservati. L'esfiltrazione avviene in genere in modo nascosto, per evitare la rilevazione, e può avvenire attraverso vari metodi, come connessioni di rete sicure o protocolli di comunicazione non rilevabili. L'obiettivo dell'esfiltrazione dei dati è rubare informazioni utili per scopi fraudolenti o vendere dati sensibili sul mercato nero.

CONSIDERAZIONI E REMEDIATION

Le analisi condotte hanno rivelato che il malware analizzato appartiene a più famiglie di codici malevoli, tra cui rootkit, bootkit e Trojan, ognuno con caratteristiche specifiche.

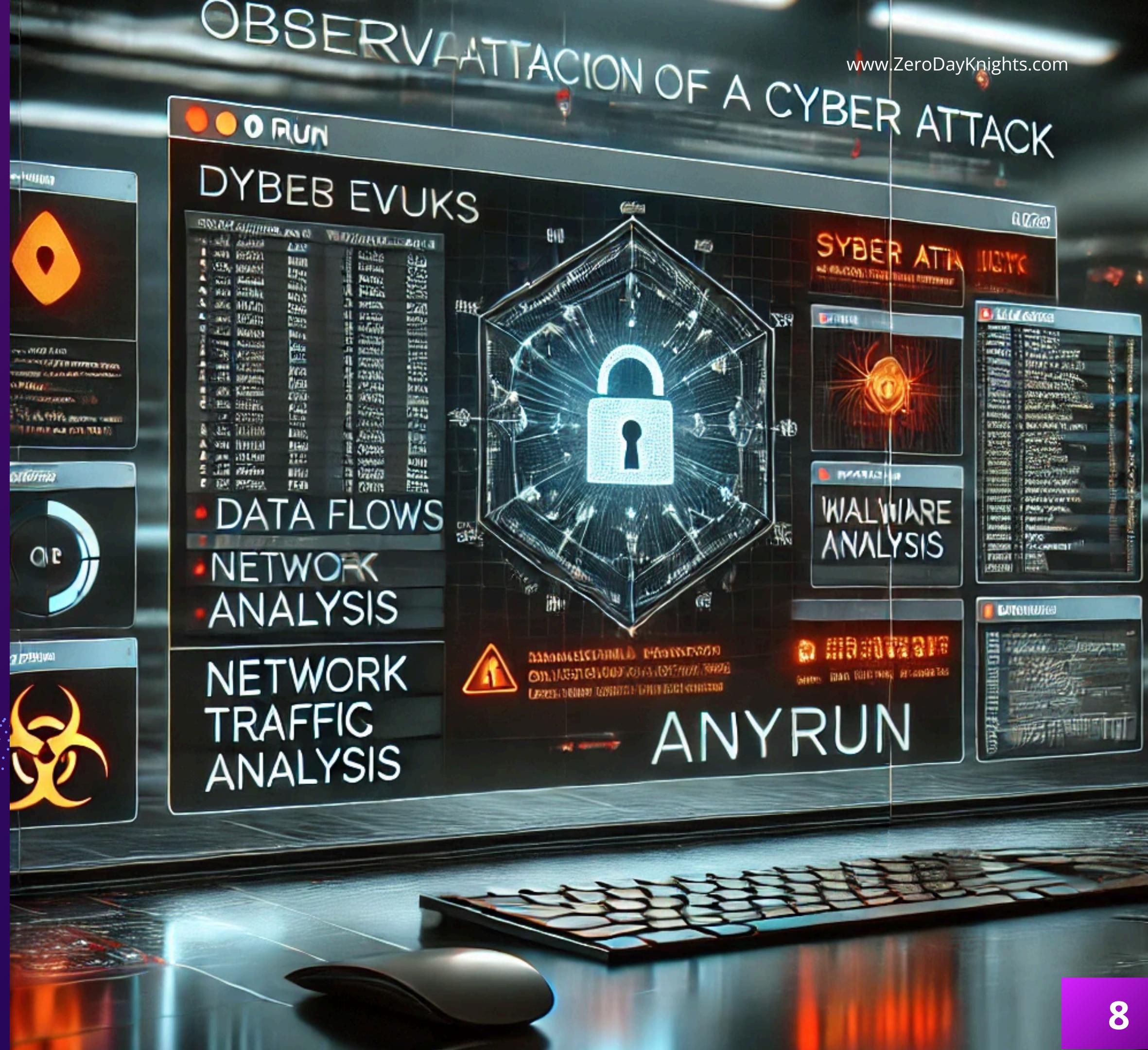
Un **rootkit** è un tipo di malware progettato per ottenere e mantenere accesso privilegiato a un sistema compromesso, mascherando la propria presenza e rendendo difficile la rilevazione. I **bootkit**, una variante dei rootkit, colpiscono invece la fase di avvio del sistema operativo, manipolando il bootloader o il settore di avvio per compromettere il sistema fin dalle prime fasi del caricamento. Infine, i **Trojan** sono programmi apparentemente legittimi che, una volta eseguiti, consentono l'accesso remoto al sistema o l'esecuzione di attività dannose, come il furto di dati o l'installazione di altri tipi di malware.

Il malware identificato è particolarmente invasivo, poiché effettua profonde modifiche all'interno del sistema target, compromettendo i suoi processi fondamentali. Inoltre, esfiltra informazioni sensibili verso un web server esterno, comunicando tramite l'indirizzo

http://www.vikingwebscanner.com/scripts/new_install.php?owner=6AdwCleaner.

Per mitigare l'impatto e contenere i danni, è fondamentale agire rapidamente. Si consiglia di **isolare** immediatamente il PC infetto per evitare la propagazione del malware o ulteriori **esfiltrazioni**. Una volta isolato, è necessario **formattare** completamente il sistema e procedere con una nuova installazione **pulita** del sistema operativo per garantire l'eliminazione completa delle minacce. Inoltre, è altamente raccomandato implementare regole di rete che blocchino qualsiasi comunicazione con il server esterno identificato, prevenendo ulteriori compromissioni o fughe di dati.

VIDAR.EXE





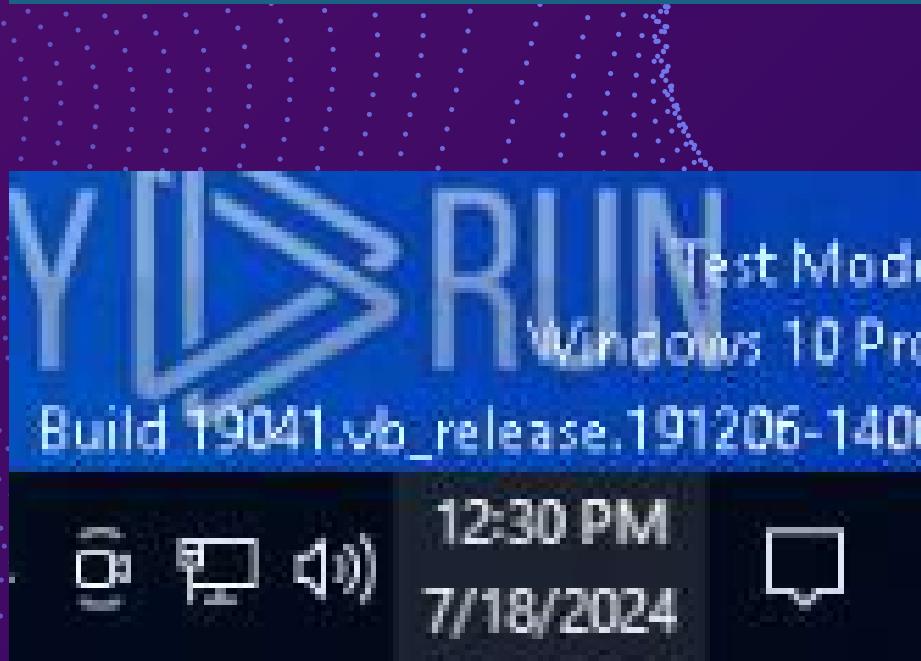
ANYRUN

COS'È

Successivamente, ci sono stati affidati due casi studio relativi a potenziali minacce informatiche riscontrate in precedenza all'interno dell'azienda. Per analizzare questi casi, abbiamo utilizzato **Anyrun**, una piattaforma avanzata di analisi dinamica del malware.

Anyrun è un ambiente interattivo di sandboxing che consente agli analisti di eseguire e monitorare software sospetto in tempo reale, osservandone il comportamento in un contesto sicuro. Grazie alla sua interfaccia intuitiva e alle sue funzionalità avanzate, permette di ottenere una visione dettagliata delle attività del malware, come connessioni di rete, creazione di processi, modifiche al registro di sistema e interazioni con i file. Questa piattaforma è particolarmente utile per individuare schemi di comportamento complessi o evasivi che potrebbero non emergere con strumenti di analisi tradizionali.

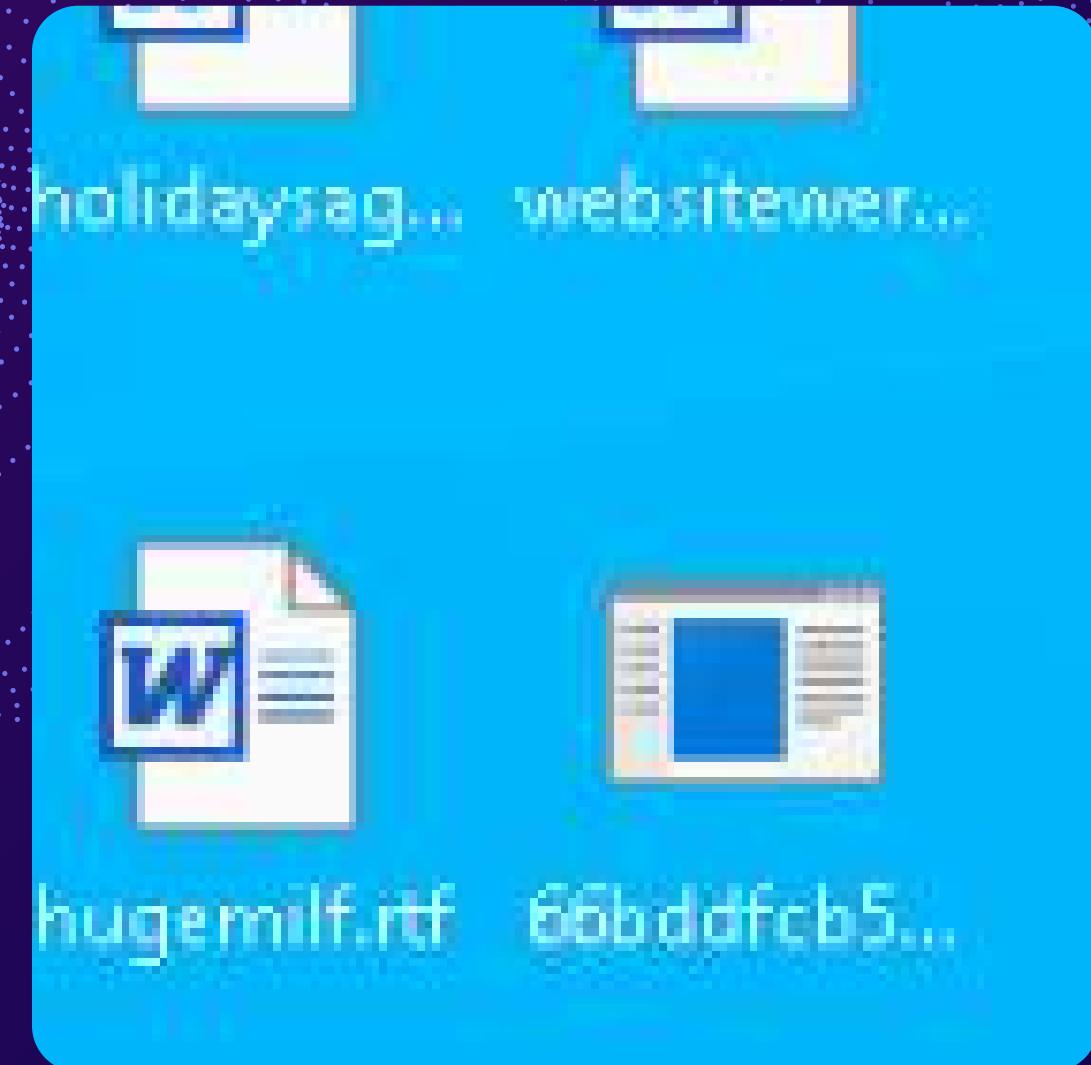
Il primo caso studio che abbiamo analizzato è stato il file **Vidar.exe**, un esempio di minaccia informatica che richiedeva un'analisi approfondita per comprenderne le modalità operative e i potenziali rischi per la sicurezza aziendale.



Il campanello di allarme che ci fa notare l'avvenuta compromissione del sistema, a livello grafico, sono senz'altro la creazione di uno strano eseguibile presente sul Desktop, e la modifica dell'orario locale della macchina.

Non avendo altre informazioni non è una cosa certa, ma vi è una buona probabilità che esso possa anche aver modificato l'orario dei log presenti all'interno del sistema.

In seguito è stata effettuata un'analisi più approfondita inerente al comportamento del software malevolo.



Vidar.exe Analisi

Procedendo con l'analisi, si è quindi scoperto che esso è una tipologia di malware in grado di eseguire un avvio automatico, riuscendo ad intaccare il sistema e creando un altro file eseguibile di nome Regasm.exe

Get to know what this threat is about

Subtechniques ▾ T1552.001

- Steals credentials from Web Browsers (3)

6908 RegAsm.exe (3)

- Actions looks like stealing of personal data (20)

6908 RegAsm.exe (10)

4704 RegAsm.exe (10)

"Credentials In Files"

Permissions required: Administrator, SYSTEM, User

Data sources: Command: Command Execution, File: File Access

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords

Get to know what this threat is about

● Danger (

- Steals credentials from Web Browsers (3)

6908 RegAsm.exe (3)

- Actions looks like stealing of personal data (20)

6908 RegAsm.exe (10)

4704 RegAsm.exe (10)

"Credentials In Files"

Permissions required: Administrator, SYSTEM, User

Data sources: Command: Command Execution, File: File Access

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords

Techniques details

Get to know what this threat is about

Subtechniques ▾ T1552.001

Danger (23)

"Credentials In Files"

Permissions required: Administrator, SYSTEM, User

Data sources: Command: Command Execution, File: File Access

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords. It is possible to extract passwords

Operation: CREATE
 Device: DISK_FILE_SYSTEM
 Object: UNKNOWN TYPE
 Name: C:\Users\admin\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini
 Status: 0xC000003A
 Created: SUPERSEDED
 Access: FILE_READ_ATTRIBUTES

Steals credentials from Web Browsers (3)
 6908 RegAsm.exe (3)

Actions looks like stealing of personal data (20)
 6908 RegAsm.exe (10)
 4704 RegAsm.exe (10)

2 of 3

Get to know what this threat is about

Subtechniques ▾ T1552.001

Danger (23)

"Credentials In Files"

Permissions required: Administrator, SYSTEM, User

Data sources: Command: Command Execution, File: File Access

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords

Operation: CREATE
 Device: DISK_FILE_SYSTEM
 Object: UNKNOWN TYPE
 Name: C:\Users\admin\AppData\Roaming\Thunderbird\profiles.ini
 Status: 0xC000003A
 Created: SUPERSEDED
 Access: FILE_READ_ATTRIBUTES

Steals credentials from Web Browsers (3)
 6908 RegAsm.exe (3)

Actions looks like stealing of personal data (20)
 6908 RegAsm.exe (10)
 4704 RegAsm.exe (10)

1 of 3

Dall'analisi eseguita mediante AnyRun, è emerso inoltre, che in seguito all'avvio esso procedeva all'esfiltrazione di dati, rubando credenziali di accesso dal Web server, nonchè dati personali anche all'interno del sistema.

Tra i dati personali che esso esfiltra sono presenti quindi credenziali, coockie dati di completamento automatico, dati bancari ed altro, ma come è possibile?

All'avvio del processo **Regasm**, viene inizializzato anche un sottoprocesso con il medesimo **Process ID** (PID) 4704, identificato come **LUMMA**. Questo comportamento evidenzia un'azione coordinata tra i due componenti, entrambi classificati come **Data Stealer**, seppur con alcune differenze comportamentali.

Pur condividendo la stessa macrofunzione, ovvero l'esfiltrazione di dati sensibili, **Vidar** e **LUMMA** mostrano una specializzazione nelle informazioni che prendono di mira. **Vidar** si concentra prevalentemente sul furto di dati generici, tra cui credenziali di accesso, informazioni bancarie e dati archiviati nei browser. **LUMMA**, invece, rivela una propensione a colpire dati di natura più specifica, come informazioni legate a criptovalute e dati aziendali sensibili.

Questa suddivisione operativa rende la combinazione dei due malware particolarmente efficace, poiché riescono a coprire un ampio spettro di obiettivi, aumentando il potenziale impatto dell'attacco. La loro capacità di agire in sinergia li rende una minaccia significativa per la sicurezza dei dati.

Differenze Chiave:

Caratteristica	Vidar	Lumma
Focalizzazione	Furto di dati generici (browser, bancari)	Furto di criptovalute e dati aziendali
Tecniche di diffusione	Phishing, siti compromessi	Social engineering, malvertising
Obiettivi principali	Credenziali, dati sensibili	Portafogli di criptovalute, seed phrase
Rilevanza temporale	Più consolidato e diffuso	Relativamente nuovo e in evoluzione

CONSIDERAZIONI E REMEDIATION

Per affrontare e mitigare l'infezione da **Vidar e Lumma**, è essenziale adottare un approccio strutturato che combini identificazione, rimozione e protezione continua.

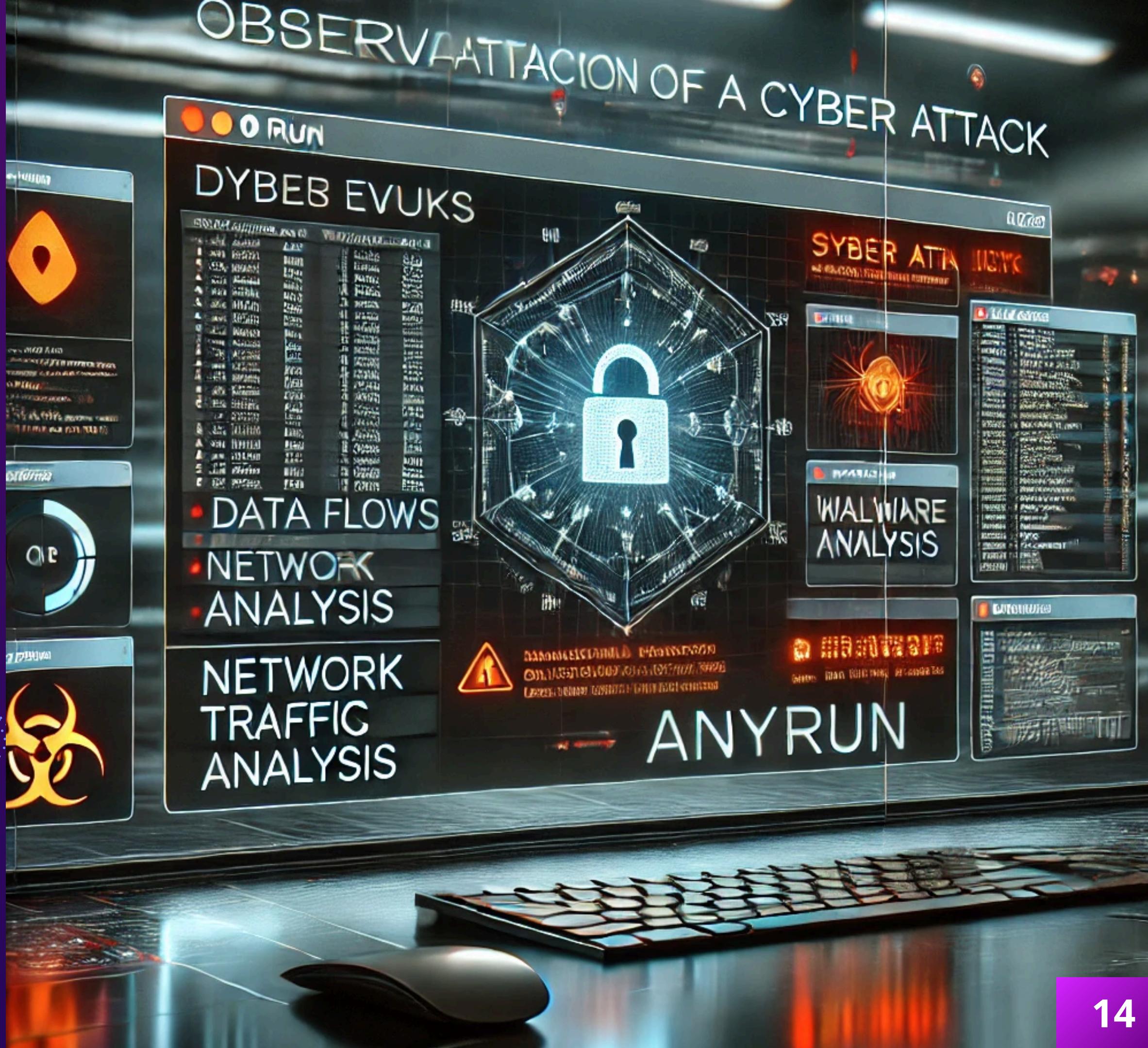
La prima fase consiste nell'individuare i processi sospetti come **Regasm** e i suoi sottoprocessi correlati. Questo può essere fatto utilizzando strumenti avanzati di monitoraggio dei processi e analisi comportamentale. Una volta identificati, è necessario terminare immediatamente i processi malevoli e isolarli dal resto del sistema per impedire ulteriori danni o esfiltrazioni di dati.

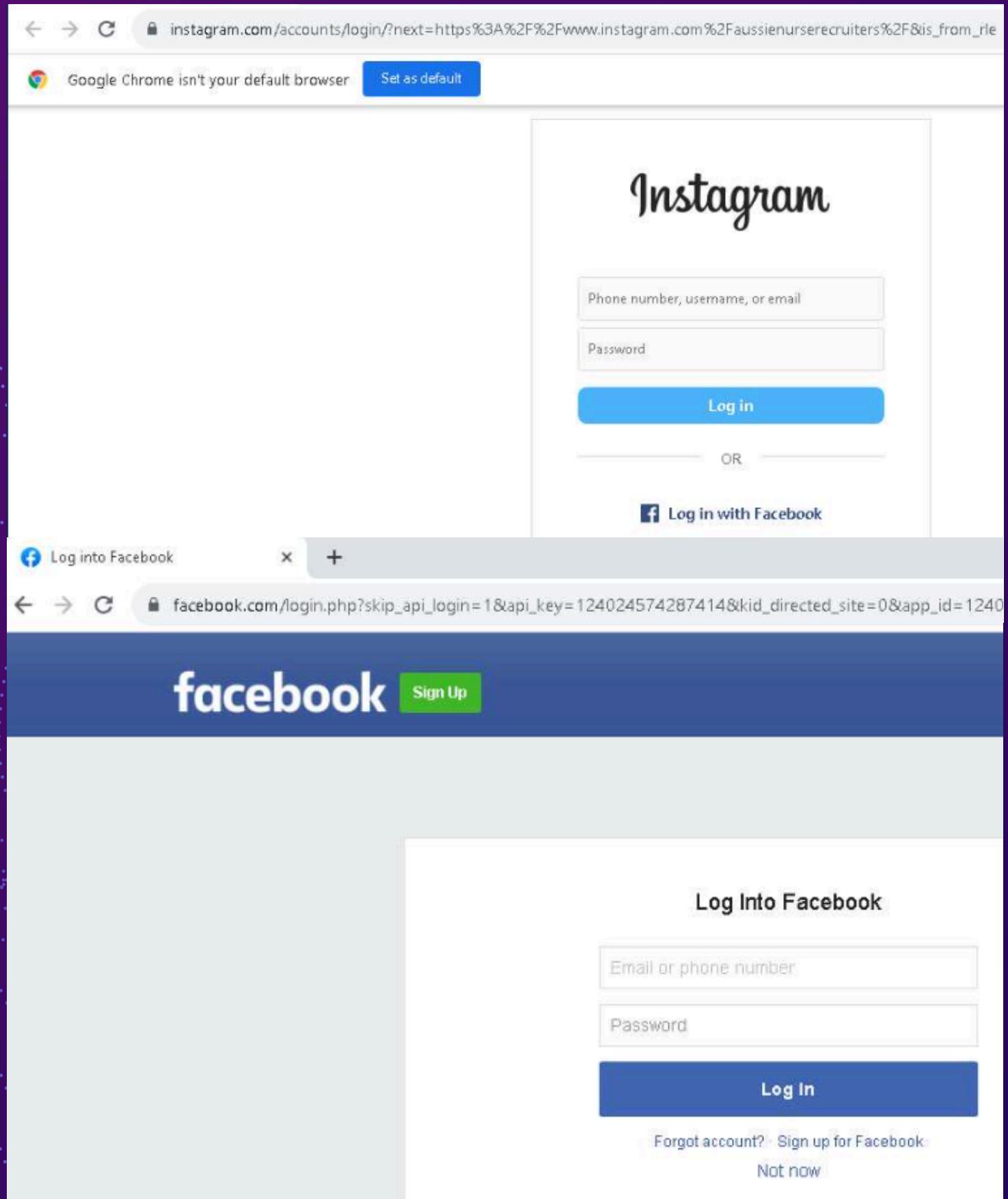
Dopo aver fermato l'esecuzione dei malware, occorre procedere con una **scansione approfondita** del sistema utilizzando software di sicurezza aggiornati. Questi strumenti devono essere in grado di rilevare e rimuovere i file associati a Vidar e Lumma, nonché **eventuali modifiche persistenti**, come chiavi di registro o attività pianificate. Durante questa fase, è fondamentale disabilitare temporaneamente la connessione a internet per impedire ulteriori comunicazioni con server di comando e controllo.

Successivamente, bisogna ripristinare la configurazione del sistema, correggendo le alterazioni effettuate dai malware. È importante controllare manualmente i punti di avvio, le voci del registro di sistema e le directory sensibili per garantire che non rimangano residui dell'infezione. Qualora fossero stati sottratti dati, è consigliabile cambiare immediatamente tutte le credenziali e monitorare eventuali attività sospette sugli account.

Infine, la protezione a lungo termine si basa sull'implementazione di misure preventive. Questo include l'installazione di un antivirus robusto con funzionalità di protezione in tempo reale, il monitoraggio continuo del sistema e la sensibilizzazione degli utenti per evitare future compromissioni, come l'apertura di file sospetti o il clic su link potenzialmente pericolosi. Aggiornare regolarmente il software e il sistema operativo è cruciale per chiudere eventuali vulnerabilità sfruttabili da minacce simili.

CHROME.EXE





Ambiente

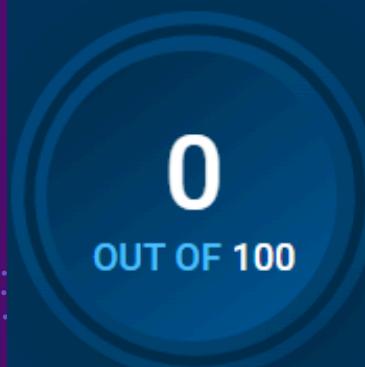
Nell'analisi effettuata sul secondo AnyRun, si osserva l'esecuzione di Chrome con l'URL:

https://www.instagram.com/accounts/login/?next=https%3A%2F%2Fwww.instagram.com%2Faussienurserecruiters%2F&is_from_rle

Questa pagina carica un profilo Instagram, ma richiede l'inserimento delle credenziali per accedere. Successivamente si passa ad una pagina facebook per tentare di effettuare l'accesso le credenziali di quest'ultimo.

[6584] chrome.exe C:\Program Files\Google\Chrome\Application\chrome.exe

Threat Verdict



No verdict

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators: ↗

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001

CMD PARENT

Questo comando sembra essere stato generato per avviare Chrome in modalità restrittiva (limitando le cache e le funzionalità di ottimizzazione) e per aprire un URL specifico.

(PID: 6584) chrome.exe	
	Source: Unknown First seen: 507 ms
?	Other / Suspicious Actions Application launched itself
CmdLine:	C:\Program Files\Google\Chrome\Application\chrome.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data"\prefetch:4 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad"\url=https://clients2.google.com/cr/report --annotation=channel="--annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=122.0.6261.70 --initial-client-data=0x224,0x228,0x22c,0x1f8,0x230,0x7ffd55cdc40,0x7ffd55cdc4c,0x7ffd55cdc58

(PID: 6584) chrome.exe	
	Source: Unknown First seen: 507 ms
?	Other / Suspicious Actions Application launched itself
CmdParent:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache --disable-background-networking --disable-features=OptimizationGuideModelDownloading,OptimizationHintsFetching,OptimizationTargetPrediction,OptimizationHints "https://click.convertkit-mail2.com/wvuqovqrwagh50nddc7hnxdlxu8/48hvhehr87opx8ux/d3d3LmIuc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydwI0ZXJz"

Timeline of the process

0 s 4.85 s

4.85 s

Other 2

T1012 Query Registry (1)
↳ Reads Microsoft Office registry keys

Application launched itself

Osservazioni

Da un primo sguardo è possibile osservare come chrome.exe si sia lanciato autonomamente, evento collegato ad una lettura delle chiavi di registro di Microsoft Office.

Andando più a fondo, nello specifico la lettura della chiave riguarda la URLASSOCIATIONS. Ciò ci porta a dedurre che l'utente abbia aperto un link URL presente all'interno di un file Office.

Behavior activities

(PID: 6584) chrome.exe

Source: registry First seen: 5466 ms

?

Other / Environment
Reads Microsoft Office registry keys

T1012 Query Registry

Operation: READ

Name: HTTP

Value:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\OFFICE\16.0\ACCESS\CAPABILITIES\URLASSOCIATIONS

Registry keys

La URL Association in una chiave di registro Office indica come gestire i link (URL) o i protocolli specifici (es. ms-word://) legati ai file e alle applicazioni Office.

VirusTotal

The screenshot shows three separate VirusTotal analysis pages:

- Top Panel:** Shows a green circle with '0 / 96' indicating no malicious findings. The URL analyzed is <https://www.instagram.com/accounts/login/?next=https://www.instagram.com/aussienurserecruiters...>. Status: 200. Content type: text/html; charset="utf-8".
- Middle Panel:** Shows a blue bar at the top stating 'No threats detected'. Below it, a link to <https://click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnx...> is shown with an 'Open in Browser' button. A tooltip for this link shows the full URL: <https://click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdxxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2lbnVyc2VyZWNydwI0ZXJz>. The interface includes tabs for 'IOC', 'MalConf', 'Restart', 'Text report', 'Graph', 'ATT&CK', 'AI Summary (beta)', and 'Export'. A CPU usage chart is visible.
- Bottom Panel:** Shows a red circle with '2 / 96' indicating 2 malicious findings. The URL analyzed is <https://click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdxxxxu8/48hvhehr87opx8ux/d3d3Lmluc3R...>. Status: 200. Content type: text/html; charset="utf-8".

VirusTotal è una piattaforma online che utilizza motori antivirus multipli e strumenti di sicurezza per analizzare file, URL, IP e domini sospetti, identificando malware, exploit e altre minacce.

Verificando l'url:

[https://www.instagram.com/accounts/login/?next=https%3A%2F%2Fwww.instagram.com%2Faussienurserecruiters%2F&is_from_rle](https://www.instagram.com/accounts/login/?next=https://www.instagram.com/aussienurserecruiters%2F&is_from_rle)

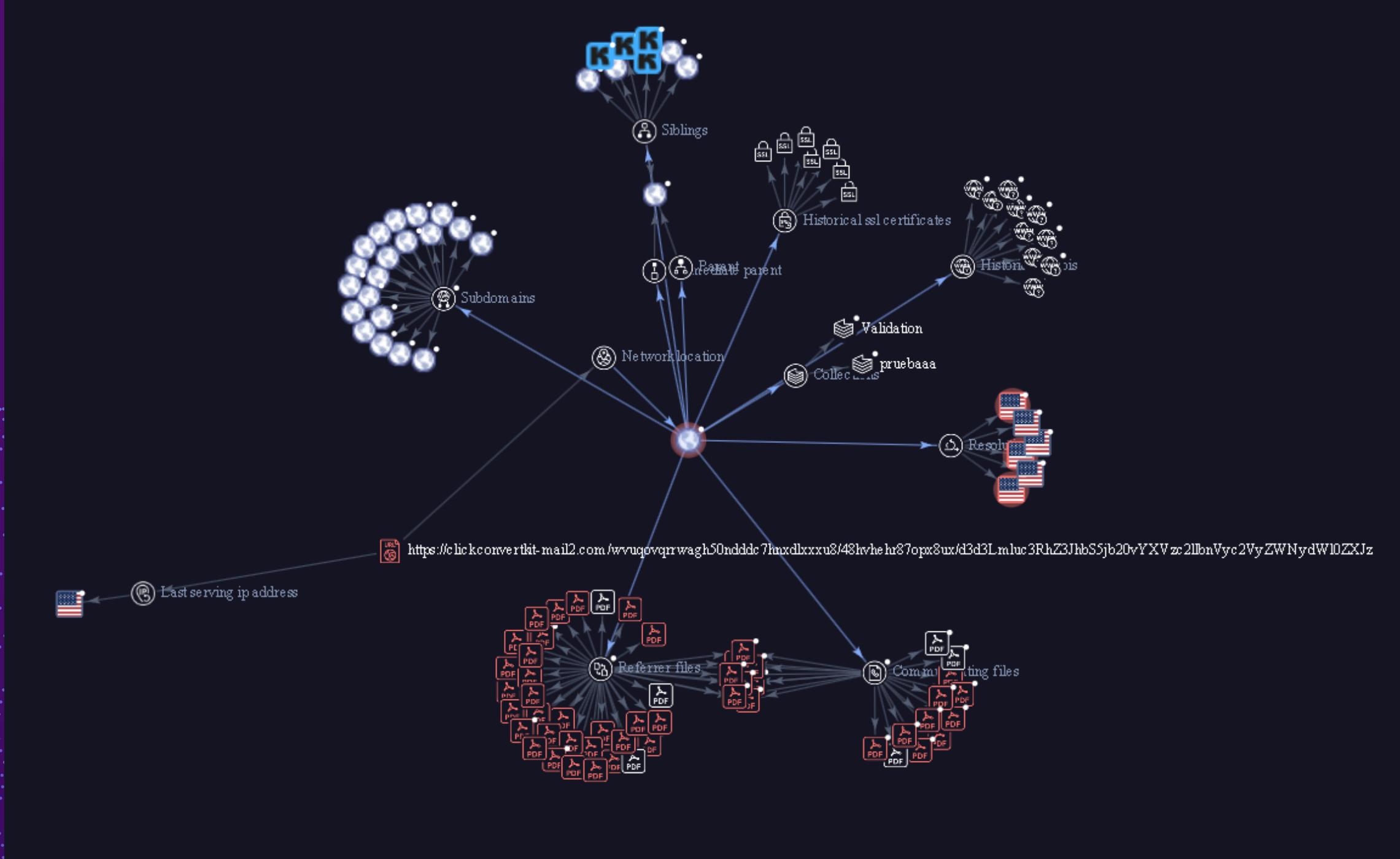
Non risultano evidenze malevoli.

Facendo però un passo indietro, possiamo osservare come l'evento da cui è scaturita l'apertura di chrome, è l'interazione con il l'URL click.convertkit-mail2.com....

Verificando quest'ultimo URL tramite VirusTotal, è emerso un leggero riscontro che lo classificasse come una possibile minaccia. Tuttavia, per maggiore sicurezza, abbiamo condotto un'analisi approfondita del traffico di rete generato dall'indirizzo <https://click.converkit-mail2.com>.

Questo approccio ci consente di indagare ulteriormente e verificare se siano presenti attività sospette o altri indicatori di compromissione che potrebbero non essere immediatamente rilevati da un'analisi automatizzata.

Probabile Minaccia



Un'analisi approfondita condotta tramite VirusTotal ci ha permesso di monitorare e verificare il traffico di rete generato dal malware, identificando i relativi **endpoint**. L'analisi di questi endpoint ha rivelato che sono già stati segnalati come malevoli, confermando la natura **sospetta** dell'attività.

Dai dati raccolti emerge che **probabilmente** si tratta di un attacco di **phishing** mirato. L'obiettivo dell'attaccante sembra essere il furto delle credenziali di accesso al profilo Facebook della vittima.

Per raggiungere questo scopo, l'attaccante ha creato una pagina web **clone**, progettata per replicare l'aspetto di una pagina legittima, inducendo così l'utente a inserire le proprie credenziali in un ambiente apparentemente sicuro. Questa tecnica sfrutta l'inganno visivo e l'affidabilità percepita per sottrarre informazioni sensibili.

CONSIDERAZIONI E REMEDIATION

Le analisi condotte hanno rivelato che il malware analizzato appartiene a più famiglie di codici malevoli, tra cui rootkit, bootkit e Trojan, ognuno con caratteristiche specifiche.

Un **rootkit** è un tipo di malware progettato per ottenere e mantenere accesso privilegiato a un sistema compromesso, mascherando la propria presenza e rendendo difficile la rilevazione. I **bootkit**, una variante dei rootkit, colpiscono invece la fase di avvio del sistema operativo, manipolando il bootloader o il settore di avvio per compromettere il sistema fin dalle prime fasi del caricamento. Infine, i **Trojan** sono programmi apparentemente legittimi che, una volta eseguiti, consentono l'accesso remoto al sistema o l'esecuzione di attività dannose, come il furto di dati o l'installazione di altri tipi di malware.

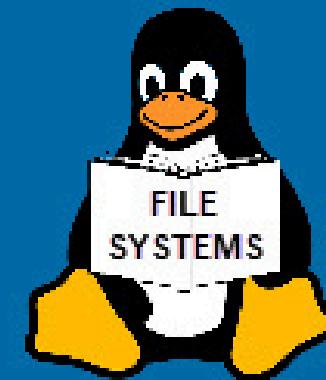
Il malware identificato è particolarmente invasivo, poiché effettua profonde modifiche all'interno del sistema target, compromettendo i suoi processi fondamentali. Inoltre, esfiltra informazioni sensibili verso un web server esterno, comunicando tramite l'indirizzo

http://www.vikingwebscanner.com/scripts/new_install.php?owner=6AdwCleaner.

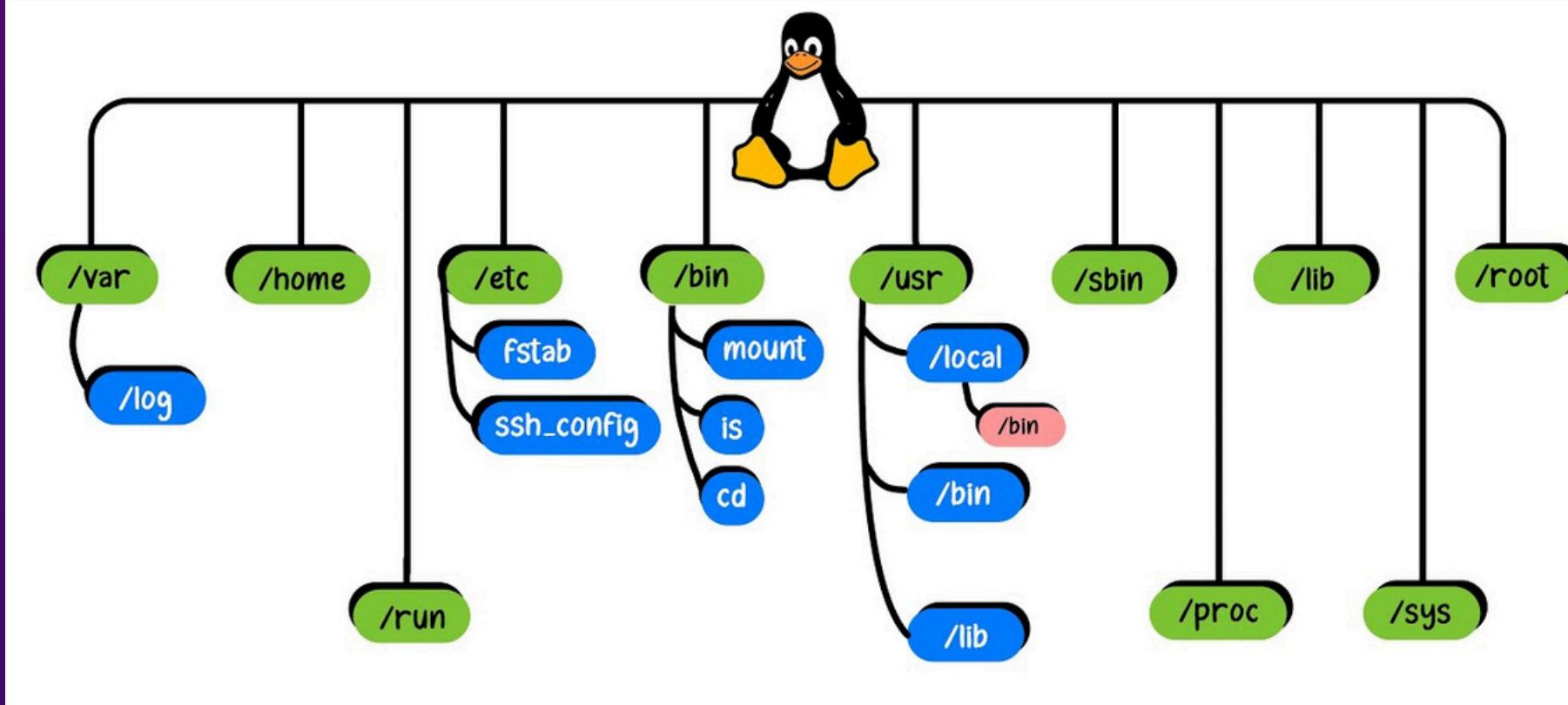
Per mitigare l'impatto e contenere i danni, è fondamentale agire rapidamente. Si consiglia di **isolare** immediatamente il PC infetto per evitare la propagazione del malware o ulteriori **esfiltrazioni**. Una volta isolato, è necessario **formattare** completamente il sistema e procedere con una nuova installazione **pulita** del sistema operativo per garantire l'eliminazione completa delle minacce. Inoltre, è altamente raccomandato implementare regole di rete che blocchino qualsiasi comunicazione con il server esterno identificato, prevenendo ulteriori compromissioni o fughe di dati.

FILESYSTEM DI LINUX

Introduction to the
Linux File System



| Linux File System Explained



FILESYSTEM DI LINUX

COS'È

I file system di Linux sono strutture organizzative che consentono al sistema operativo di archiviare, gestire e accedere ai dati su vari dispositivi di archiviazione come hard disk, SSD, pendrive e altro. Linux supporta diversi file system, ognuno con caratteristiche e funzionalità specifiche.

Struttura del File System Linux:

/Root (/): Punto di partenza di tutti i file e le directory.

/home: Contiene le directory degli utenti.

/var: File variabili come log di sistema.

/tmp: File temporanei.

/boot: File necessari per l'avvio del sistema.

/usr: Programmi e librerie di sistema.

```
Terminal - analyst@secOps
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   10G  0 disk 
└─sda1   8:1    0   10G  0 part /
sdb      8:16   0    1G  0 disk 
└─sdb1   8:17   0 1023M 0 part /
sr0     11:0   1 1024M 0 rom 

[analyst@secOps ~]$
```

```
Terminal - analyst@secOps
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ mount | grep sda1
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx  1 root root    7 Jan  5 2018 bin  -> usr/bin
drwxr-xr-x  3 root root 4096 Apr 16 2018 boot
drwxr-xr-x 19 root root 3120 Dec 17 03:35 dev
drwxr-xr-x 58 root root 4096 Apr 17 2018 etc
drwxr-xr-x  3 root root 4096 Mar 20 2018 home
lrwxrwxrwx  1 root root    7 Jan  5 2018 lib  -> usr/lib
lrwxrwxrwx  1 root root    7 Jan  5 2018 lib64 -> usr/lib
drwx-----  2 root root 16384 Mar 20 2018 lost+found
drwxr-xr-x  2 root root 4096 Jan  5 2018 mnt
drwxr-xr-x  2 root root 4096 Jan  5 2018 opt
dr-xr-xr-x 119 root root    0 Dec 17 03:34 proc
drwxr-x--- 10 root root 4096 Dec 11 08:02 root
drwxr-xr-x  17 root root   480 Dec 17 03:35 run
lrwxrwxrwx  1 root root    7 Jan  5 2018 sbin -> usr/bin
drwxr-xr-x  6 root root 4096 Mar 24 2018 srv
dr-xr-xr-x 13 root root    0 Dec 17 03:34 sys
drwxrwxrwt  8 root root 200 Dec 17 03:35 tmp
drwxr-xr-x  9 root root 4096 Apr 17 2018 usr
drwxr-xr-x 12 root root 4096 Apr 17 2018 var

[analyst@secOps /]$
```

In un sistema Linux, la gestione dei dispositivi di archiviazione e dei file system è un aspetto fondamentale per comprendere come vengono organizzati e utilizzati i dati. Utilizzando comandi come **lsblk** e **mount**, è possibile visualizzare rispettivamente i dispositivi di archiviazione disponibili e i file system attualmente montati.

Il comando **lsblk** elenca in modo dettagliato tutti i dispositivi di archiviazione rilevati dal sistema, mostrando informazioni come il nome del dispositivo, le dimensioni, il tipo e i punti di montaggio. Questo comando è particolarmente utile per identificare le partizioni e i dispositivi fisici collegati al computer, come dischi rigidi o unità USB.

Il comando **mount**, invece, consente di vedere quali file system sono attualmente montati, ovvero collegati a una directory del sistema. Il processo di montaggio rappresenta un passaggio cruciale nell'accesso ai dati: una partizione o un dispositivo di archiviazione viene collegato a una directory locale, nota come punto di montaggio, rendendo i file e le directory contenuti nel dispositivo accessibili al sistema operativo.

Un esempio pratico di questa configurazione si osserva nell'uso della partizione principale, generalmente indicata come **/dev/sda1**, che rappresenta il file system di tipo ext4. Questa partizione è spesso associata alla directory radice (**/**), il punto di partenza dell'intero sistema di file di Linux. Essendo il cuore del sistema operativo, la directory radice ospita tutte le altre directory e file necessari per il funzionamento del sistema. Il file system ext4, utilizzato frequentemente, è scelto per la sua affidabilità, efficienza e capacità di gestire grandi quantità di dati.

Attraverso questa organizzazione e l'uso dei comandi descritti, Linux fornisce una struttura flessibile e potente per gestire dispositivi di archiviazione e file system, garantendo un controllo preciso e una gestione efficiente delle risorse del sistema.

In Linux, è possibile montare manualmente una partizione utilizzando il comando **mount**, una procedura che consente di rendere accessibile il contenuto di un dispositivo di archiviazione. Per farlo, l'utente deve prima creare una directory che fungerà da punto di montaggio, cioè una cartella in cui i dati contenuti nel dispositivo saranno visibili e manipolabili. Ad esempio, l'utente potrebbe creare una directory chiamata **second_drive**. Successivamente, utilizzando il comando **mount**, può collegare una partizione, come ad esempio **/dev/sdb1**, a questa directory. Una volta eseguito il montaggio, il contenuto della partizione diventa disponibile per l'accesso e la gestione tramite la directory **second_drive**, come se fosse una normale parte del file system.

Tuttavia, è altrettanto importante comprendere come smontare un file system una volta che non è più necessario. Per fare ciò, si utilizza il comando **umount**, che disconnette la partizione dal punto di montaggio, liberando risorse e garantendo che i dati vengano correttamente salvati prima della rimozione. Prima di smontare un file system, è fondamentale uscire dalla directory in cui è stato montato il dispositivo, poiché il sistema non permette di smontare una partizione se ci sono ancora processi o terminali che la utilizzano. Pertanto, l'utente deve assicurarsi di aver lasciato la directory di montaggio prima di procedere con il comando **umount**, per evitare possibili errori o danni ai dati.

Questa operazione di montaggio e smontaggio manuale è una pratica comune per la gestione dei dispositivi di archiviazione esterni o di partizioni multiple su un sistema Linux, permettendo all'utente di accedere e utilizzare efficientemente le risorse di archiviazione.

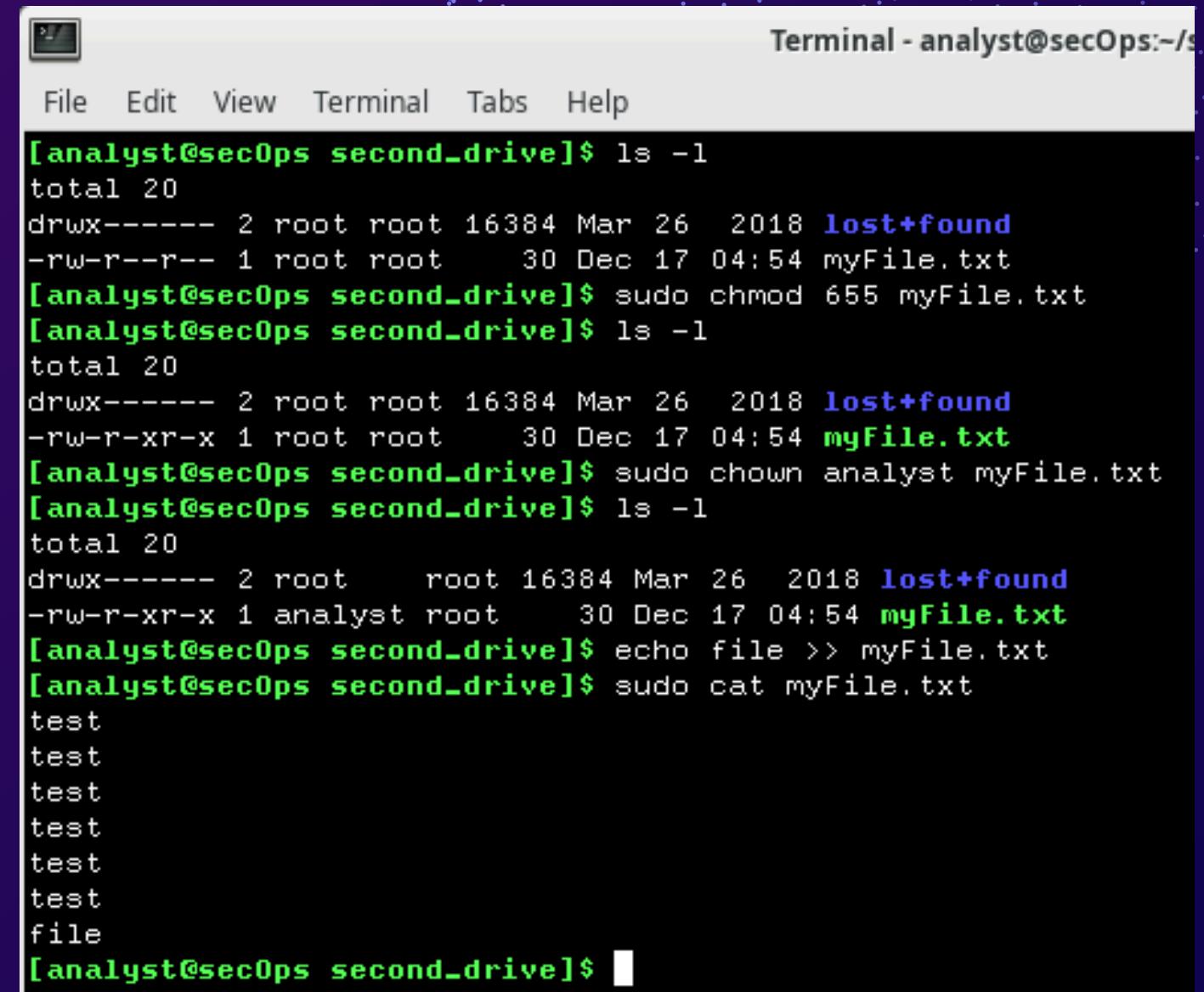
```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ ls -l second_drive/  
total 0  
[analyst@secOps ~]$ sudo mount /dev/sdb1 second_drive  
[sudo] password for analyst:  
[analyst@secOps ~]$ ls -l second_drive/  
total 20  
drwx----- 2 root root 16384 Mar 26 2018 lost+found  
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt  
[analyst@secOps ~]$ █
```

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ mount | grep /dev/sd  
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)  
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime,data=ordered)  
[analyst@secOps ~]$ sudo umount /dev/sdb1  
[analyst@secOps ~]$ ls -l second_drive/  
total 0  
[analyst@secOps ~]$ █
```

Il comando **chmod** è utilizzato in Linux per modificare i permessi di un file, e può essere applicato sia attraverso la rappresentazione simbolica che quella numerica. Nella rappresentazione simbolica, i permessi sono espressi con lettere che indicano le diverse azioni che possono essere eseguite su un file: lettura (**r**), scrittura (**w**) ed esecuzione (**x**). Questi permessi possono essere configurati separatamente per il proprietario del file, il gruppo e gli altri utenti. Ad esempio, un file con permessi **rw-r--r--** permette al proprietario di leggere e scrivere, mentre il gruppo e gli altri utenti possono solo leggere il file. In alternativa, **chmod** può essere usato con una rappresentazione numerica, in cui i permessi sono espressi tramite valori ottali. Ogni permesso è associato a un numero: **lettura corrisponde a 4, scrittura a 2 ed esecuzione a 1**. Combinando questi numeri si ottengono i permessi desiderati, come nel caso del comando **chmod 665**, che concede al proprietario e al gruppo i permessi di lettura e scrittura, mentre gli altri utenti hanno solo il permesso di lettura.

Un altro comando importante è **chown**, che permette di cambiare il proprietario di un file. Ad esempio, se si desidera assegnare un file, come **myFile.txt**, all'utente **analyst**, si può utilizzare il comando **chown analyst myFile.txt**. Dopo aver acquisito i diritti appropriati, l'utente analyst sarà in grado di manipolare il file in base ai permessi che gli sono stati concessi, ad esempio per modificarlo, leggerlo o eseguirlo, a seconda delle autorizzazioni assegnate.

Inoltre, la gestione dei permessi per le directory è un aspetto altrettanto cruciale, sebbene presenti alcune differenze rispetto ai file normali. Mentre il permesso di esecuzione su un file indica che esso può essere eseguito come programma, per una directory il permesso di esecuzione consente di accedere al suo contenuto. In altre parole, per poter "entrare" in una directory e visualizzarne il contenuto, è necessario avere il permesso di esecuzione su di essa. I permessi delle directory possono essere gestiti come quelli dei file, utilizzando i comandi **chmod** e **chown**, per assegnare i diritti di accesso e modificare il proprietario, permettendo così di controllare chi può navigare all'interno di esse e chi può modificarne il contenuto.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The window contains the following command-line session:

```
[analyst@secOps second-drive]$ ls -l
total 20
drwx----- 2 root root 16384 Mar 26 2018 lost+found
-rw-r--r-- 1 root root     30 Dec 17 04:54 myFile.txt
[analyst@secOps second-drive]$ sudo chmod 655 myFile.txt
[analyst@secOps second-drive]$ ls -l
total 20
drwx----- 2 root root 16384 Mar 26 2018 lost+found
-rw-r-xr-x 1 root root     30 Dec 17 04:54 myFile.txt
[analyst@secOps second-drive]$ sudo chown analyst myFile.txt
[analyst@secOps second-drive]$ ls -l
total 20
drwx----- 2 root      root 16384 Mar 26 2018 lost+found
-rw-r-xr-x 1 analyst root     30 Dec 17 04:54 myFile.txt
[analyst@secOps second-drive]$ echo file >> myFile.txt
[analyst@secOps second-drive]$ sudo cat myFile.txt
test
test
test
test
test
test
file
[analyst@secOps second-drive]$
```

La terza parte della discussione esplora le diverse tipologie di file presenti nei sistemi Linux, che possono essere identificati tramite il primo carattere visibile nell'output del comando `ls -l`. I file regolari sono indicati dal simbolo "-", mentre le directory sono rappresentate dalla lettera "d". Esistono anche vari tipi di file speciali, che includono i collegamenti simbolici, i file di blocco, i file di carattere, le **pipe**, i **socket** e i file **FIFO**.

Un aspetto centrale di questa parte riguarda i collegamenti simbolici e gli hard link. I collegamenti simbolici, creati con il comando `ln -s`, agiscono come scorcianti per altri file, puntando al nome del file originale. Questi collegamenti, tuttavia, sono sensibili ai cambiamenti nel nome del file: se il file originale viene rinominato o eliminato, il collegamento simbolico diventa "interrotto" e non più funzionante. Al contrario, gli **hard link**, creati con il comando `ln`, puntano direttamente alla struttura di indice del file, condividendo i dati fisici memorizzati nel disco. In questo caso, anche se il nome del file originale viene modificato o rimosso, gli hard link continuano a funzionare correttamente, poiché puntano direttamente ai dati, non al nome del file.

Un esempio pratico di questa distinzione dimostra come la modifica del nome di un file influisca sui collegamenti simbolici, che diventano non più validi, mentre gli hard link rimangono operativi. Questo fenomeno evidenzia l'importanza di comprendere le differenze tra questi due tipi di collegamenti, specialmente in contesti in cui è fondamentale mantenere l'accesso ai dati anche in caso di modifiche ai nomi dei file.

```
[analyst@secOps ~]$ ls -l
total 2104
drwxr-xr-x 3 analyst analyst 4096 Dec 13 10:12 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 Downloads
-rw-r--r-- 1 analyst analyst 9 Dec 17 05:15 file1.txt
-rw-r--r-- 1 analyst analyst 5 Dec 17 05:15 file2.txt
-rw-r--r-- 1 root   root   2127468 Dec 13 10:22 httpdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
drwxr-xr-x 3 root   root   4096 Mar 26 2018 second_drive
[analyst@secOps ~]$ ln -s file1.txt Fileutenti
[analyst@secOps ~]$ ln -s file2.txt Password
[analyst@secOps ~]$ ls -l
total 2104
drwxr-xr-x 3 analyst analyst 4096 Dec 13 10:12 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 Downloads
-rw-r--r-- 1 analyst analyst 9 Dec 17 05:15 file1.txt
-rw-r--r-- 1 analyst analyst 5 Dec 17 05:15 file2.txt
1rwxrwxrwx 1 analyst analyst 9 Dec 17 05:17 Fileutenti -> file1.txt
-rw-r--r-- 1 root   root   2127468 Dec 13 10:22 httpdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
1rwxrwxrwx 1 analyst analyst 9 Dec 17 05:18 Password -> file2.txt
drwxr-xr-x 3 root   root   4096 Mar 26 2018 second_drive
[analyst@secOps ~]$
```

PCAP FILE

PCAP file

L'obiettivo è analizzare un file PCAP per trovare ed estrarre un eseguibile di un malware.

Il software utilizzato per l'analisi è Wireshark, un tool che permette di catturare il traffico di rete per poi poterlo analizzare.

Una volta scaricato il file e localizzato nella directory pcaps, è stato analizzato concentrandosi sui pacchetti HTTP, poichè essi possono contenere file scaricati durante le sessioni di rete.

- è stato selezionato Analyze > Follow > HTTP Stream.
- è stato individuato lo stream HTTP sospetto che conteneva riferimenti a un file chiamato W32.Nimda.Amm.exe.
- La funzionalità “Follow HTTP Stream” di Wireshark permette di vedere l'intero contenuto di una sessione HTTP come se fosse un file di testo, mostrando sia le richieste del client che le risposte del server. Qui ho potuto osservare i metadati del file e confermare che si trattava di un download.

Terminal - analyst@secOps:~/lab.support.files/pcaps

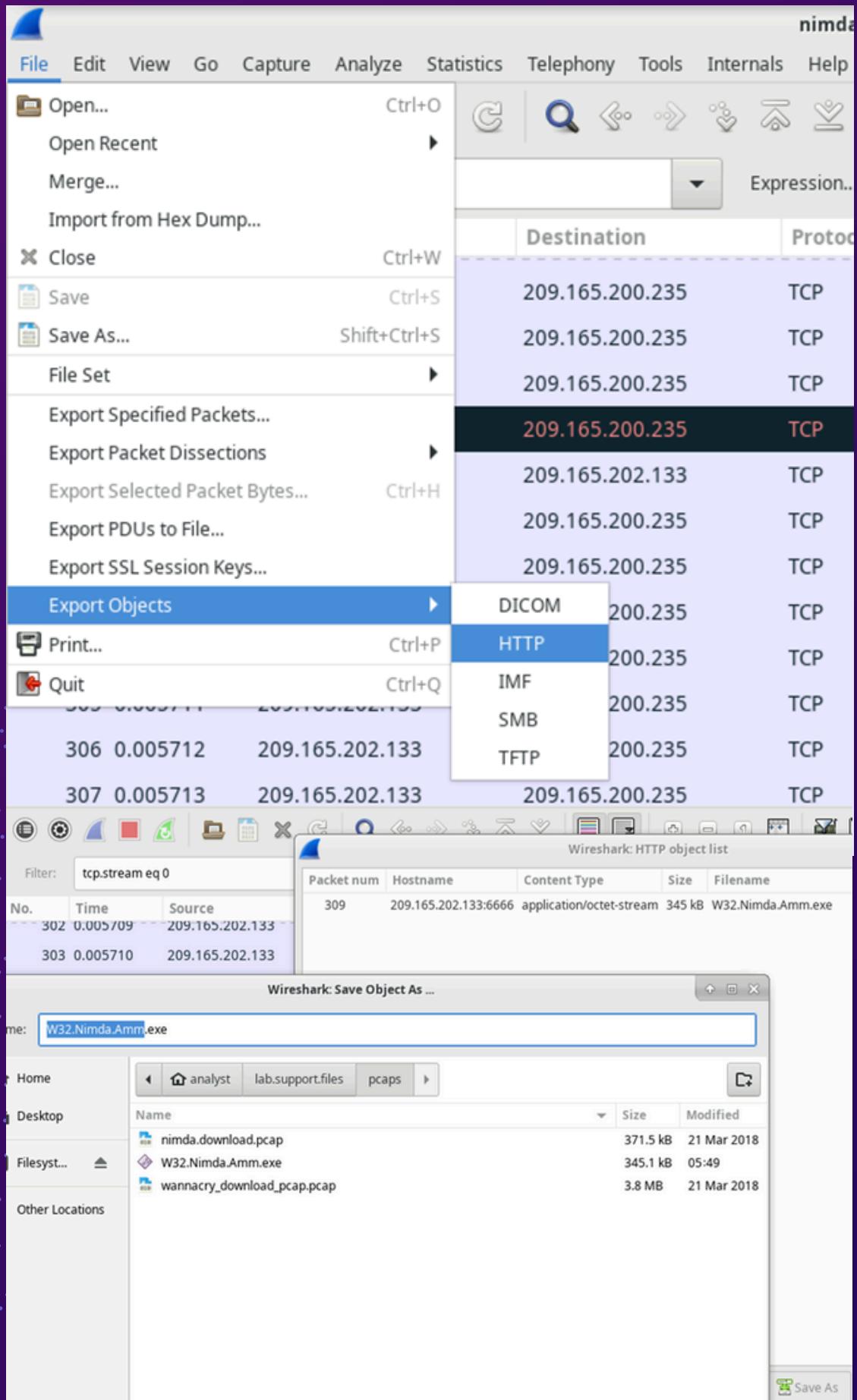
```
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$
```

Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
GET /W32.Nimda.Amm.exe HTTP/1.1
User-Agent: Wget/1.19.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 209.165.202.133:6666
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.12.0
Date: Tue, 02 May 2017 14:26:50 GMT
Content-Type: application/octet-stream
Content-Length: 345088
Last-Modified: Fri, 14 Apr 2017 19:17:25 GMT
Connection: keep-alive
ETag: "58f12045-54400"
Accept-Ranges: bytes
```



Dopo aver identificato che lo stream HTTP conteneva un file scaricato, il passo successivo è stato estrarre il file dal traffico di rete.

Tramite la funzionalità Export Objects di Wireshark è stato estratto l'eseguibile.

- File > Export Objects > HTTP.
- Nella finestra che si è aperta, vi era una lista di oggetti HTTP disponibili nel traffico catturato.
- Successivamente è stato selezionato il file W32.Nimda.Amm.exe ed stato salvato localmente nella directory .

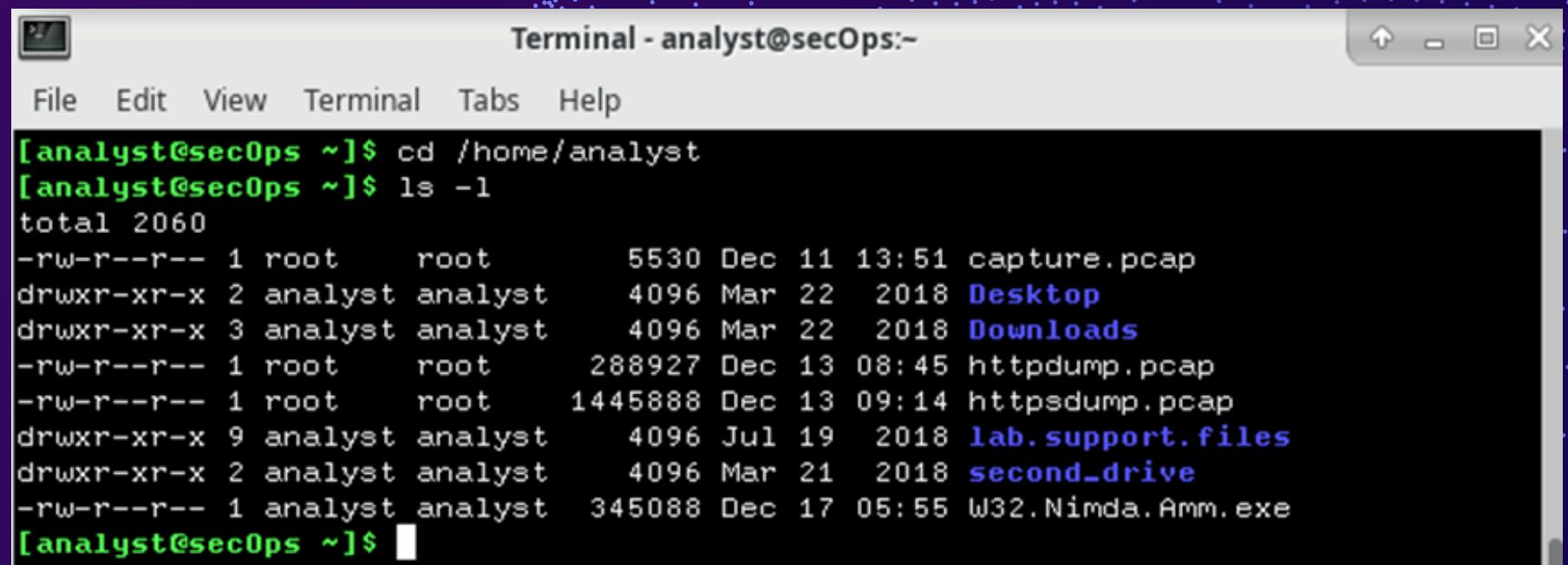
Questa funzionalità è estremamente utile perché permette di estrarre file direttamente dai pacchetti HTTP catturati senza bisogno di strumenti aggiuntivi.

Dopo aver salvato il file sospetto nella directory di lavoro, è stato necessario verificare la tipologia di file per confermare che fosse effettivamente un eseguibile.

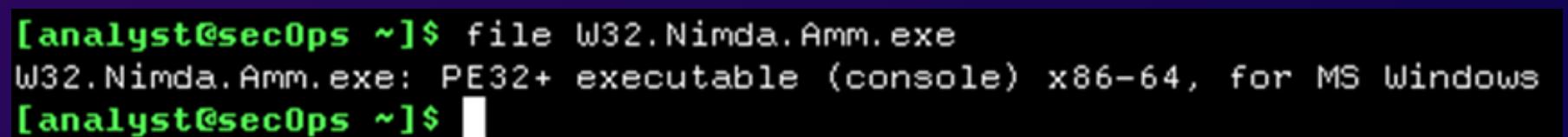
Per procedere con questa verifica, è stato utilizzato il comando `file`, che permette di analizzare i contenuti di un file a livello binario e di identificarne la tipologia. È uno strumento molto utile soprattutto in contesti di analisi forense, poiché non si limita al semplice nome o all'estensione del file, ma esamina il suo contenuto effettivo. Il comando che ho eseguito è stato: “`file W32.Nimda.Amm.exe`”

L'output mi ha confermato che si tratta di un eseguibile PE32 (console) per sistemi Windows a 64 bit.

Questa verifica finale è fondamentale non solo per confermare la natura del file, ma anche per proseguire con ulteriori analisi, come l'esecuzione in un ambiente isolato (sandbox) o l'utilizzo di strumenti di reverse engineering per comprendere il comportamento del malware. Identificare il tipo di file è solo il primo passo: una volta confermata la sua natura malevola, è possibile mettere in atto contromisure o analisi più approfondite



```
[analyst@secOps ~]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 2060
-rw-r--r-- 1 root      root      5530 Dec 11 13:51 capture.pcap
drwxr-xr-x  2 analyst   analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x  3 analyst   analyst    4096 Mar 22  2018 Downloads
-rw-r--r--  1 root      root     288927 Dec 13 08:45 httpdump.pcap
-rw-r--r--  1 root      root    1445888 Dec 13 09:14 httpsdump.pcap
drwxr-xr-x  9 analyst   analyst    4096 Jul 19  2018 lab.support.files
drwxr-xr-x  2 analyst   analyst    4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst   analyst  345088 Dec 17 05:55 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```



```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

L'analisi del file PCAP con Wireshark mi ha permesso di individuare e isolare un file eseguibile sospetto nascosto nel traffico di rete. Dopo aver estratto l'oggetto, ho verificato con il comando file che si trattava di un eseguibile PE32+ per Windows, confermando la natura potenzialmente malevola del file. Questo processo dimostra quanto sia importante monitorare il traffico di rete e utilizzare strumenti adeguati per individuare minacce nascoste, fondamentali per l'analisi forense e la difesa dagli attacchi informatici.

THANK YOU

W W W . Z E R O D A Y K N I G H T S . C O M