

# BW III ANALYST

18.04.2025



# SOMMARIO:

Introduzione

Pag. 3

ANALISI MALWARE: AdwareCleaner

Pag. 4

ANALISI MALWARE: Anyrun (primo link)

Pag. 10

ANALISI MALWARE: Anyrun (secondo link)

Pag. 17

Pag. 26

ANALISI MALWARE: Anyrun (terzo link)

LABORATORY:

LAB 1: Familiarization with Linux systems

Pag. 33

LAB 2: PCAP file extraction and analysis

Pag. 40

LAB 3: Investigation of SQL injection and DNS exfiltration

Pag. 42

LAB 4: Isolation of a compromised host using the 5-tuple

Pag. 58



# INTRODUZIONE:

Nel contesto dell'analisi e della gestione della sicurezza informatica, la presente relazione documenta il lavoro svolto su una serie di esercitazioni pratiche mirate allo sviluppo di competenze tecniche fondamentali. I test svolti da sistemi di monitoraggio, l'utilizzo operativo dei dati di sicurezza per identificare potenziali minacce e vulnerabilità, e infine l'applicazione di tecniche di Digital Forensics e Incident Analysis and Response.

L'obiettivo del lavoro è stato quello di simulare attività reali tipiche di un ambiente SOC (Security Operations Center), acquisendo familiarità con strumenti e metodologie utili per riconoscere e rispondere in modo efficace a eventi di sicurezza.



# Analisi Malware

AdwereCleaner



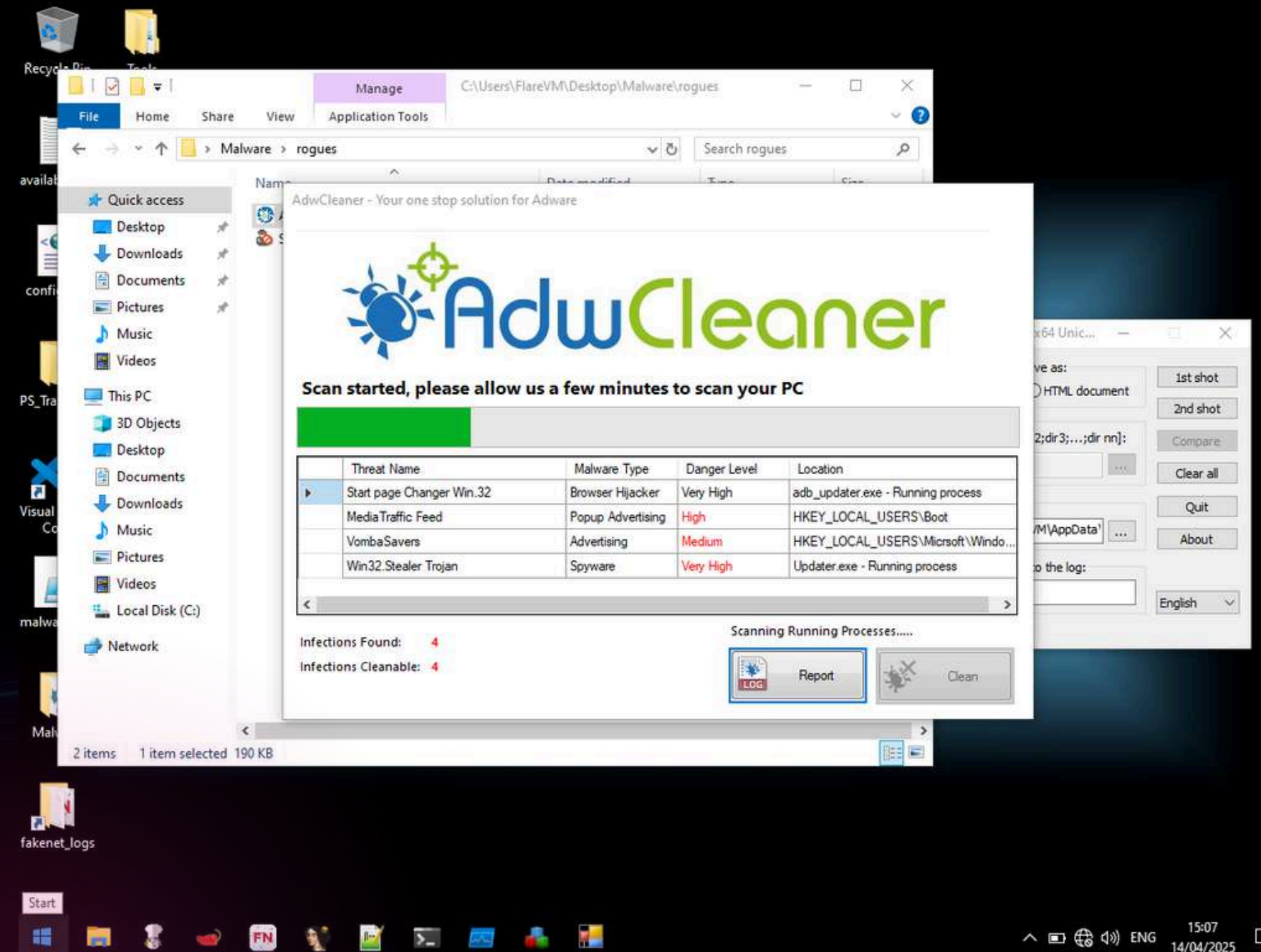
# Introduzione

Il campione oggetto di analisi è un file eseguibile denominato adwerecoleaner.exe, il cui nome richiama intenzionalmente il legittimo strumento "AdwCleaner", noto per la rimozione di adware. Tuttavia, questo eseguibile non risulta provenire da fonti ufficiali e presenta caratteristiche sospette che suggeriscono un possibile utilizzo malevolo.

Malware di questo tipo rientrano tipicamente nella categoria dei Trojan-FakeTool, ovvero file che si mascherano da strumenti di sicurezza per ingannare l'utente e indurlo a eseguirli. Una volta eseguiti, questi malware possono svolgere attività dannose come:

- Scaricare ed eseguire ulteriori payload da remoto (dropper behavior)
- Installare adware reale o spyware
- Modificare configurazioni di sistema o inserire chiavi di persistenza
- Creare backdoor per l'accesso remoto

Il file in esame sarà sottoposto a un'analisi completa, sia statica che dinamica.



# ANALISI COMPLETA

Dall'analisi dei log emergono attività sospette che fanno pensare alla presenza di un adware nel sistema. I due processi principali coinvolti sono AdwereCleaner.exe e 6AdwCleaner.exe, che hanno modificato impostazioni importanti di Windows, soprattutto quelle legate a Internet.

Anche WINWORD.EXE, cioè Microsoft Word, si è comportato in modo strano: ha cambiato impostazioni di rete e cancellato dati come il recupero dei documenti e la lista dei file recenti, il che fa pensare che sia stato influenzato dall'adware.

Inoltre, 6AdwCleaner.exe ha comunicato con siti noti per diffondere pubblicità malevole o truffe, confermando che si tratta di un software pericoloso.





# REGISTRI DI SISTEMA e MACRO WORD



## Attività Sospette nel Registro di Sistema

**1. Processi sospetti: AdwereCleaner.exe e 6AdwCleaner.exe hanno modificato alcune impostazioni fondamentali di Windows legate a Internet. In particolare:**

- **Impostazioni di sicurezza Internet:** Hanno cambiato delle opzioni che determinano come Windows gestisce i siti sicuri o non sicuri e la rete locale. Questo potrebbe servire per evitare controlli di sicurezza o per forzare il traffico web a passare su percorsi controllati dal malware.
- **Impostazioni proxy:** Uno dei due processi (6AdwCleaner.exe) ha attivato e configurato un server proxy (un intermediario tra il computer e Internet), cosa che può servire a intercettare o reindirizzare la navigazione.
- **Altre modifiche:** Ha anche cambiato alcune impostazioni relative a lingua, cookie e cronologia di navigazione.

**2. Comportamento anomalo di Microsoft Word (WINWORD.EXE) in quanto ha fatto cose che normalmente non dovrebbe fare, tra cui:**

- **Modifica delle stesse impostazioni di rete viste sopra, cosa molto insolita per un programma di scrittura.**
- **Cancellazione dei dati di recupero (usati in caso di crash) e della cronologia dei documenti recenti, per nascondere le tracce di file aperti o modificati.**
- **Cambi di lingua insoliti:** Ha attivato e poi disattivato più lingue in modo anomalo.

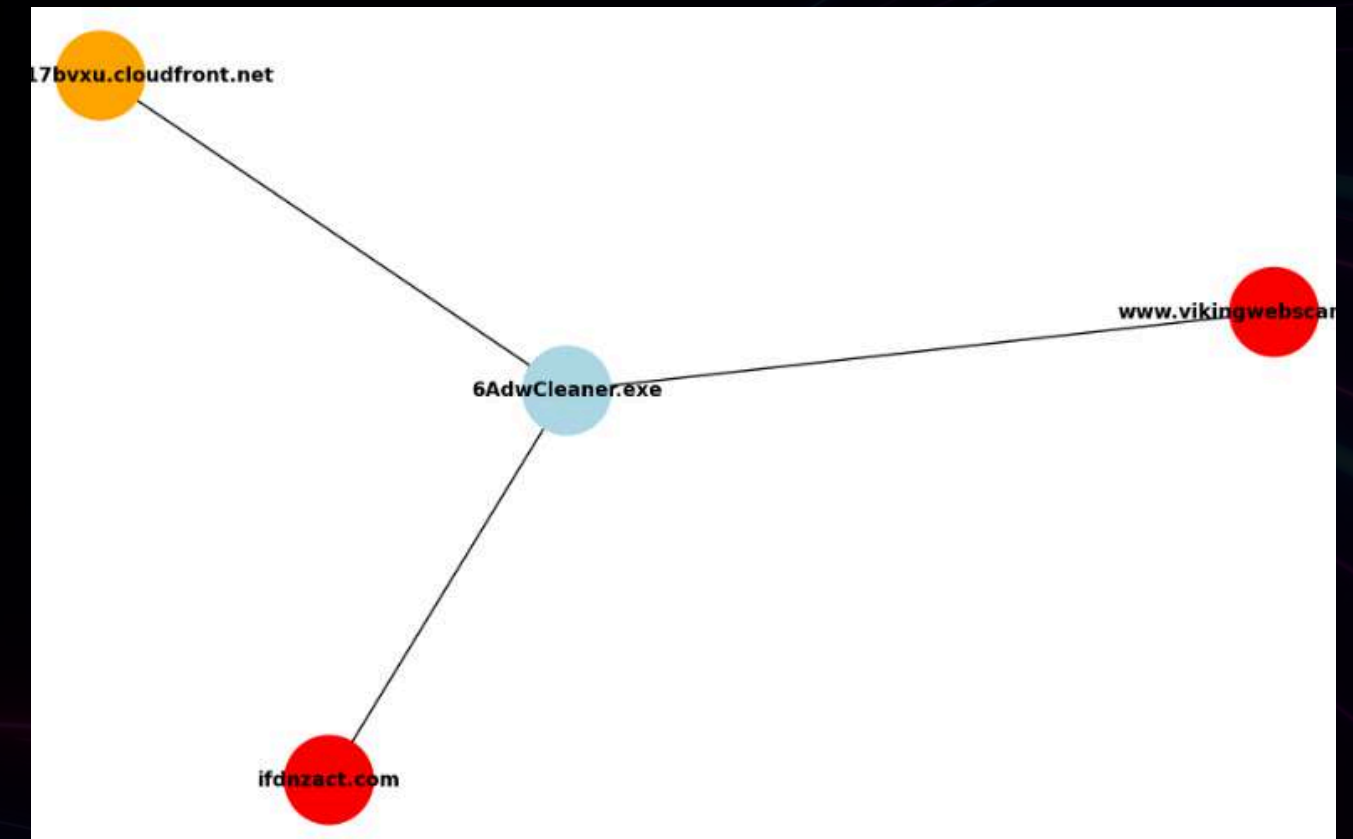
15:07:...	AdwereCleaner...	3328	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77b...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
15:07:...	AdwereCleaner...	3328	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
15:07:...	AdwereCleaner...	3328	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:07:...	AdwereCleaner...	3328	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fa...
15:07:...	AdwereCleaner...	3328	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fa...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\Software\Microsoft\Wow64\...	SUCCESS	Desired Access: R...
15:07:...	AdwereCleaner...	3328	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
15:07:...	AdwereCleaner...	3328	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Le...
15:07:...	AdwereCleaner...	3328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
15:07:...	AdwereCleaner...	3328	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x776...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
15:07:...	AdwereCleaner...	3328	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
15:07:...	AdwereCleaner...	3328	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
15:07:...	AdwereCleaner...	3328	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
15:07:...	AdwereCleaner...	3328	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:07:...	AdwereCleaner...	3328	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x767...
15:07:...	AdwereCleaner...	3328	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x773...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\Software\WOW6432Node\Polic...	REPARSE	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
15:07:...	AdwereCleaner...	3328	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
15:07:...	AdwereCleaner...	3328	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80

# CONNESSIONI

**Il processo 6AdwCleaner.exe ha effettuato diverse connessioni verso siti sospetti o noti per attività malevole:**

- **www.vikingwebscanner.com (Germania):** È il dominio più contattato. Le richieste puntano a script PHP (paymore.php, paydefault.php, status.php, get\_data.php, track.php, ls.php) i cui nomi suggeriscono funzioni legate a pagamenti, controllo dello stato, recupero dati, tracciamento e licenze/registrazione. Molte di queste comunicazioni sono classificate come malevoli.
- **ifdnzact.com (Isole Vergini Britanniche):** Sito sospetto usato probabilmente come passaggio per reindirizzare o tracciare attività legate all'altro dominio.
- **cloudfront.net (USA):** È una rete legittima (Amazon CloudFront), ma qui è stata usata per scaricare uno script (js3.js) potenzialmente dannoso.

**I codici di risposta ricevuti (200, 201, 403, ecc.) indicano che il malware sta attivamente tentando di comunicare con questi server, scaricare file o inviare informazioni.**





# MITIGATION e REMEDATION

- Scansione completa con un antivirus affidabile
- Assicurarsi che rilevi anche adware e programmi potenzialmente indesiderati (PUP).
- Prestare attenzione al ripristino delle impostazioni Internet e proxy di Windows, usando il pannello di controllo o le impostazioni di rete.

## Verifica di Microsoft Word:

- Controllare se ci sono componenti aggiuntivi strani.
- Controllare il file Normal.dotm, che potrebbe essere stato modificato (si trova nella cartella dei template di Word).
- Controllare i programmi in avvio automatico, usando Gestione Attività o strumenti come Autoruns per vedere se ci sono eseguibili sospetti.
- Valutare un ripristino del sistema (a un punto precedente) o, nei casi peggiori, una reinstallazione pulita di Windows.

**Bloccare i domini/IP pericolosi nel firewall o nel router:**

- 185.53.177.53
- 208.91.196.46
- vikingwebscanner.com
- ifdnzact.com



**Primo link sospetto**



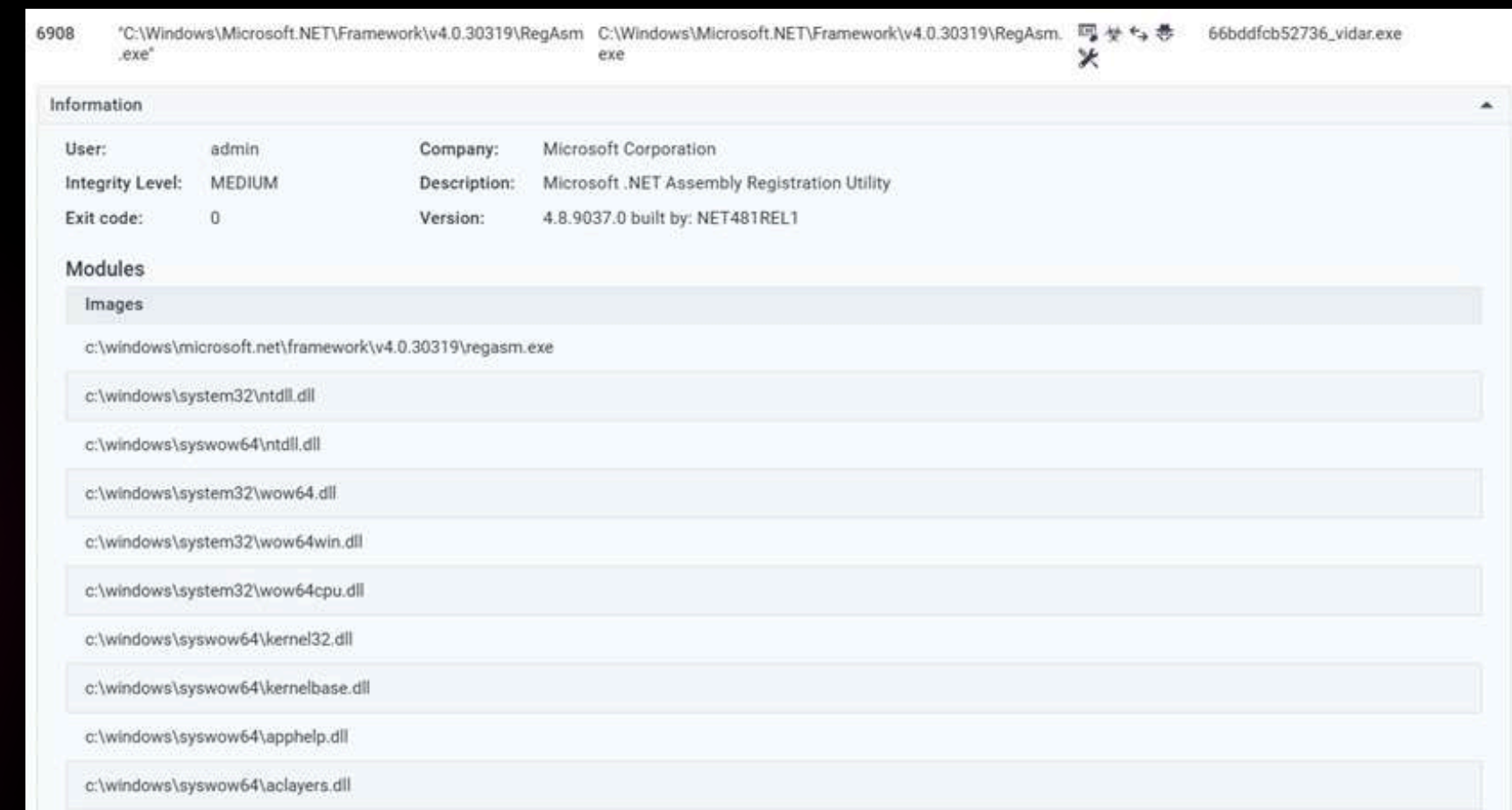
# Introduzione:

Il presente report illustra in modo chiaro e accessibile i risultati dell'analisi di un file sospetto, eseguita tramite la piattaforma professionale ANY.RUN ([link al report](#)).

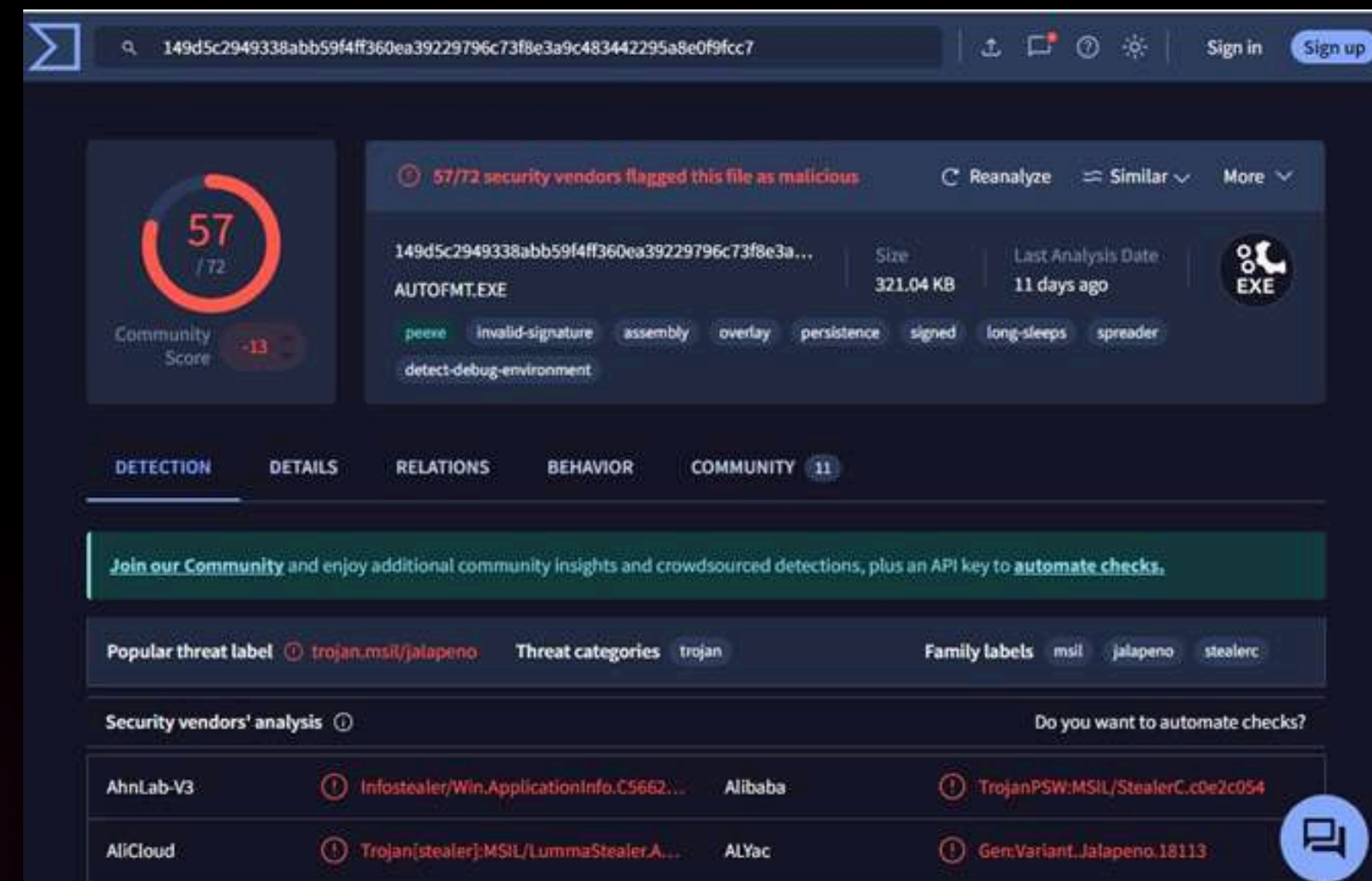
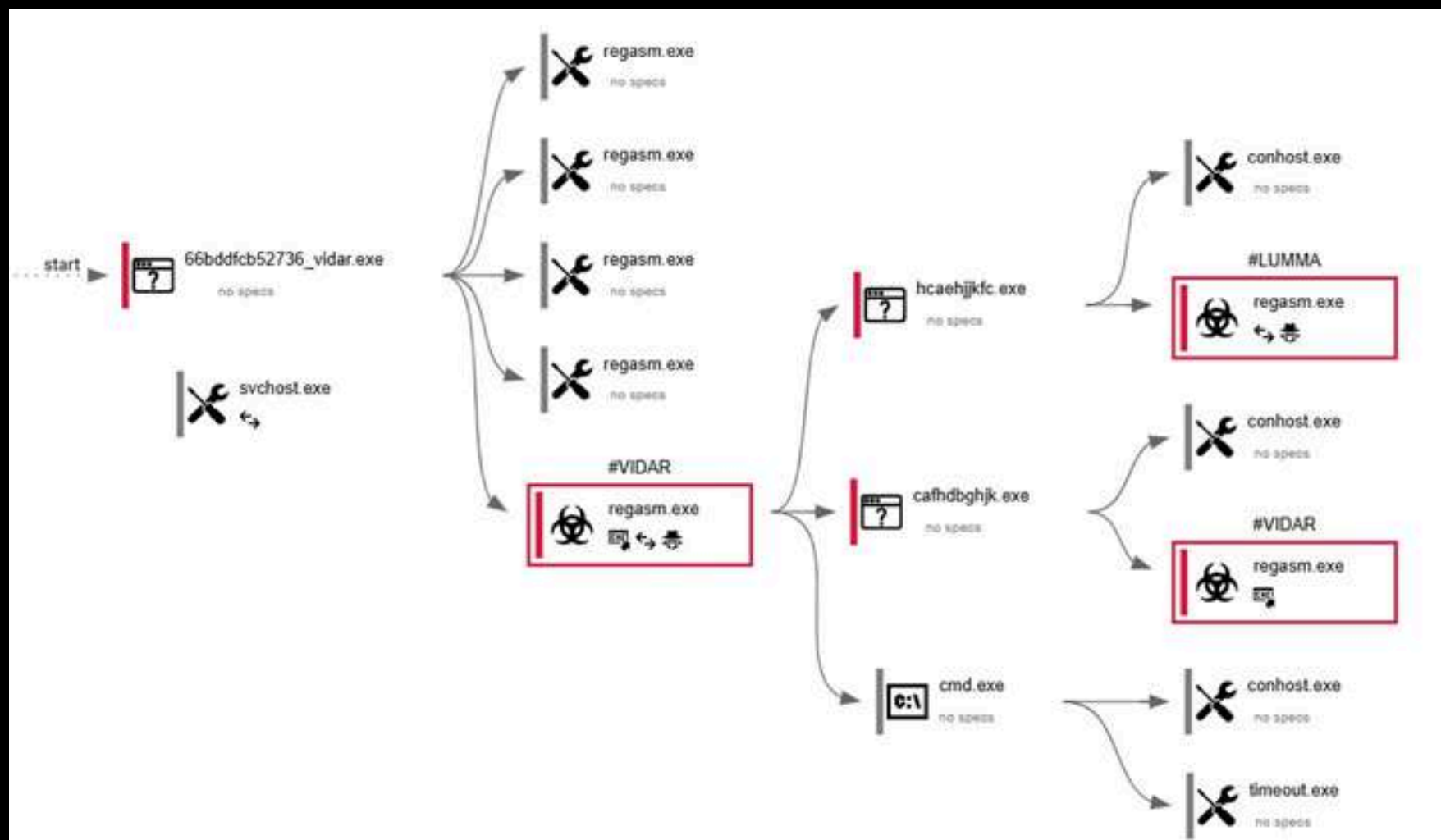
## Come è Avvenuta l'Infezione e Cos'è un Trojan?

Tutto è iniziato quando, probabilmente per errore o senza rendersene conto la vittima ha aperto un file chiamato 66bddtcb52736\_vidar.exe.

Questo file, apparentemente innocuo, in realtà è un Trojan, un tipo di malware che si finge qualcosa di legittimo per infiltrarsi nel sistema. Una volta eseguito, ha scatenato l'attacco.



## Cosa Fa Questo Malware?



Questa immagine mostra il comportamento di un file malevolo (malware) che si propaga e avvia altre attività sospette sul sistema infettato


Il trojan Vidar/Lumma identificato nel sistema è progettato principalmente per rubare informazioni sensibili, come password, credenziali di accesso, dati bancari o persino criptovalute.



Per evitare di essere scoperto, si camuffa abilmente da programma normale sfruttando processi di Windows:

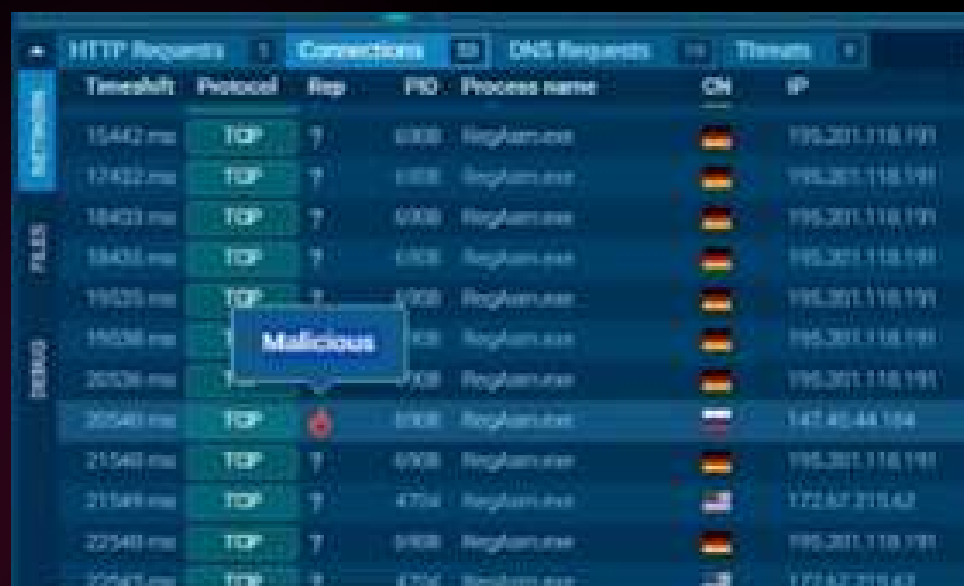
- **svchost.exe**: Di solito è un processo di sistema fondamentale, ma il malware lo ha usato come copertura per eseguire operazioni dannose in background.
- **regasm.exe**: Un altro componente legittimo di Windows, che però in questo caso è stato "clonato" più volte per far girare il codice malevolo senza destare sospetti.

Nota: alcune copie di regasm.exe erano addirittura scritte male (reqasm.exe), un trucco per confondere eventuali controlli di sicurezza.



Wireshark network traffic capture showing HTTP requests. The 'Process name' column highlights 'svchost.exe' and 'RegAsm.exe'.

Headers	Rep	PID	Process name	CN	URL
GET 200 OK	🟢	5468	svchost.exe	🇺🇸	http://ocsp.digicert.com
GET 200 OK	🟡	6908	RegAsm.exe	🇵🇱	http://147.45.44.104
GET 200 OK	🟡	6908	RegAsm.exe	🇵🇱	http://147.45.44.104
GET 200 OK	🟢	6344	SIHClient.exe	🇩🇪	http://www.microsoft.com
GET 200 OK	🟢	6344	SIHClient.exe	🇩🇪	http://www.microsoft.com



Wireshark network traffic capture showing connections. A red circle highlights a connection to 147.45.44.104, which is labeled 'Malicious'.

TimeShift	Protocol	Rep	PID	Process name	CN	IP
15442 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
17422 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
18403 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
18403 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
19525 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
19525 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
20726 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
20740 ms	TCP	7	6908	RegAsm.exe	🇵🇱	147.45.44.104
21540 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
21540 ms	TCP	7	4704	RegAsm.exe	🇵🇱	172.67.219.62
22540 ms	TCP	7	6908	RegAsm.exe	🇵🇱	195.201.118.191
22540 ms	TCP	7	4704	RegAsm.exe	🇵🇱	172.67.219.62



Process details window for RegAsm.exe (ID 6908, Malicious). The window shows a security score of 100 (OUT OF 100) and a danger level of 4. The command line is "D:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe".

Process details ID 6908 Malicious

**RegAsm.exe** AI

4.8.9037.0 built by: NET481REL1  
Microsoft .NET Assembly Registration Utility

Username: admin  
Start: +951ms Indicators: 🚩 🚩 🚩 🚩 🚩 🚩

Command line AI

"D:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"

More Info

Show all

**Danger 4**

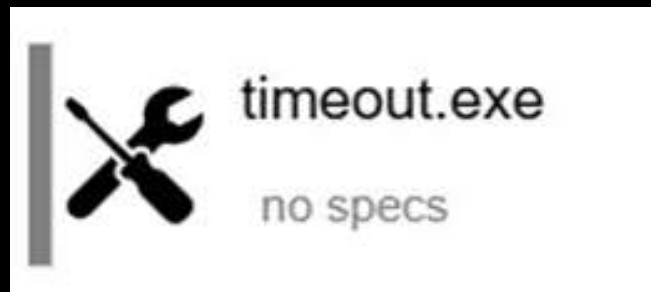
T1555.003 Credentials from Web Browsers (1)

# Il malware si espande

A questo punto, il sistema è compromesso e il malware ha iniziato a generare numerosi file eseguibili con nomi casuali e insoliti, una tattica comune per evitare il rilevamento. Questi file malevoli potrebbero essere utilizzati per:

- Rubare informazioni sensibili, come password, credenziali finanziarie o documenti importanti.
- Scaricare ulteriori minacce, incluso ransomware in grado di bloccare l'intero sistema e richiedere un riscatto.

## Il malware rallenta il sistema per non farsi beccare



Uno dei dettagli più subdoli è l'uso di timeout.exe, un comando legittimo di Windows normalmente innocuo che qui viene sfruttato per rallentare le operazioni del malware e ostacolare l'analisi dei sistemi di sicurezza.



# Spiegazione di Vidar e Lumma:



## Ecco cosa fanno:

### 1. Vidar:

- Ruba informazioni dal computer, come password, dati di carte di credito e file personali.
- Si diffonde spesso attraverso email ingannevoli o download fraudolenti.
- Lavora in silenzio, senza che l'utente se ne accorga.

### 2. Lumma:

- Specializzato nel rubare credenziali (ad esempio, quelle dei conti bancari online).
- Può registrare ciò che digiti sulla tastiera o catturare schermate del tuo computer.
- Si nasconde bene ed è difficile da rilevare senza strumenti adeguati.

Per ulteriori dettagli su Vidar e Lumma, consultare i seguenti link: [Vidar](#), [Lumma](#)

# Come Comunica il Malware con gli Attaccanti?

Il malware stabilisce connessioni sospette con server remoti, tra cui l'indirizzo IP russo 147.45.44.104 o il dominio caffegclasiqwp.shop. Per mascherare il traffico dannoso, sfrutta servizi legittimi come Cloudflare, rendendo più difficile il blocco delle comunicazioni.

Opzioni di Intervento (Remediation):

Mettere in quarantena il file (Isolamento)

- Cosa significa: Spostare il file in un'area sicura dove non può fare danni, come mettere in una scatola chiusa un oggetto pericoloso.

Perché farlo:

- Permette di bloccare immediatamente il malware senza cancellarlo, così possiamo
- studiarlo meglio se serve.
- Evita che infetti altri computer o danneggi ulteriormente il sistema.

Eliminare il file (Rimozione definitiva)

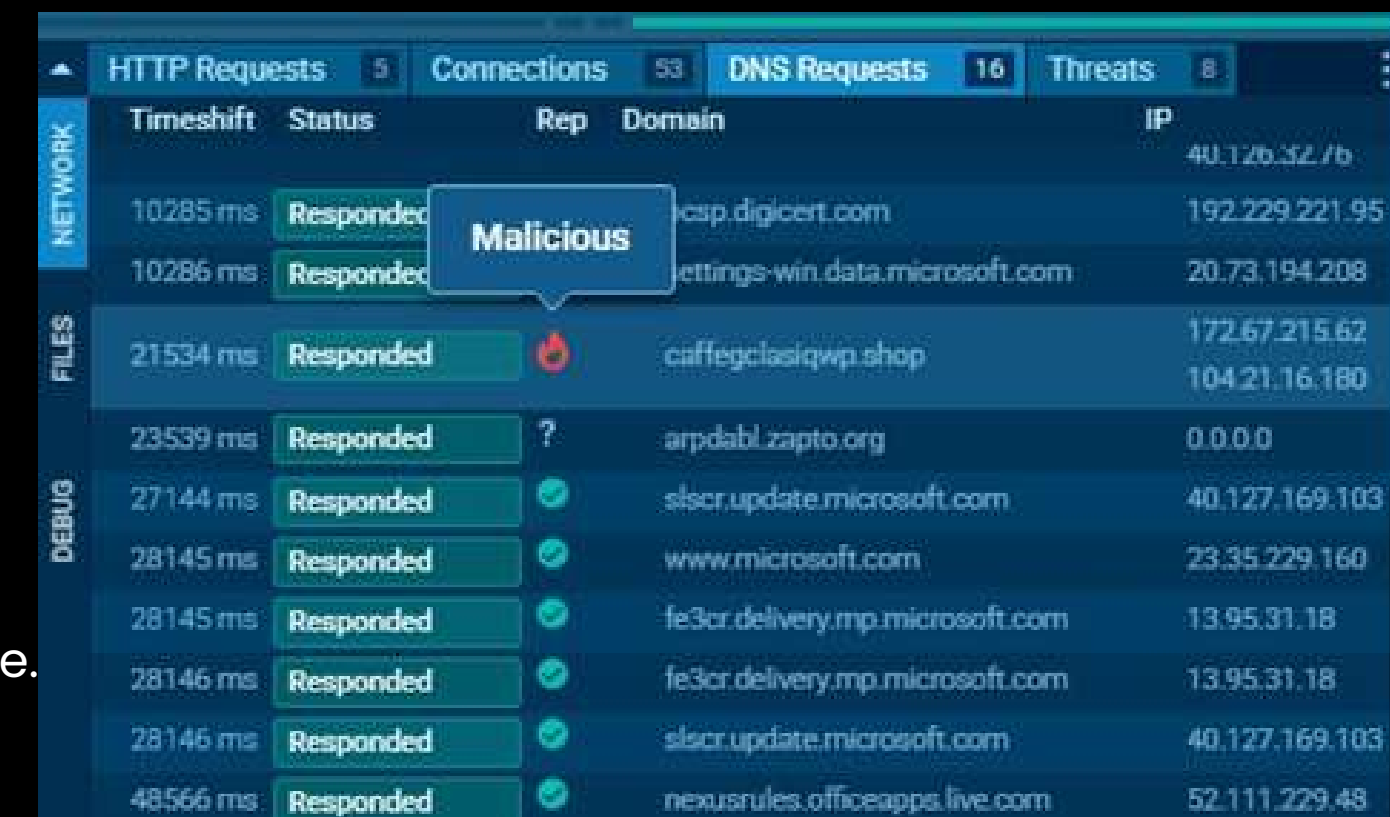
Cosa significa: Cancellare completamente il file infetto dal computer.

Perché farlo:

- Se siamo certi che sia un malware (vero positivo), eliminandolo si risolve il problema alla radice.
- Riduce il rischio che qualcuno lo esegua per sbaglio in futuro.

Quando sceglierlo:

- Dopo averlo messo in quarantena e confermato che è dannoso.
- Se il file non è necessario per il business (es. non è un programma aziendale legittimo).



HTTP Requests 5   Connections 53   DNS Requests 16   Threats 8				
	Timeshift	Status	Rep	Domain
NETWORK				IP
	10285 ms	Responded		40.127.32.7b
	10286 ms	Responded		192.229.221.95
FILES				
	21534 ms	Responded		settings-win.data.microsoft.com
				20.73.194.208
DEBUG	21534 ms	Responded		caffegclasiqwp.shop
				172.67.215.62
				104.21.16.180
	23539 ms	Responded	?	arpdabl.zapto.org
				0.0.0.0
	27144 ms	Responded	✓	slscr.update.microsoft.com
				40.127.169.103
	28145 ms	Responded	✓	www.microsoft.com
				23.35.229.160
	28145 ms	Responded	✓	fe3cr.delivery.mp.microsoft.com
				13.95.31.18
	28146 ms	Responded	✓	fe3cr.delivery.mp.microsoft.com
				13.95.31.18
	28146 ms	Responded	✓	slscr.update.microsoft.com
				40.127.169.103
	48566 ms	Responded	✓	nexusrules.officeapps.live.com
				52.111.229.48





**Secondo link sospetto**

Iniziamo l'analisi sul secondo link, da uno sguardo superficiale non sembrano esserci minacce in corso che facciano presagire attività sospette o malevole.

Ma prima di dare un giudizio, approfondiamo ogni aspetto.

Partiamo dalle HTTP request, dalle connections e dalle DNS Request.

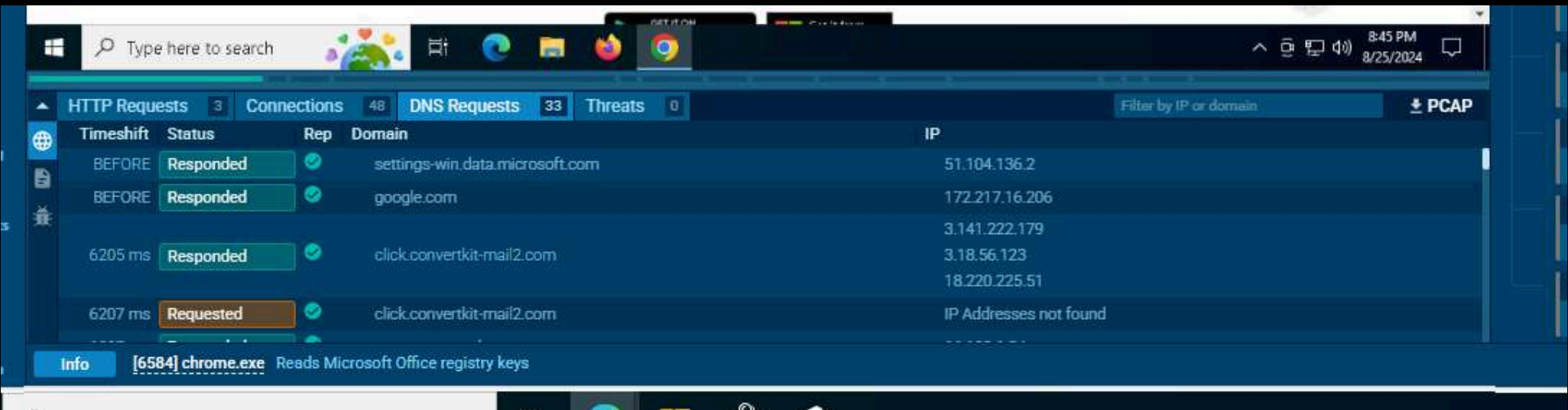


Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
8047 ms	GET   200: OK	✓	2228	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgU...	471 b ↓ binary
28546 ms	GET   200: OK	✓	6296	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Pr...	419 b ↓ binary
28548 ms	GET   200: OK	✓	6296	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Up...	407 b ↓ binary



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	UDP	✓	4	System		192.168.100.255	138	-	-	↑ 558 b ↓ -
BEFORE	TCP	✓	4436	svchost.exe		51.104.136.2	443	settings-win.data.micro...	MICROSOFT-CORP-MSN-A...	No Data
BEFORE	TCP	✓	608	RUXIMICS.exe		51.104.136.2	443	settings-win.data.micro...	MICROSOFT-CORP-MSN-A...	No Data
BEFORE	TCP	✓	2120	MoUsoCoreWorker.exe		51.104.136.2	443	settings-win.data.micro...	MICROSOFT-CORP-MSN-A...	No Data
6226 ms	UDP	✓	6584	chrome.exe		239.255.255.250	1900	-	-	↑ 696 b ↓ -
6227 ms	TCP	?	6840	chrome.exe		3.141.222.179	443	click.convertkit-mail2.c...	AMAZON-02	↑ 1 Kb ↓ 6 Kb

Info [6584] chrome.exe Reads Microsoft Office registry keys

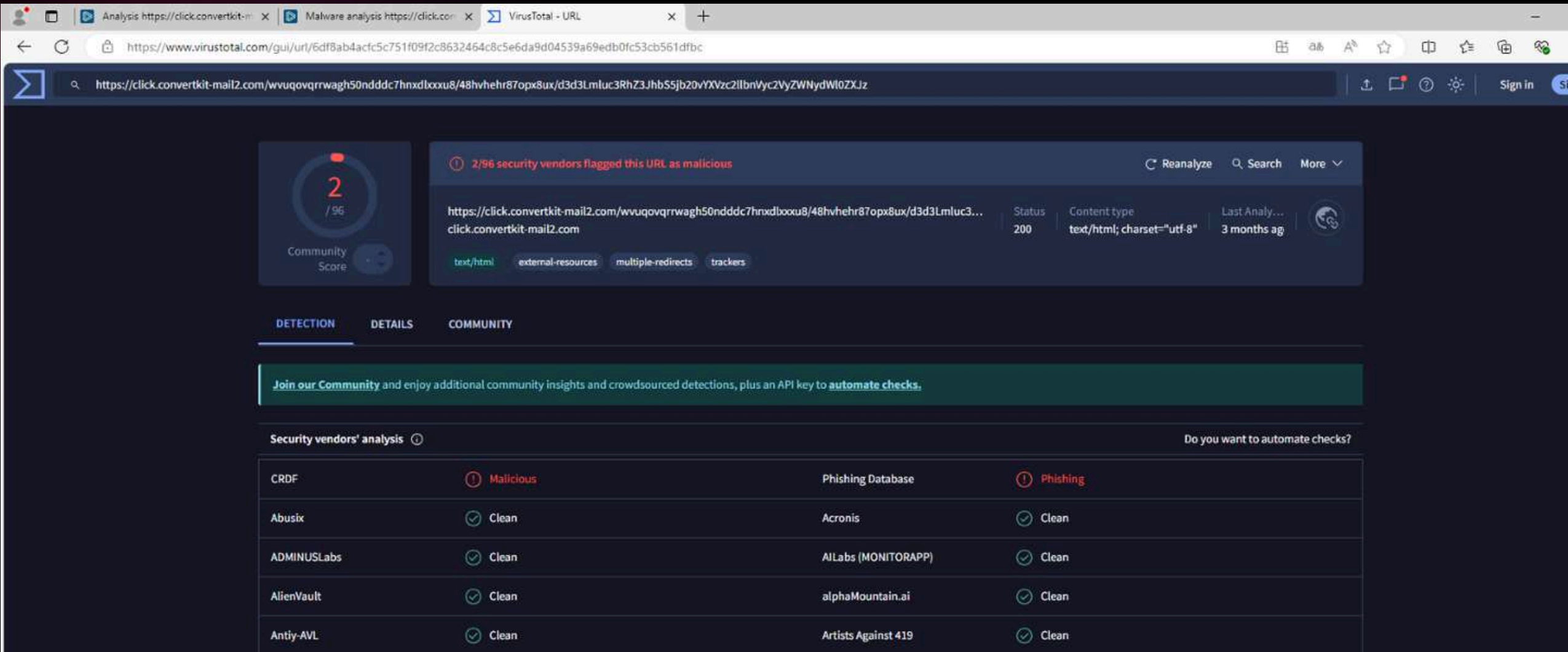


Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.104.136.2
BEFORE	Responded	✓	google.com	172.217.16.206
				3.141.222.179
6205 ms	Responded	✓	click.convertkit-mail2.com	3.18.56.123
				18.220.225.51
6207 ms	Requested	✓	click.convertkit-mail2.com	IP Addresses not found

Info [6584] chrome.exe Reads Microsoft Office registry keys



Attenzioniamo ogni IP delle DNS requests, tra cui troviamo un domain sospetto “click.convertkit-mail2.com”,



analizzandolo su virustotal restituisce un valore molto interessante: solo 2 su 96 analisti di sicurezza considera questo link sospetto e nello specifico è stato segnalato come tentativo di phishing.

Statisticamente è abbastanza basso come risultato ma merita comunque massima attenzione, ragione per cui, continuiamo con l’analisi.

Uno degli aspetti più innovativi e sorprendenti di anyrun è la possibilità di ottenere un report delle minacce, così da semplificare anche il nostro lavoro da analisti:

Ampliando le DNS requests

DNS requests		
Domain	IP	Reputation
settings-win.data.microsoft.com	51.104.136.2	whitelisted
google.com	172.217.16.206	whitelisted
click.convertkit-mail2.com	3.141.222.179 3.18.56.123 18.220.225.51	whitelisted
accounts.google.com	66.102.1.84	whitelisted
www.instagram.com	157.240.0.174	whitelisted
static.cdninstagram.com	157.240.0.63	whitelisted

Controlliamo gli IP del dominio sospetto, su virus total e notiamo i risultati.

1 / 94

Community Score

1/94 security vendor flagged this IP address as malicious

Reanalyze Similar More

3.141.222.179 (3.128.0.0/10)

US Last Analysis Date 3 days ago

AS 16509 (AMAZON-02)

DETECTION

DETAILS

RELATIONS

COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antly-AVL	Clean
benkow.cc	Clean	BitDefender	Clean

1 / 94

Community Score

1/94 security vendor flagged this IP address as malicious

Reanalyze Similar More

3.18.56.123 (3.16.0.0/13)

US Last Analysis Date 3 days ago

AS 16509 (AMAZON-02)

DETECTION

DETAILS

RELATIONS

COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antly-AVL	Clean

1 / 94

Community Score

1/94 security vendor flagged this IP address as malicious

Reanalyze Similar More

18.220.225.51 (18.216.0.0/13)

US Last Analysis Date 3 days ago

AS 16509 (AMAZON-02)

DETECTION

DETAILS

RELATIONS

COMMUNITY

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

Security vendors' analysis

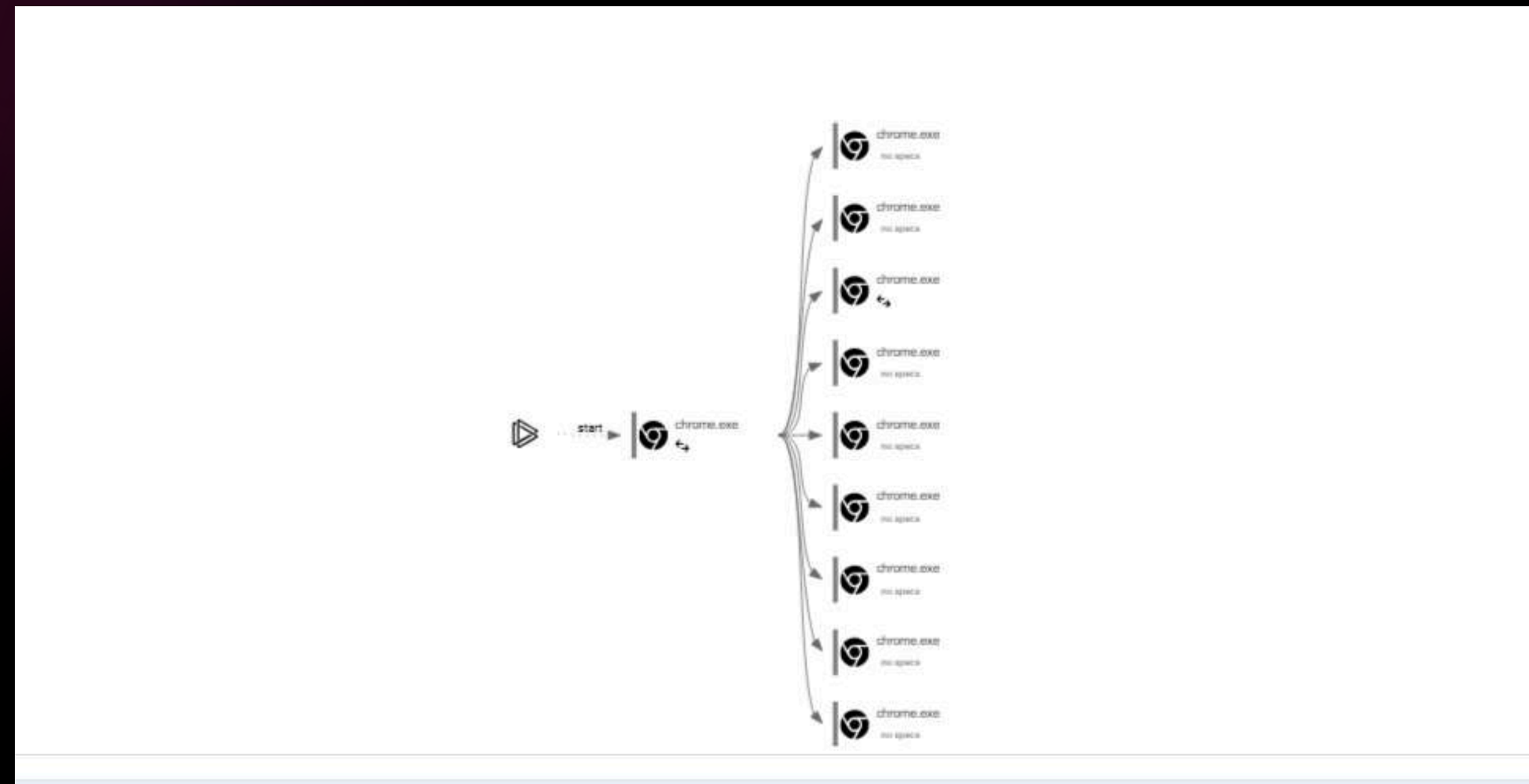
Do you want to automate checks?

Criminal IP	Malicious	ArcSight Threat Intelligence	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

Pur essendo una valutazione abbastanza bassa, la percezione è che ci sia molto altro.

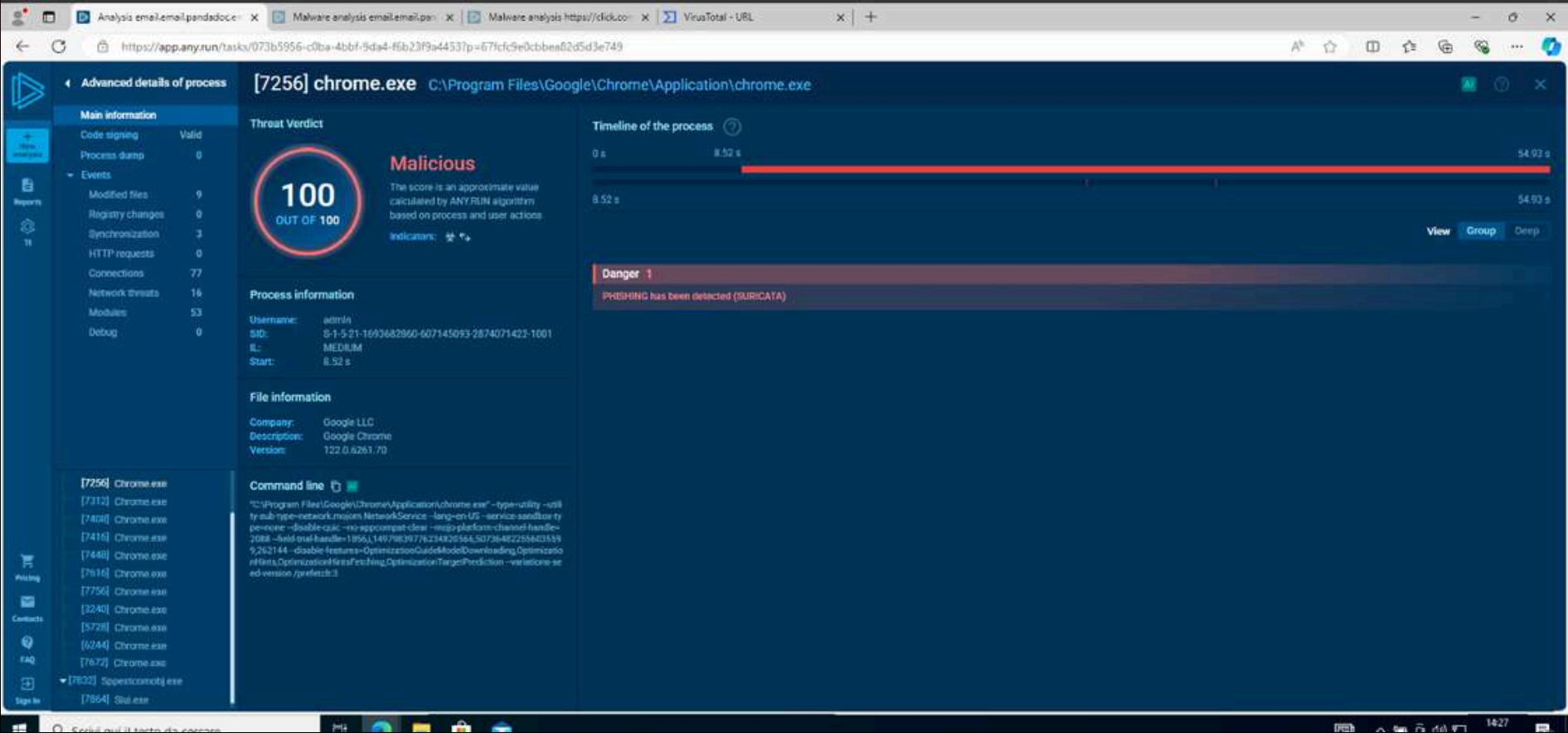


Quindi procediamo all'analisi del report generato e cerchiamo il process tree che si rivela altamente sospetto,



In ragione al fatto che un singolo processo, nello specifico Chrome.exe avvia altre 10 istanze contemporaneamente. E conoscendo le abitudini di un utente tipico, apre una singola finestra di Chrome o diverse schede in modo sequenziale mentre l'avvio simultaneo dallo stesso processo genitore suggerisce sicuramente un'attività automatizzata e quindi potenzialmente dannosa.

A questo punto, andando sui dettagli avanzati del processo, osserviamo il verdetto:

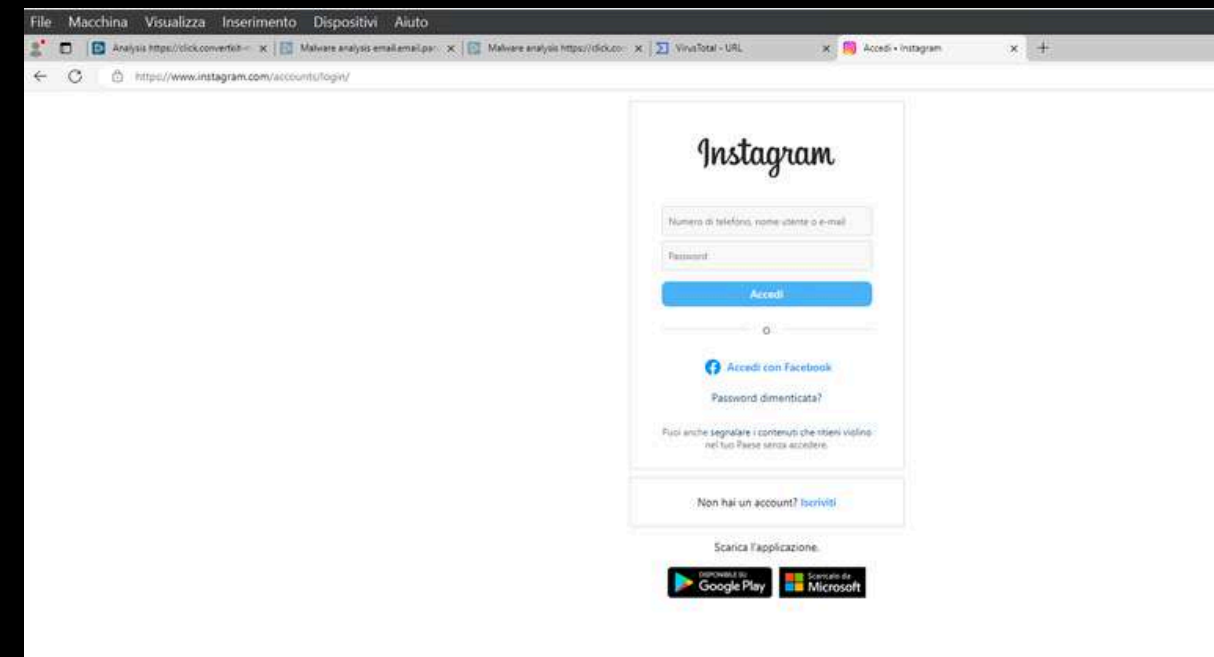
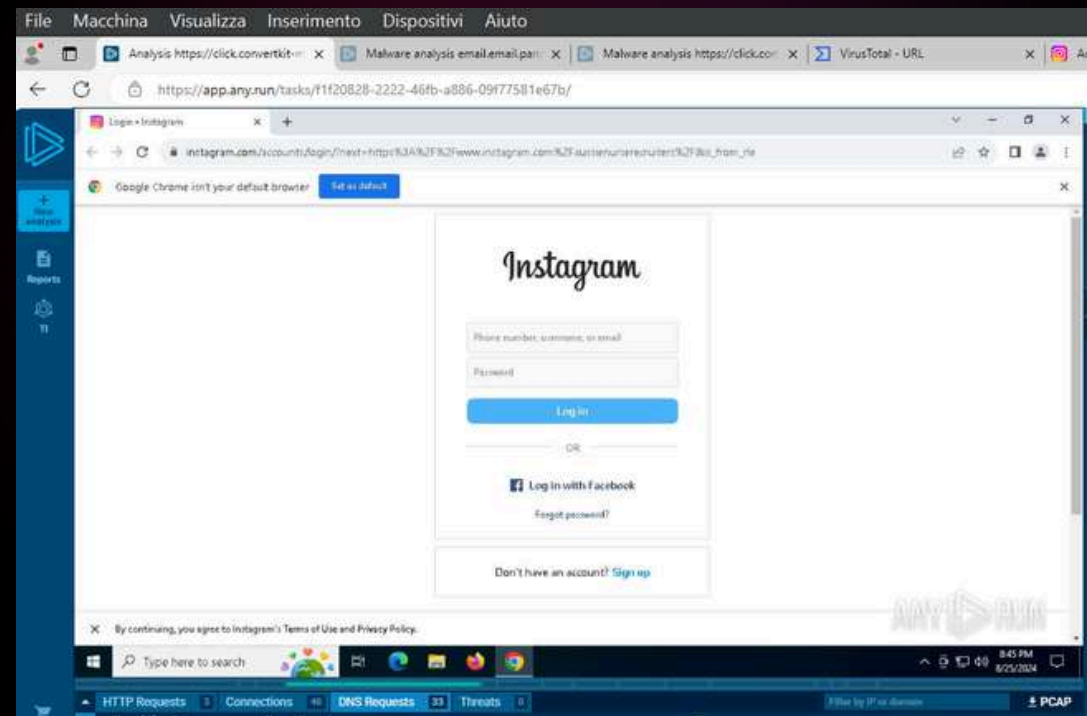


100 su 100 Malicious.

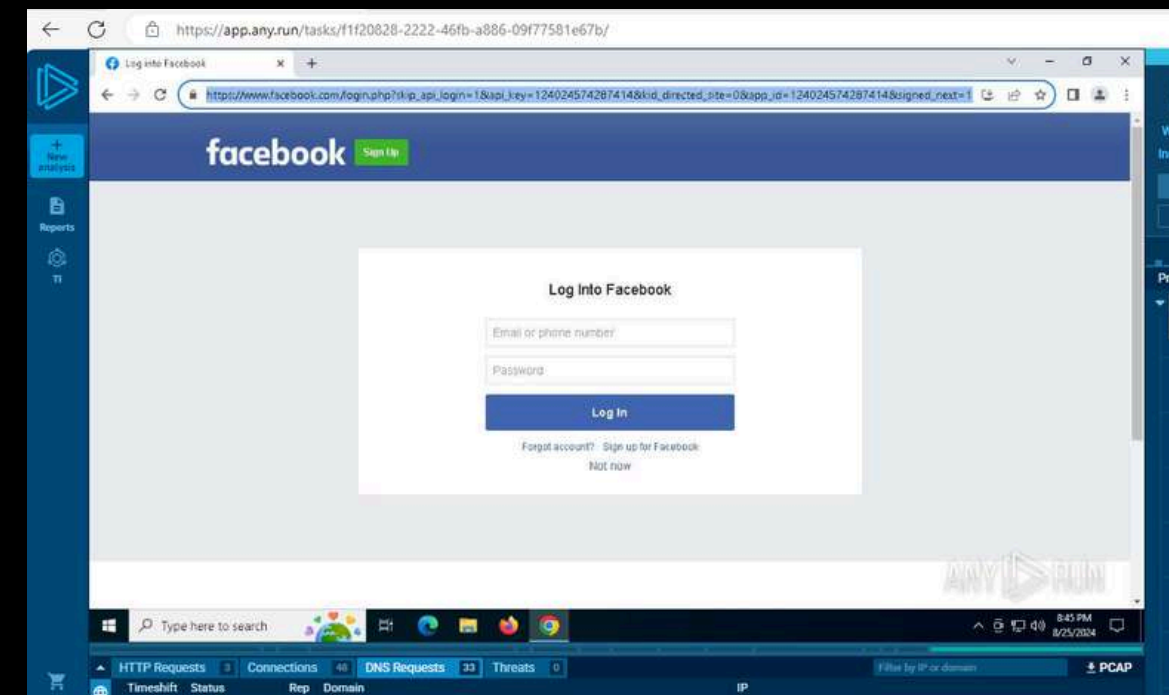
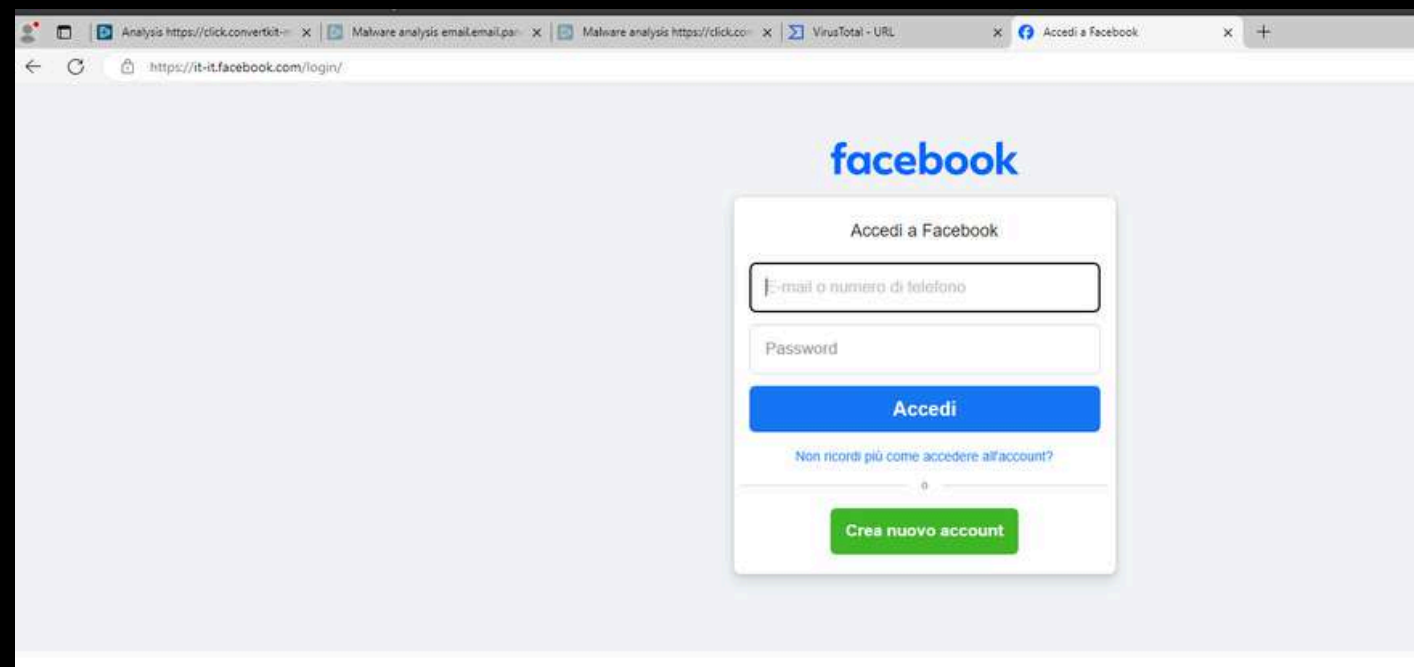
E non solo quello che all’inizio sembrava un sospetto di phishing, viene confermato da suricata.

A questo punto, in base agli screen forniti nel link, facciamo una controprova:

Lo screen presente mostra la schermata di accesso su Instagram, con un determinato link ma se andiamo a cercare, esattamente la stessa pagina di login, osserviamo che il link è differente



stesso discorso per quanto riguarda il login di Facebook





# REMEDIATION

L'analisi di un link inizialmente sottovalutato come minaccia ha rivelato un sofisticato tentativo di phishing, evidenziando la necessità di meccanismi di difesa che vadano oltre la semplice reputazione dei domini. Per affrontare efficacemente questa tipologia di minaccia, si propone l'implementazione di una strategia di remediation multi-livello focalizzata sull'analisi comportamentale e contestuale direttamente all'interno del browser aziendale.

Un approccio primario consiste nell'integrare un sistema di "honeypot dinamico" a livello di browser. Questo sistema presenta elementi interattivi "esca" su pagine web sospette, permettendo di rilevare attivamente interazioni anomale tipiche di tentativi di phishing o attività automatizzate, anche in presenza di bassi segnali di allarme tradizionali. Parallelamente, si suggerisce l'implementazione di un sistema di "analisi comportamentale in tempo reale" delle interazioni utente. Questo monitorerebbe le sequenze di azioni all'interno delle pagine web sospette, correlando pattern inusuali con l'attività dei processi del browser per identificare comportamenti malevoli.

# REMEDIATION

Inoltre, per contrastare la discrepanza tra il contenuto visualizzato e il link effettivo, si raccomanda lo sviluppo di un "plugin di autenticazione visiva contestuale". Questo strumento analizzerebbe visivamente le pagine di login confrontandole con database di siti legittimi e verificando la coerenza con il dominio visualizzato, allertando l'utente in caso di incongruenze.

Infine, per una valutazione rapida e autonoma dei link sospetti, si propone l'integrazione di un sistema di "sandboxing dinamico on-demand" direttamente nel browser. Questo permetterebbe agli utenti o al sistema di analizzare in isolamento il comportamento di un link, fornendo un feedback immediato sul potenziale rischio e inviando automaticamente i risultati per un'analisi più approfondita se necessario.

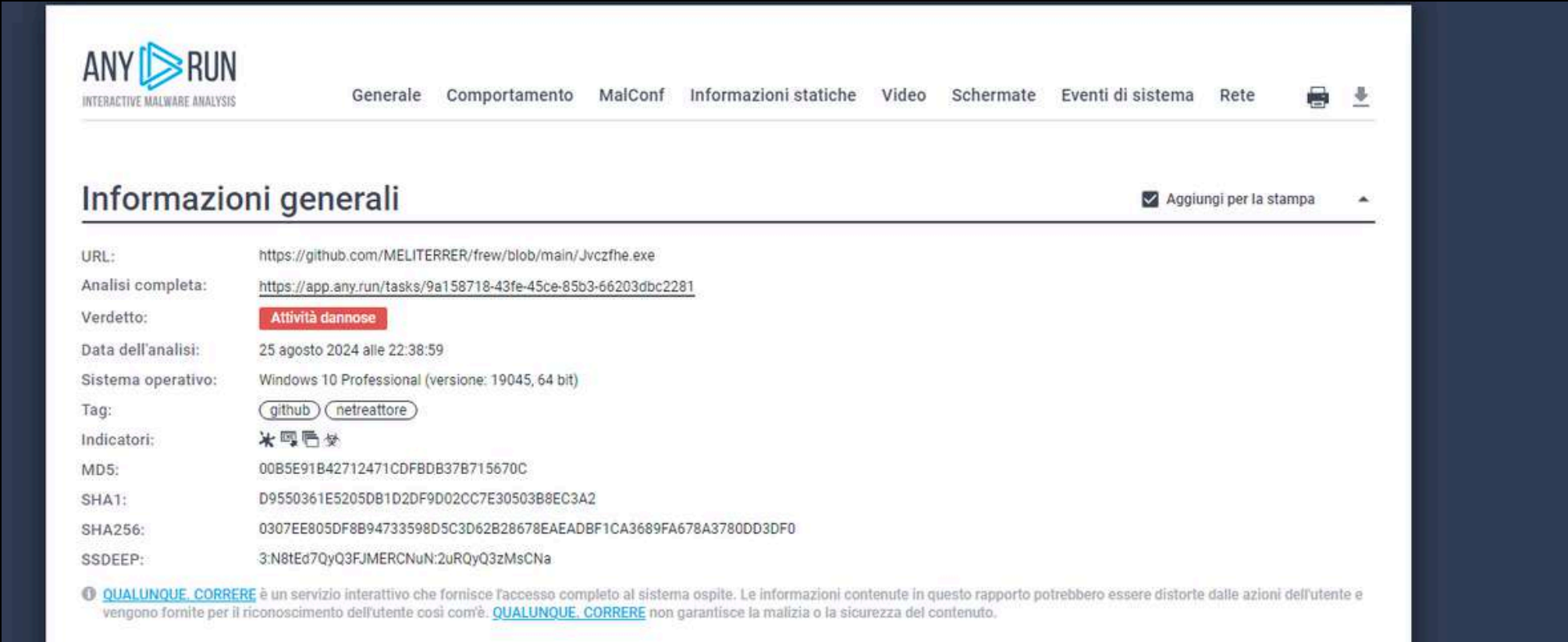
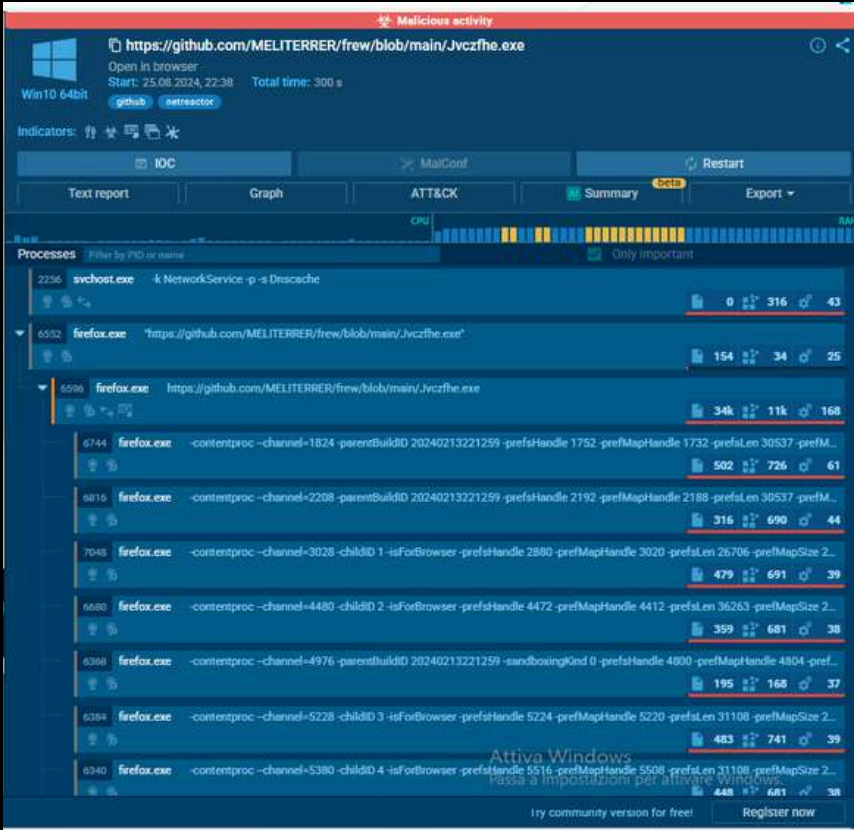
L'adozione combinata di queste strategie, incentrate sull'analisi comportamentale, contestuale e sulla capacità di analisi locale, mira a rafforzare la resilienza contro attacchi di phishing evoluti, riducendo la dipendenza da valutazioni esterne iniziali e fornendo meccanismi di rilevamento e allerta più proattivi e mirati direttamente all'interno dell'ambiente di navigazione dell'utente.



**Terzo link sospetto**



L’analisi del nostro laboratorio ha rilevato una serie di indicatori di compromissione (IOC) che confermano, di fatto, la presenza di attività malevole sul sistema, in quanto i comportamenti osservati non sono compatibili con l’uso lecito della macchina e indicano chiaramente una compromissione.



I primi campanelli d’allarme li troviamo con l’esecuzione di malware: Jvezfhe.exe ossia un processo sconosciuto, non legittimo in quanto avvia cmd.exe per eseguire comandi in background.

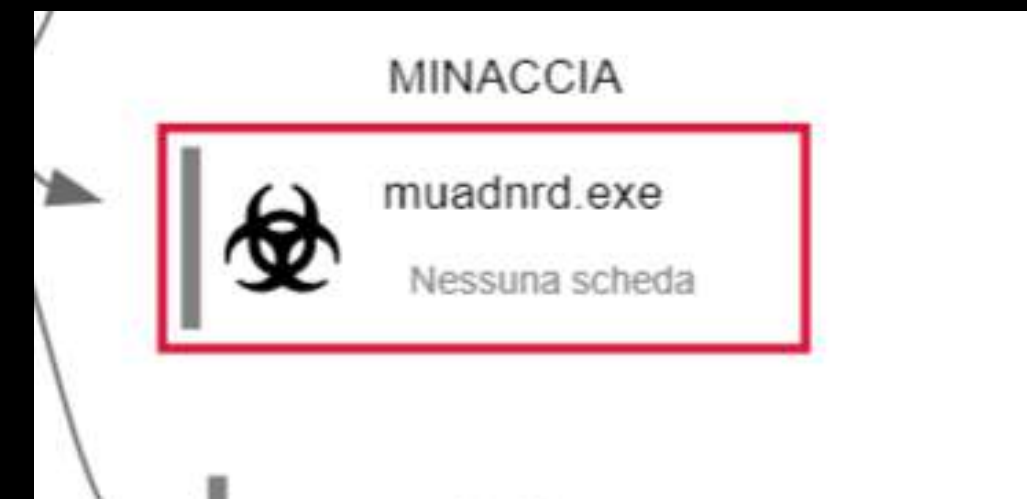
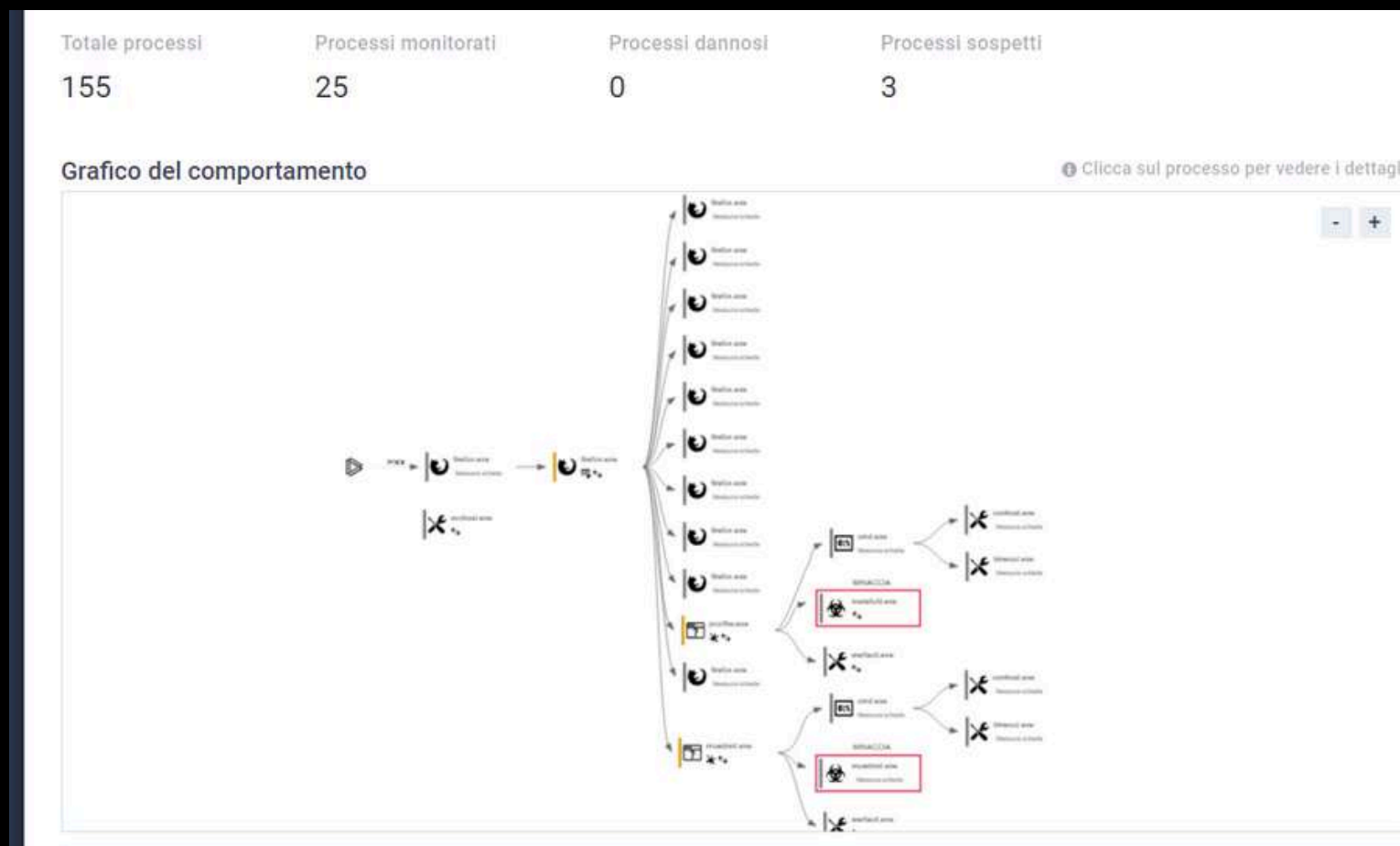
Informazioni sul processo				
PID	CMD	Sentiero	Indicatori	Processo padre
1356	C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676	C:\Windows\SysWOW64\WerFault.exe		Jvczfhe.exe
Informazione				
Utente:	Admin	Società:	Società Microsoft	
Livello di integrità:	MEDIO	Descrizione:	Segnalazione problemi di Windows	
Codice di uscita:	0	Versione:	10.0.19041.3995 (WinBuild.160101.0800)	
Moduli				
Immagini				
C:\Windows\Syswow64\ucrtbase.dll				
C:\Windows\Syswow64\iprct4.dll				
C:\Windows\Syswow64\oleaut32.dll				
C:\Windows\Syswow64\cryptsp.dll				
C:\Windows\Syswow64\msvc_p_win.dll				
C:\Windows\Syswow64\sechost.dll				
C:\Windows\Syswow64\bcrypt.dll				
C:\Windows\Syswow64\advapi32.dll				
C:\Windows\Syswow64\ntcore.dll				

Inoltre interroga impostazioni di sicurezza del sistema (Internet Explorer e Windows Trust Settings). Con il chiaro obiettivo di identificare e aggirare le barriere di sicurezza. Questi comportamenti sono tipici di malware perchè preparano il sistema all’esecuzione di payload dannosi o alla persistenza.

MALIGNO	SOSPETTOSO	INFORMAZIONI
Nessun indicatore dannoso.	<p>Il processo elimina l'eseguibile legittimo di Windows</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul> <p>Avvia CMD.EXE per l'esecuzione dei comandi</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Utilizza TIMEOUT.EXE per ritardare l'esecuzione</p> <ul style="list-style-type: none"><li>• cmd.exe (PID: 7520)</li><li>• cmd.exe (PID: 7876)</li></ul> <p>Controlla le impostazioni di attendibilità di Windows</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Legge le impostazioni di sicurezza di Internet Explorer</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Esegue l'applicazione che si arresta in modo anomalo</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Si collega a una porta insolita</p> <ul style="list-style-type: none"><li>• InstallUtil.exe (PID: 5152)</li></ul> <p>L'applicazione è stata avviata da sola</p> <ul style="list-style-type: none"><li>• Muadnrd.exe (PID: 7824)</li></ul>	<p>L'applicazione è stata avviata da sola</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6552)</li><li>• firefox.exe (PID: 6596)</li></ul> <p>Legge le chiavi del Registro di sistema di Microsoft Office</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul> <p>Il contenuto dell'eseguibile è stato eliminato o sovrascritto</p> <ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul> <p>Controlla le lingue supportate</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li><li>• InstallUtil.exe (PID: 5152)</li></ul> <p>Legge il nome del computer</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li><li>• InstallUtil.exe (PID: 5152)</li></ul> <p>Legge il GUID del computer dal Registro di sistema</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul> <p>Disabilita i log di traccia</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul> <p>Legge i valori dell'ambiente</p> <ul style="list-style-type: none"><li>• Jvczfne.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li></ul>

Legge il GUID del computer dal Registro di sistema
• Jvczfne.exe (PID: 7492)
• InstallUtil.exe (PID: 5152)
• Muadnrd.exe (PID: 7824)
• Muadnrd.exe (PID: 7248)
Disabilita i log di traccia
• Jvczfne.exe (PID: 7492)
• Muadnrd.exe (PID: 7824)
Legge i valori dell'ambiente
• Jvczfne.exe (PID: 7492)
• InstallUtil.exe (PID: 5152)
• Muadnrd.exe (PID: 7824)
Controlla le informazioni sul server proxy
• Jvczfne.exe (PID: 7492)
• WerFault.exe (PID: 1356)
• Muadnrd.exe (PID: 7824)
• WerFault.exe (PID: 7584)
Legge le impostazioni dei criteri software
• Jvczfne.exe (PID: 7492)
• WerFault.exe (PID: 1356)
• Muadnrd.exe (PID: 7824)
• WerFault.exe (PID: 7584)
Crea file o cartelle nella directory utente
• WerFault.exe (PID: 1356)
• WerFault.exe (PID: 7584)
È stata rilevata la protezione .NET Reactor
• InstallUtil.exe (PID: 5152)
• Muadnrd.exe (PID: 7248)

Un ulteriore utilizzo sospetto è quello di InstallUtil.exe, un eseguibile legittimo del framework .NET, comunemente sfruttato da attori malevoli per eseguire codice. Questo stabilisce connessioni su porte non standard, potenzialmente verso server di controllo remoto. Dalla nostra analisi emerge la minaccia e viene considerato sospetto perchè InstallUtil viene spesso utilizzato in attacchi per eludere antivirus, sfruttando la sua natura “trusted” per eseguire codice malevolo senza rilevamento.



Muadnrd.exe è una variante del malware principale, si esegue autonomamente senza trigger manuali, ripete gli stessi comportamenti: interrogazione delle impostazioni di sicurezza, uso di cmd.exe, creazione di file e cartelle. Dalla nostra analisi risulta sospetto perchè l'auto-esecuzione e l'interazione con le impostazioni di sistema indicano un chiaro tentativo di ottenere persistenza e controllo.

WerFault.exe ossia un processo di Windows utilizzato per la gestione di errori che viene sfruttato per creare file e cartelle e modificare configurazioni di sistema. Questo processo viene segnalato come sospetto perchè il processo viene strumentalizzato per introdurre modifiche persistenti e silenziose, mascherando le operazioni sotto un'applicazione di sistema.



Abbiamo anche osservato i tentativi di tecniche evasive con l'uso di timeout.exe , volto al ritardo dell'esecuzione per sfuggire a sandbox o comunque ad analisi automatizzate, inoltre anche connessioni verso DNS sospetti e porte non standard come tentativi di comunicazione con server di comando e controllo e disattivazione delle funzioni di tracciamento, bypass del proxy.

Quindi, l'insieme dei comportamenti rilevati conferma con elevata certezza che:

Il sistema è stato compromesso da uno o più malware, sono in atto tecniche di persistenza, evasione dei controlli e comunicazione remota.

È quindi molto probabile che un loader (malware che carica altri payload) sia stato eseguito per innescare queste azioni.

## REMEDICATION

A seguito della compromissione rilevata, è necessario intervenire con urgenza per contenere la minaccia, ripristinare la sicurezza del sistema e prevenire ulteriori impatti. La prima azione da intraprendere è l'isolamento immediato della macchina compromessa dalla rete, sia cablata che wireless, al fine di interrompere qualsiasi potenziale comunicazione con server remoti o tentativi di movimento laterale all'interno della rete aziendale.

Successivamente, si raccomanda una bonifica completa del sistema attraverso strumenti EDR o antivirus avanzati. Tuttavia, considerata la natura delle attività malevole osservate (persistenza, esecuzione stealth, uso di tool legittimi), è fortemente consigliato il ripristino del sistema tramite formattazione, per garantire l'eliminazione totale del malware e di eventuali backdoor.

Parallelamente, è fondamentale effettuare una verifica approfondita degli altri endpoint collegati alla stessa rete, per identificare eventuali compromissioni collaterali.

Questa attività dovrebbe includere il controllo di accessi anomali, processi sospetti e comunicazioni tra dispositivi.

Si raccomanda inoltre di monitorare il traffico di rete, in particolare quello DNS e le connessioni in uscita verso domini o IP non riconosciuti, con attenzione alle porte non standard. Ciò permetterà di identificare attività residue del malware o tentativi di esfiltrazione dati.

Infine, è necessario attivare formalmente la procedura di incident response, coinvolgendo il team di sicurezza per raccogliere log, preservare eventuali evidenze forensi, documentare l'incidente e implementare misure correttive. Questo passaggio è cruciale per limitare l'impatto, comprendere l'origine dell'attacco e rafforzare la postura di sicurezza dell'infrastruttura.



# LABORATORY

**In this series of labs, we carried out the following activities:**

1. Familiarization with Linux systems
2. PCAP file extraction and analysis
3. Investigation of SQL injection and DNS exfiltration
4. Isolation of a compromised host using the 5-tuple





# **Lab – Navigating the Linux Filesystem and Permission Settings**

Nella slide 1 per prima cosa utilizzo il comando `lsblk` che mostra i dispositivi a blocchi (es: `/dev/sda`, `/dev/sdb`) e le partizioni. Il comando `mount` mostra invece tutti i file system montati in Linux. Un file system è il metodo con cui i file vengono organizzati e memorizzati su un disco (HDD, SSD, USB, ecc.). Ne esistono di vari tipi: `ext4` che è un file system predefinito per Linux (journaling, affidabile), `NTFS` supporta permessi avanzati e file grandi usati in Windows `FAT32` senza permessi ed è compatibile con tutti i sistemi (ma ha un limite ossia file <4GB) ed è utilizzato per le chiavette usb. `Tmpfs` file system in RAM (veloce ma volatile). In questo caso, siamo interessati al file system di `sda` quindi utilizziamo il comando `mount | grep sda` per isolarlo e analizzarlo. Il risultato mostra che il file system di `/dev/sda1` è montato come root file system (/) con file system `ext4`. Con il comando `ls -l` eseguito nella cartella root "/" troviamo la cartella `dev` nella quale è montato `sda`. Il file system del disco rigido `sdb` non è ancora montato in `dev` quindi andiamo a montarlo.

```
[analyst@sec0ps ~]$ 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@sec0ps ~]$ 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 Apr 14 06:53 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 118 root root 0 Apr 14 06:53 proc
drwxr-xr-x 7 root root 4096 Apr 17 2018 root
drwxr-xr-x 17 root root 480 Apr 14 06:53 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 Apr 14 06:53 sys
drwxrwxrwt 8 root root 200 Apr 14 06:54 tmp
drwxr-xr-x 9 root root 4096 Apr 17 2018 usr
drwxr-xr-x 12 root root 4096 Apr 17 2018 var
```

```
[analyst@sec0ps ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=500780k,nr_inodes=125195,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nodelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=28,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=10463)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
mqueue on /dev/mqueue type mqueue (rw,relatime)
configfs on /sys/kernel/config type configfs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=101288k,mode=700,uid=1000,gid=1000)
```

```
[analyst@sec0ps ~]$ mount | grep sda1
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
```



Nella slide 2 entro nella home dell'utente analyst e poi nella cartella second\_drive per creare la partizione del file system, ma prima con ls vedo che la cartella è vuota. Con il comando sudo mount /dev/sdb1 ~/second\_drive/ montiamo il file system sdb1 dentro second\_drive, mentre con ls -l second\_drive/ vediamo le informazioni dei files contenuti dentro di esso, così come il loro proprietario, i permessi, il nome, il tipo etc. Con mount | grep sdb1 adesso vediamo la partizione di sdb e i dettagli relativi come il path, il tipo di file system e le opzioni. Se volessimo smontare il file system basterebbe eseguire il comando sudo umount /dev/sdb1.

```
[analyst@sec0ps ~]$ cd second_drive/
[analyst@sec0ps second_drive]$ ls
[analyst@sec0ps second_drive]$

[analyst@sec0ps ~]$ 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@sec0ps ~]$

[analyst@sec0ps ~]$ mount | grep /dev/sdb1
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime,data=ordered)
[analyst@sec0ps ~]$

[analyst@sec0ps second_drive]$ cd
[analyst@sec0ps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@sec0ps ~]$
```



Nella slide 3 andiamo a testare le autorizzazioni del file system, grazie alle funzionalità integrate di Linux. Per prima cosa eseguiamo `cd lab.support.files/scripts/` per entrare in scripts, poi `ls -l` sempre per vedere informazioni sui file contenuti e le autorizzazioni. Le colonne dalla 2 alla 4 mostrano i permessi degli utenti. La colonna 2 mostra i permessi dell'utente "proprietario", la 3 del suo "gruppo" mentre la 4 di "altri". Nella colonna 6 e 7 si può vedere chi sono rispettivamente il proprietario e il gruppo di cui fa parte. Poi utilizziamo il comando `touch /mnt/myNewFile.txt` che permette di creare un file di testo vuoto velocemente ma viene negato il permesso. Infatti se andiamo a vedere i permessi della cartella `mnt` con `ls -ld /mnt` notiamo che il proprietario è `root`, mentre noi siamo loggati come `analyst` e le autorizzazioni della cartella che riguardano "altri" (quindi la 4 colonna), sono settate su `r-x` quindi su lettura ed esecuzione, ma non sulla scrittura (`w`).

```
[analyst@secOps ~]$ cd lab.support.files/scripts/
[analyst@secOps scripts]$ ls
configure-as.dhcp.sh      cyops.nn                start-llik.sh
configure-as.static.sh    fw.rules                start-miniedit.sh
cyberops-extended-topo-no-fw.py  mail-server.start.sh  start-pox.sh
cyberops-extended-topo.py  net.configuration.files start-smart.sh
cyberops-topo.py          reg-server.start.sh     start-tftpd.sh
[analyst@secOps scripts]$

[analyst@secOps scripts]$ ls -l
total 60
-rwxr-xr-x 1 analyst analyst 952 Mar 21 2018 configure-as.dhcp.sh
-rwxr-xr-x 1 analyst analyst 1153 Mar 21 2018 configure-as.static.sh
-rwxr-xr-x 1 analyst analyst 3459 Mar 21 2018 cyberops-extended-topo-no-fw.py
-rwxr-xr-x 1 analyst analyst 4062 Mar 21 2018 cyberops-extended-topo.py
-rwxr-xr-x 1 analyst analyst 2669 Mar 21 2018 cyberops-topo.py
-rwxr-xr-x 1 analyst analyst 2871 Mar 21 2018 cyops.nn
-rwxr-xr-x 1 analyst analyst 458 Mar 21 2018 fw.rules
-rwxr-xr-x 1 analyst analyst 70 Mar 21 2018 mail-server.start.sh
-rwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 net.configuration.files
-rwxr-xr-x 1 analyst analyst 65 Mar 21 2018 reg-server.start.sh
-rwxr-xr-x 1 analyst analyst 189 Mar 21 2018 start-llik.sh
-rwxr-xr-x 1 analyst analyst 85 Mar 21 2018 start-miniedit.sh
-rwxr-xr-x 1 analyst analyst 76 Mar 21 2018 start-pox.sh
-rwxr-xr-x 1 analyst analyst 106 Mar 21 2018 start-smart.sh
-rwxr-xr-x 1 analyst analyst 61 Mar 21 2018 start-tftpd.sh
[analyst@secOps scripts]$

[analyst@secOps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@secOps scripts]$

[analyst@secOps scripts]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan 5 2018 /mnt
[analyst@secOps scripts]$

[analyst@secOps second-drive]$ sudo chmod 777 myFile.txt
[analyst@secOps second-drive]$ ls -l
total 20
-rwxr-xr-x 2 root root 16384 Mar 26 2018 lost+found
-rwxr-xr-x 1 analyst analyst 183 Mar 26 2018 myFile.txt
[analyst@secOps second-drive]$

[analyst@secOps second-drive]$ echo test >> myFile.txt

[analyst@secOps second-drive]$ cat myFile.txt
This is a file stored in the /dev/sdb1 disk.
Notice that even though this file has been sitting in this disk for a while, it couldn't be accessed until the disk was properly mounted.
test
[analyst@secOps second-drive]$
```

In questo caso quello che si può fare è testare il comando con sudo cioè i permessi di super user, (meccanismo che concede temporaneamente permessi root a utenti normali). Nella slide 2 quando abbiamo testato le autorizzazioni dei file dentro second\_drive abbiamo notato che myFile.txt erano configurate su -rw-r--r-- e che il proprietario è analyst. Proviamo a modificare le autorizzazioni con il comando chmod. Con chmod 777 myFile.txt possiamo dare qualsiasi autorizzazione a chiunque. I permessi sono gestiti nel formato ottale cioè da 0 a 7. Ad esempio 0 non dà nessun permesso mentre 1 dà i permessi di esecuzione, 2 di scrittura, 4 di lettura. L'unione di questi numeri dà i relativi permessi quindi 7 li dà tutti e 3. Esistono anche 3 bit extra (SUID, SGID, Sticky Bit) che si possono configurare nei file. SUID (Set User ID), che fa eseguire un file con i permessi del proprietario. SGID (Set Group ID) è come il SUID, ma per quanto riguarda tutto il gruppo. Sticky Bit : protegge i file in directory condivise (es: /tmp). Se volessimo modificare anche il proprietario potremmo usare il comando chown. Per modificare contemporaneamente sia proprietario che gruppo, possiamo utilizzare i due punti " : " ad esempio chown proprietario:gruppo test.txt poi eseguiamo echo test >> myFile.txt per scrivere "test" su myFile.txt e aprendo il file con cat vediamo che "test" è correttamente scritto sul file di testo.







Il primo comando `ln -s` è un *symbolic link*, ossia un link che collega `file1symbolic` a il file `file1.txt`. Ogni cosa che modificheremo all'interno di `file1.txt` verrà modificata anche in `file1symbolic`. Ma eliminando o rinominando `file1.txt`, `file1symbolic` diventerebbe un file vuoto. Mentre il comando `ln` crea un *hard link*, ovvero un link che collega un file (`file2hard`) al "contenuto" di un altro file (`file2.txt`).

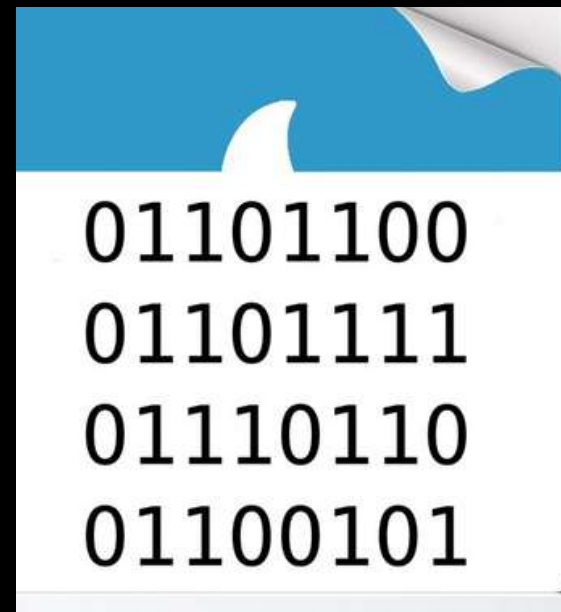
Se rinominiamo o cancelliamo il file originale, continuerà ad esistere il contenuto nel file linkato, quindi è più resiliente. Come mostrato nelle slide, una volta linkati i 2 file, eseguendo `ls -l`, nella cartella vedremo che il file (`file1symbolic`) è linkato a `file1.txt` tramite *symbolic link* attraverso la freccetta mentre `file2hard` e `file2.txt` hanno l'*hard link count* settato a 2 (la colonna 5), ovvero il numero di link fisici al file. Facendo invece dei test rinominando i file originali con il comando `mv` dimostriamo invece quanto detto in precedenza sui link.

```
[analyst@sec0ps ~]$ sudo echo "symbolic" > file1.txt
[analyst@sec0ps ~]$ cat file1.txt
symbolic
[analyst@sec0ps ~]$ echo "hard" > file2.txt
[analyst@sec0ps ~]$ cat file2.txt
hard
[analyst@sec0ps ~]$

[analyst@sec0ps ~]$ ln -s file1.txt file1symbolic
[analyst@sec0ps ~]$ ln file2.txt file2hard
[analyst@sec0ps ~]$

[analyst@sec0ps ~]$ ls -l
total 28
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 Downloads
drwxrwxrwx 1 analyst analyst  9 Apr 14 09:55 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst  9 Apr 14 09:42 file1.txt
-rw-r--r-- 2 analyst analyst  5 Apr 14 09:42 file2hard
-rw-r--r-- 2 analyst analyst  5 Apr 14 09:42 file2.txt
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@sec0ps ~]$

[analyst@sec0ps ~]$ mv file1.txt file1new.txt
[analyst@sec0ps ~]$ mv file2.txt file2new.txt
[analyst@sec0ps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@sec0ps ~]$ cat file2hard
hard
[analyst@sec0ps ~]$
```



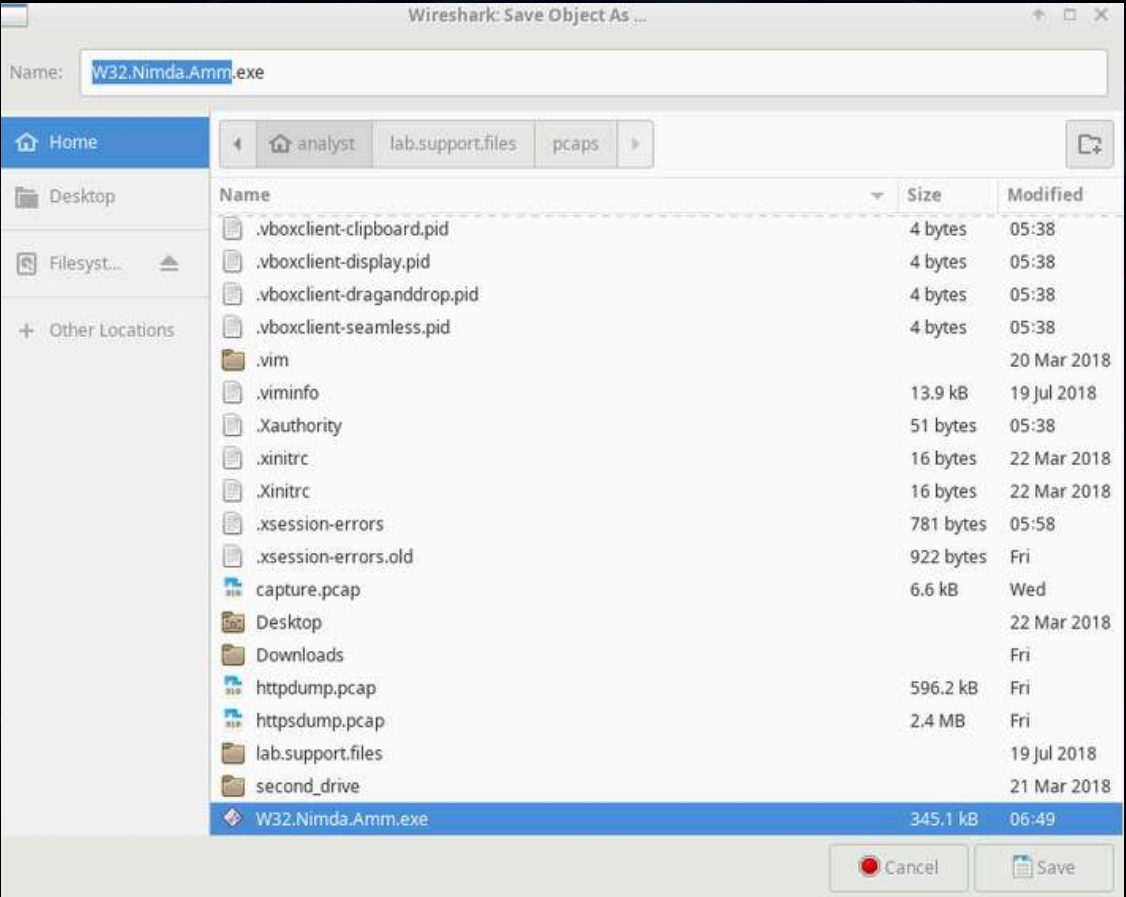
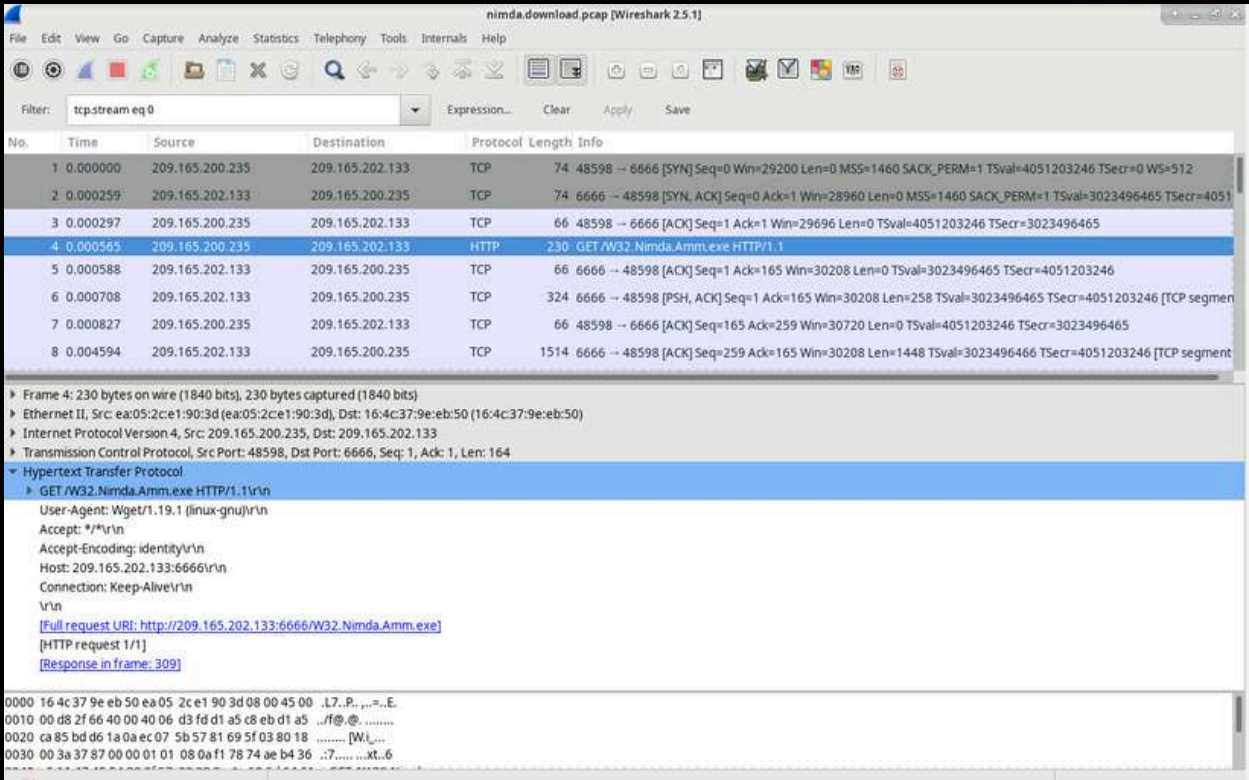
# Lab – Extract an Executable from a PCAP



Abbiamo analizzato una cattura pacchetti di un worm chiamato Nimda.

Prima di tutto il worm chiede un 3 way hand-shake, una volta avviata la connessione TCP manda una richiesta HTTP GET e così il worm riesce a moltiplicarsi e a spostarsi sulla rete.

Una volta capito come il worm opera abbiamo esportato l'oggetto dalla cattura PCAP a un file .EXE e abbiamo capito fosse un'eseguibile windows.





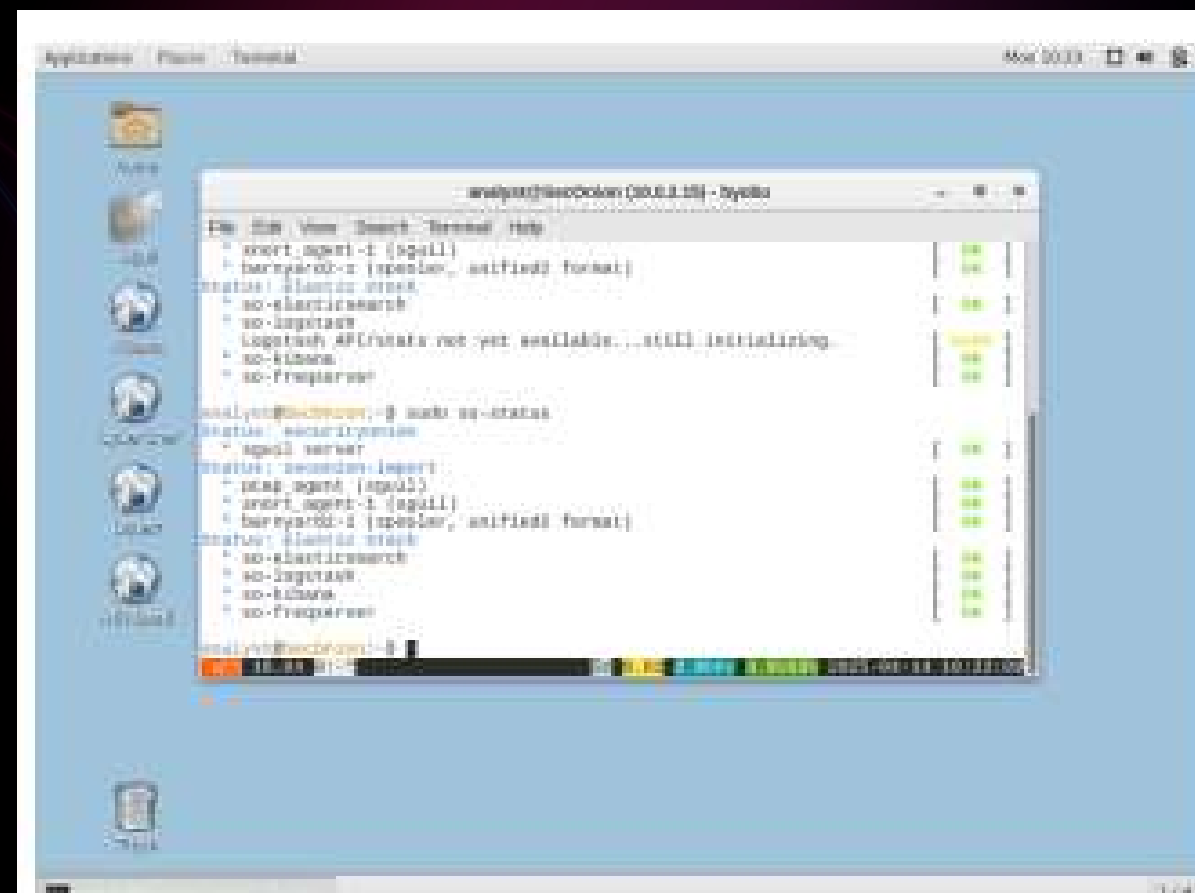


# **Lab – Interpret HTTP and DNS Data to Isolate Threat Actor**

## **INTRODUZIONE:**

*Questo laboratorio analizzeremo log di traffico HTTP e DNS per individuare attività malevole e capire quali dati sono stati esfiltrati da un Threat Actor . Utilizzeremo gli strumenti di Security Onion (in particolare Kibana), per visualizzare i log generati da Zeek/Bro e capME!, per esaminare le tracce di traffico al fine di investigare su due scenari: (1) un attacco SQL Injection che ha colpito un server web esponendo dati sensibili via HTTP; (2) un caso di esfiltrazione di dati via DNS mediante query DNS anomale.*

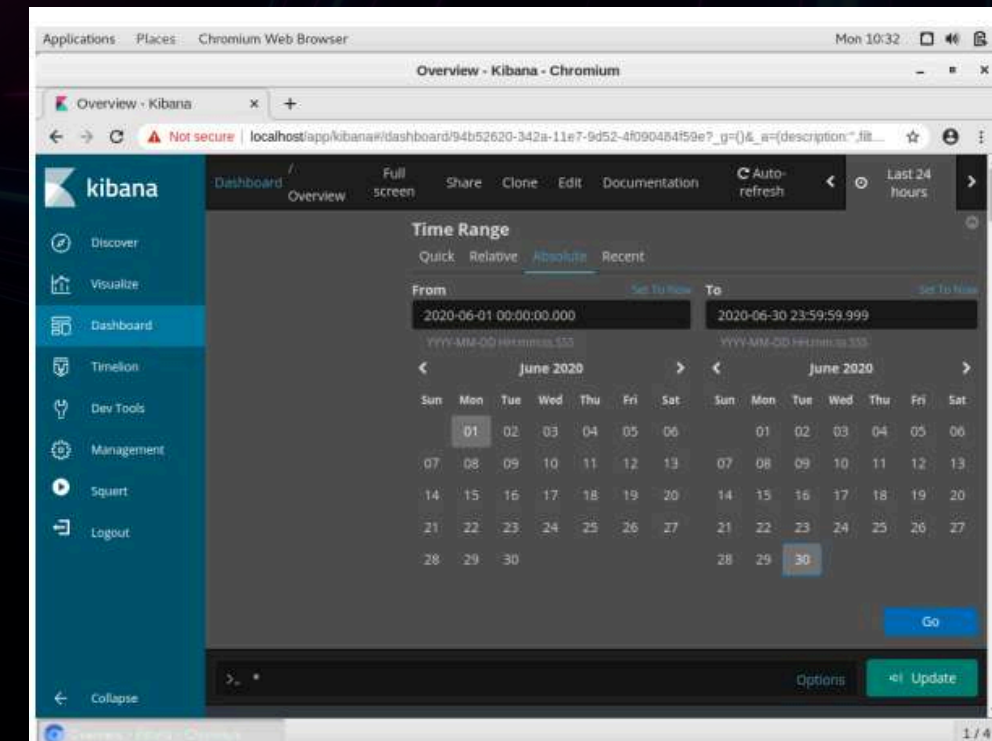
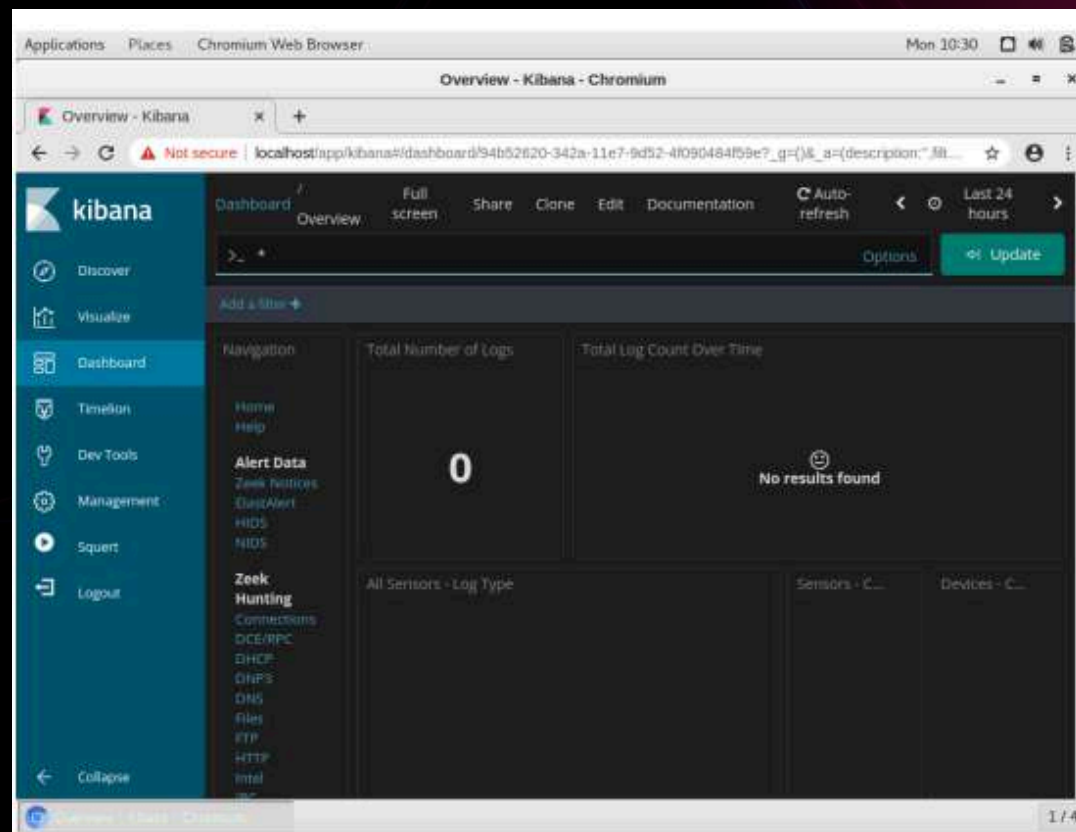
Nel Part 1 esamineremo un attacco in cui un aggressore ha sfruttato una vulnerabilità SQL Injection su un'applicazione web per ottenere accesso non autorizzato a informazioni sensibili (es. dati personali o finanziari) memorizzate su un server. Il nostro obiettivo è identificare la fonte dell'attacco (IP di origine) e determinare quali informazioni l'attaccante ha potuto ottenere. Passo 1: Cambiare l'intervallo temporale in Kibana (a) Avviare la macchina virtuale Security Onion e accedere con le credenziali fornite (utente: analyst, password: cyberops). Una volta avviata, aprire un Terminale (tasto destro sul desktop e selezionare "Open Terminal"). (b) Eseguire il comando `sudo so-status` nel terminale per verificare lo stato dei servizi di Security Onion. Inserire la password (cyberops) se richiesto. Attendere finché é tutti i servizi risultano [OK] prima di procedere con l'analisi (l'output mostrerà lo stato di componenti come sgul server, snort\_agent, so-kibana, etc., tutti su OK



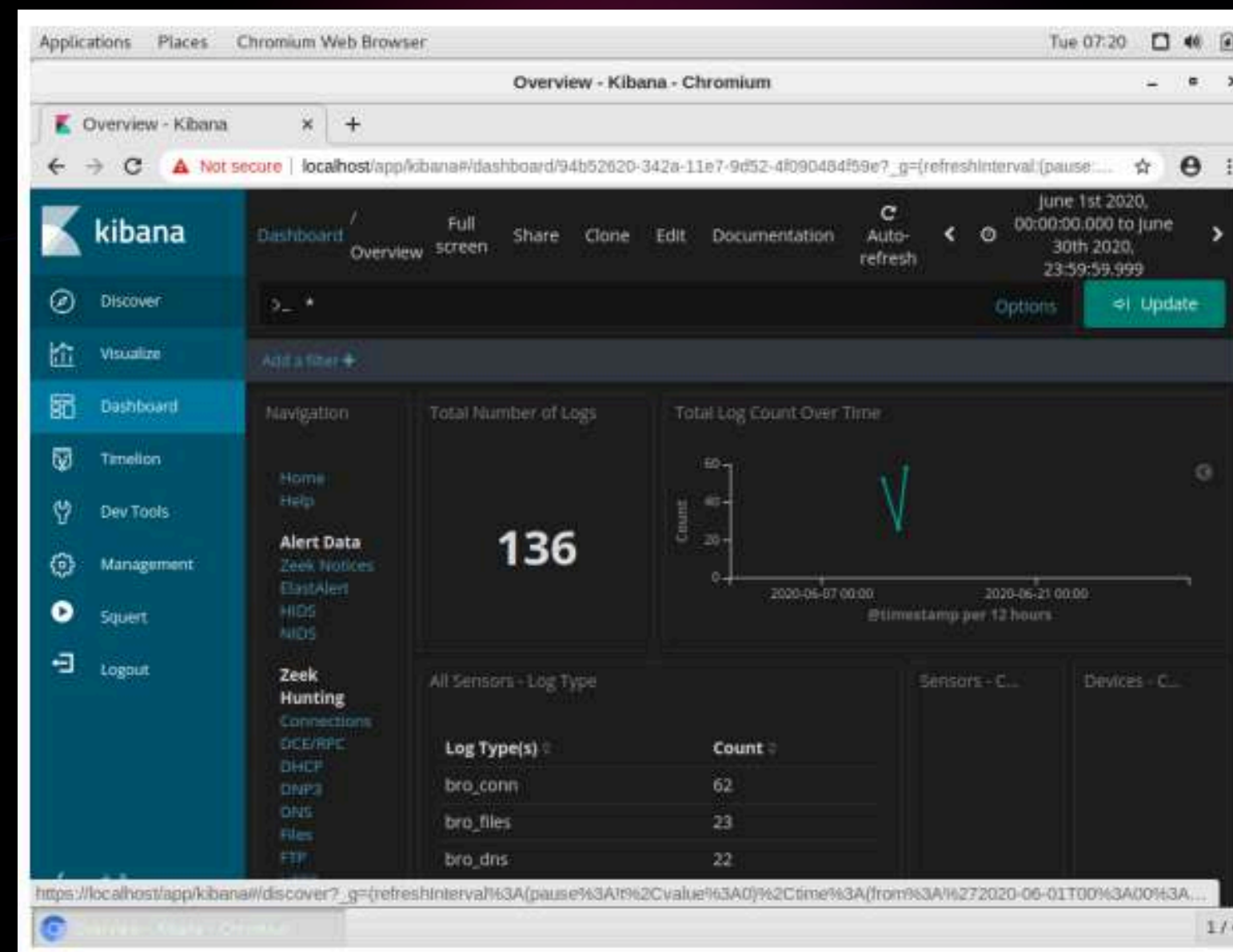


*Avviare Kibana utilizzando il collegamento presente sul desktop di Security Onion. Potrebbe apparire un avviso di certificato non valido sul browser; procedere cliccando su "Advanced" > "Proceed to localhost (unsafe)" per continuare. Alla schermata di login di Kibana, autenticarsi di nuovo come analyst con password cyberops.*

Osservare che la dashboard di Kibana per default mostra i dati delle ultime 24 ore. Poiché sappiamo (dalle informazioni fornite) che l'exploit è avvenuto nel mese di giugno 2020, sarà necessario ampliare l'intervallo temporale visualizzato. Nell'angolo in alto a destra della finestra di Kibana, cliccare sul menu a tendina che indica l'intervallo temporale (es. "Last 24 hours") e selezionare l'opzione per impostare un intervallo assoluto (Absolute). Impostare la data di inizio (From) al 1° giugno 2020, 00:00 e la data di fine (To) al 30 giugno 2020, 23:59, in modo da coprire l'intero mese di giugno 2020. Confermare cliccando su Go o Update.



Verificare che ora Kibana stia mostrando i log per il periodo selezionato. Dovreste vedere il numero totale di log relativi a tutto giugno 2020 (ad esempio, un certo conteggio di eventi) e vari pannelli di visualizzazione. La dashboard dovrebbe somigliare a quella mostrata nella figura di riferimento (se fornita nella guida) e includere grafici come il conteggio log nel tempo, suddivisione per categorie di log, ecc. Prendetevi un momento per familiarizzare con le informazioni fornite dall'interfaccia di Kibana per questo intervallo temporale.





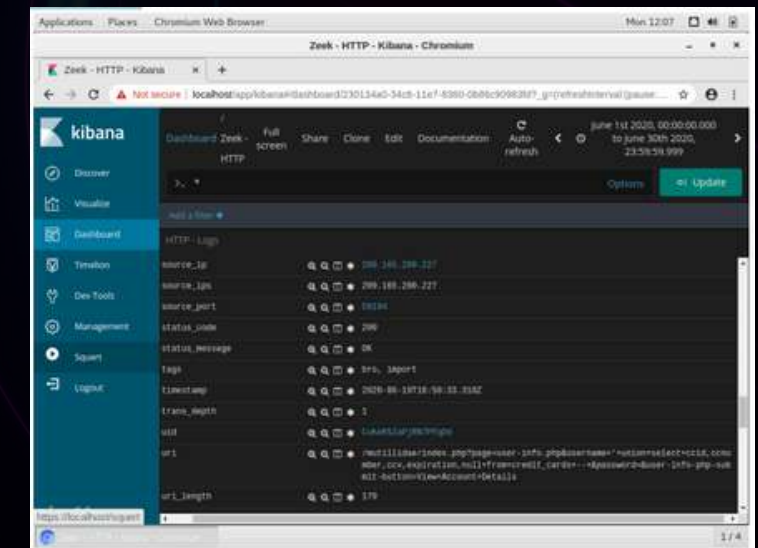
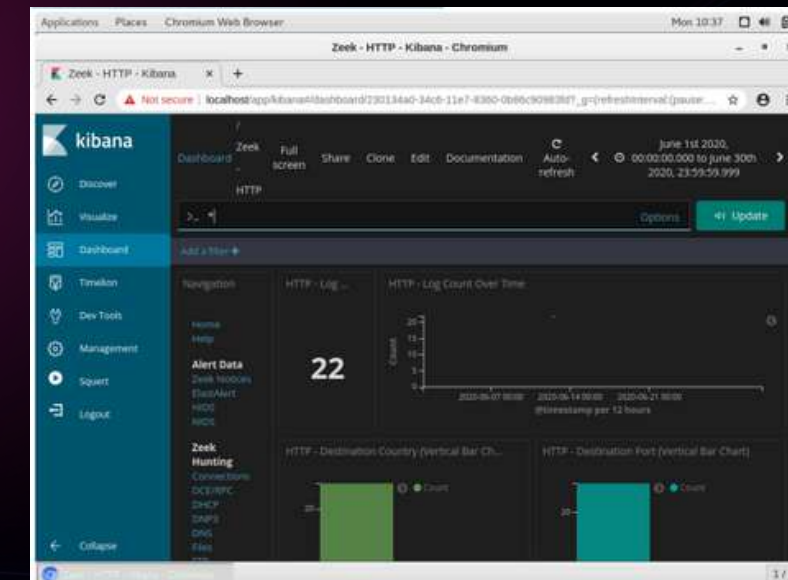
## Filtrare il traffico HTTP rilevante:

*Dal momento che l'attore malintenzionato ha sottratto dati tramite il servizio web (HTTP), applichiamo un filtro per visualizzare solo i log HTTP. Nella dashboard Kibana, individuare la sezione "Zeek Hunting" (di solito presente nella pagina Home o Navigation) e cliccare su "HTTP". In questo modo filtreremo i log per mostrare solo quelli relativi al protocollo HTTP.*

*Kibana aggiornerà la vista mostrando solo gli eventi HTTP. Scorrere tra i risultati elencati (vedrete una lista di voci di log HTTP). A questo punto, rispondiamo ad alcune domande chiave identificando le informazioni negli eventi HTTP visualizzati. In particolare, osserviamo il primo evento (il più vecchio di giugno 2020) nell'elenco dei log HTTP:*

Indirizzo IP sorgente: è l'IP dell'host che ha effettuato la richiesta HTTP. Espandendo i dettagli del primo evento (clic sul pulsante a forma di freccia accanto al timestamp), si trova il campo `src_ip` o equivalente. Dalla nostra analisi, l'IP di origine risulta essere 209.165.200.227, che presumibilmente corrisponde all'attore di minaccia (un host esterno che ha lanciato l'attacco).

*Indirizzo IP di destinazione: è l'IP del server web di destinazione attaccato. Nei dettagli dello stesso evento iniziale (campo dest\_ip), vediamo che l'IP destinazione è 209.165.200.235, ossia il server che ospita l'applicazione web bersaglio.*

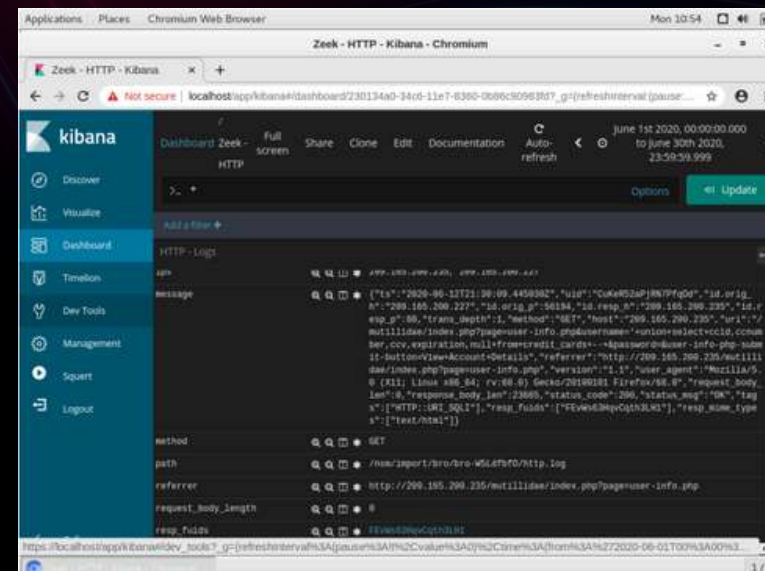




*Porta di destinazione: il traffico HTTP normalmente avviene sulla porta TCP 80 (HTTP non cifrato) o 443 (HTTPS). Dall'evento si conferma che la porta destinazione è 80 (HTTP non cifrato), indicando che l'attacco è avvenuto su HTTP normale.*

*Timestamp del primo evento: sempre nel log, possiamo annotare la data e ora del primo evento sospetto. Nel nostro caso, il timestamp è 12 giugno 2020 alle 21:30:09.445 (UTC). Ciò indica quando l'attacco (o almeno la prima richiesta HTTP malevola) è avvenuto. Tipo di evento: Kibana indica il tipo di log Zeek nel campo event type. Per i log HTTP di Zeek, il tipo è denominato bro\_http (Bro era il vecchio nome di Zeek). Questo conferma che stiamo guardando i log HTTP analizzati da Zeek.*

*Contenuto del campo "message": Nei dettagli del log HTTP, c'è un campo denominato "message" (o descrizione) che riassume la richiesta. In questo caso, il message mostra parametri della richiesta HTTP GET effettuata. Dall'analisi del contenuto, notiamo che il message include parametri come username, ccid, ccnumber, ccv, expiration, e password. In altre parole, la richiesta HTTP sembra contenere riferimenti a "username" e ad una serie di campi che assomigliano a dati di carta di credito (numero carta, codice di sicurezza, data di scadenza) e persino una password. Questa è una prima forte indicazione che l'attaccante potrebbe aver sfruttato un SQL injection per estrarre dati sensibili (come dettagli di carte di credito e password) dal database del sito web.*





*Interpretazione preliminare: La presenza di campi relativi a carte di credito nella richiesta indica che l'attaccante stava probabilmente tentando di ottenere informazioni finanziarie. Infatti, la combinazione di username e campi di carta di credito nel message suggerisce una richiesta anomala in cui questi dati vengono richiesti al server web. Molto probabilmente, l'attaccante ha manipolato la query SQL sul server tramite un input malevolo, facendogli restituire dati sensibili. Con queste osservazioni in mente, procediamo ad esaminare più a fondo l'evento per confermare l'SQL injection e vedere esattamente quali dati sono stati esfiltrati.*

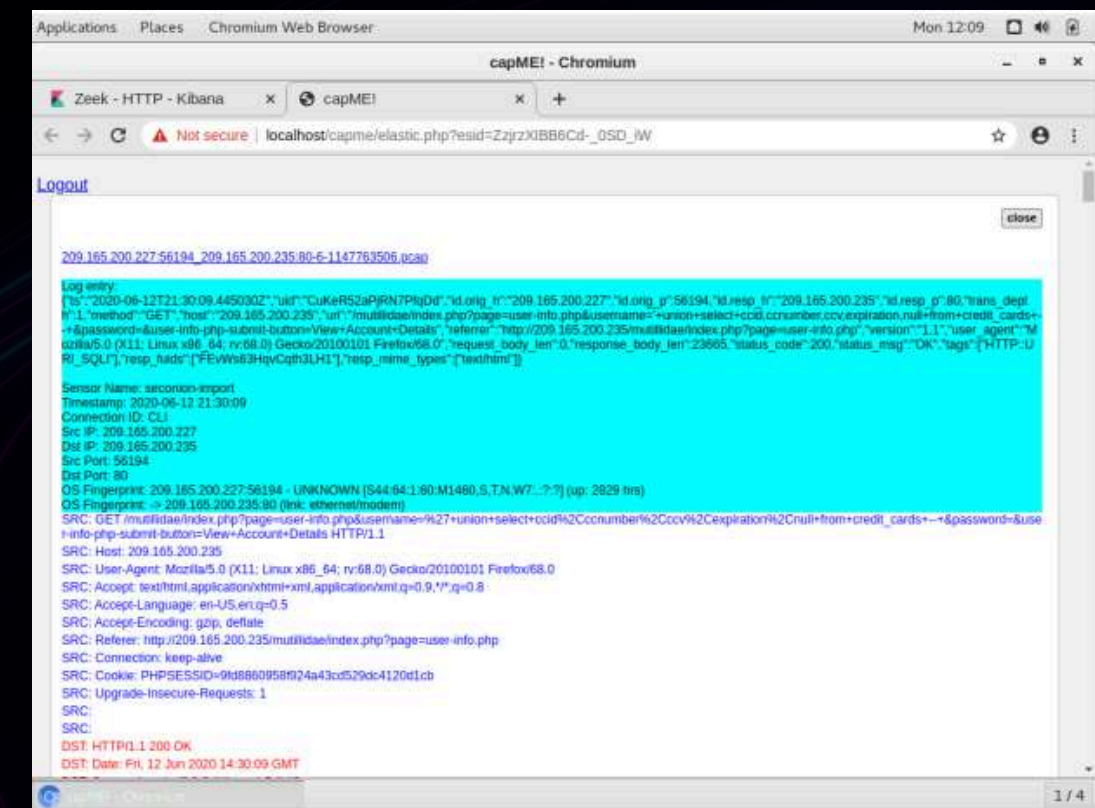
### ***Esaminare i risultati dettagliati dell'attacco SQLi:***

*(a) Kibana ci permette di approfondire i dettagli di ciascun evento log. Alcuni campi, come l'identificativo univoco dell'allarme/log (\_id), sono cliccabili e ci reindirizzano verso strumenti di analisi più specifici. Clicchiamo sul valore dell>alert \_id associato all'evento HTTP sospetto che abbiamo individuato. Questo aprirà una nuova scheda del browser caricando capME!, un'interfaccia web integrata in Security Onion che consente di visualizzare la trascrizione (ricostruzione) del traffico a partire dai dati PCAP catturati. (b) Nella scheda capME! vedremo una ricostruzione testuale della comunicazione HTTP tra l'host sorgente (attaccante) e il server destinazione. Il testo in blu rappresenta le richieste HTTP inviate dalla sorgente (SRC) al server, mentre il testo in rosso rappresenta le risposte del server di destinazione (DST). Scorrere questa trascrizione per analizzare lo scambio completo.*



(c) All’inizio della trascrizione, nella sezione di Log entry (che mostra la richiesta HTTP GET iniziale), individuare di nuovo la porzione di query sospetta. Dovrebbe comparire una stringa all’interno della richiesta che contiene termini come `username=' + union + select + ....` In effetti, nella trascrizione troviamo una porzione simile a: `username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credi t_cards+--+&password=`

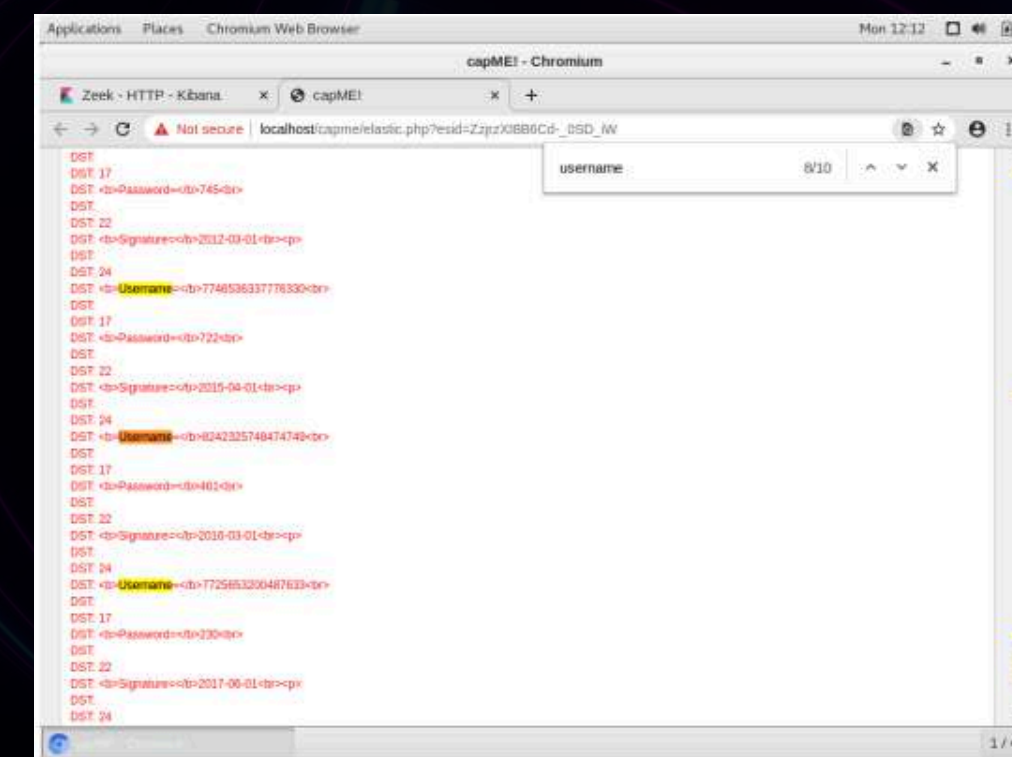
Questa stringa indica chiaramente che l’attaccante ha inserito nella richiesta HTTP una serie di parametri che chiudono il campo username e concatenano una query SQL aggiuntiva (UNION SELECT) per ottenere dati dalla tabella `credit_cards`. In particolare, la query malevola sta selezionando i campi `ccid` (id carta), `ccnumber` (numero di carta), `ccv` (codice di sicurezza), `expiration` (data di scadenza) dalla tabella `credit_cards`. L’operatore `--` denota un commento in SQL, usato per ignorare la restante parte della query legittima (in questo caso probabilmente bypassa la verifica della password). Questo è un evidente tentativo di SQL injection volto ad aggirare l’autenticazione e estrarre informazioni sulle carte di credito dal database. Le parole chiave “union” e “select” nel contesto di un input utente confermano l’attacco SQLi. (d) Adesso cerchiamo di capire quali dati sono effettivamente stati ottenuti dall’attaccante. La trascrizione di capME! include sia la richiesta che la risposta HTTP. Per comodità, utilizziamo la funzione di ricerca all’interno della pagina (Ctrl+F) per cercare ulteriori occorrenze della parola “username” nella trascrizione. Scorrendo tra i risultati trovati, noteremo che più in basso nella risposta del server compare qualcosa di insolito.





(e) Osservazione nella risposta: Continuando a scorrere la trascrizione (dopo la parte iniziale di login), si vede che il server ha restituito un elenco di dati dove normalmente non dovrebbe. In particolare, più avanti nella risposta HTTP c'è un elenco di coppie di username e password in chiaro (ovvero nomi utente e relative password) che fanno parte delle informazioni restituite dal server. Questa lista di credenziali utente non sarebbe normalmente visibile in una normale interazione e rappresenta un forte indizio che l'attaccante, tramite l'SQL injection, è riuscito a far sì che il server rivelasse informazioni dal database. In condizioni normali, un'applicazione web non dovrebbe mai inviare al client tutte le coppie username/password degli utenti! Il fatto che ciò appaia nella risposta è estremamente anomalo e conferma che l'attacco ha avuto successo esfiltrando dati sensibili.

(f) Dati esfiltrati via HTTP: Dalla risposta HTTP ricostruita possiamo quindi elencare i dati sottratti. Troviamo credenziali di account utente (username e password). Ad esempio, tra i dati esfiltrati vediamo: Username 4444111122223333 – Password 745 – Signature 2012-03-01 Username 7746536337776330 – Password 722 – Signature 2015-04-01 Username 8242325748474749 – Password 461 – Signature 2016-03-01 Username 7725653200487633 – Password 230 – Signature 2017-06-01 Username 1234567812345678 – Password 627 – Signature 2018-11-01 ○ Una serie di possibili username (in realtà appaiono come stringhe numeriche) accompagnati da password (numeriche) e un campo "signature" che contiene valori che somigliano a date. Probabilmente, a causa dell'UNION usato, i campi delle carte di credito sono stati mappati sui campi username, password e signature della query originale. Per esempio, una parte della risposta mostra qualcosa come:





Questi valori corrispondono molto probabilmente a numeri di carte di credito (16 cifre) e codici di sicurezza CVV (3 cifre), associati a date (che interpretate correttamente rappresentano le date di scadenza delle carte). In totale, dall'attacco emergono almeno cinque record di carte di credito con relativi codici e date. Quindi, l'attore di minaccia è riuscito a estrarre dal database informazioni finanziarie sensibili (carte di credito) e anche un elenco di credenziali (username e password) di utenti.

(g) A questo punto, abbiamo isolato i dettagli principali dell'attacco HTTP: IP sorgente (attaccante): 209.165.200.227 IP destinazione (server web colpito): 209.165.200.235 Vulnerabilità sfruttata: SQL Injection (notata dalla stringa union+select nella richiesta) Dati esfiltrati via HTTP: record dal database contenenti numeri di carta di credito, codici CVV, date di scadenza, nonché liste di username e password di utenti (informazioni personali e finanziarie, tutte considerate PII – Personally Identifiable Information). Conseguenza: L'attaccante ha bypassato l'autenticazione e ha ottenuto dati riservati che dovevano essere protetti, esponendo l'organizzazione a un grave breach di dati.

Chiudere la scheda capME! dopo aver raccolto tutte le informazioni necessarie e tornare alla dashboard Kibana per passare all'analisi successiva.



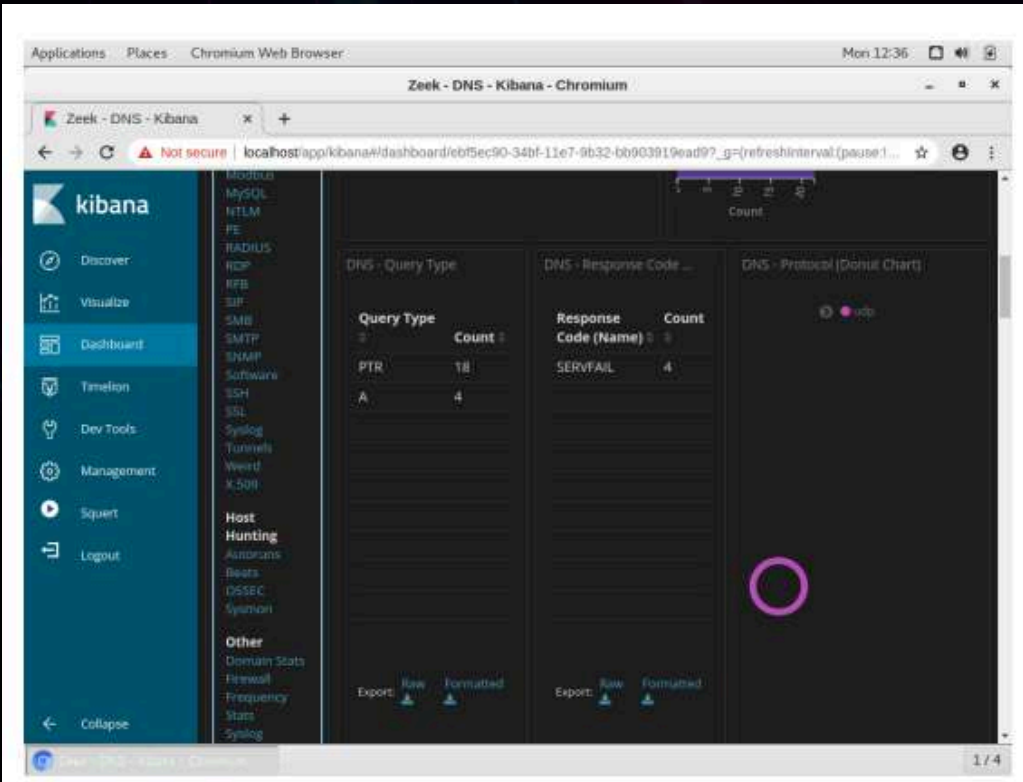
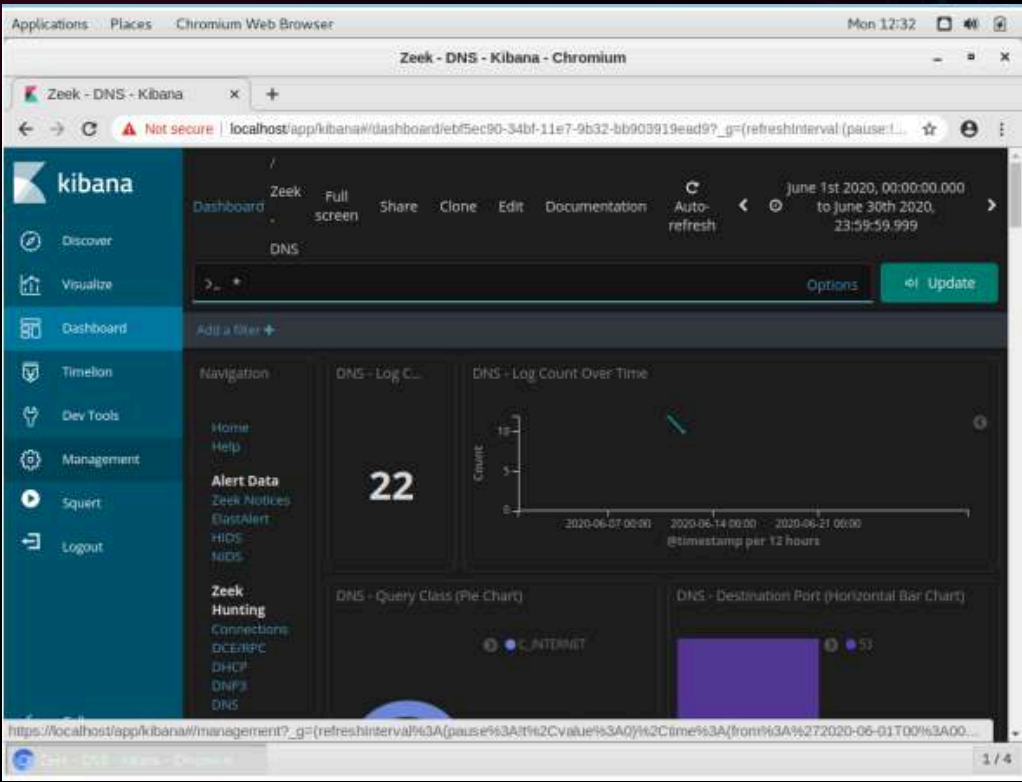
## Analisi di una possibile esfiltrazione di dati tramite DNS

Nel Part 2 indagheremo su un traffico DNS anomalo che potrebbe indicare un metodo di esfiltrazione dati diverso. Un amministratore di rete ha notato query DNS insolitamente lunghe, con sottodomini strani, e ci viene chiesto di investigare questa anomalia. L'ipotesi è che l'attore di minaccia possa aver utilizzato le query DNS come canale per trasportare dati rubati fuori dalla rete, sfruttando il fatto che il traffico DNS spesso non viene filtrato o monitorato con attenzione (tecnica nota come DNS tunneling o esfiltrazione via DNS).

### Filtrare il traffico DNS

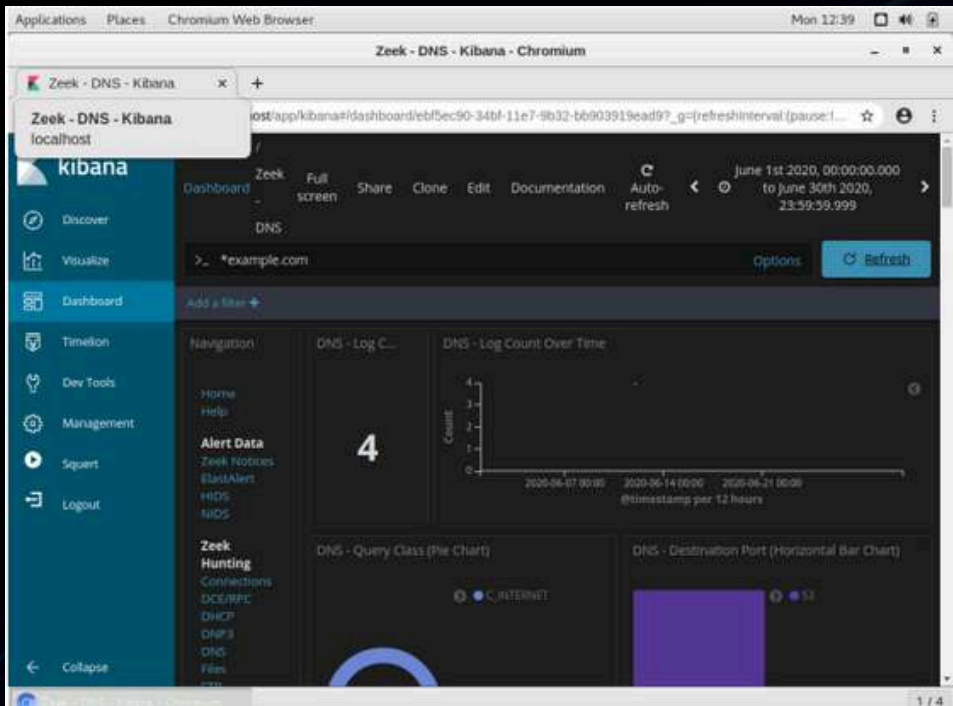
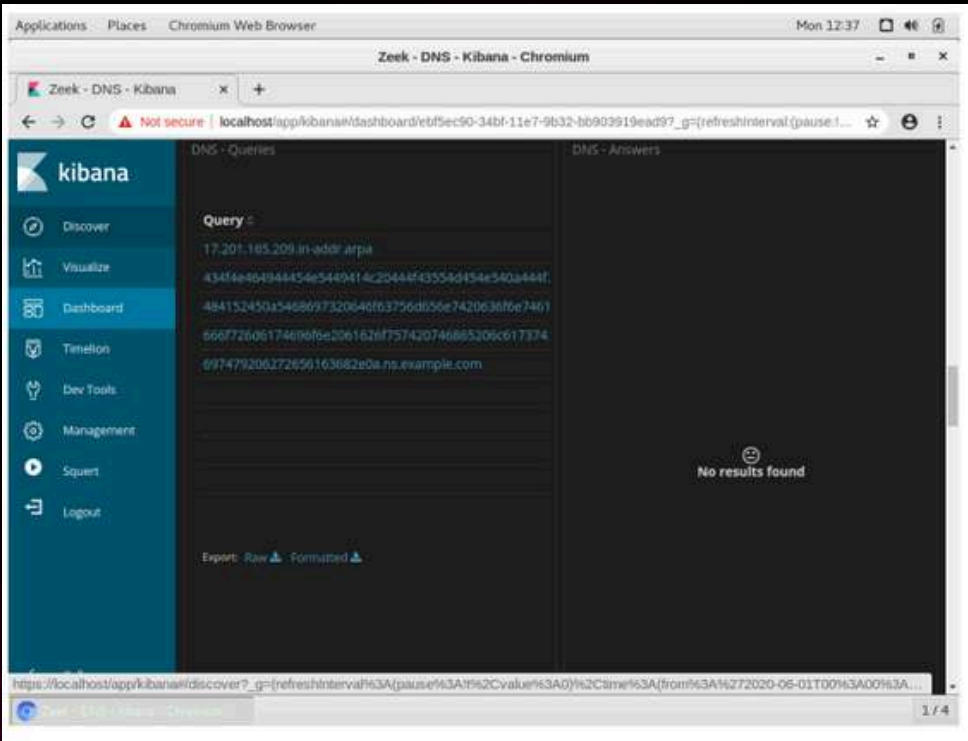
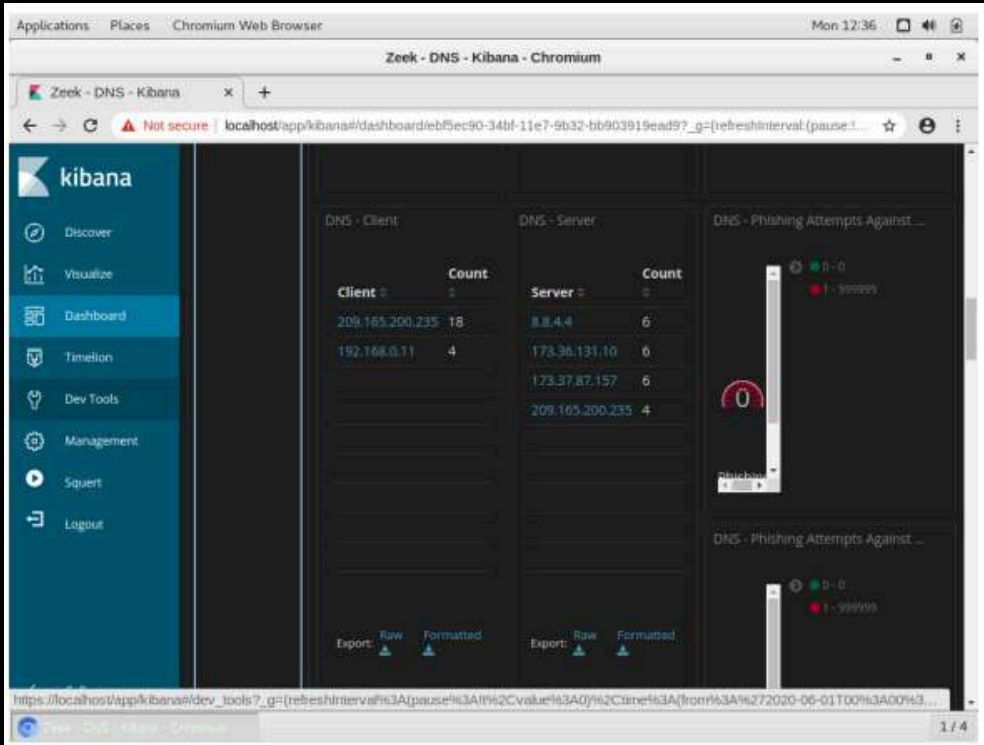
(a) Nella sezione “Zeek Hunting” della Home di Kibana, cliccare ora su “DNS”. Questo filtrerà i log per mostrare solo quelli relativi al protocollo DNS. Osservando i pannelli, dovrete vedere metriche come il conteggio di log DNS, la distribuzione per porte (le query DNS standard usano la porta 53/udp) e altri grafici specifici DNS.

(b) Scorrere verso il basso nella pagina per esaminare i dettagli dei log DNS. In Kibana sono fornite alcune viste aggregate utili: ○ È presente un elenco dei tipi di query DNS più frequenti (ad esempio tipi A per indirizzi IPv4, AAAA per IPv6, NB per NetBIOS, PTR per record puntatori, ecc.) insieme ai codici di risposta DNS. Verificare questi elementi per avere contesto: un traffico DNS legittimo dovrebbe mostrare query A, AAAA, PTR comuni.





Scorrendo ulteriormente, troviamo una lista dei client DNS e server DNS più attivi (ordinati per numero di richieste e risposte). Questo ci dà un'idea di quali host stanno effettuando più query DNS e quali server stanno rispondendo.



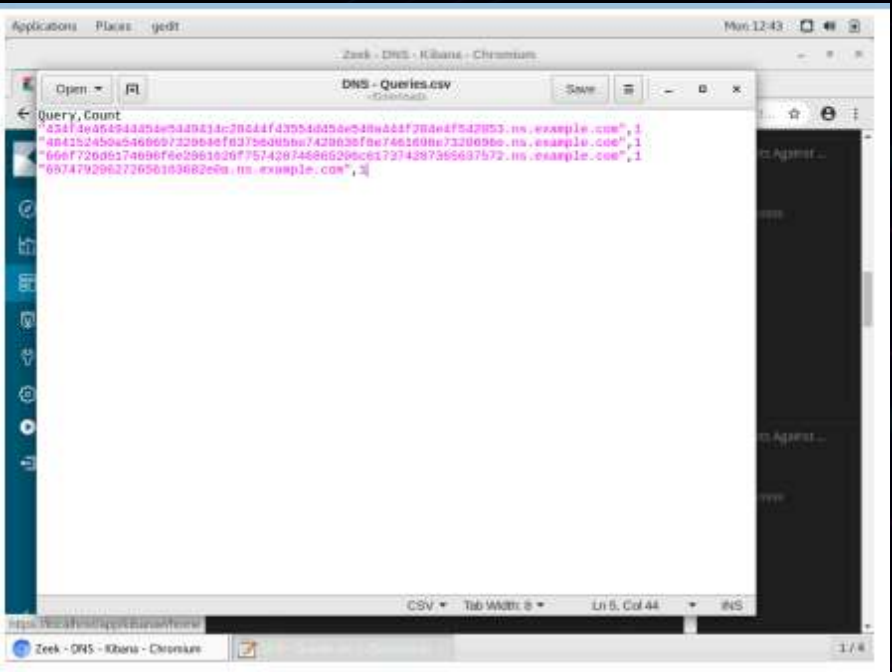
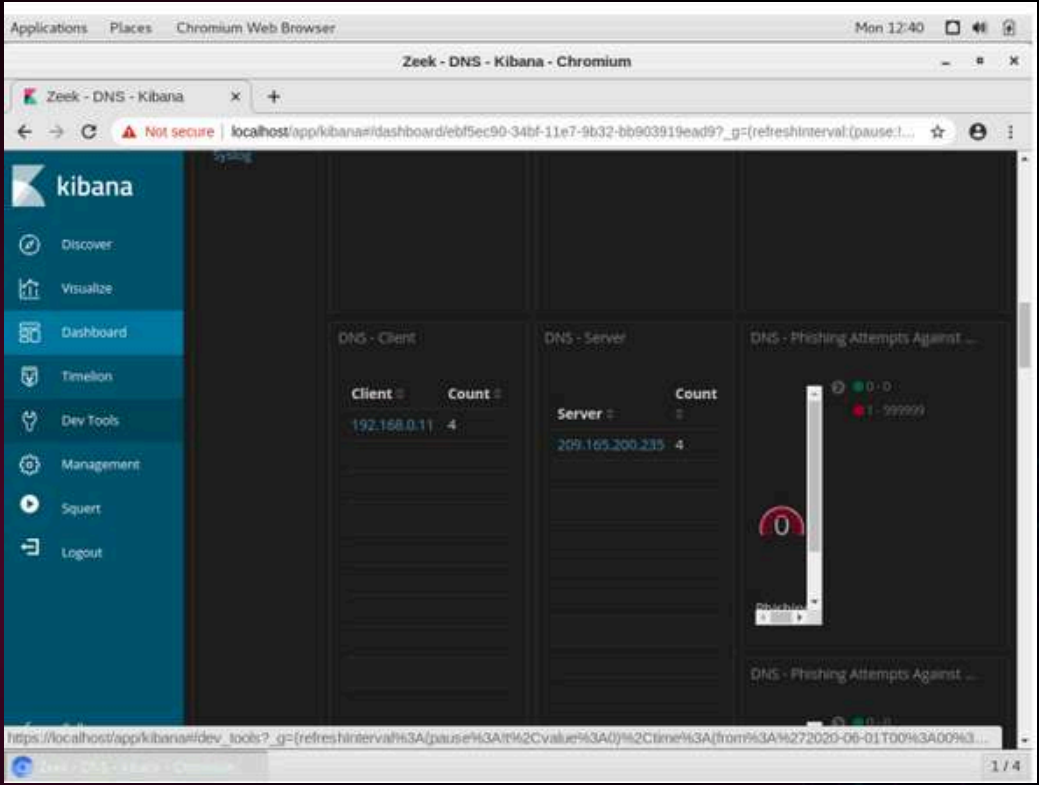
Ancora più in basso, c'è una sezione con le principali query DNS per nome di dominio. Ed ecco l'anomalia: notiamo che per il dominio `ns.example.com` (sotto il dominio `example.com`) ci sono delle query con sottodomini insolitamente lunghi – lunghe stringhe alfanumeriche precedono `.ns.example.com`. Questa è un'indicazione chiave: tali stringhe lunghe composte da numeri e lettere (in particolare caratteri esadecimali, 0-9 e a-f) non assomigliano a nomi di host legittimi.

Per concentrarci su queste query anomale, applichiamo un filtro di ricerca. Tornare verso l'alto e, nella barra di ricerca di Kibana, digitare `example.com` come termine di filtro, quindi cliccare su Update per aggiornare la vista. In questo modo Kibana mostrerà soltanto i log DNS che riguardano il dominio `example.com`. Noterete immediatamente che il conteggio totale dei log DNS è diminuito, poiché ora stiamo visualizzando solo le query dirette a `example.com` (specificamente quelle con sottodominio lungo che avevamo individuato).



(d) Individuare nei log filtrati le informazioni sul client DNS che ha effettuato queste query e sul server DNS che ha risposto. Dalle nostre osservazioni, l'IP del client DNS che ha generato le query sospette risulta essere 192.168.0.11, mentre il server DNS contattato (destinazione delle query) è 209.165.200.235. Ciò suggerisce che un host interno (192.168.0.11) compromesso stia tentando di inviare dati ad un server (o intermediario DNS) all'indirizzo 209.165.200.235 usando il meccanismo delle query

DNS



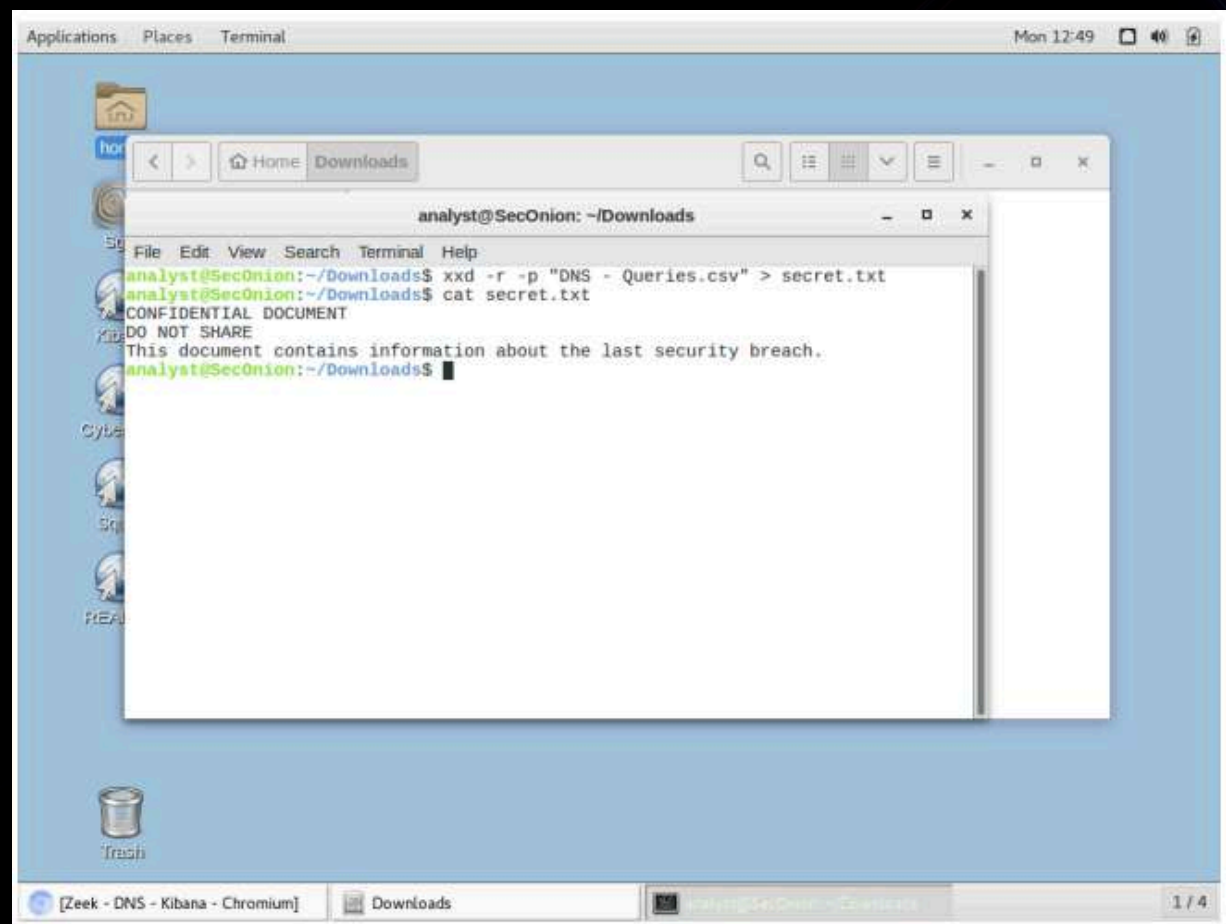
**Analizzare le query DNS sospette in dettaglio**

(a) Con il filtro attivo su example.com, Kibana dovrebbe elencare quattro log di query DNS uniche indirizzate a sottodomini molto lunghi di ns.example.com. Ciascun log rappresenta una query DNS fatta dal client compromesso. Osservando attentamente queste voci, notiamo che le stringhe nei sottodomini sono sequenze alfanumeriche apparentemente random, ma composte solo da cifre e lettere dalla a alla f. Questo è un forte indizio che tali stringhe siano in realtà dati codificati in esadecimale e non normali nomi di sottodominio. In altre parole, l'attaccante potrebbe aver convertito del testo (dati rubati) in una rappresentazione esadecimale e li sta inviando fuori rete sfruttando il campo del nome di dominio nelle query DNS. ● (b) Per confermare i nostri sospetti e leggere il contenuto, è necessario decodificare queste stringhe esadecimali. Kibana offre la possibilità di esportare i dati dei log. In alto a destra della sezione dei risultati, cliccare su Export: Raw (o un'icona di download) per esportare i log DNS filtrati in un file CSV. Salvare il file (di default dovrebbe chiamarsi ad es. "DNS - Queries.csv")



(c) Aprire il file CSV esportato con un editor di testo. Il file conterrà righe con molti campi; identificare le parti di testo che corrispondono ai sottodomini esadecimali sospetti e rimuovere tutto il resto attorno. In pratica, occorre ripulire il file lasciando solo le stringhe esadecimali pure, eliminando eventuali virgolette e altri caratteri non appartenenti alla codifica hex.

(d) Adesso utilizziamo uno strumento per la decodifica. Security Onion (Ubuntu) include il comando `xxd` che può convertire da esadecimale a ASCII. Aprire un Terminale e posizionarsi nella cartella dove avete salvato il CSV pulito (es: `cd ~/Downloads`). Eseguire il comando: `xxd -r -p "DNS - Queries.csv" > secret.txt` ● Questo comando legge il contenuto esadecimale dal file CSV e scrive il risultato decodificato nel file `secret.txt`. (e) Sempre nel terminale, eseguire `cat secret.txt` per visualizzare il contenuto decodificato. In output apparirà una porzione di testo in chiaro. Sorprendentemente (o forse non così sorprendente visto il contesto), il testo ricomposto costituisce un messaggio che era stato frammentato nelle query DNS. Nel nostro scenario, il messaggio risulta essere: **CONFIDENTIAL DOCUMENT DO NOT SHARE** This document contains information about the last security breach.



Abbiamo quindi scoperto che le lunghe stringhe esadecimali nelle query DNS in realtà rappresentavano il contenuto di un documento riservato. L'attaccante ha suddiviso ed esfiltrato il contenuto di un documento confidenziale (probabilmente contenente dettagli di una violazione di sicurezza) attraverso richieste DNS. Ogni query ha inviato una parte del testo codificata in esadecimale al server DNS esterno. ● (f) Ora possiamo rispondere ad alcune domande finali per interpretare la significatività di questo risultato: ○ Le sottodomini erano realmente nomi di host? No. Come ipotizzato, quelle lunghe stringhe non erano nomi di sottodominio validi, ma dati codificati (in formato esadecimale) incapsulati nelle query DNS. Il messaggio ricostruito "CONFIDENTIAL DOCUMENT DO NOT SHARE..." lo conferma: l'attore di minaccia ha usato il protocollo DNS per trasportare furtivamente un messaggio/testo.



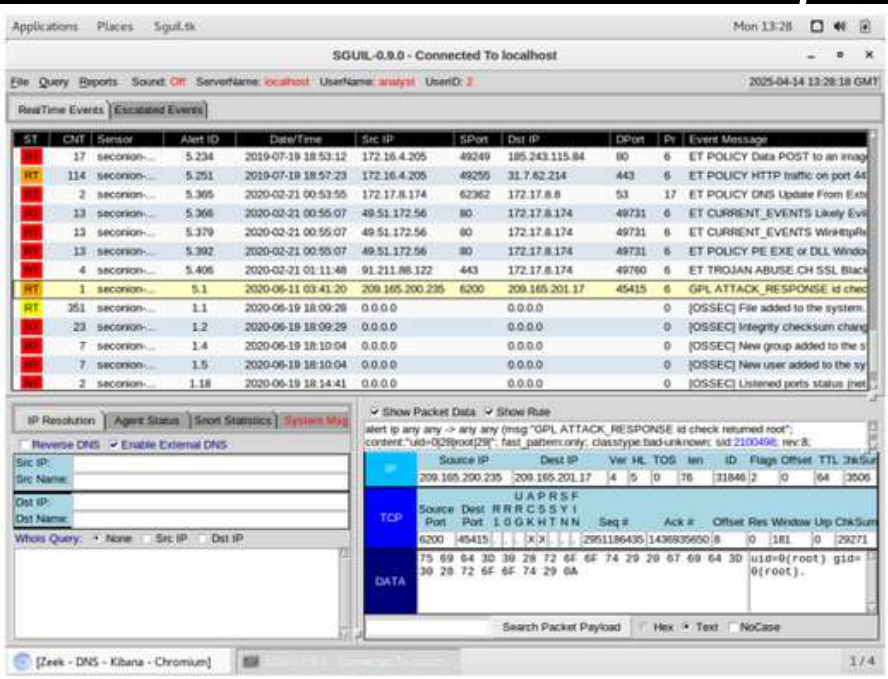
Cosa implica questo riguardo quelle richieste DNS? Implica che le query DNS in questione costituivano un canale di esfiltrazione dati. L'attaccante ha trovato un metodo per far uscire informazioni dalla rete non attraverso il web o altri canali tradizionali, ma attraverso risoluzioni DNS apparentemente innocue. Come potrebbero essere state generate queste query DNS codificate e perché usare DNS? Con alta probabilità, un malware o uno script malevolo in esecuzione sull'host interno (192.168.0.11) ha letto il contenuto del documento confidenziale (forse ottenuto in un precedente attacco) e lo ha frammentato, convertendo ogni porzione in esadecimale. Dopodiché, ha generato una serie di query DNS verso un dominio controllato dall'attaccante (example.com in questo caso fittizio), inserendo i dati codificati nei nomi di sottodominio (prima di .ns.example.com). Il motivo per cui è stato scelto DNS come mezzo è che le query DNS sono generalmente permesse attraverso i firewall e spesso non vengono monitorate rigorosamente.



# **Lab – Isolate Compromised Host Using 5-Tuple**



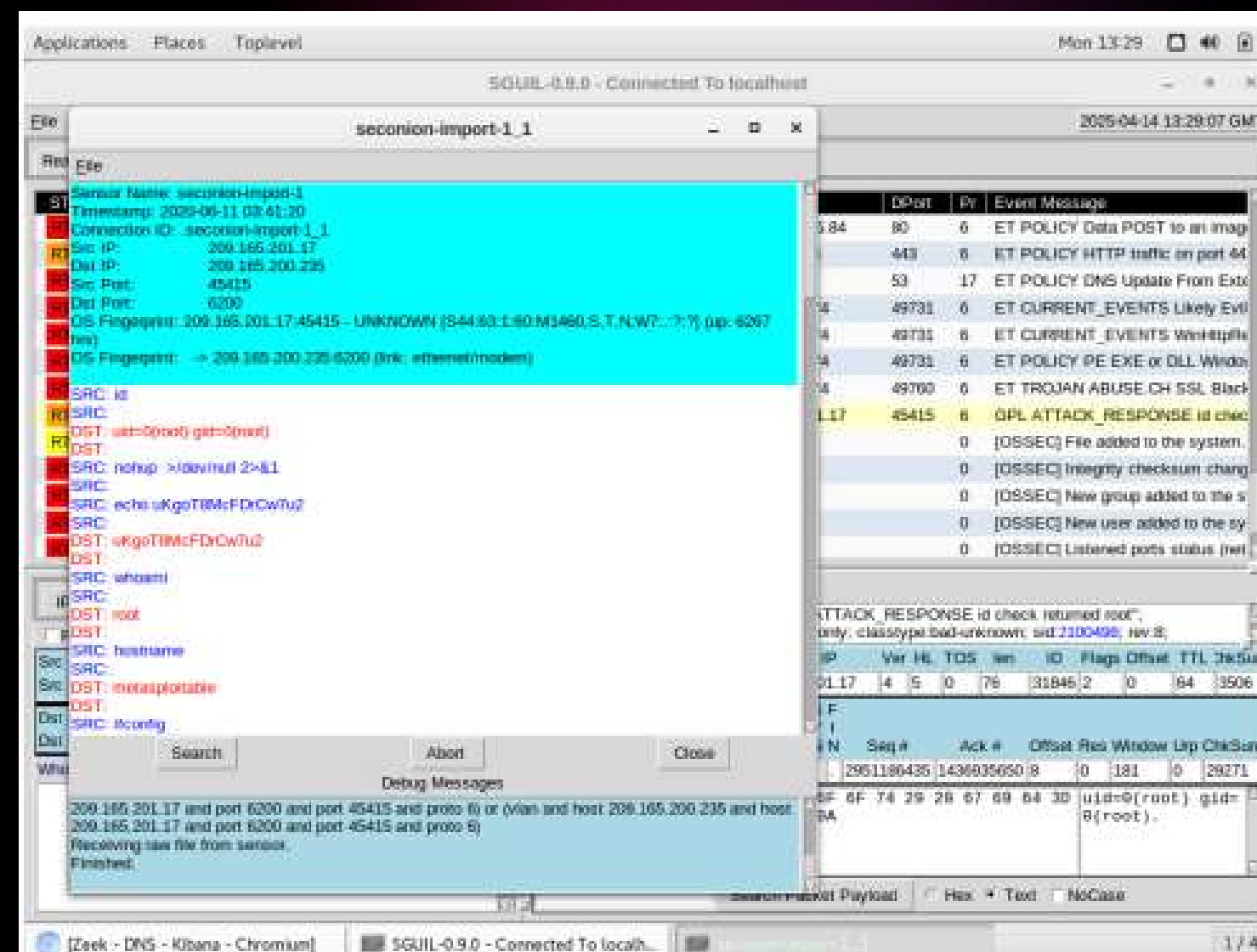
Accesso alla macchina Security Onion: Avviare la macchina virtuale Security Onion (una distribuzione Linux per monitoraggio di sicurezza) e effettuare il login con le credenziali fornite. Usare il nome utente analyst e la password cyberops. Dopo l'accesso, ci si trova nell'ambiente desktop di Security Onion con i privilegi dell'utente analyst.



Aprire l'applicazione Sguil e accedere se richiesto. Nella finestra di login di Sguil, selezionare tutte le interfacce di rete disponibili e cliccare Start Sguil per iniziare a ricevere gli alert. Una volta avviato, Sguil mostrerà una lista di eventi/allerte di sicurezza in tempo reale. Esaminare la colonna Event Message e individuare un messaggio significativo: "GPL ATTACK\_RESPONSE id check returned root". In questo scenario, l>alert con ID 5.1 corrisponde a questo messaggio. Questa descrizione indica che durante un attacco è stato probabilmente ottenuto un accesso root su un host bersaglio. In particolare, l'host con IP 209.165.200.235 avrebbe restituito un risultato che indica accesso root a una richiesta proveniente dall'IP 209.165.201.17. Ciò suggerisce che l'attaccante (209.165.201.17) è riuscito a ottenere privilegi di amministratore (root) sulla macchina di destinazione 209.165.200.235.

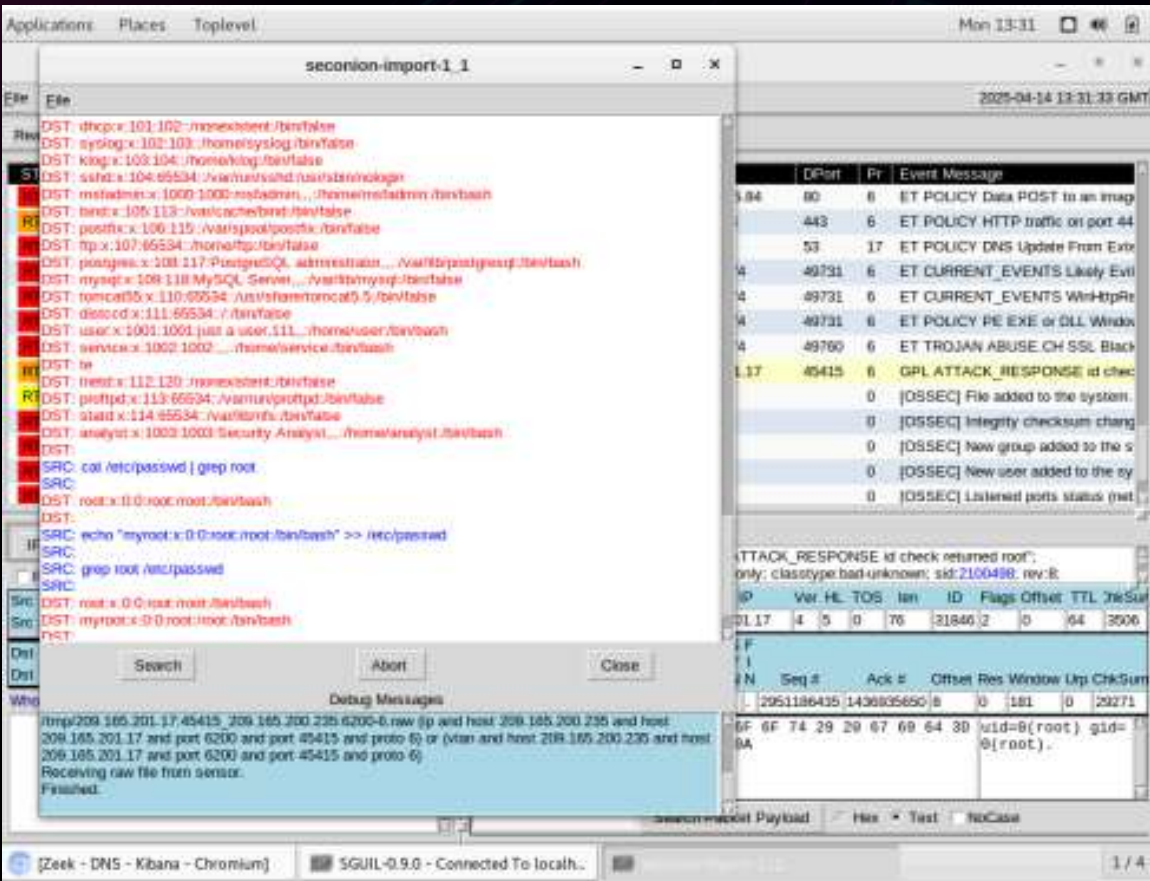
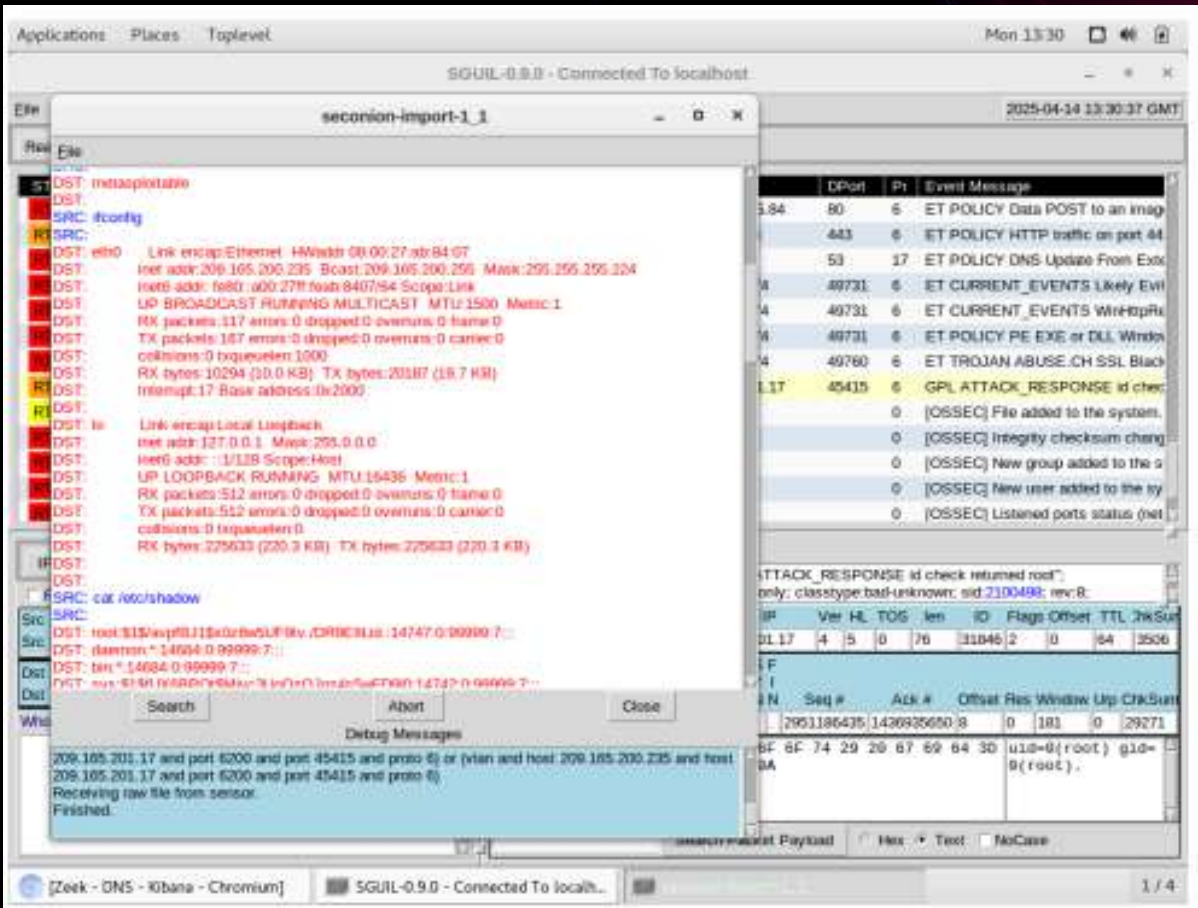


Visualizzazione dei dettagli del pacchetto e della regola dell>alert: Per approfondire l>alert selezionato (ID 5.1), spuntare le caselle "Show Packet Data" e "Show Rule" nell'interfaccia di Sguil. In questo modo si visualizzano rispettivamente i dati grezzi del pacchetto (payload) e la regola IDS/IPS che ha generato l>alert. Dall'Packet Data dell'evento si può osservare il contenuto testuale del traffico sospetto intercettato. Ad esempio, è probabile individuare una stringa come uid=0(root) all'interno del payload, indicativa dell'esecuzione del comando Unix id il cui output conferma l'utente root.



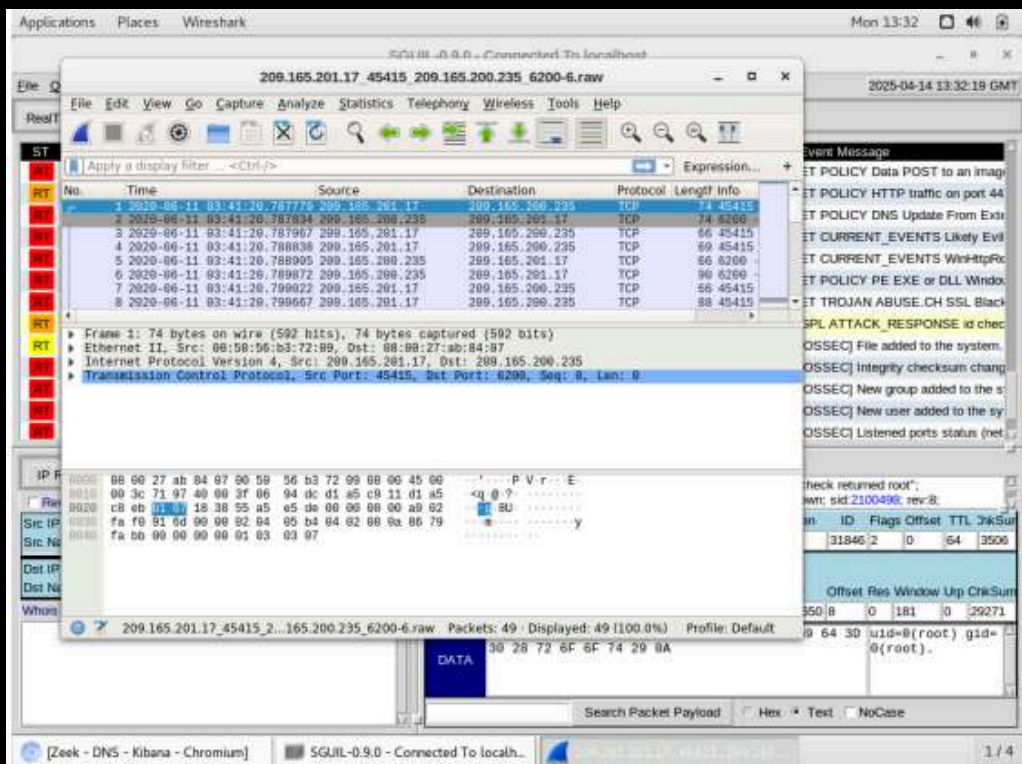


Analisi della trascrizione (Transcript) dell’evento: Fare right-click (clic destro) sull’alert ID 5.1 in Sguil e selezionare l’opzione “Transcript”. Questo aprirà una finestra con la trascrizione testuale della sessione di rete relativa all’alert, ricostruendo il dialogo tra l’indirizzo sorgente (209.165.201.17, l’attaccante) e l’indirizzo destinazione (209.165.200.235, l’host compromesso) durante l’attacco. Dalla trascrizione si può vedere che l’attaccante sta eseguendo comandi Linux sul sistema bersaglio. In particolare, l’attaccante (209.165.201.17) ha ottenuto accesso root sul server 209.165.200.235 e procede a esplorare il file system della vittima. Ad esempio, si notano operazioni come la lettura/copia del file di sistema /etc/shadow (che contiene gli hash delle password) e modifiche ai file /etc/shadow e /etc/passwd. Queste azioni indicano che l’attaccante sta probabilmente creando o modificando account per mantenere l’accesso persistente (escalation e conservazione dei privilegi amministrativi sulla macchina compromessa).

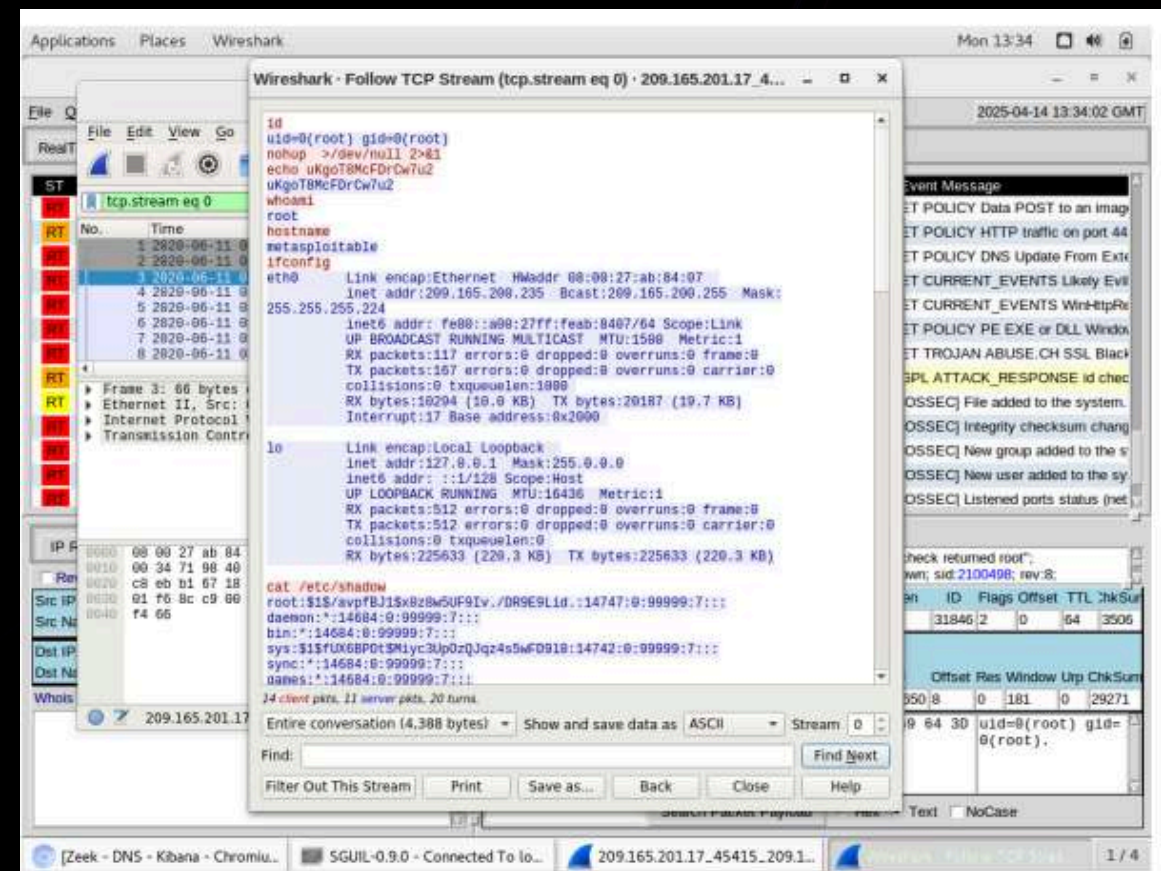




*Pivot su Wireshark per analizzare la conversazione TCP: Dalla finestra di Sguil, con l’alert 5.1 ancora selezionato, fare clic destro e scegliere “Wireshark” per aprire il traffico di rete grezzo relativo a questo alert all’interno di Wireshark.*

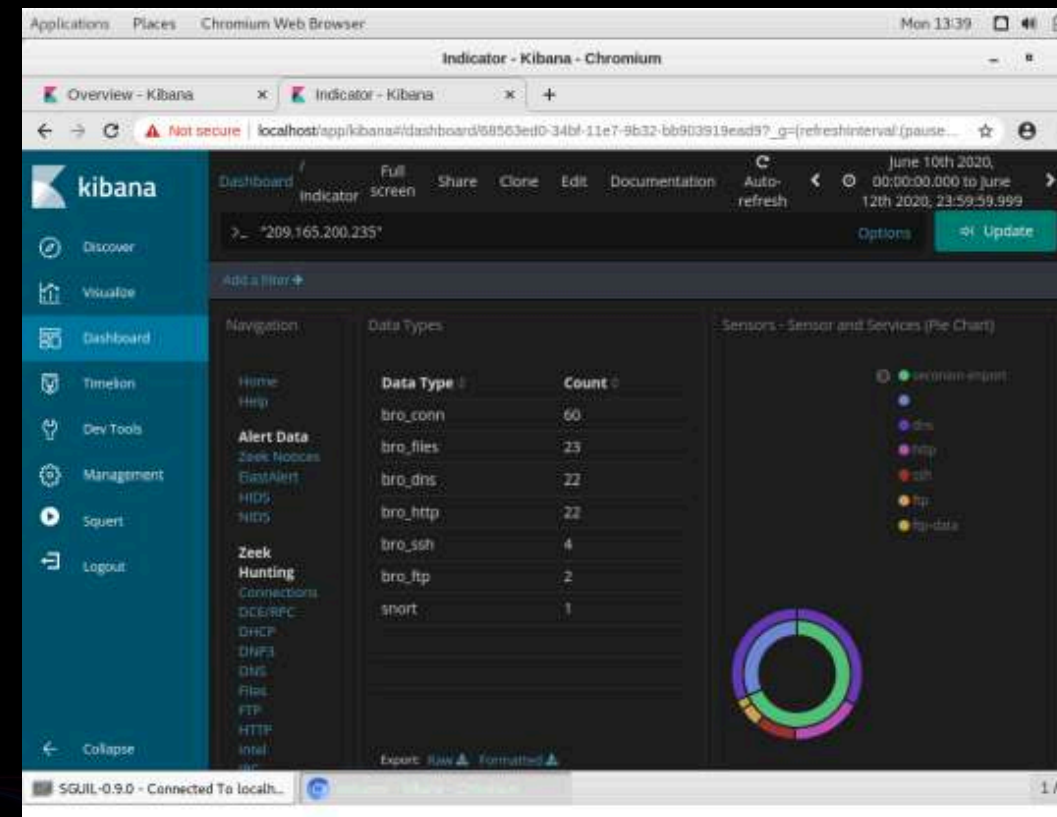


*In Wireshark si aprirà il pacchetto specifico dell’alert; per ricostruire l’intera conversazione TCP tra i due host, fare clic destro su uno dei pacchetti e selezionare “Follow → TCP Stream”. Si aprirà una finestra che mostra il dialogo completo tra client e server in forma testuale. Osservando questo flusso, si notano i comandi inviati dall’attaccante e le risposte della vittima, esattamente come visti nella trascrizione di Sguil (i contenuti coincidono). Dall’analisi del flusso, si può confermare che l’attaccante ha pieno controllo come utente root sulla macchina vittima: ad esempio, viene eseguito il comando whoami e la risposta mostrata è “root”, a conferma dei privilegi elevati. Scorrendo nella conversazione TCP si trovano inoltre dati che l’attaccante ha visualizzato, come informazioni sugli account utente del sistema (derivate dalla lettura dei file di configurazione utenti). Questi riscontri in Wireshark rafforzano la comprensione della sequenza di comandi malevoli eseguiti.*



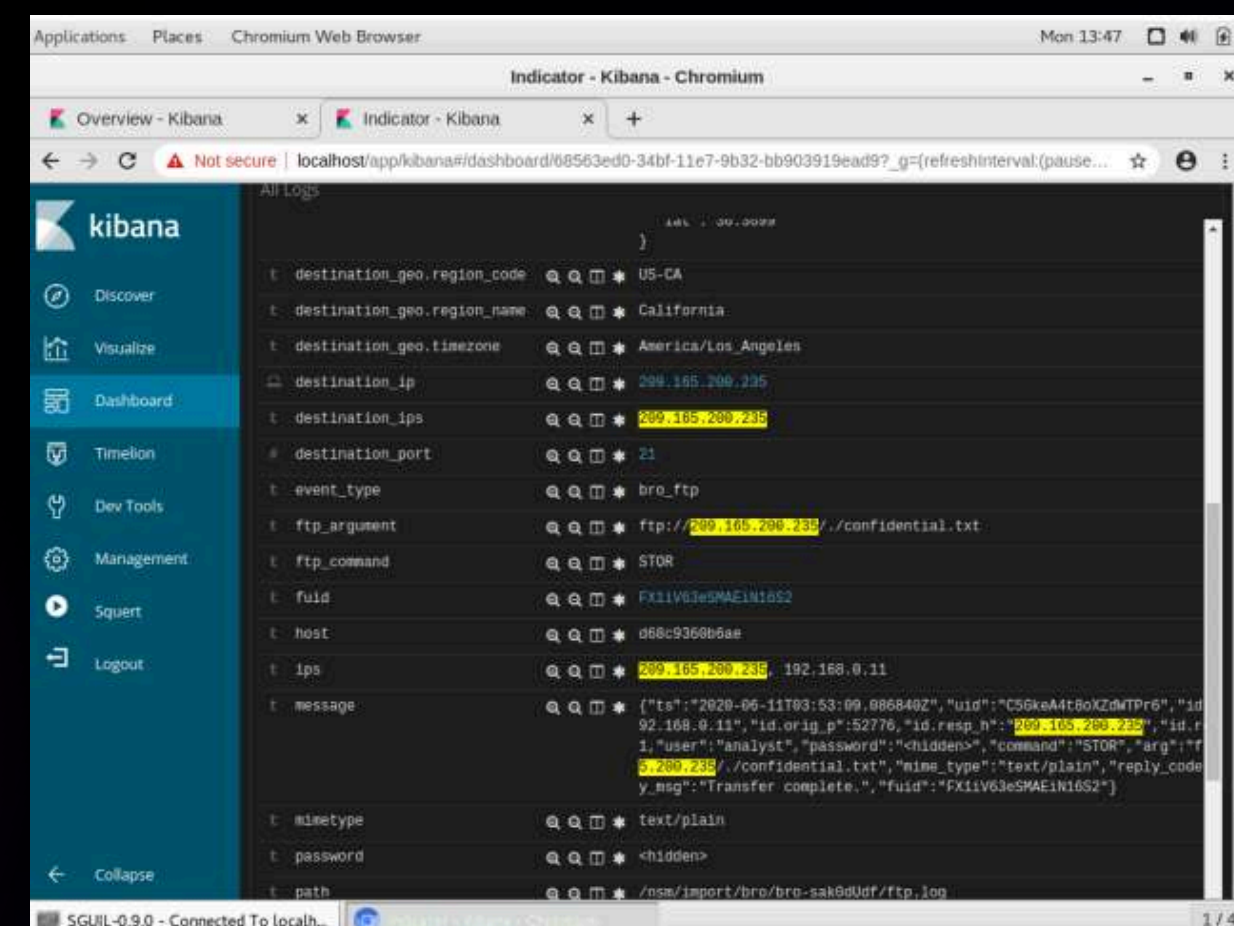
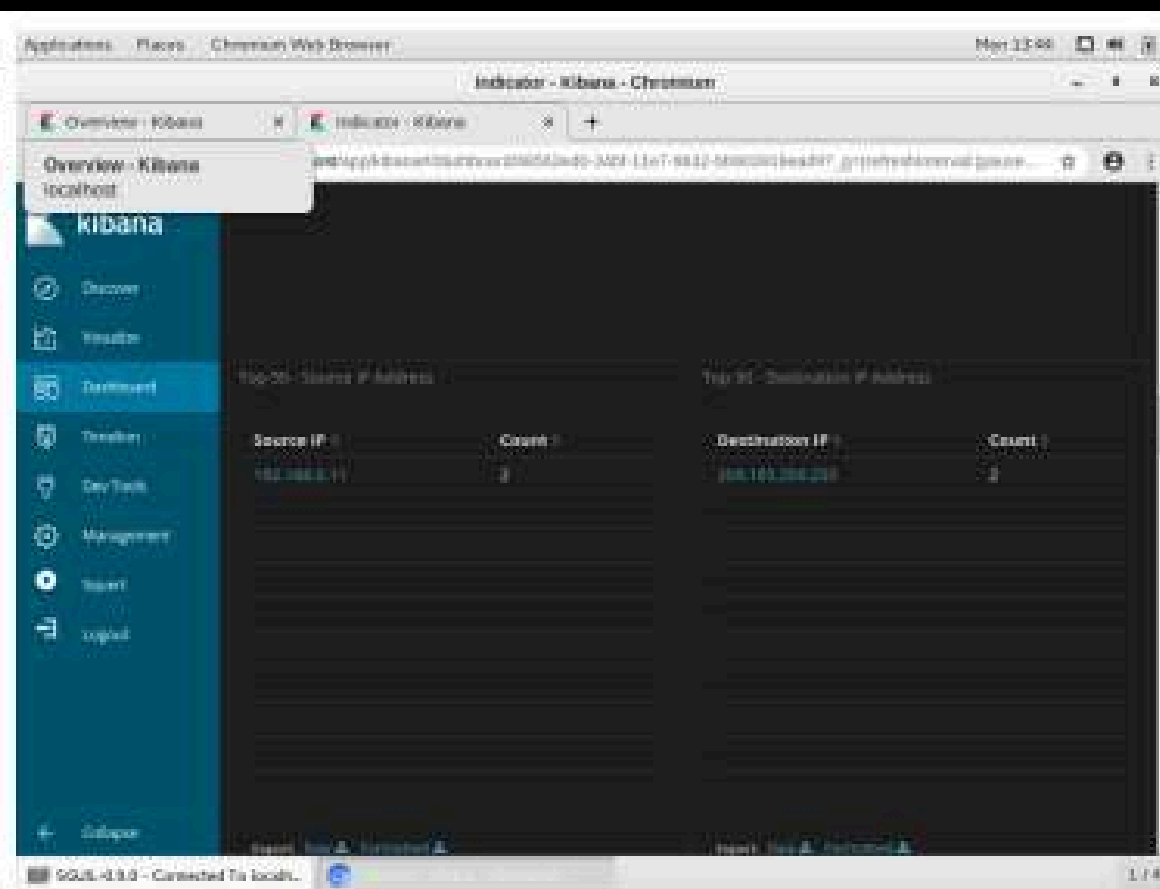
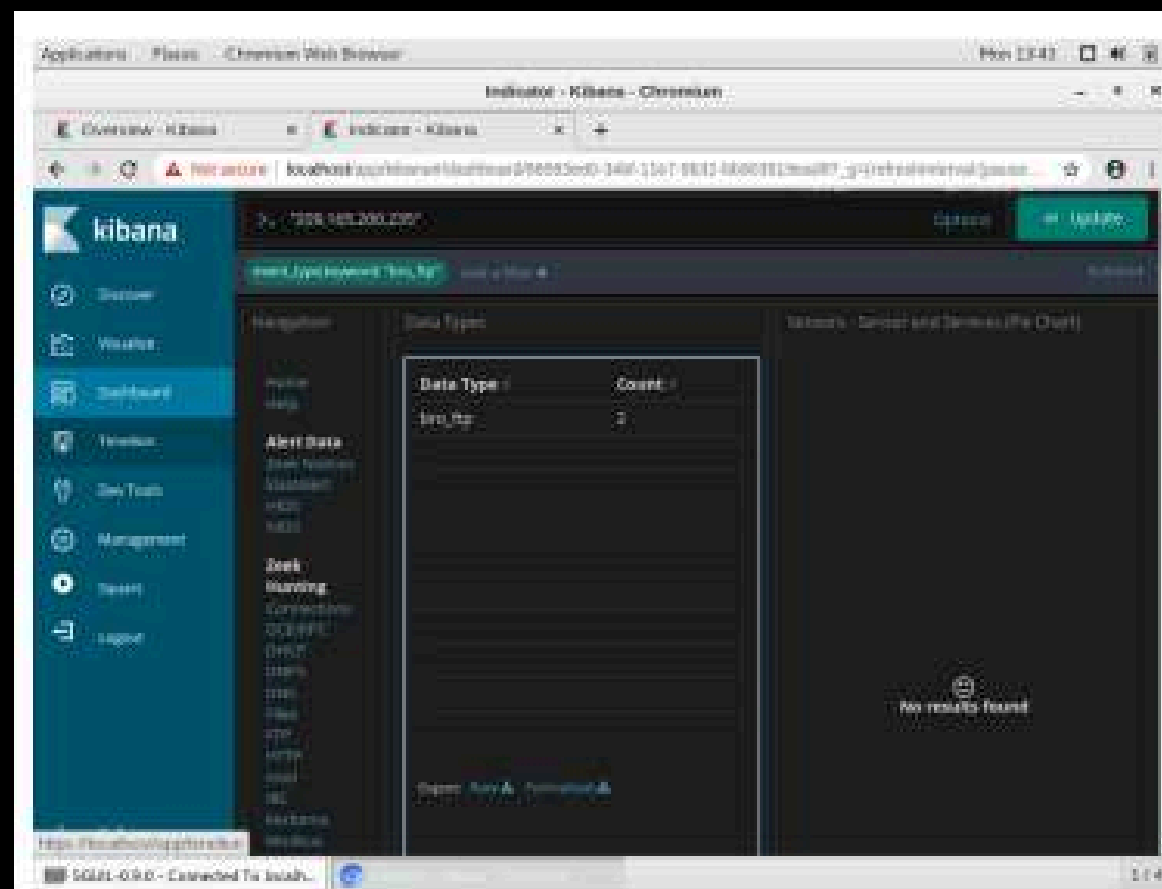
*Pivot su Kibana per arricchire l’analisi tramite i log (IP Lookup): Per investigare ulteriormente utilizzando i log aggregati (forniti da Elastic Stack/Kibana in Security Onion), fare clic destro sull’indirizzo IP di interesse nell’alert 5.1. È possibile scegliere uno dei due IP coinvolti; ad esempio, fare clic destro sull’IP sorgente 209.165.201.17 (attaccante) o sull’IP destinazione 209.165.200.235 (vittima) e selezionare “Kibana IP Lookup > SrcIP” (o DstIP a seconda della scelta) dal menu contestuale. In questo modo si apre Kibana in un browser web, già filtrato per mostrare i log relativi a quell’IP. Una volta dentro Kibana, impostare il giusto intervallo temporale per assicurare di includere la finestra in cui si è verificato l’attacco. Ad esempio, se i log sono stati raccolti l’11 giugno 2020 (come indicato dal lab), modificare il filtro temporale (in alto a destra) selezionando la scheda Absolute e inserendo l’intervallo che copre l’11 giugno 2020 (anziché l’ultimo 24 ore di default). Applicare il nuovo filtro temporale: Kibana mostrerà un dashboard relativo all’IP selezionato con vari pannelli (ad esempio conteggio degli eventi e grafici dei tipi di log registrati).*





Verifica dei log FTP e identificazione del file esfiltrato: Nel dashboard Kibana per l'IP selezionato, individuare il pannello "Sensors and Services" (o simile) che presenta un elenco dei tipi di dati registrati (derivati dai log di Zeek/Bro e altri sensori). In questo elenco dovrebbero comparire voci come ftp e ftp-data, il che indica che del traffico FTP è stato osservato per l'host in questione. Poiché sappiamo che il file confidential.txt non è più accessibile agli utenti (sintomo di una possibile esfiltrazione), concentrarci sul traffico FTP per vedere se è stato usato per rubare il file. Nel pannello dei tipi di log, passare con il mouse sopra la voce relativa a bro\_ftp (FTP) e cliccare sul simbolo "+" che appare accanto ad essa per filtrare i log mostrando solo quelli correlati al traffico FTP. Scorrere quindi verso il basso fino alla sezione All Logs (tutti i log): dovrebbero comparire solo pochi risultati (in questo scenario due voci) corrispondenti alla sessione FTP individuata. Esaminare queste voci di log FTP.

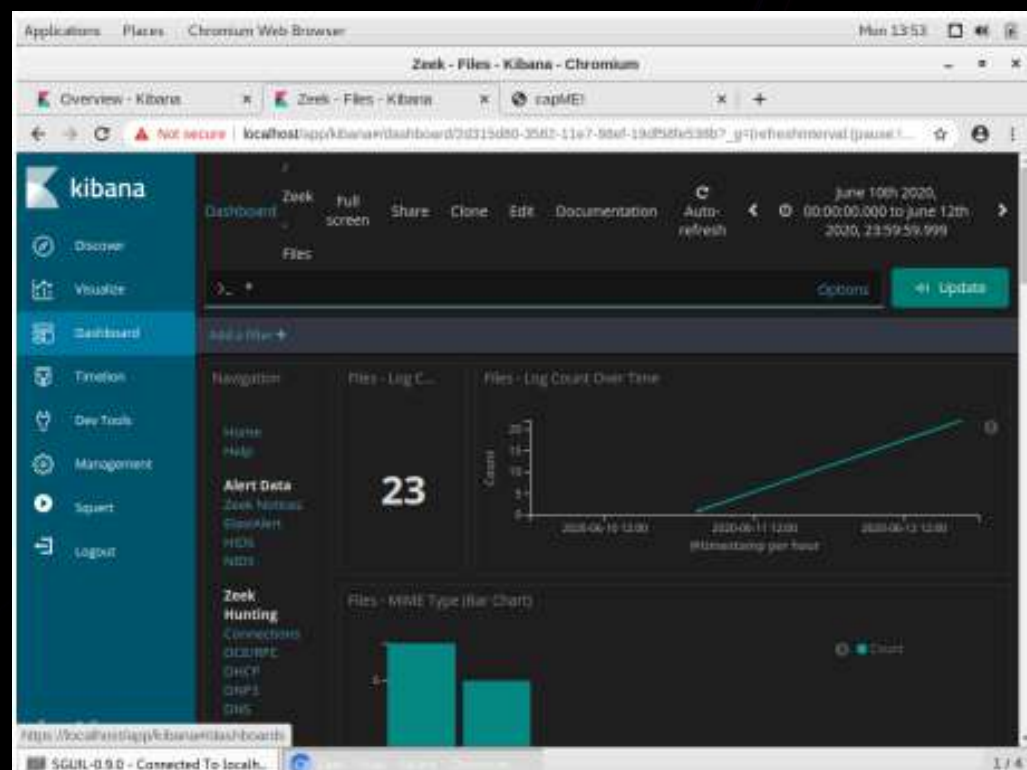




Dall'analisi emergono chiaramente i dettagli della connessione FTP utilizzata dall'attaccante: l'indirizzo IP sorgente risulta essere 192.168.0.11 (porta sorgente 52776), mentre l'indirizzo IP di destinazione è 209.165.200.235 (porta 21, la porta FTP standard). Ciò significa che l'host 192.168.0.11 (controllato dall'attaccante) si è connesso alla macchina compromessa 209.165.200.235 avviando una sessione FTP sulla porta 21. Inoltre, espandendo le informazioni di uno di questi log (cliccando sulla freccia o sul riquadro del singolo evento), si trova un campo come `ftp_argument` che riporta il path del file coinvolto. In particolare, si osserva un riferimento al file `confidential.txt` – ad esempio una stringa del tipo `ftp://209.165.200.235/./confidential.txt` – confermando che proprio quel file è stato oggetto della sessione FTP. Questo indica che l'attaccante ha probabilmente scaricato (o comunque accesso via FTP) il file `confidential.txt` dalla macchina 209.165.200.235.

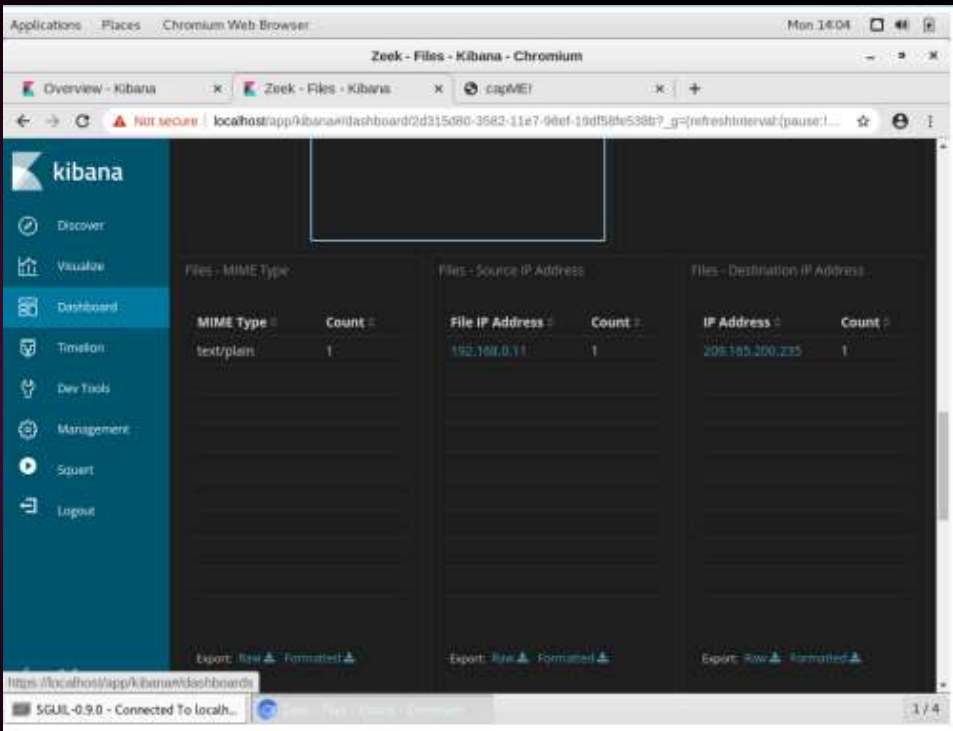
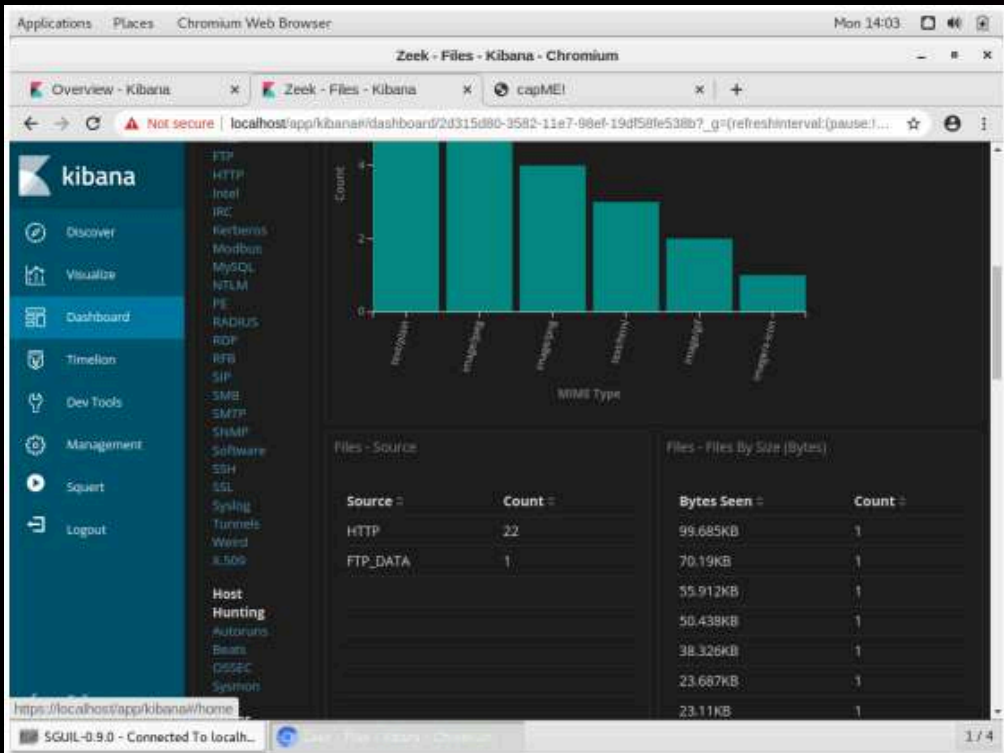


*Analisi dei log FTP: credenziali utilizzate e azioni dell'attaccante: Sempre nella vista dettagliata dei log FTP in Kibana, esaminare i campi di ciascun evento per ricavare ulteriori informazioni. Uno dei log FTP registrerà l'evento di login al server FTP. Cliccando sull>alert \_id (identificativo univoco del log/evento) o espandendo i dettagli completi, è possibile visualizzare la transcript della sessione FTP tra l'attaccante (client) e la vittima (server FTP). Dalla transcript dell'FTP emergono le credenziali che l'attaccante ha usato per autenticarsi sul server FTP di 209.165.200.235. In particolare, si vede che l'attaccante ha effettuato il login con username analyst e password cyberops. Queste sono le stesse credenziali dell'utente analyst che era presente sul sistema vittima (e le stesse usate per accedere alla VM Security Onion), segno che l'attaccante potrebbe averle scoperte durante l'intrusione. Ad esempio, avendo copiato e aperto il file /etc/shadow, l'attaccante potrebbe aver ottenuto gli hash delle password degli utenti e quindi ricavato (o già conosciuto) la password cyberops dell'account analyst, riutilizzandola per l'accesso FTP. La transcript FTP o i campi del log mostrano anche i comandi FTP eseguiti: con ogni probabilità l'attaccante ha eseguito un comando RETR (retrieve) per scaricare il file confidential.txt e poi un DELE (delete) per cancellarlo dal server, spiegando perché il file non è più presente sulla macchina compromessa. Questa sequenza spiega come il file sia stato esfiltrato dal sistema bersaglio.*





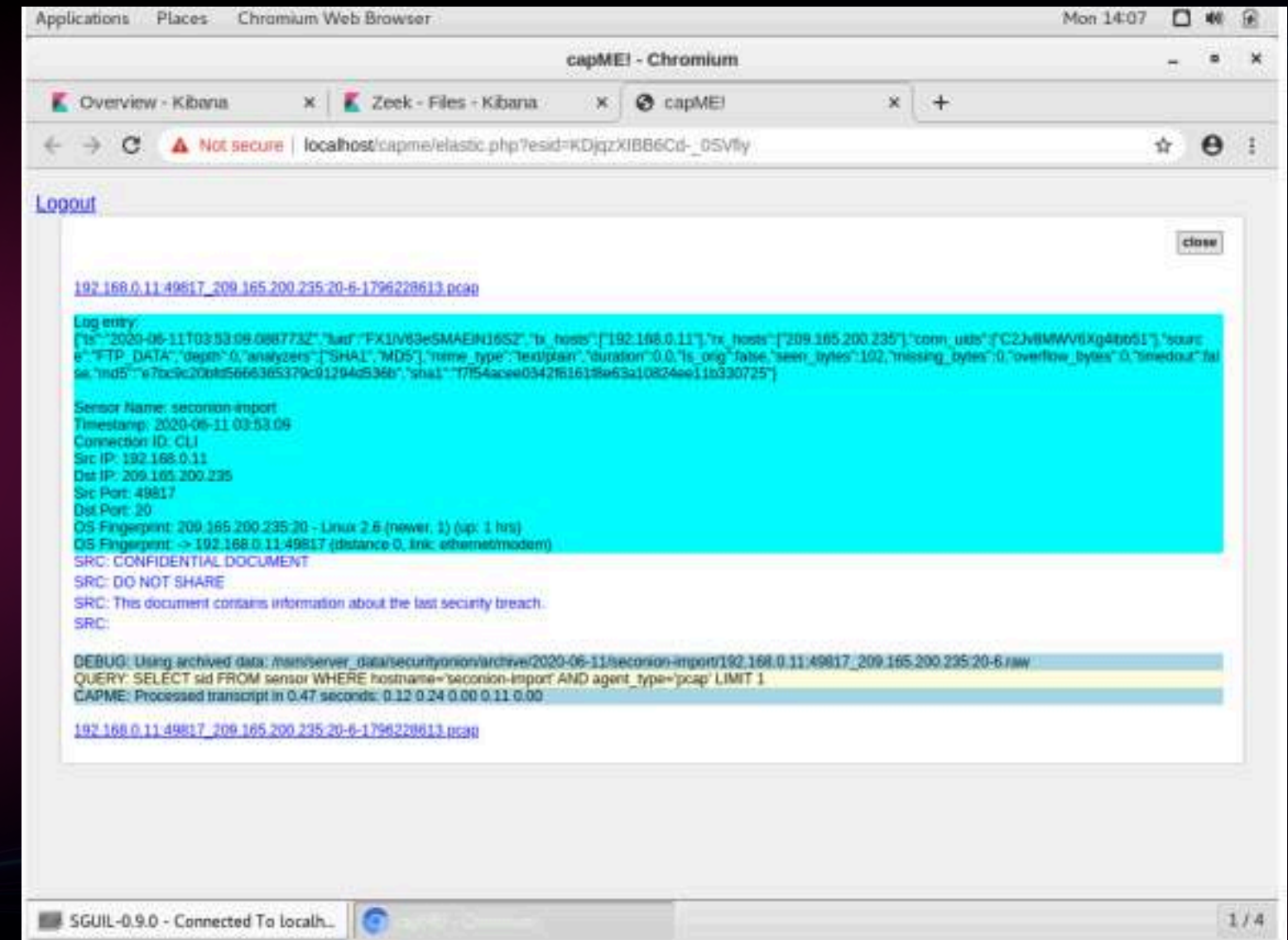
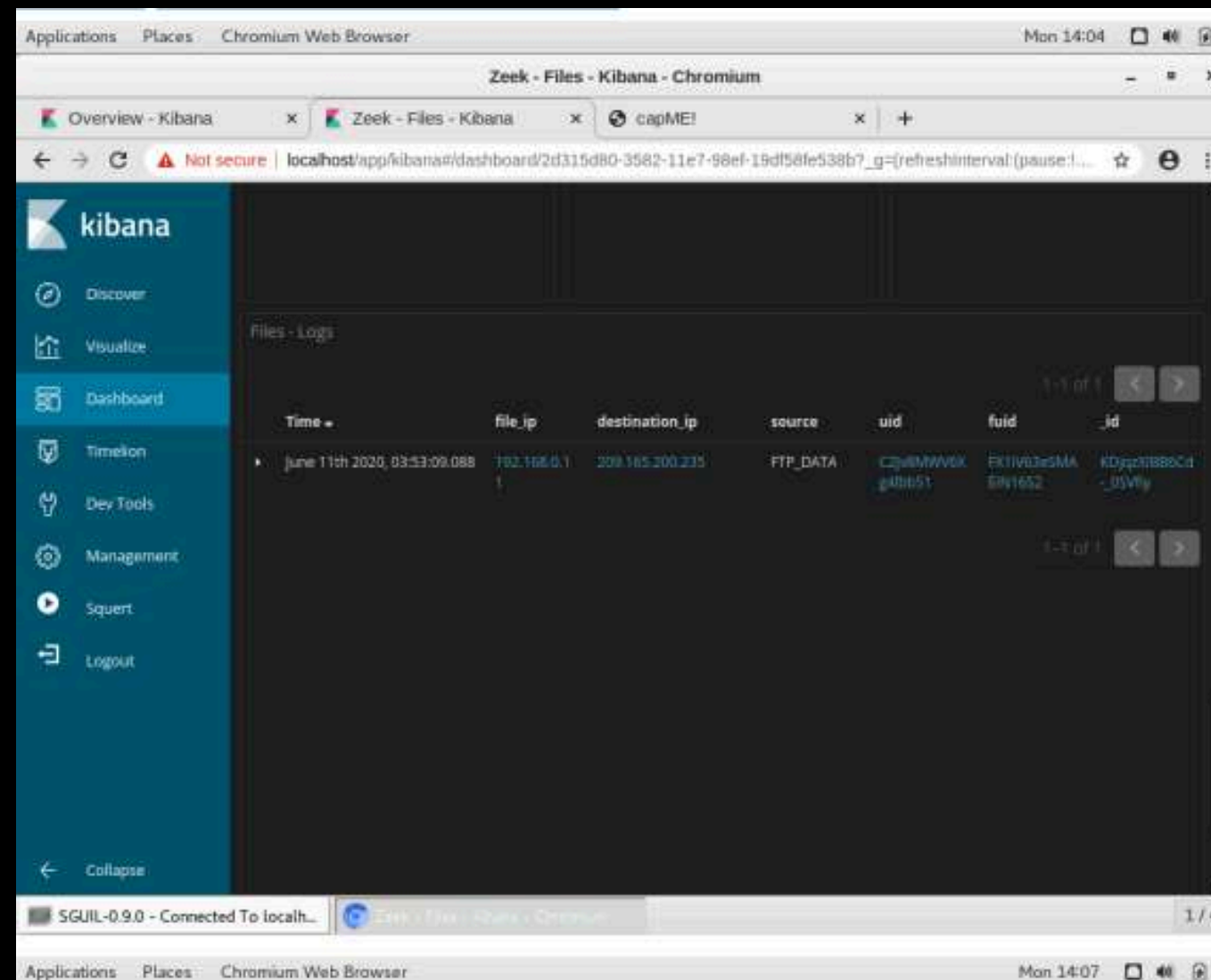
*In cima alla pagina è presente un riepilogo dei MIME types (tipi di file) osservati. In questo scenario, il grafico/elenchi dei MIME types mostrerà la presenza di file di testo e anche alcuni file immagine (ad esempio dovuti ad altri traffici web catturati). Inoltre, nel riquadro Files – Source si noteranno le fonti dei trasferimenti di file registrati, tra cui le voci HTTP e FTP (indicando che alcuni file sono stati trasferiti via HTTP e via FTP rispettivamente).*



*Poiché siamo interessati al file sottratto via FTP, filtrare ulteriormente i risultati per mostrare solo i trasferimenti FTP. Nel pannello dei Types cercare la categoria FTP\_DATA (che rappresenta i dati dei file trasferiti via FTP) e cliccare sul simbolo “+” accanto ad essa per applicare il filtro. Scorrere poi la pagina verso il basso fino alla sezione All Logs per vedere gli eventi filtrati relativi ai file trasferiti via FTP. Dovrebbe apparire il log del trasferimento del file confidential.txt. Analizzando questo log, si possono ricavare dettagli importanti: il tipo MIME del file trasferito risulta text/plain (cioè un semplice file di testo) e viene confermato l’indirizzo IP sorgente e destinazione coinvolti nello scambio. Il log indica infatti un trasferimento di un file di testo tra l’IP 209.165.200.235 e 192.168.0.11 avvenuto il 11 giugno 2020 alle ore 3:53 (ora presumibilmente UTC). Questo orario coincide con la finestra temporale dell’attacco e conferma esattamente quando è avvenuta l’esfiltrazione.*



*Esplorando il log del file, è possibile trovare ulteriori dettagli, incluso un possibile estratto del contenuto del file stesso (Zeek, infatti, registra anche l'inizio del contenuto per alcuni file di testo trasferiti). Nel nostro caso, viene rivelato il contenuto del file confidential.txt:*



**DOCUMENTO CONFIDENZIALE – NON CONDIVIDERE.** Questo documento contiene informazioni sull'ultima breccia di sicurezza...

*Il messaggio sopra, contenuto nel file rubato, conferma che si trattava di un documento riservato riguardante una recente violazione della sicurezza. (Nella transcript originale fornita dal lab, il testo era in lingua spagnola, qui sopra tradotto in italiano per chiarezza.) Questo contenuto chiarisce la natura sensibile del file confidential.txt sottratto.*



## **Raccomandazione di sicurezza finale:**

*Sulla base di tutti i dati raccolti, è evidente che l'attaccante ha sfruttato le credenziali dell'utente analyst per accedere ai servizi (FTP) e sottrarre informazioni. Come misura minima e immediata, è necessario cambiare la password dell'account "analyst" su tutti i sistemi coinvolti. Nel contesto del lab, ciò significa aggiornare la password su 209.165.200.235 (la macchina compromessa) e anche su 192.168.0.11, assicurandosi che l'attaccante non possa più riutilizzare quelle credenziali. In un ambiente reale, si raccomanda inoltre di cambiare le password di tutti gli account privilegiati (incluso eventualmente root), verificare che non siano stati creati account backdoor nei file /etc/passwd.*

# CONCLUSIONE:

Il lavoro svolto durante questi test ha rappresentato un'importante occasione per mettere in pratica concetti fondamentali della sicurezza informatica. Attraverso l'analisi dei dati di rete, la valutazione degli alert, l'utilizzo operativo delle informazioni di sicurezza e l'applicazione di tecniche di digital forensics e incident response, è stato possibile acquisire una visione più completa e concreta delle attività che caratterizzano un ambiente SOC.

In particolare, i test eseguiti hanno dato modo di approfondire un aspetto critico della sicurezza a livello di sistema, evidenziando come vulnerabilità apparentemente semplici possano avere conseguenze gravi se non adeguatamente gestite.

Il lavoro di squadra svolto con il team RaptorShield ha avuto un ruolo fondamentale nel raggiungimento degli obiettivi, favorendo il confronto, la condivisione di competenze e la risoluzione collaborativa dei problemi.

Nel complesso, l'esperienza si è rivelata formativa e ha fornito solide basi pratiche per affrontare con maggiore consapevolezza le sfide del settore della cybersecurity.