

BUILDWEEK III



01

MALWARE ANALYSIS

02

ANYRUN

03

NAVIGATING THE LINUX
FILESYSTEM

04

EXTRACT AN EXECUTABLE FROM
A PCAP

05

BONUS 1 ANYRUN

06

BONUS 2 INTERPRET HTTP AND
DNS DATA TO ISOLATE THREAT
ACTOR

07

BONUS 3 ISOLATE
COMPROMISED HOST USING 5-
TUPLE



MALWARE ANALYSIS

INFORMAZIONI PRINCIPALI - AdwareCleaner.exe

Questo rapporto fornisce i risultati di un'Analisi Statica condotta sul file AdwareCleaner.exe.

L'analisi si concentra sulle librerie importate e sulle loro funzioni per determinare il comportamento e le capacità potenziali del malware.

Informazioni sul File

- Nome del File: AdwareCleaner.exe
- Tipo di Analisi: Analisi Statica
- Tipo di File: Portable Executable 32
- Peso File: 190.82 KB

Risultati Principali: Il file importa diverse librerie di sistema utilizzate comunemente dagli eseguibili Windows. Tuttavia, la combinazione di queste importazioni può indicare comportamenti specifici e potenzialmente dannosi.

Analisi delle Importazioni

Le seguenti librerie DLL di Windows sono state identificate nella **Import Address Table (IAT)**. L'analisi di queste importazioni permette di dedurre le funzionalità potenziali del malware.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00006E12	N/A	000066B0	000066B4	000066B8	000066BC	000066C0
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
RPCRT4.dll	8

1

KERNEL32.dll

La libreria KERNEL32.dll fornisce funzioni di base per la gestione del sistema, inclusi memoria, processi e operazioni sui file.

- **CreateFile**: Può essere utilizzata per creare, aprire o modificare file, potenzialmente per depositare payload o registri.
- **WriteFile**: Suggerisce la capacità di scrivere dati nei file, forse per esfiltrazione o persistenza.
- **DeleteFile**: Indica la capacità di cancellare file, ed aumenta la capacità distruttiva del malware.
- **ReadFile**: Indica la capacità di leggere file, ad esempio per accedere a informazioni sensibili.
- **LoadLibrary**: Indica il caricamento dinamico di librerie, possibilmente per comportamenti modulari.

AdwareCleaner.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
00006E12	N/A	000066B0	000066B4	000066B8	000066BC	000066C0
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
00007A40	00007A40	01DF	GetTickCount			
000079B0	000079B0	0169	GetFullPathNameA			
000079C4	000079C4	026E	MoveFileA			
000079D0	000079D0	030A	SetCurrentDirectoryA			
000079E8	000079E8	015E	GetFileAttributesA			
000079FE	000079FE	0171	GetLastError			
00007A0E	00007A0E	004B	CreateDirectoryA			
00007A22	00007A22	0319	SetFileAttributesA			
0000798E	0000798E	02DB	SearchPathA			
0000799C	0000799C	01B5	GetShortPathNameA			
00007A50	00007A50	0163	GetFileSize			
00007A5E	00007A5E	017D	GetModuleFileNameA			
00007A74	00007A74	0142	GetCurrentProcess			
00007A88	00007A88	0043	CopyFileA			

2

User32.dll

La libreria USER32.dll è utilizzata per interagire con l'interfaccia utente (UI) e per gestire input.

Le funzioni più usate da malware a scopo malevolo sono:

- **MessageBox**: Potrebbe essere usata per mostrare falsi messaggi di errore o avvisi per ingannare gli utenti.
- **FindWindow**: Può essere utilizzata per individuare finestre specifiche, forse per monitorare o dirottare applicazioni.

AdwareCleaner.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
00007222	N/A	000066C4	000066C8	000066CC	000066D0	000066D4
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
00007DDE	00007DDE	0060	CreateWindowExA			
00007E1A	00007E1A	00C6	EndDialog			
00007E26	00007E26	0231	ScreenToClient			
00007E38	00007E38	0174	GetWindowRect			
00007E48	00007E48	00C2	EnableMenuItem			
00007E5A	00007E5A	015C	GetSystemMenu			
00007E6A	00007E6A	0247	SetClassLongA			
00007E7A	00007E7A	01AE	IsWindowEnabled			
00007E8C	00007E8C	0283	SetWindowPos			
00007E9C	00007E9C	015A	GetSysColor			
00007EAA	00007EAA	016E	GetWindowLongA			
00007EBC	00007EBC	024D	SetCursor			
00007EC8	00007EC8	01BA	LoadCursorA			
00007ED6	00007ED6	0038	CheckDlgButton			

3

GDI32.dll

La libreria GDI32.dll è utilizzata per il rendering grafico e la manipolazione di immagini.

- **GetDeviceCaps:** Viene utilizzato per reperire informazioni sensibili riguardo il dispositivo video (memoria disponibile, risoluzione schermo, etc.)

AdwareCleaner.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
000072B4	N/A	000066D8	000066DC	000066E0	000066E4	000066E8
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
0000802E	0000802E	020E	SelectObject			
0000804E	0000804E	0216	SetBkMode			
0000805A	0000805A	003A	CreateFontIndirectA			
0000803E	0000803E	023C	SetTextColor			
00008086	00008086	008F	DeleteObject			
00008096	00008096	016B	GetDeviceCaps			
00008070	00008070	0029	CreateBrushIndirect			
000080A6	000080A6	0215	SetBkColor			

4

SHELL32.dll

La libreria SHELL32.dll fornisce accesso alle operazioni della shell, come la gestione di file e cartelle.

- **ShellExecute**: Consente al malware di eseguire file o comandi, forse per lanciare payload aggiuntivi o script.
- **SHGetFolderPath**: Può individuare directory di sistema come la cartella di avvio, utilizzabile per la persistenza.

AdwareCleaner.exe				
Module Name	Imports	OFTs	TimeStamp	ForwarderCh
00007340	N/A	000066EC	000066F0	000066F4
szAnsi	(nFunctions)	Dword	Dword	Dword
SHELL32.dll	6	000076BC	00000000	00000000
OFTs	FTs (IAT)	Hint	Name	
Dword	Dword	Word	szAnsi	
00008122	00008122	00C3	SHGetSpecialFolderLocation	
0000810A	0000810A	00BC	SHGetPathFromIDListA	
000080F4	000080F4	0079	SHBrowseForFolderA	
000080E2	000080E2	00AC	SHGetFileInfoA	
000080D2	000080D2	0107	ShellExecuteA	
000080BE	000080BE	009A	SHFileOperationA	

5

ADVAPI32.dll

La libreria ADVAPI32.dll offre funzioni avanzate, inclusa la gestione del registro di sistema e delle autorizzazioni.

- **RegOpenKeyEx**: Suggerisce la capacità di leggere chiavi di registro, forse per ricognizione o configurazione.
- **RegSetValueEx**: Indica la capacità di modificare chiavi di registro, possibilmente per persistenza o disabilitazione di meccanismi di sicurezza.

AdwareCleaner.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
000073E2	N/A	00006700	00006704	00006708	0000670C	00006710
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
000081A2	000081A2	01CB	RegCloseKey			
000081D2	000081D2	01EC	RegOpenKeyExA			
000081C2	000081C2	01D4	RegDeleteKeyA			
000081B0	000081B0	01D8	RegDeleteValueA			
0000814C	0000814C	01E1	RegEnumValueA			
00008190	00008190	01D1	RegCreateKeyExA			
0000817E	0000817E	0204	RegSetValueExA			
0000816A	0000816A	01F7	RegQueryValueExA			
0000815C	0000815C	01DD	RegEnumKeyA			

6

VERSION.dll

La libreria VERSION.dll è utilizzata per recuperare informazioni sulle versioni dei file.

- **GetFileVersionInfo**: Potrebbe essere usata per estrarre dettagli sulle versioni dei file di sistema, forse per riconoscione o verifiche di compatibilità.
- **VerQueryValue**: Può aiutare a verificare i dati delle versioni dei file, forse per evitare il rilevamento mirato a specifiche versioni di sistema operativo.

AdwareCleaner.exe				
Module Name	Imports	OFTs	TimeStamp	Forwarders
000074CE	N/A	0000673C	00006740	00006744
szAnsi	(nFunctions)	Dword	Dword	Dword
VERSION.dll	3	000077D8	00000000	00000000
OFTs	FTs (IAT)	Hint	Name	
Dword	Dword	Word	szAnsi	
000082B4	000082B4	0001	GetFileVersionInfoSizeA	
0000829E	0000829E	0000	GetFileVersionInfoA	
0000828C	0000828C	000A	VerQueryValueA	

Indicatori Comportamentali

In base alle librerie importate e alle loro funzioni, si possono dedurre i seguenti comportamenti potenziali:

1. Manipolazione di File:

Capacità di creare, leggere, scrivere o eliminare file, forse per consegnare payload o alterare file di sistema.

2. Manipolazione del Registro di Sistema:

Probabile modifica di chiavi di registro per persistenza o disabilitazione di misure di sicurezza.

3. Interazione con l'Utente:

Possibilità di mostrare falsi avvisi o di intercettare input utilizzando funzioni di USER32.dll.

4. Ricognizione di Sistema:

Probabile raccolta di informazioni sul sistema, come versioni dei file o processi in esecuzione.

5. Persistenza:

L'uso di SHGetFolderPath o modifiche al registro suggeriscono tentativi di persistenza nel sistema.

Raccomandazioni

1. Non Eseguire:

- Evitare di eseguire il file su macchine di produzione. Utilizzare una sandbox o una macchina virtuale per analisi dinamiche.

2. Verifica degli Hash:

- Inviare l'hash del file (MD5/SHA256) a VirusTotal o altre piattaforme di intelligence per verificare la reputazione.

3. Indurimento del Sistema:

- Configurare correttamente le autorizzazioni del registro e dei file per minimizzare l'impatto del malware.

4. Monitoraggio della Rete:

- Monitorare attività di rete insolite, come connessioni in uscita o esfiltrazione di dati.

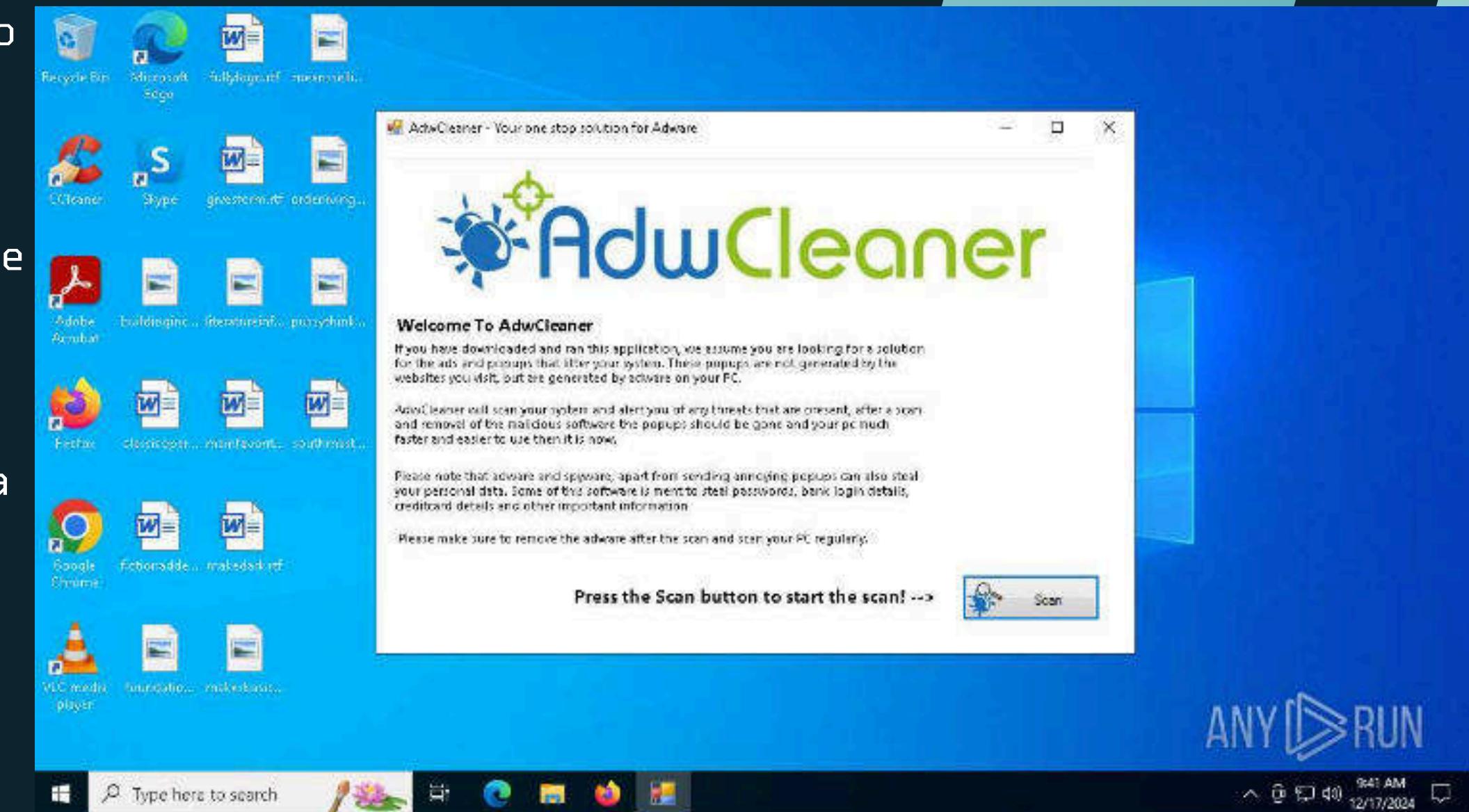
Conclusioni

L'analisi statica di AdwareCleaner.exe rivela potenziali comportamenti dannosi, tra cui manipolazione di file e registro e persistenza. La combinazione di librerie importate e funzioni suggerisce che il file possa utilizzare tecniche di offuscamento, ricognizione e manipolazione del sistema.

Analisi Dinamica - AdwereCleaner.exe

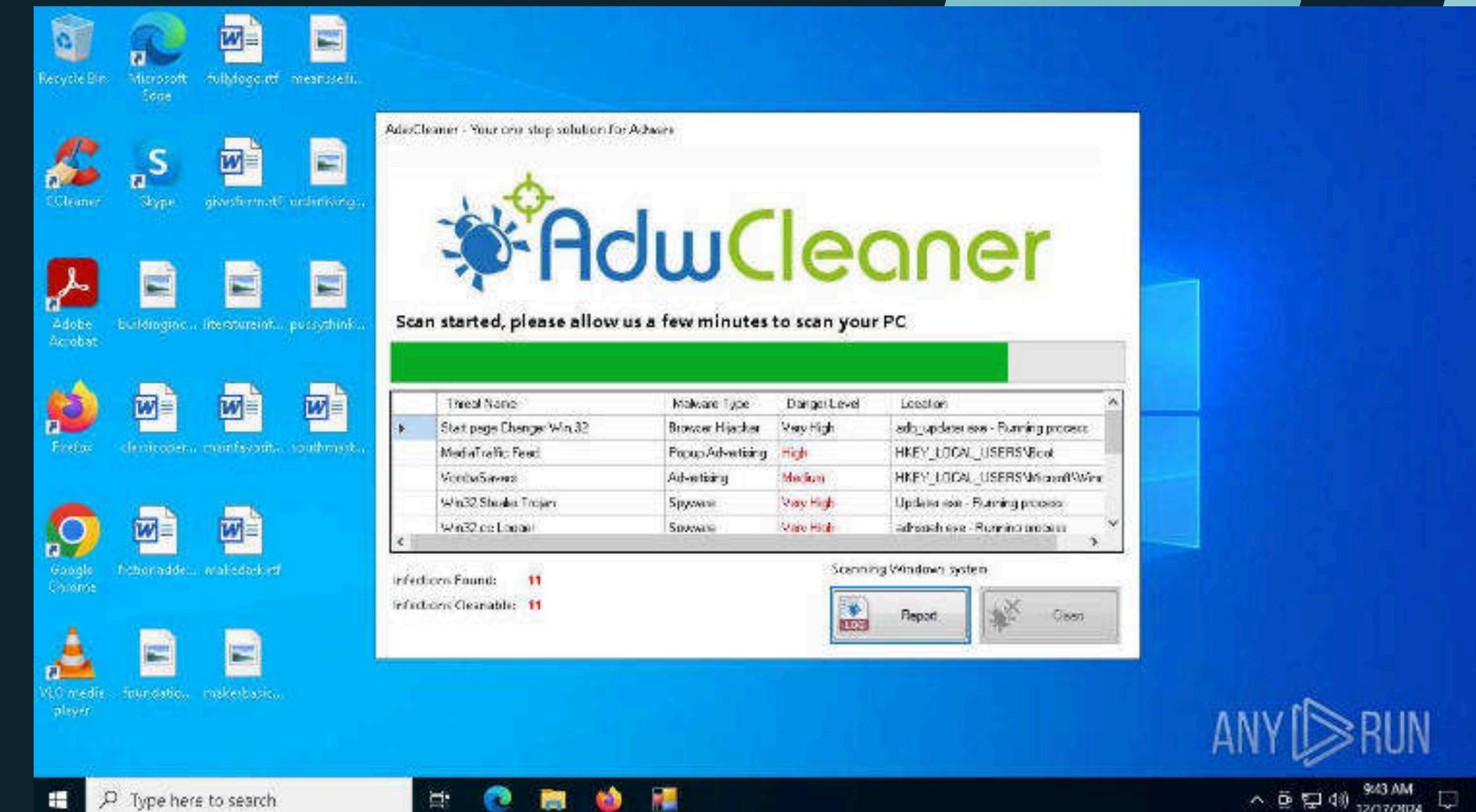
Per l'analisi dinamica del malware è stato usato AnyRun.

Immediatamente durante l'esecuzione di AdwereCleaner, il programma malevolo cerca e legge le specifiche del sistema, le opzioni di sicurezza e modifica i registri di sistema per avviarsi automaticamente ad ogni futura accensione del computer. Poi apre una finestra mirata ad imitare la controparte legittima del software "AdwCleaner" distribuito da MalwareBytes.



Analisi Dinamica - AdwereCleaner.exe

Premendo "Scan" il programma finge uno scan del sistema e "rileva" una serie di virus il quale ha l'unico scopo di spaventare l'utente e spingerlo a premere "Clean" il prima possibile (social engineering/pretexting). Oltre ad esso, il malware non esegue altre azioni in background.



Analisi Dinamica - AdwereCleaner.exe

Una volta finita la “scansione” e premuto il pulsante Pulisci, appare una finestra che avverte che il software non può rimuovere le minacce rilevate in quanto un software di prova, e che l’opzione di rimuovere i programmi indesiderati è bloccata sotto il pagamento di 60 dollari.

Fortunatamente, il redirect al sito web di pagamento presumibilmente falso non funziona più, ma la teoria più realistica dell’obiettivo del malware è di spingere l’utente sfortunato a dare via i propri dati bancari per rimuovere delle minacce inesistenti.

AdwCleaner - Your one stop solution for Adware

Upgrade to the full version now!

This is the trial version of AdwCleaner, it can only scan threats but cannot remove them. To remove the found malware and clean your system, please buy the full version.

On sale now!

Only \$59,99

Normal price: \$99,99. Sale ending on: 12/16/2024

[After purchase your serial number will be E-mailed to you. click here to enter it.](#)

 Navigation 1

Analisi Dinamica - AdwereCleaner.exe

Comportamenti Sospetti rilevati da AnyRun:

MALICIOUS	SUSPICIOUS	INFO
<p>Changes the autorun value in the registry</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260)	<p>Reads security settings of Internet Explorer</p> <ul style="list-style-type: none">• AdwereCleaner.exe (PID: 6176)• 6AdwCleaner.exe (PID: 6260) <p>Executable content was dropped or overwritten</p> <ul style="list-style-type: none">• AdwereCleaner.exe (PID: 6176) <p>Checks Windows Trust Settings</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>Reads Internet Explorer settings</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260)	<p>Checks supported languages</p> <ul style="list-style-type: none">• AdwereCleaner.exe (PID: 6176)• 6AdwCleaner.exe (PID: 6260) <p>Reads the computer name</p> <ul style="list-style-type: none">• AdwereCleaner.exe (PID: 6176)• 6AdwCleaner.exe (PID: 6260) <p>Process checks computer location settings</p> <ul style="list-style-type: none">• AdwereCleaner.exe (PID: 6176) <p>Disables trace logs</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>Reads Environment values</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>Reads the machine GUID from the registry</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>Reads the software policy settings</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>The process uses the downloaded file</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>Creates files or folders in the user directory</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260) <p>Checks proxy server information</p> <ul style="list-style-type: none">• 6AdwCleaner.exe (PID: 6260)

02

Esercizio 2 ANY.RUN

Attraverso l'utilizzo di AnyRun andiamo ad analizzare due log dall'applicativo e andremo a vedere come identificare e risolvere le vulnerabilità

Il primo link

<https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d/>

L'analisi è stata condotta il 25 agosto 2024 su un sistema operativo Windows 10 Professional (build: 19045, 64 bit).

Il file analizzato, "66bddfcb52736_vidar.exe", è stato identificato come un malware appartenente alla categoria degli "stealer", specificamente Vidar e Lumma. Questi malware sono progettati per sottrarre informazioni sensibili dal sistema infetto, come credenziali di accesso e portafogli di criptovalute.

02

Esercizio 2

ANY.RUN

FASI DELL'ANALISI E INDIVIDUAZIONE DEL MALWARE

The image shows a dual-screen setup for malware analysis. The left screen displays a Windows 10 desktop with various icons and a taskbar. A watermark in the center of the desktop reads "MOVE YOUR MOUSE TO VIEW SCREENSHOTS". The right screen is a detailed analysis interface for the ANY.RUN platform.

Analysis Window Details:

- Title Bar:** Malicious activity
- Sample Information:** 66bddfc52736_vidar.exe, MD5: FEDB687ED23F77925835623027F7998B, Win10 64 bit, Complete
- Indicators:** vider, lumma, stealer, loader
- Tracker:** Loader, Lumma, Stealer, Vida
- Tool Buttons:** Get sample, IOC, MalConf, Restart, Text report, Graph, ATT&CK, Summary (beta), Export
- Process List:** CPU tab, Processes section, Filter by PID or name: 6780, 66bddfc52736_vidar.exe. The list includes multiple entries for RegAsm.exe (PIDs 6804, 6872, 6884, 6896) and one entry for HCAEHJJKFC.exe (PID 1560).

02

Esercizio 2

ANY.RUN

Creazione di processi secondari

Il malware ha avviato più istanze del processo "RegAsm.exe", un'utilità legittima di Microsoft .NET Framework, con i PID 6864, 6872, 6884, 6896 e 6908. Questo comportamento suggerisce l'uso di tecniche di "process hollowing" o "process injection" per mascherare le attività malevoli all'interno di processi legittimi.

[6908] RegAsm.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Threat Verdict

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

Indicators: 🛡️ ↻ 🔍 ✎

100 OUT OF 100

Process information

- Username: admin
- SID: S-1-5-21-1693682860-607145093-2874071422-1001
- IL: MEDIUM
- Start: 6.86 s

File information

- Company: Microsoft Corporation
- Description: Microsoft .NET Assembly Registration Utility
- Version: 4.8.9037.0 built by: NET481REL1

Command line

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
```

Timeline of the process

0 s - 6.86 s

Danger 4

- T1555.003 Credentials from Web Browsers (1)
- Steals credentials from Web Browsers
- T1552.001 Credentials In Files (2)
- Steals credentials from Web Browsers
- Actions looks like stealing of personal data
- VIDAR has been detected (YARA)
- T1518 Software Discovery (1)
- Actions looks like stealing of personal data

Warning 12

- Potential Corporate Privacy Violation
- T1059.003 Windows Command Shell (1)
- Starts CMD.EXE for commands execution
- T1012 Query Registry (4)
- Reads the date of Windows installation
- Searches for installed software
- Checks Windows Trust Settings

Processes Filter by PID or name Only important

PID	Process Name	File Path	CFG	DMP	Actions
6908	RegAsm.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	vidar	18k	6k 111
1568	HCAEHJJKFC.exe	PE		266	83 38
2572	conhost.exe	0xffffffff -ForceV1		70	101 25
4704	RegAsm.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	lumma	4k	546 75
6248	CAFHDBGHJK.exe	PE		264	83 37
1292	conhost.exe	0xffffffff -ForceV1		69	101 25
6340	RegAsm.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	vidar	4k	30 34
6284	cmd.exe	/c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit		214	50 15

02

Esercizio 2

ANY.RUN

Attività sospette rilevate

I processi "RegAsm.exe" hanno eseguito diverse azioni indicative di attività malevole:

Lettura delle impostazioni di sicurezza di Internet Explorer.

Creazione di file eseguibili immediatamente dopo l'avvio.

Verifica delle impostazioni di fiducia di Windows.

Ricerca di software installato nel sistema.

Utilizzo di "cmd.exe" per eseguire comandi, inclusa l'esecuzione di "timeout.exe" per introdurre ritardi nell'esecuzione.

Process details ID 6908 Malicious
Danger 4

[T1555.003](#) Credentials from Web Browsers (1)
Steals credentials from Web Browsers

[T1552.001](#) Credentials In Files (2)
Steals credentials from Web Browsers
Actions looks like stealing of personal data

VIDAR has been detected (YARA)

[T1518](#) Software Discovery (1)
Actions looks like stealing of personal data

02

Esercizio 2

ANY.RUN

Comportamento di furto di informazioni:

I processi "RegAsm.exe" hanno mostrato comportamenti tipici di un "stealer":

Furto di credenziali dai browser web.

Accesso a directory e file contenenti informazioni sensibili.

Comunicazione con server di comando e controllo (C2) per l'esfiltrazione dei dati raccolti.

[4704] RegAsm.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAs

Threat Verdict	
100 OUT OF 100	Malicious <small>The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions</small> Indicators:

Timeline of the process 0 s 26.70 s

Danger 5
LUMMA has been detected (YARA)
Stealers network behavior
LUMMA has been detected (SURICATA)
[T1552.001](#) Credentials In Files (1)
Actions looks like stealing of personal data
[T1518](#) Software Discovery (1)
Actions looks like stealing of personal data

Warning 2
[T1012](#) Query Registry (1)
Searches for installed software
[T1518](#) Software Discovery (1)
Searches for installed software

Process information

Username:	admin
SID:	S-1-5-21-1693682860-607145093-2874071422-1001
IL:	MEDIUM
Start:	26.70 s

File information

Company:	Microsoft Corporation
Description:	Microsoft .NET Assembly Registration Utility
Version:	4.8.9037.0 built by: NET481REL1

Command line
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"

02

Esercizio 2

ANY.RUN

Indicatori di compromissione (IoC)

Hash del file

MD5: FEDB687ED23F77925B35623027F799BB

SHA1: 7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81

SHA256: 325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1

Nome del file

66bddfcb52736_vidar.exe

Percorso del file

C:\Users\admin\Desktop\66bddfcb52736_vidar.exe

? 66bddfcb52736_vidar.exe

Submit

Downloaded | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows (194.56 kb)

Mime: application/x-dosexec Entropy: 7.97

Main HEX PE

MD5	FEDB687ED23F77925B35623027F799BB
SHA1	7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
SHA256	325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1
SSDEEP	6144:yZlGEaS7npmSNlfI330znhlBf4hJYBaZaH55B:rGEaSVmSmI30znhSYaZa5

TriID 82.9% Generic CIL Executable (.NET, Mono, etc.)

7.4% Win32 Dynamic Link Library (generic)

5.1% Win32 Executable (generic)

2.2% Generic Win/DOS Executable

2.2% DOS Executable Generic

02

Esercizio 2

ANY.RUN

Comunicazioni di rete

Il malware ha tentato di comunicare con server remoti per l'esfiltrazione dei dati. Sono stati rilevati tentativi di connessione a domini sospetti e indirizzi IP non riconosciuti.

Azioni dell'utente vittima

L'utente ha eseguito manualmente il file "66bddfcb52736_vidar.exe", probabilmente ingannato da tecniche di ingegneria sociale o phishing.

Azioni dell'attaccante

Distribuzione del malware tramite tecniche di social engineering.

Utilizzo di processi legittimi come "RegAsm.exe" per mascherare le attività malevoli.

Furto di informazioni sensibili dal sistema infetto.

Esfiltroazione dei dati raccolti verso server controllati dall'attaccante.

L'analisi dettagliata del file "66bddfcb52736_vidar.exe" ha rivelato la presenza di un malware sofisticato, capace di sottrarre informazioni sensibili utilizzando tecniche avanzate per eludere la rilevazione.

È fondamentale adottare misure di sicurezza adeguate, come l'educazione degli utenti sui rischi del phishing, l'implementazione di soluzioni antivirus aggiornate e il monitoraggio continuo delle attività di rete, per prevenire infezioni simili in futuro.

02

Esercizio 2

ANY.RUN

IL SECONDO LINK

[HTTPS://APP.ANY.RUN/TASKS/F1F20828-2222-46FB-A886-09F77581E67B/](https://app.any.run/tasks/F1F20828-2222-46FB-A886-09F77581E67B/)

La scansione condotta su un file sospetto tramite la piattaforma ANY.RUN ha prodotto un esito negativo, indicando che non sono state rilevate minacce nel file in questione. L'analisi è stata effettuata su un sistema Windows 10 (versione 19045, 64 bit). Non sono stati riscontrati comportamenti anomali che suggeriscano una compromissione del sistema o attività dannose.

02

Esercizio 2

ANY.RUN

DETTAGLI DELL'ANALISI URL COLLEGATO

L'URL È STATO SEGNALATO COME SOSPETTO, TUTTAVIA L'ANALISI EFFETTUATA SUL FILE TRAMITE LA PIATTAFORMA ANY.RUN NON HA RILEVATO MINACCE. POTREBBE TRATTARSI DI UN URL DI PHISHING O DI UN LINK LEGITTIMO UTILIZZATO IN MODO FRAUDOLENTO. LA VERIFICA TRAMITE ANY.RUN, PERÒ, HA DATO UN ESITO NEGATIVO IN TERMINI DI SICUREZZA.

[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: ↗

Timeline of the process

0 s - 4.85 s

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 4.85 s

File information

Company: Google LLC
Description: Google Chrome
Version: 122.0.6261.70

Command line ⓘ ⓘ

"C:\Program Files\Google\Chrome\Application\chrome.exe" --disk-cache-dir=n ull --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache -- disable-background-networking --disable-features=OptimizationGuideModelDown loading,OptimizationHintsFetching,OptimizationTargetPrediction,OptimizationHints "https://click.convertkit-mail2.com/wwwuqvqrrwagh50nddc7hnxdxxx u8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2lbnVyc2VyZWNy dwI0ZXJz"

02

Esercizio 2 ANY.RUN

SE IL FILE È GIÀ PRESENTE IN DATABASE DI MINACCE COMUNI, CIÒ POTREBBE INFLUENZARE IL GIUDIZIO SULL'EVENTUALE PERICOLO. NEL CASO DI UN ESITO NEGATIVO DA PARTE DI ANY.RUN, POSSIAMO CONCLUDERE CHE NON È STATO IDENTIFICATO COME FILE DANNOSO.

RISULTATO DELLA SCANSIONE
L'ANALISI EFFETTUATA IL 25 AGOSTO 2024 NON HA INDIVIDUATO ATTIVITÀ MALEVOLI O PERICOLOSE ALL'INTERNO DEL FILE. QUESTO POTREBBE INDICARE CHE IL FILE ESAMINATO È SICURO O CHE I COMPORTAMENTI MALEVOLI NON SONO STATI ANCORA RILEVATI DA QUESTA PIATTAFORMA.

02

Esercizio 2

ANY.RUN

Riflessioni e possibilità di Falso Positivo

Sebbene ANY.RUN non abbia rilevato minacce, è possibile che la scansione non abbia identificato alcuni comportamenti dannosi più sottili, che potrebbero essere rilevabili solo con analisi più approfondite o mediante l'uso di soluzioni antivirus più specifiche.

I file analizzati in ambienti di sandboxing come ANY.RUN potrebbero comportarsi diversamente in ambienti di produzione o su macchine non protette. Per esempio, il file potrebbe attivarsi solo sotto certe condizioni (come una connessione a Internet o il download di altri componenti).

Falso Positivo?

La scansione non ha rilevato alcuna minaccia. Tuttavia, questo non esclude la possibilità di un falso negativo, in cui il file potrebbe comportarsi in modo malevolo in contesti o configurazioni particolari non rilevati durante la scansione. L'analisi è stata eseguita in un ambiente controllato, e non possiamo escludere la possibilità che il file, se eseguito in un sistema operativo "live" non protetto, possa interagire con altre applicazioni o con risorse di rete in modo dannoso.

02

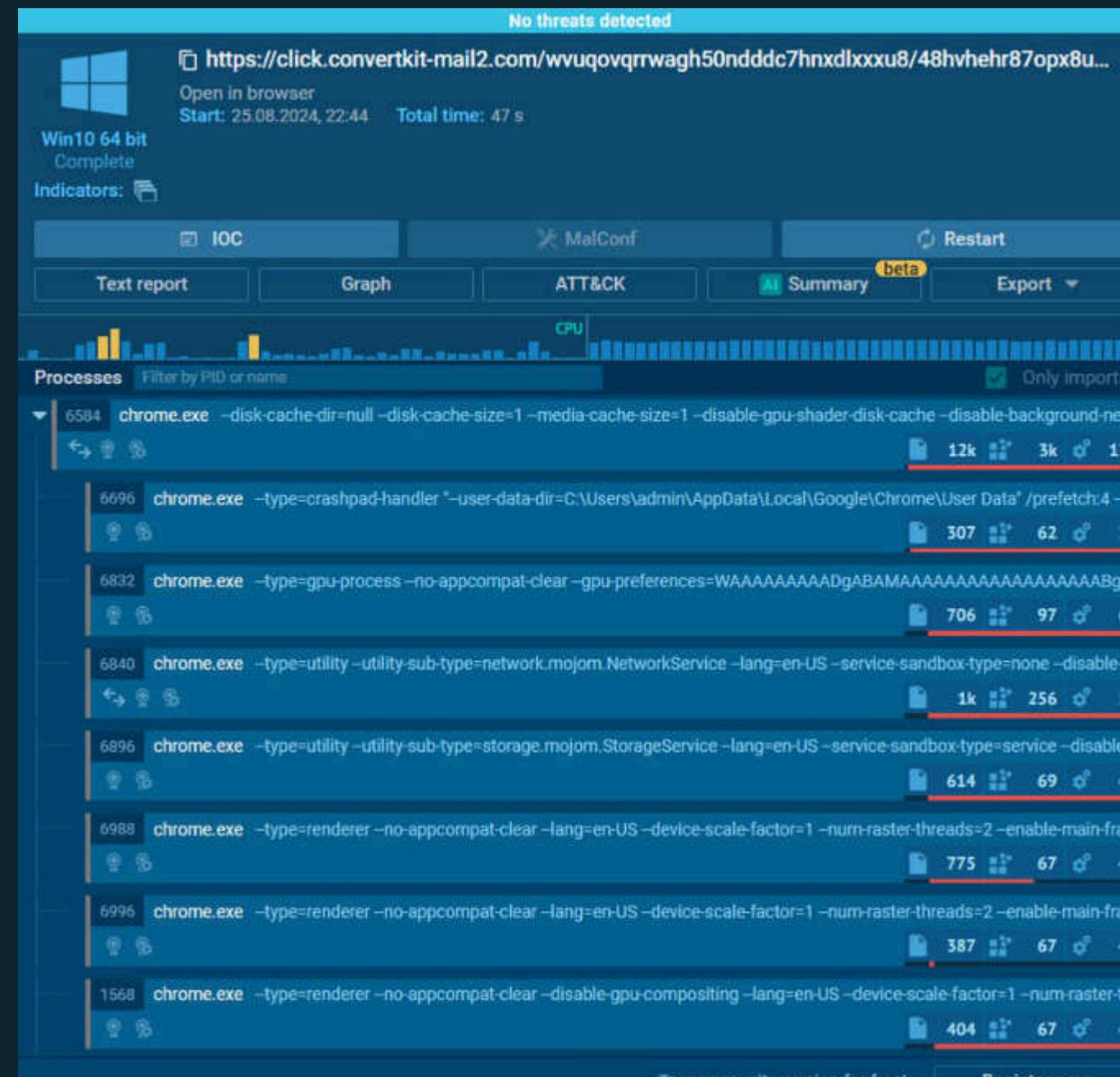
Esercizio 2

ANY.RUN

PROSSIMI PASSI

ULTERIORE ANALISI APPROFONDITA

NONOSTANTE L'ASSENZA DI MINACCE RILEVATE DA ANY.RUN, È CONSIGLIABILE ESEGUIRE UNA SCANSIONE CON ALTRI STRUMENTI DI SICUREZZA AGGIORNATI COME VIRUSTOTAL PER CONFERMARE CHE NON SI TRATTI DI UN FALSO NEGATIVO.



Esercizio 2

ANY.RUN

Monitoraggio delle comunicazioni di rete

Se il file fosse stato eseguito su una macchina di produzione, sarebbe utile monitorare il traffico di rete per eventuali connessioni sospette o tentativi di esfiltrazione di dati.

Anche se non sono stati rilevati comportamenti malevoli diretti, è sempre utile continuare a monitorare il sistema in cui il file è stato eseguito, soprattutto per quanto riguarda l'attività di rete. Se il file fosse stato eseguito in un ambiente non controllato, sarebbe opportuno continuare a sorvegliare eventuali azioni sospette nel tempo.

Verifica dell'URL sospetto

Esaminare ulteriormente l'URL segnalato per determinare se è stato utilizzato per ingannare gli utenti o per attacchi di tipo phishing od malvertising.

Aggiornamenti di Sicurezza

È essenziale mantenere aggiornati i software di sicurezza, in quanto gli strumenti di analisi potrebbero non rilevare nuove minacce se non sono aggiornati alle ultime definizioni di malware.

02

Esercizio 2

ANY.RUN

Sebbene ANY.RUN non abbia rilevato minacce, si consiglia di non abbassare la guardia. Potrebbe essere necessario un controllo più approfondito su vari fronti, tra cui la sicurezza della rete e l'autenticità delle risorse online da cui provengono il file e l'URL.

Basandoci sulle informazioni fornite, l'analisi ha prodotto un esito positivo, con nessuna minaccia rilevata. Tuttavia, come precauzione, è sempre meglio eseguire verifiche multiple su file sospetti e continuare a monitorare il sistema in caso emergano attività anomale in futuro. La sicurezza informatica richiede una vigilanza costante e un approccio multi-livello per proteggere efficacemente l'infrastruttura IT da minacce non rilevate in fase iniziale.

Navigazione nel file system Linux e impostazioni dei permessi

OBIETTIVI

Parte 1:
Esplorazione dei file system in Linux

Parte 2:
Permessi dei file

Parte 3:
Collegamenti simbolici e altri tipi di file speciali

Esplorazione dei file

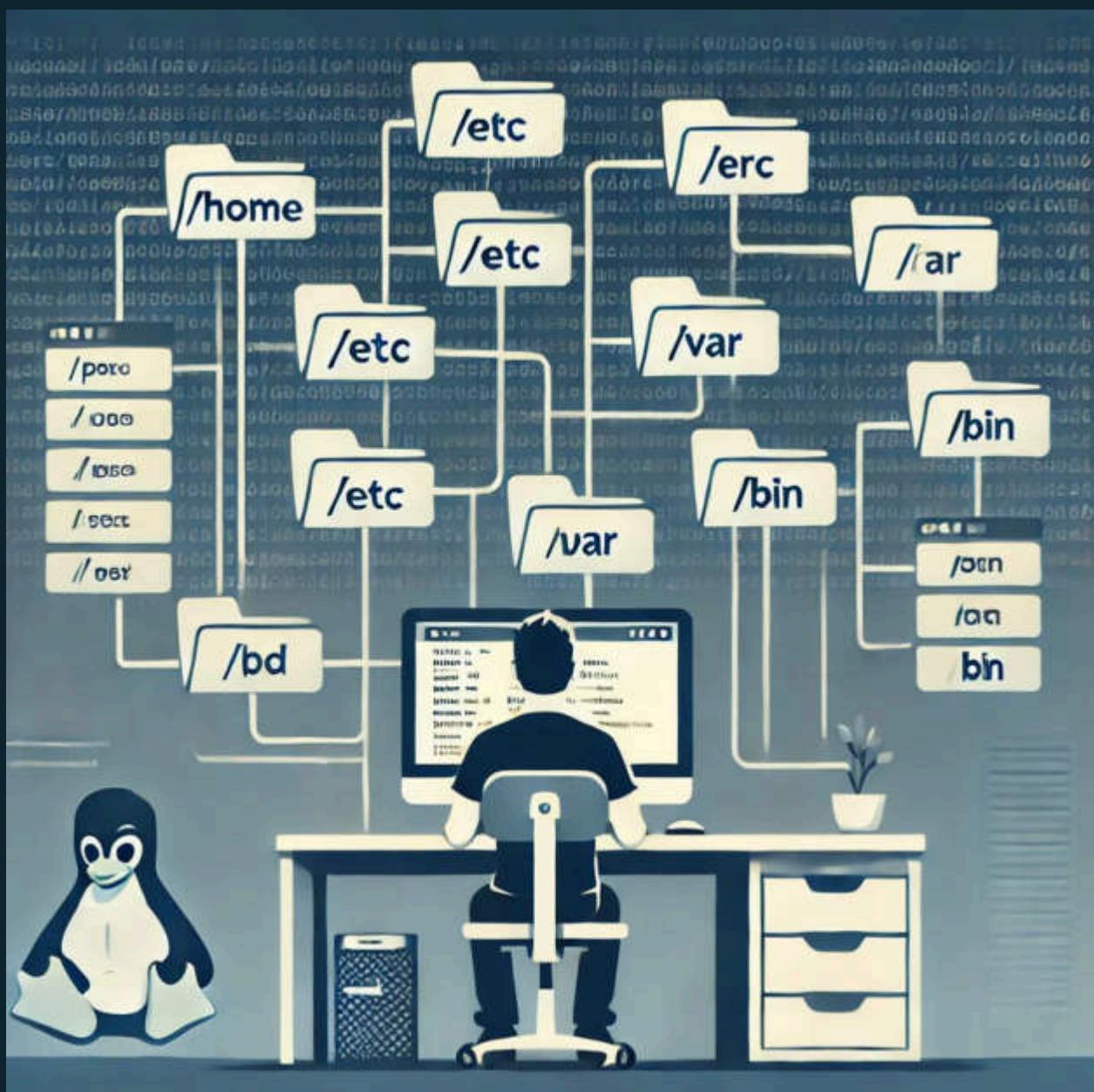
Il file system di Linux è organizzato come un albero, dove tutto parte dalla directory principale, chiamata radice ("/").

Da qui si accede a tutte le altre cartelle e file.

Comandi come:

- `pwd` mostrano dove ti trovi,
- `ls` elenca i file di una cartella e
- `cd` ti sposta da una directory all'altra.

Sapere come navigare è essenziale per gestire file, trovare informazioni utili e analizzare problemi.



Esplorazione dei file

esempi di Comandi Linux

- **pwd:** Mostra il percorso completo della directory in cui ti trovi.
- **ls:** Elenca i file e le directory nella posizione corrente.
- **cd:** Cambia la directory corrente.
- **mkdir:** Crea una nuova directory
- **rm:** Rimuove file o directory
- **chmod:** Modifica i permessi di file o directory.
- **chown:** Cambia il proprietario di un file o directory.
- **find:** Cerca file o directory.
- **cat:** Visualizza il contenuto di un file.
- **man:** Mostra il manuale di un comando.

```
[analyst@sec0ps ~]$ cd /
[analyst@sec0ps /]$ ls -L
bin  boot  dev  etc  home  lib  lib64  lost+found
[analyst@sec0ps /]$
```

Permessi dei File in Linux

I permessi dei file in Linux sono un meccanismo fondamentale per gestire la sicurezza e il controllo degli accessi a file e directory. Ogni file e directory ha un insieme di permessi che determina chi può leggerli, modificarli o eseguirli.

Questi permessi si applicano a tre categorie di utenti:

Utente (owner): il creatore o proprietario del file.

Gruppo (group): un insieme di utenti che condividono gli stessi permessi su un file.

Altri (others): tutti gli altri utenti che non appartengono né al gruppo né sono il proprietario.

Permessi dei File in Linux

I permessi sono suddivisi in tre tipi principali:

Read (r): consente di leggere il contenuto del file o visualizzare il contenuto di una directory.

Write (w): permette di modificare il contenuto di un file o aggiungere, eliminare e rinominare file in una directory.

Execute (x): abilita l'esecuzione di un file come programma o l'accesso a una directory.

Permessi dei File in Linux

```
[analyst@secOps ~]$ ls -l
total 18584
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   14909440 Dec 13 11:06 httpdump.pcap
-rw-r--r-- 1 root    root   3377063 Dec 13 08:28 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 root    root    723116 Dec 13 06:03 ttpdump.pcap
[analyst@secOps ~]$
```

- Il proprietario del file (l'utente analista) può leggere e scrivere sul file ma non eseguirlo (-rw).
- I membri del gruppo analista diversi dal proprietario possono solo leggere il file (-r-), nessuna esecuzione o scrittura è consentita.
- A tutti gli altri utenti non è consentito scrivere o eseguire quel file, ma solo leggere

Collegamenti simbolici e altri tipi di file speciali

Collegamenti simbolici (Symlink):

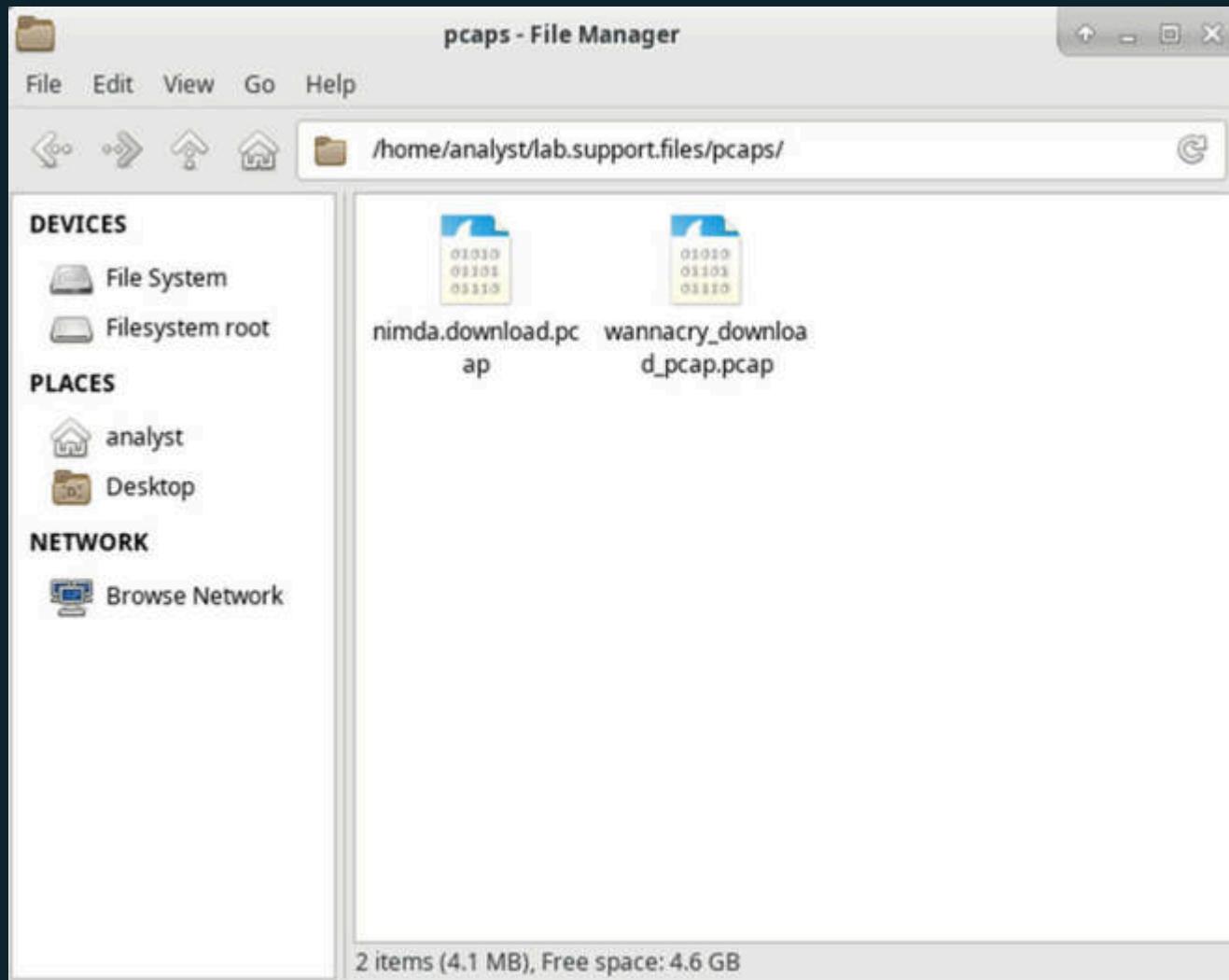
Un file che funge da "scorciatoia" per un altro file o cartella. Permette di accedere a un file da un'altra posizione senza copiarlo.

Altri tipi di file speciali:

- **File di dispositivo:** Rappresentano oggetti hardware (come dischi o terminali) e permettono di interagire con essi.
- **Pipes (FIFO):** Permettono a diversi programmi di scambiarsi dati tra loro.
- **Sockets:** Usati per permettere la comunicazione tra programmi su una rete.

Extract an Executable from a PCAP

Utilizzando la VM CyberOps Workstation, verrà analizzato il traffico di rete catturato in precedenza con Wireshark. L'analisi riguarderà un file .pcap che evidenzia il download di un potenziale file malevolo.

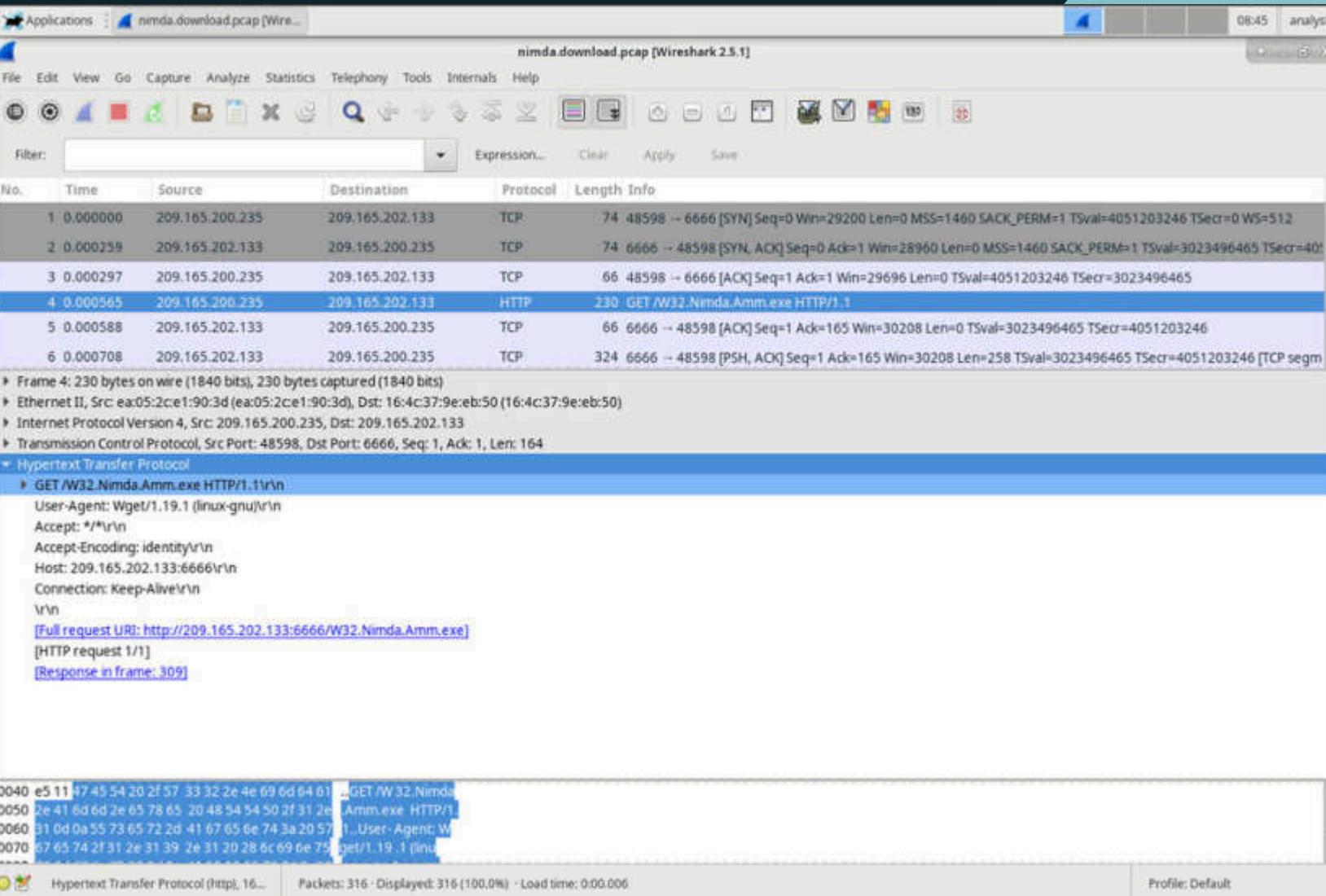


All'interno della directory troveremo due file .pcap. Per questa analisi, ci concentreremo sul file **nimda.download.pcap**.

Aprendo il file, sarà possibile esaminare nel dettaglio il traffico di rete e comprendere cosa è accaduto esattamente prima del download del presunto file malevolo.

Il file .pcap da analizzare è disponibile nella directory:
/home/analyst/lab.support.files/pcaps/

Wireshark

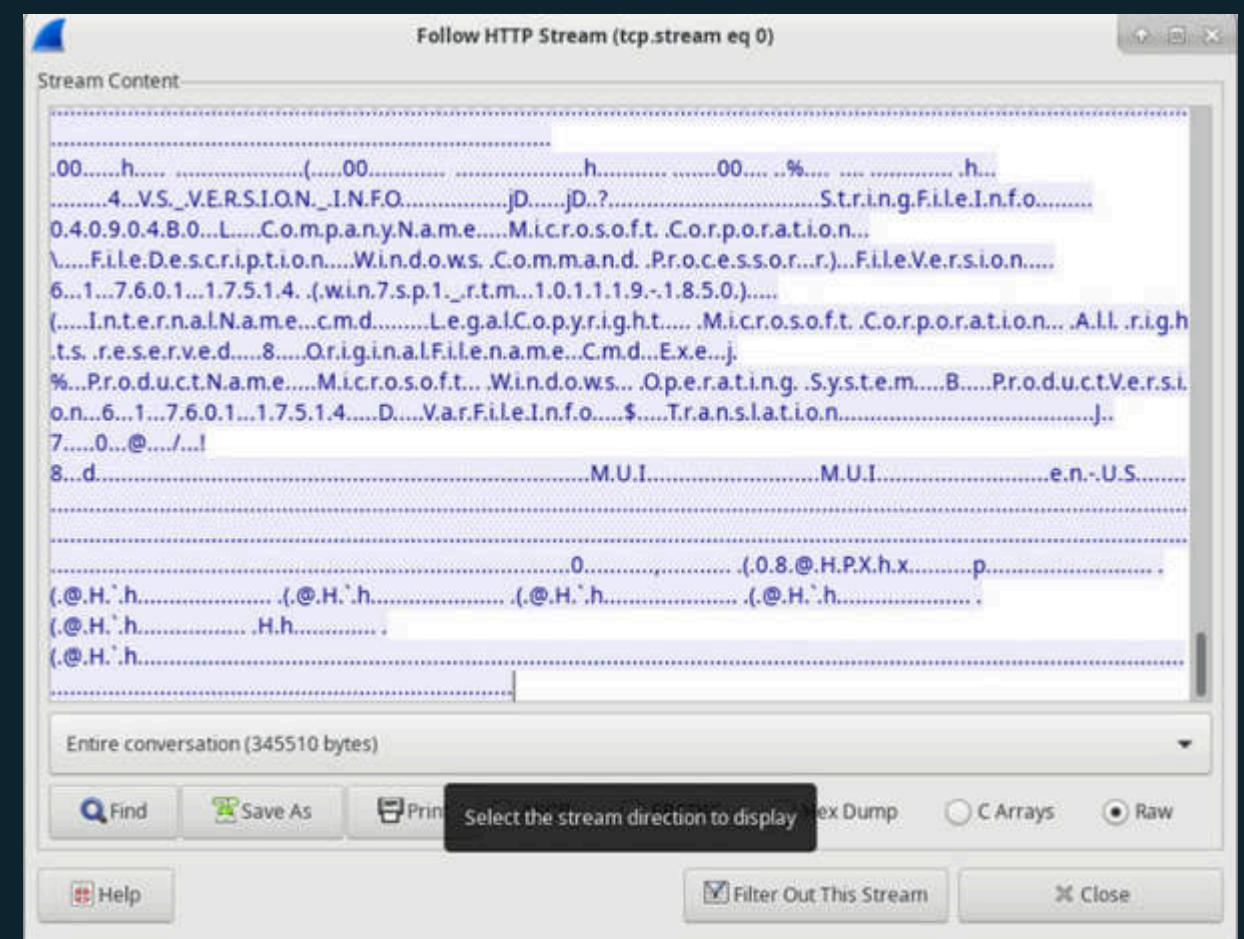
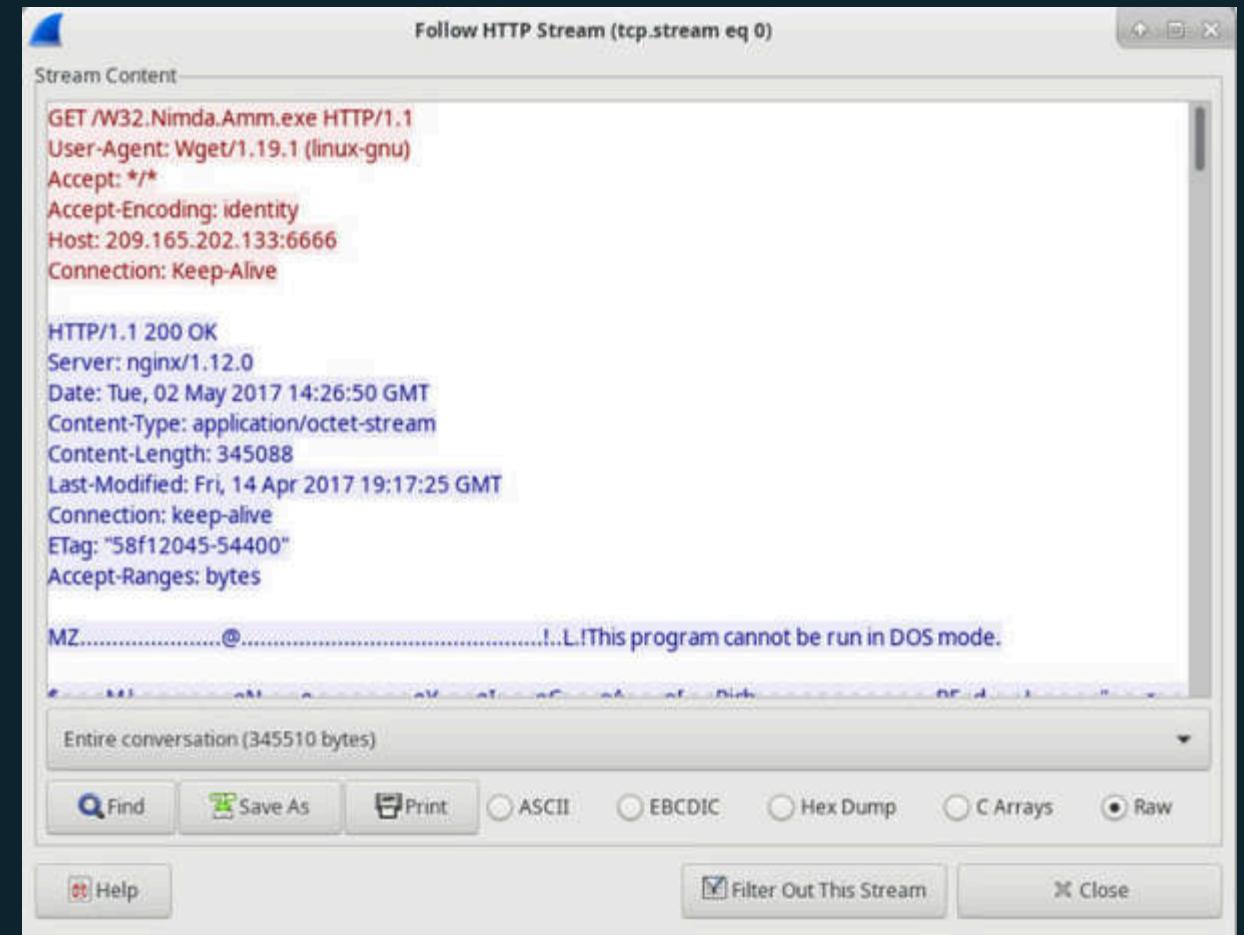


Le prime quattro righe dell'immagine mostrano il processo iniziale di connessione e la richiesta di un file tramite protocollo HTTP. La connessione inizia con un pacchetto TCP inviato dal client (indirizzo IP 209.165.200.235 con porta 48598) al server (indirizzo IP 209.165.202.133 con porta 6666).

Il traffico spiega la presenza di un messaggio SYN per richiedere l'apertura di una connessione TCP. Il server risponde con un pacchetto SYN, ACK, confermando la ricezione e la disponibilità a stabilire la connessione. Successivamente, il client invia un pacchetto ACK, completando la stretta di mano TCP (three-way handshake) e stabilendo la connessione.

A connessione avvenuta, nella quarta riga si può notare una richiesta HTTP GET inviata dal client al server. Il client utilizza il comando wget (indicato dal campo User-Agent) per effettuare il download del file W32.Nimda.Amm.exe. Questa richiesta, indirizzata al server sulla porta 6666, rappresenta un tentativo di scaricare un file potenzialmente malevolo.

HTTP Stream

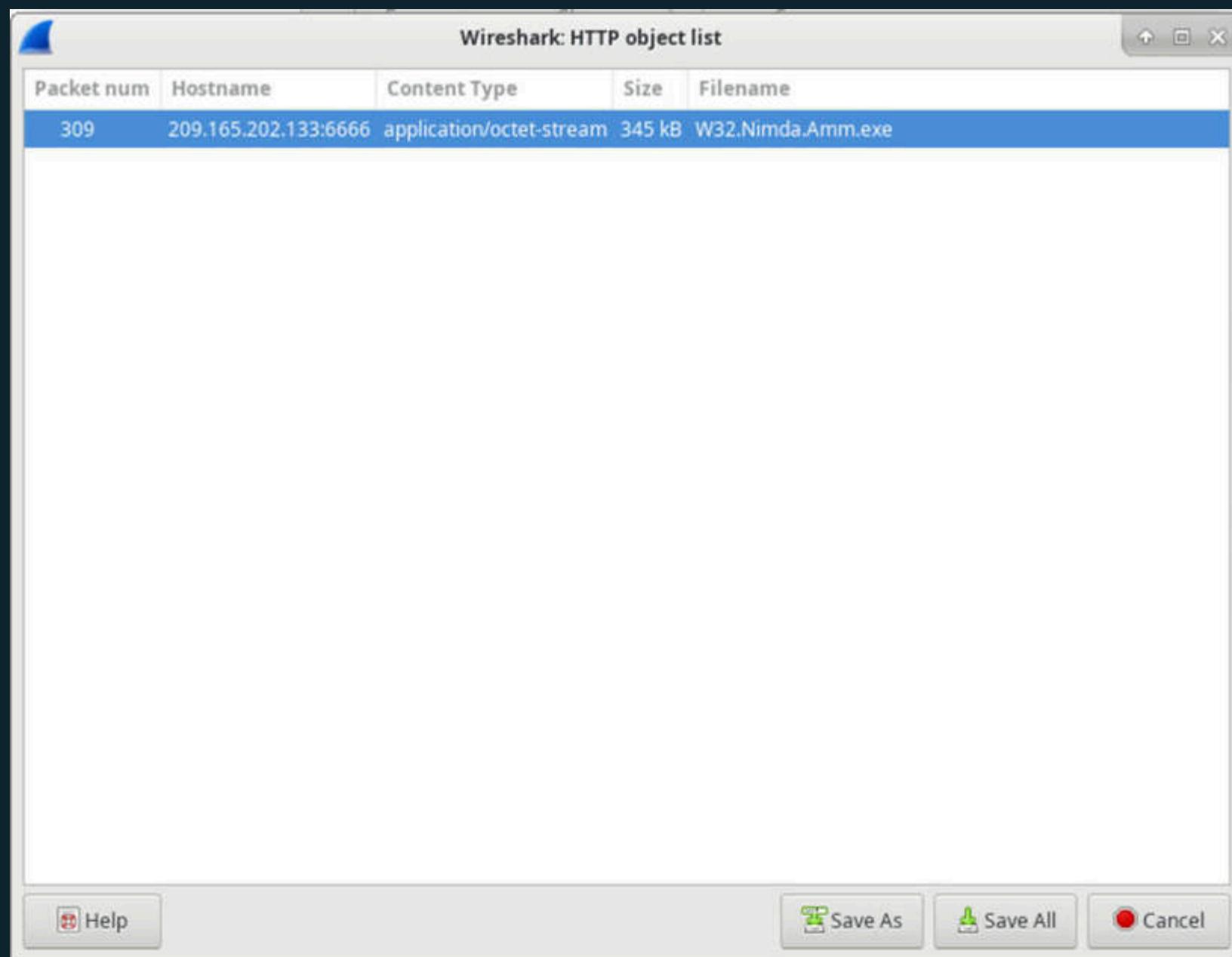


Grazie alla funzione “**Follow HTTP Stream**” di Wireshark sarà possibile analizzare nel dettaglio la richiesta HTTP GET

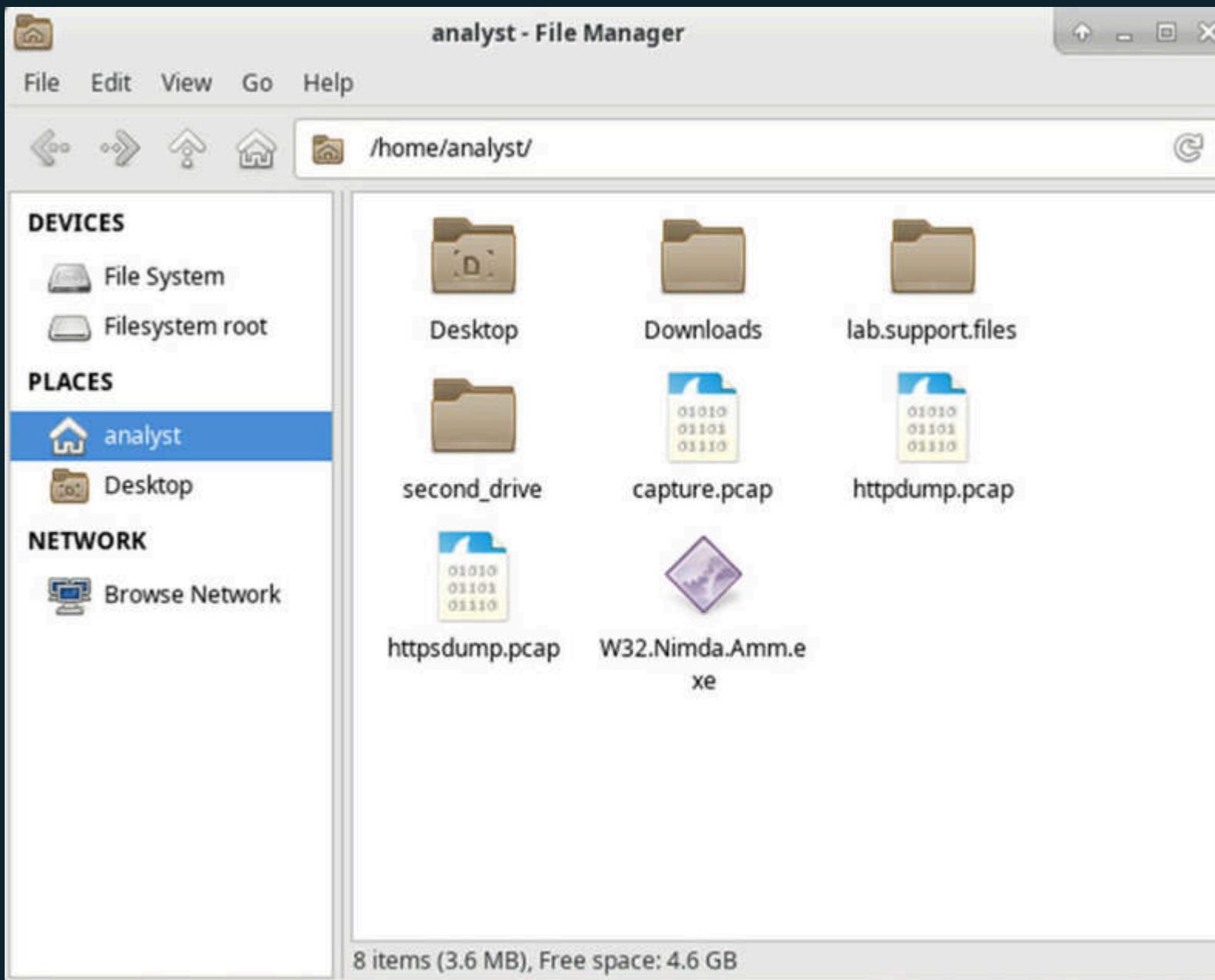
Con questa funzione, possiamo esaminare il contenuto del file scaricato. Tuttavia, ciò che vediamo sono principalmente simboli e caratteri casuali, poiché Wireshark non riesce a decodificare correttamente il formato del file. Di conseguenza, restiamo con una serie di codici, per lo più illeggibili. Nonostante ciò, un'analisi attenta potrebbe permetterci di estrapolare informazioni rilevanti. Alla fine del codice, infatti, sarà possibile individuare alcune informazioni leggibili che ci consentono di ricavare dettagli rilevanti, come il fatto che il programma è un file eseguibile .exe, quindi destinato ad essere avviato su macchine Windows. Possiamo quindi dedurre che il potenziale file malevolo in questione sia progettato per colpire i sistemi operativi Windows.

Analisi del file malevolo

Una volta analizzato il traffico HTTP, è il momento di recuperare il file scaricato per un'analisi più approfondita. Wireshark offre una funzionalità che ci consente di farlo: l'opzione "Export Objects > HTTP". Grazie a questa funzione, possiamo estrarre il file in questione e analizzarne il suo contenuto.



Una volta scaricato il file, basterà aprire la directory in cui è stato salvato per poterlo esaminare. A quel punto, si potrà procedere con un'analisi approfondita del file, con l'obiettivo di comprenderne le funzionalità.



Ottenuto il file, sarà necessario identificare il tipo di malware e studiarne il comportamento. Per farlo, il file malevolo deve essere spostato in un ambiente controllato ed eseguito, in modo da monitorare le sue azioni tramite un'analisi malware dinamica. In questo caso, una sandbox rappresenta l'ambiente ideale per testare il malware. Programmi come Cuckoo o Anyrun sono strumenti fondamentali per effettuare un'analisi approfondita del comportamento del malware. Inoltre, per una valutazione più efficace, sarà possibile eseguire un'analisi statica del malware, che consente di prevedere il suo comportamento all'interno della sandbox prima di eseguirlo. Piattaforme come VirusTotal sono molto utili in queste situazioni. Dopo l'esecuzione del malware e una serie di controlli, VirusTotal fornisce un rapporto dettagliato con informazioni preziose per valutare il comportamento del malware.

01

MALWARE ANALYSIS

02

ANYRUN

03

NAVIGATING THE LINUX
FILESYSTEM

04

EXTRACT AN EXECUTABLE FROM
A PCAP

05

BONUS 1 ANYRUN

06

BONUS 2 INTERPRET HTTP AND
DNS DATA TO ISOLATE THREAT
ACTOR

07

BONUS 3 ISOLATE
COMPROMISED HOST USING 5-
TUPLE

05

Bonus 1

AnyRun Malware

Introduzione

Questa relazione descrive il comportamento sospetto osservato durante l'analisi di un file eseguibile scaricato tramite AnyRun. Il file, inizialmente denominato "OOD5yt-b.exe.part", viene rinominato automaticamente in "Jvczfhe.exe" una volta completato il download. Successivamente, la natura dannosa di questo file è stata confermata utilizzando VirusTotal. L'esecuzione del file in ambiente controllato ha rivelato diverse attività anomale che meritano un approfondimento.

The screenshot shows the AnyRun malware analysis interface. On the left, there's a timeline of network requests from a Firefox process (PID 6596) to various URLs, including detectportal.mozilla.com and ocap.settings.com. On the right, a detailed view of a suspicious process named Jvczfhe.exe (PID 7492) is shown. The process is identified as Microsoft Edge, running under the admin user. It has a command line path: C:\Users\admin\Downloads\Jvczfhe.exe. A warning section indicates that the application crashes. Threat details show T1012 (Query Registry) and T1059 (Windows Command Shell) threats, both of which read Windows registry values. Other threats include reading software policy settings and environment values.

Comportamenti rilevati

Durante l'analisi, sono emersi numerosi elementi sospetti relativi alle attività del file:

Download e Rinomina del File Il file scaricato, denominato inizialmente "OOD5yt-b.exe.part", viene rinominato in "Jvczfhe.exe" al completamento del download. Questo comportamento suggerisce che il file rinominato sia una versione completa dell'originale.

+ BEFORE	Process drops legitimate windows executable T1036.003	Hide ▾
Filename:	C:\Users\admin\Downloads\OOD5yt-b.exe.part	
Md5:	5ec4256e6a2367502a8058f4bc8f4ecc	
Sha1:	c6f996570b6f34cb813028c601b9d27bf8df0550	
Sha256:	e6a7aaff54eb6d06acf6f1dfa21a85b767dbf7ff3e9bfd2ddbdeced86aa9b2	
+ BEFORE	Application launched itself	Hide ▾
CmdChild:	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -channel=1824 -parentBuildID 20240213221259 -prefsHandle 1752 -prefMapHandle 1732 -prefsLen 30537 -prefMapSize 244343 -appDir "C:\Program Files\Mozilla Firefox\browser" -{cb10680d-0044-4e6b-8433-6e05fa363c18} 6596 "\\\pipe\gecko-crash-server-pipe.6596" 256ba9c2b10 gpu	
CmdParent:	"C:\Program Files\Mozilla Firefox\firefox.exe" https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe	
Image:	C:\Program Files\Mozilla Firefox\firefox.exe	

Interazioni con Internet Explorer e Windows

Sono state osservate azioni come:

- La lettura delle impostazioni di sicurezza di Internet Explorer.
- Il controllo delle impostazioni di attendibilità di Windows.

Tuttavia sono abbastanza comuni queste operazioni poiché possono essere parte del funzionamento normale di un software legittimo, in particolare la verifica di compatibilità, sicurezza o configurazione dell'ambiente, di conseguenza non è possibile dire con sicurezza che ciò sia un comportamento malevolo senza avere prove.



Raccolta di Informazioni dal Sistema

Il file legge diverse informazioni dal sistema, tra cui:

- Politiche software.
- Informazioni sul server proxy.
- Variabili d'ambiente.
- GUID della macchina e nome del computer.
- Lingue supportate dal sistema operativo. Inoltre, il malware disabilita i trace logs

T1012 Query Registry (6)

Reads the software policy settings

Checks proxy server information

Reads Environment values

Reads the machine GUID from the registry

Reads the computer name

Checks supported languages

T1562.002 Disable Windows Event Logging (1)

Disables trace logs

T1082 System Information Discovery (4)

Reads Environment values

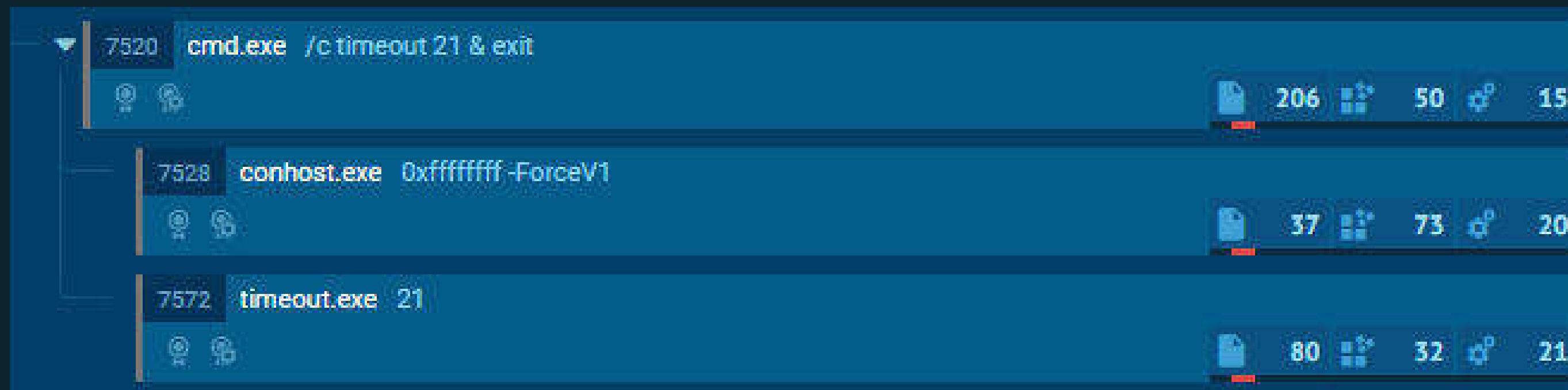
Reads the machine GUID from the registry

Reads the computer name

Checks supported languages

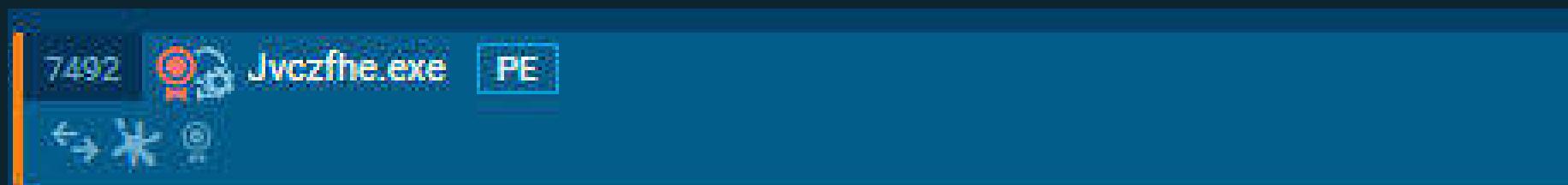
CMD.exe

Avvio di CMD.exe con il comando "timeout 21" Il malware utilizza CMD.exe per eseguire un comando che introduce un ritardo di 21 secondi nell'avvio del programma. Questa tecnica potrebbe essere impiegata per eludere i sistemi di rilevamento automatico o per sincronizzare l'esecuzione con altri processi.



Esecuzione di WerFault.exe

Durante l'esecuzione, è stato osservato il lancio del processo WerFault.exe con il seguente comando:
C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676. WerFault.exe è un componente di Windows utilizzato per la gestione degli errori. L'opzione -p 7492 specifica il PID del processo sospetto ("Jvczfhe.exe").



Process information	
Username:	admin
SID:	S-1-5-21-1693682860-607145093-2874071422-1001
IL:	MEDIUM
Start:	59.33 s
File information	
Company:	Microsoft Corporation
Description:	Windows Problem Reporting
Version:	10.0.19041.3996 (WinBuild.160101.0800)
Command line	
C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676	

InstallUtil.exe

Un altro elemento interessante è l'utilizzo di InstallUtil.exe, uno strumento legittimo di Microsoft progettato per l'installazione e configurazione di applicazioni .NET. Nonostante il file presenti il logo Microsoft, mancano certificati di firma digitale. Inoltre, il codice è protetto con .NET Reactor.

InstallUtil.exe AI
.NET Framework installation utility
Username: admin
Start: +54586ms Indicators:

Command line AI
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"
More Info

Warning 1
[T1571 Non-Standard Port \(1\)](#)
 Connects to unusual port

Threat Verdict
10 OUT OF 100
No verdict
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators:

Timeline of the process
0 s 58.99 s

Process information
Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 58.99 s

File information
Company: Microsoft Corporation
Description: .NET Framework installation utility
Version: 4.8.9037.0 built by: NET481REL1

Command line AI
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"

Warning 1
[T1571 Non-Standard Port \(1\)](#)
 Connects to unusual port

Other 3
.NET Reactor protector has been detected

T1012 Query Registry (4)
- Reads Environment values
- Reads the machine GUID from the registry
- Reads the computer name
- Checks supported languages

T1082 System Information Discovery (4)
- Reads Environment values
- Reads the machine GUID from the registry
- Reads the computer name
- Checks supported languages

.NET Reactor

.NET Reactor è uno strumento di protezione del codice utilizzato per offuscare e proteggere applicazioni .NET. Come per esempio la variazioni di metodi, classi e variabili in maniera criptica e delle tecniche di "control flow obfuscation".

Connessioni Rilevate

Durante l'analisi delle connessioni, è stato osservato quanto segue:

- Una connessione sulla porta 7702 verso l'indirizzo IP 91.92.253.47.
 - Risoluzioni DNS e comunicazioni verso il sottodominio “egehgdehjhjt.re.duckdns.org”, appartenente al dominio “duckdns.org”.

L'analisi del file PCAP fornito da AnyRun mostra una serie di tentativi di connessione TCP tra l'indirizzo IP sorgente 192.168.100.139 e l'indirizzo di destinazione 91.92.253.47, con porta di destinazione 7702.

Time	Type	Rep	CN	Src IP	Port	Dst IP	Port
+1077 ms	TCP	?		91.92.253.47	7702	VM	59005
HTTP Requests 31 Connections 99 DNS Requests 161 Threats 19							
Timeshift	Status	Rep	Domain			IP	
55659 ms	Responded	?	egehgdehbjhjtre.duckdns.org			91.92.253.47	
134.01 s	Responded	?	egehgdehbjhjtre.duckdns.org			91.92.253.47	
186.26 s	Responded	?	egehgdehbjhjtre.duckdns.org			91.92.253.47	
212.88 s	Responded	?	egehgdehbjhjtre.duckdns.org			91.92.253.47	
264.12 s	Responded	?	egehgdehbjhjtre.duckdns.org			91.92.253.47	

Tentativo di Connessione

ip.dst == 91.92.253.47						
No.	Time	Source	Destination	Protocol	Length	Info
24584	58.100506	192.168.100.139	91.92.253.47	TCP	66	59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24605	59.101188	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24652	61.112902	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24660	65.120472	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24681	73.132440	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24697	84.155793	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24700	85.158683	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24708	87.165674	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24716	91.195748	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
24731	99.208026	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
26739	110.228036	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
26741	111.234738	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
26755	113.242704	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
26767	117.257415	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
26836	125.257525	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33206	136.299146	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33209	137.311985	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33222	139.322019	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33240	143.336606	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33260	151.349371	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33282	162.390150	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33284	163.393347	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33298	165.400657	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33314	169.414792	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33337	177.420649	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33388	188.495611	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33390	189.501202	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33394	191.509373	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33398	195.528233	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33408	203.535086	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33416	214.549801	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33418	215.561710	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33421	217.568548	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33435	221.582427	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33481	229.595721	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33493	240.603274	192.168.100.139	91.92.253.47	TCP	66	[TCP Port numbers reused] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33495	241.606033	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33497	243.613460	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33506	247.627216	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
33516	255.639640	192.168.100.139	91.92.253.47	TCP	66	[TCP Retransmission] 59005 → 7702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM

Conclusione

L'analisi ha evidenziato numerosi comportamenti anomali, sufficienti a classificare l'eseguibile come potenzialmente malevolo. Ulteriori analisi sono necessarie per confermare la natura e lo scopo del malware.

Mitigation

Si consiglia di:

- Isolare l'ambiente in cui il file è stato eseguito;
- Eseguire i file sospetti in sandbox, come AnyRun;
- Approfondire l'analisi del malware, analizzando il codice del malware, per vedere aspetti non visibili tramite ANYRun
- Bloccare il dominio o i suoi sottodomini sul firewall



Bonus 2:
Interpreter HTTP
and DNS Data to
Isolate Threat
Actor

Introduction

In questo laboratorio esamineremo e documenteremo i registri di un exploitation DNS e SQL Injection.

Divideremo il laboratorio nel seguente modo:

- Parte 1: Indagare su un attacco di SQL Injection
- Parte 2: indagare sull'esfiltrazione dei dati DNS

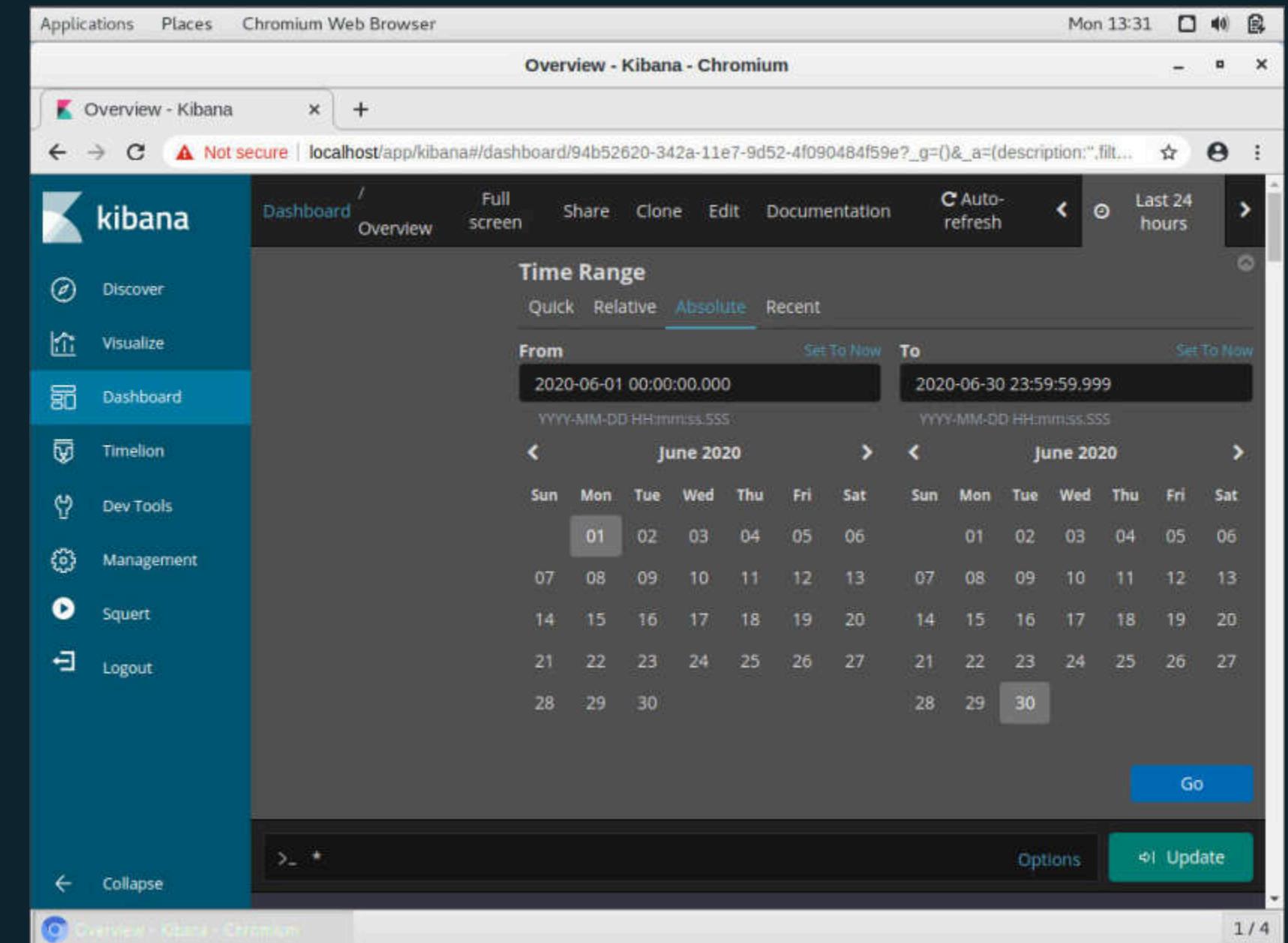
Avvio Security Onion

Per questo laboratorio utilizzeremo la nostra macchina virtuale Security Onion la quale ci servirà per analizzare dei log attraverso l'utilizzo di Kibana ovvero un tool che ci consente di esplorare, visualizzare e analizzare i dati raccolti in Elasticsearch, utilizzando una varietà di strumenti di visualizzazione come grafici, tavole, mappe e dashboard.



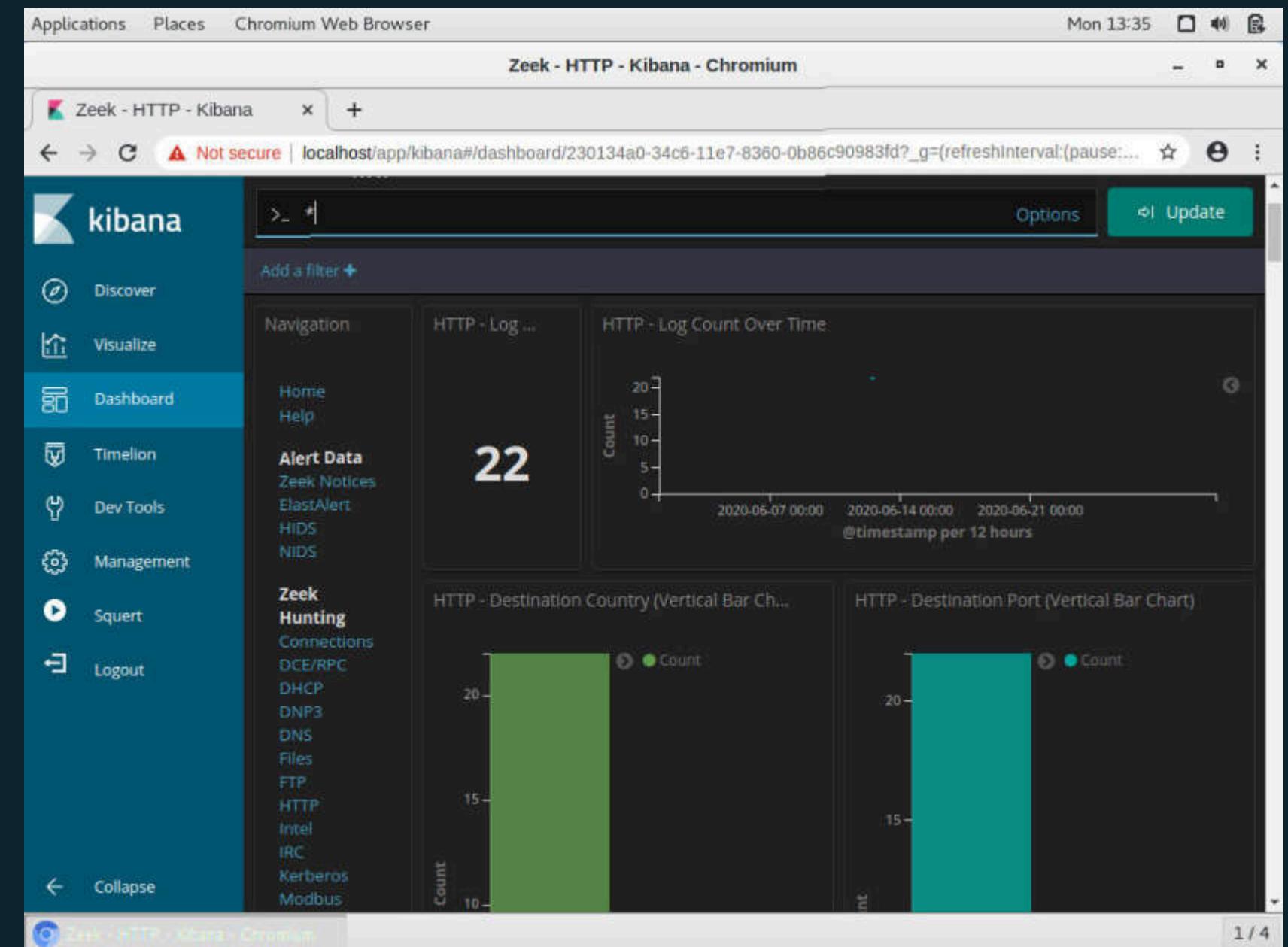
impostare time range

Andremo ad analizzare due attacchi registrati nel mese di Giugno 2020. Per il suddetto time range richiesto, abbiamo dovuto cambiare le impostazioni inserendo il suddetto mese.



Analisi Log HTTP

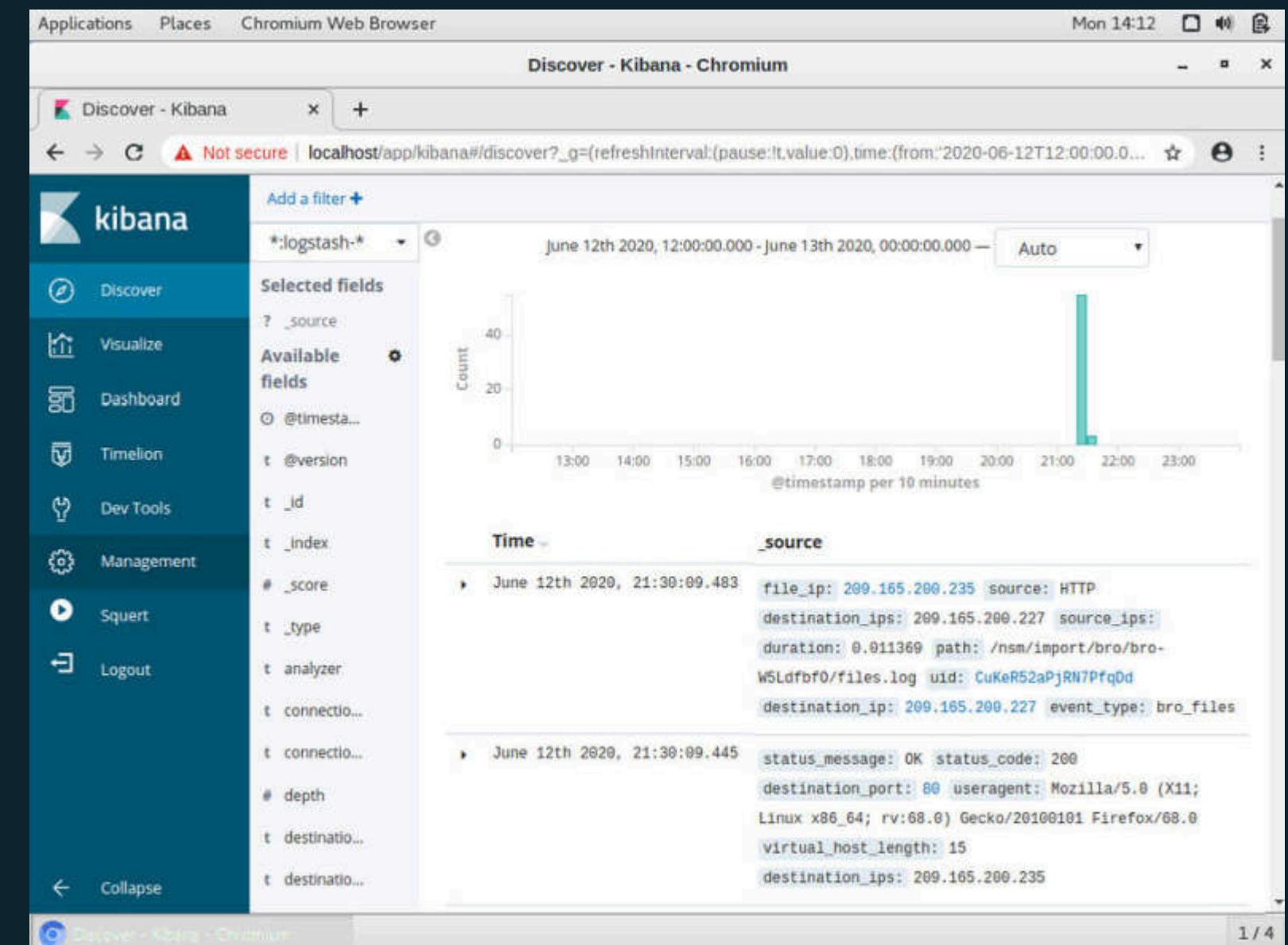
Una volta applicato il time range, andiamo ad effettuare l'analisi dei log HTTP utilizzando zeek ovvero uno strumento di monitoraggio della rete che analizza il traffico e produce log dettagliati sui protocolli utilizzati.



Discover Log HTTP

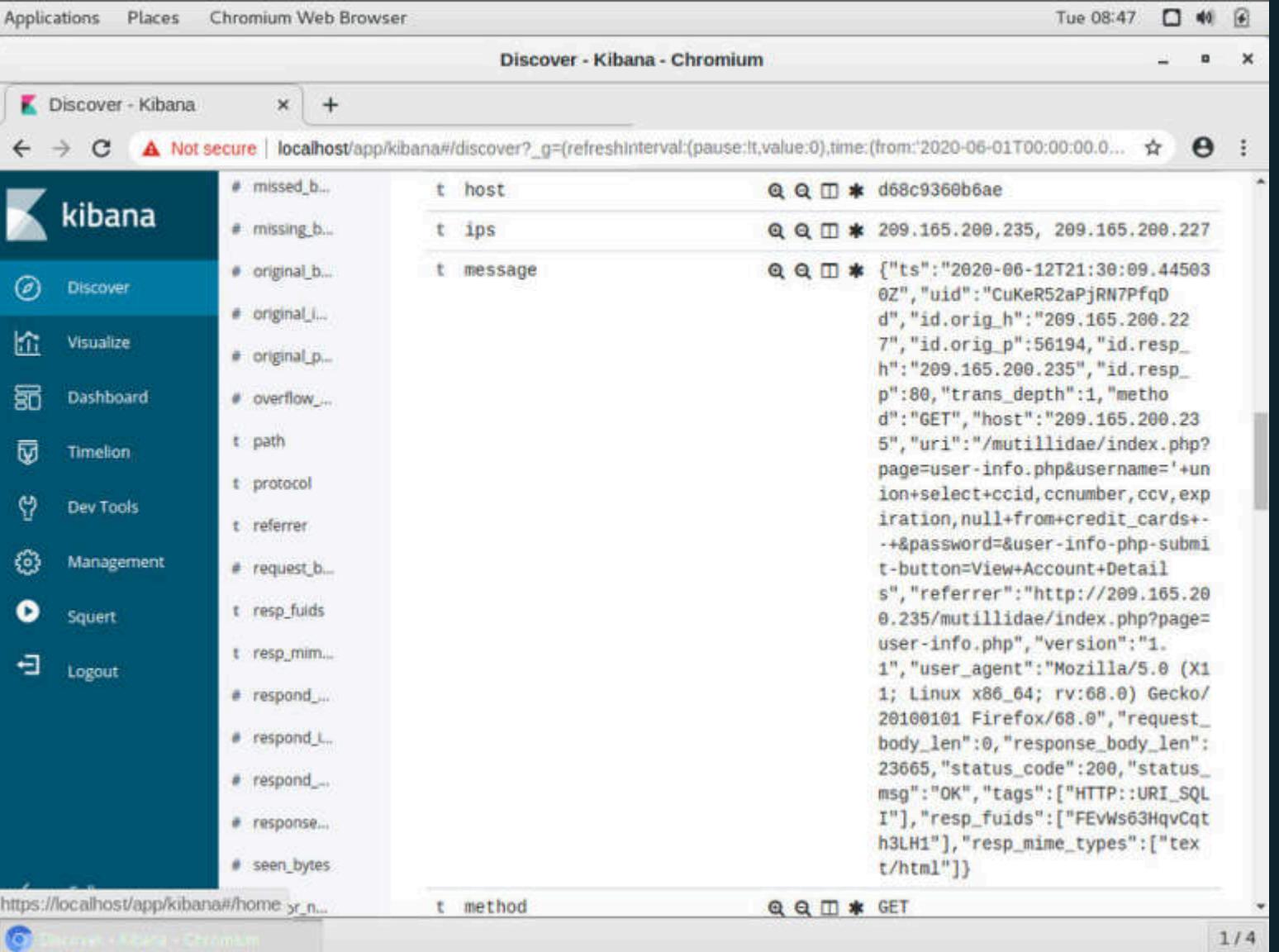
Abbiamo notato che nel mese di Giugno 2020 c'è stato un picco di attività il 12 Giugno che si è verificato tra le 21 e le 22 più precisamente alle 21:30. Le comunicazioni analizzate sono, per la precisione, tra due indirizzi IP specifici:

- Source IP Address
209.165.200.227
- Destination IP Address
209.165.200.235



Esplorazione dei Log

Andando ad analizzare i log, abbiamo notato che uno in particolare aveva delle strane richieste HTTP GET fatte dal client al server in cui si chiedevano delle informazioni sulla carta di credito.



The screenshot shows the Kibana Discover interface within a Chromium browser window. The URL in the address bar is `localhost/app/kibana#/discover?_g=(refreshInterval:(pause:lt,value:0),time:(from:'2020-06-01T00:00:00.0..., to:'2020-06-12T21:30:09.445030Z',value:1),version:1)`. The interface includes a sidebar with links to Discover, Visualize, Dashboard, Timeline, Dev Tools, Management, Squert, and Logout. The main area displays a table of log entries with columns: host, ips, message, path, protocol, referrer, request_body, resp_fuids, resp_mime_types, respond, respond_length, respond_time, response, and seen_bytes. One specific log entry is highlighted in the message column:

```
{"ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfqD", "id.orig_h": "209.165.200.227", "id.orig_p": "56194", "id.resp_h": "209.165.200.235", "id.resp_p": "80", "trans_depth": 1, "method": "GET", "host": "209.165.200.235", "uri": "/mutillidae/index.php?page=user-info.php&username='union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards++&password=&user-info-php-submit=button=View+Account+Details", "referrer": "http://209.165.200.235/mutillidae/index.php?page=user-info.php", "version": "1.1", "user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "request_body_len": 0, "response_body_len": 23665, "status_code": 200, "status_msg": "OK", "tags": ["HTTP::URI_SQL"], "resp_fuids": ["FEVWs63HqvCqth3LH1"], "resp_mime_types": ["text/html"]}
```

Dettagli CapME!

Andiamo a visualizzare il contenuto di uno dei log con CapME! che ci facilita l'analisi di file .pcap. Il suo scopo è quello di automatizzare la decodifica e la visualizzazione di specifiche informazioni presenti nel file, per rendere più facile il lavoro di analisi da parte di un'analista. Nell'analisi abbiamo notato che c'è stato l'inserimento di un codice malevolo riconducibile a un SQL Injection che sfrutta le vulnerabilità dell'applicazione web.

codice in questione:

`username='+union+select+ccid,ccnumber,ccv,e
xpiration,null+from+credit_cards+-
+&password=`

```
209.165.200.227:56194_209.165.200.235:80-6-1755005513.pcap

Log entry:
[{"ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PtqDd", "id.orig_h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "id.resp_p": 80, "trans_depth": 1, "method": "GET", "host": "209.165.200.235", "uri": "/mutilidae/index.php?page=user-info.php&username=%27+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+-+&password=&user-info-php-submit-button=View+Account+Details", "referrer": "http://209.165.200.235/mutilidae/index.php?page=user-info.php", "version": "1.1", "user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "request_body_len": 0, "response_body_len": 23665, "status_code": 200, "status_msg": "OK", "tags": ["HTTP:URI_SQL"], "resp_headers": [{"FevWs63HqvCqth3LH1"}, {"resp_mime_types": ["text/html"]}], "Sensor Name": "seconion-import", "Timestamp": "2020-06-12 21:30:09", "Connection ID": "CLI", "Src IP": "209.165.200.227", "Dst IP": "209.165.200.235", "Src Port": 56194, "Dst Port": 80, "OS Fingerprint": "209.165.200.227:56194 - UNKNOWN [S44:64:1:60:M1460,S,T,N,W7:?:?] (up: 2829 hrs)", "OS Fingerprint_2": "209.165.200.235:80 (link: ethernet/modem)", "SRC": "GET /mutilidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+-+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1", "SRC": "Host: 209.165.200.235", "SRC": "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "SRC": "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8", "SRC": "Accept-Language: en-US,en;q=0.5", "SRC": "Accept-Encoding: gzip, deflate", "SRC": "Referer: http://209.165.200.235/mutilidae/index.php?page=user-info.php", "SRC": "Connection: keep-alive", "SRC": "Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb", "SRC": "Upgrade-Insecure-Requests: 1", "SRC": "DST: HTTP/1.1 200 OK", "DST": "Date: Fri, 12 Jun 2020 14:30:09 GMT"}]
```

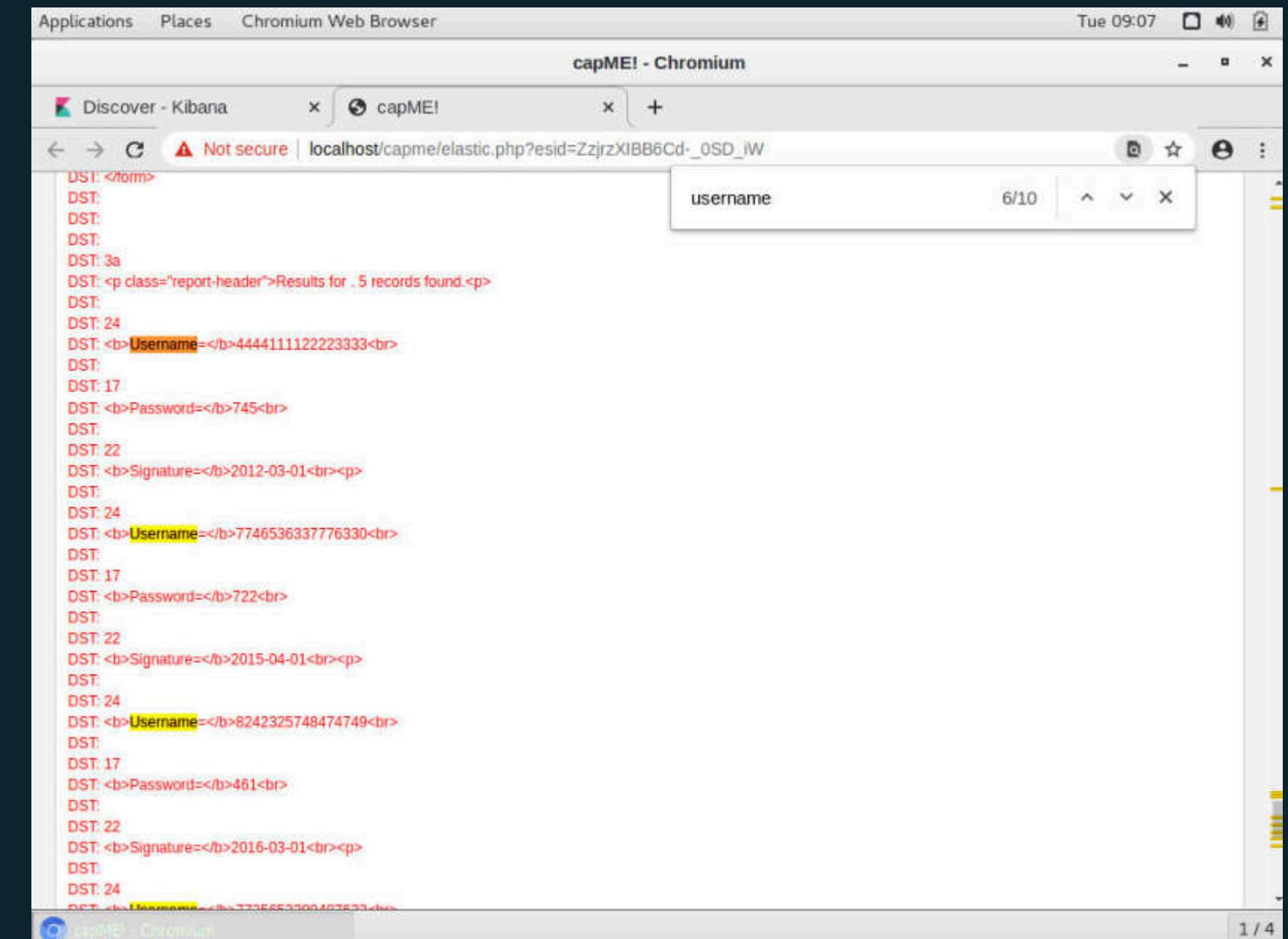
Cos'è SQL Injection

L'SQL Injection (SQLi) è una vulnerabilità di sicurezza che consente a un attaccante di manipolare le query SQL inviate a un database attraverso un'applicazione web. Il suo obiettivo è quello di sfruttare l'input non filtrato dall'utente per eseguire comandi arbitrari sul database. Permette a un eventuale malintenzionato di ottenere:

- Un accesso non autorizzato per ottenere credenziali di accesso come username e password;
- Rubare informazioni sensibili come dati personali o numeri di carte di credito;
- Inserire il codice malevolo per controllare il server o l'applicazione;
- Modificare o eliminare informazioni importanti nel database.

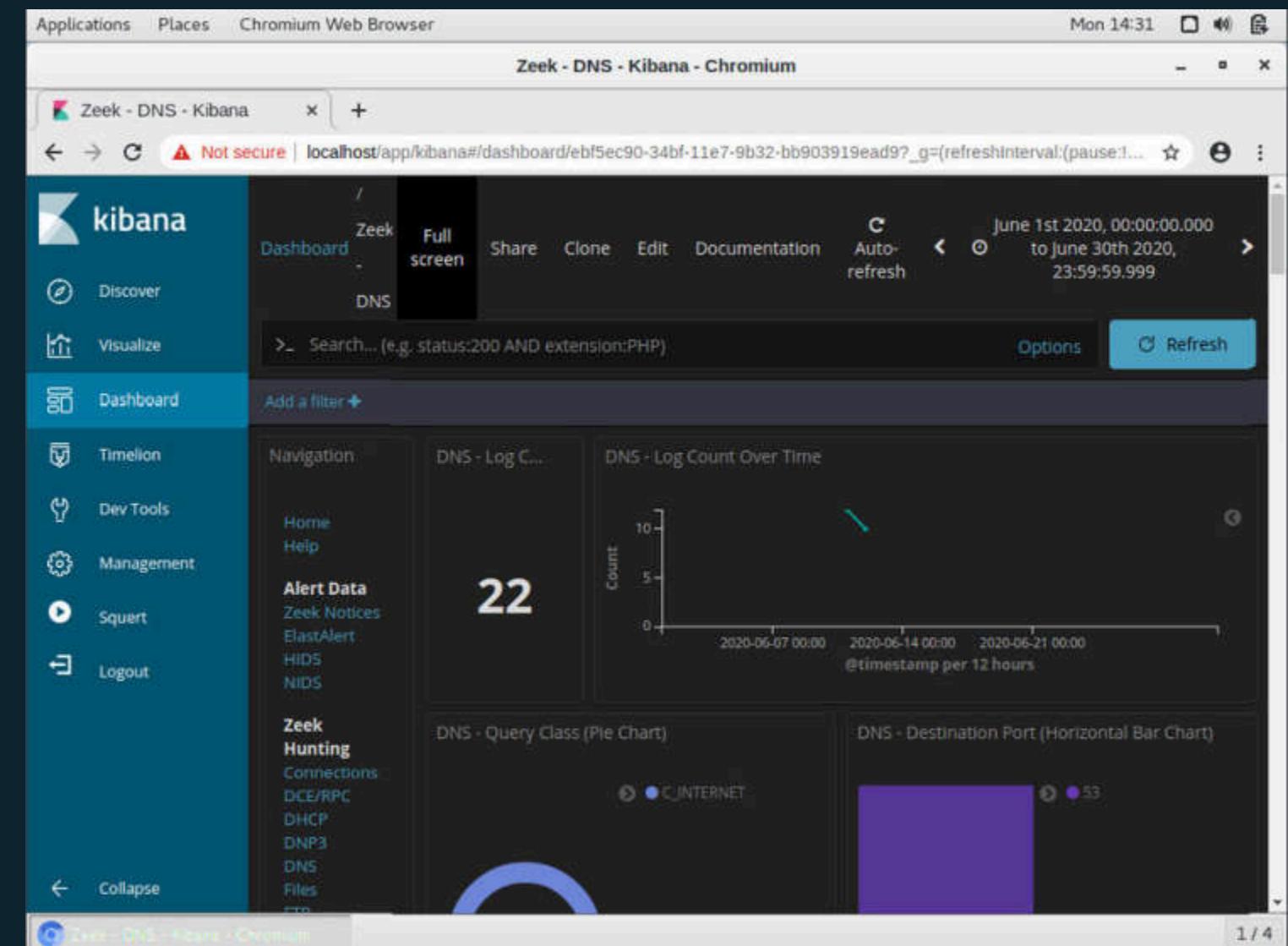
Credenziali

all'interno del CapME! possiamo filtrare per username per verificare se effettivamente ci sia stata un'esfiltrazione di dati e sfortunatamente c'è stata in quanto sono presenti tutti gli username e password come si può vedere dall'immagine. L'applicativo web ha restituito all'attaccante tutte quante le credenziali di accesso.



Analisi Log DNS

Andiamo ora a filtrare il traffico DNS in quanto un'amministratore di rete ci ha avvisato che nello stesso periodo ci sono state query DNS anomale molto lunghe con sottodomini dall'aspetto strano.



Analisi Query DNS

Andando a filtrare per il sottodominio example.com in questione, abbiamo notato la presenza di queste 4 query di lunghezza importante.

The screenshot shows the Kibana interface with a dark theme. On the left, a sidebar menu includes options like Discover, Visualize, Dashboard (which is selected), Timeline, Dev Tools, Management, Squert, and Logout. The main area has two tabs: 'DNS - Queries' and 'DNS - Answers'. The 'DNS - Queries' tab displays four long hex string queries:

- 434f4e464944454e5449414c20444f43554d454e540a444f.
- 484152450a5468697320646f63756d656e7420636f6e7461
- 666f726d6174696f6e2061626f757420746865206c617374.
- 697479206272656163682e0a.ns.example.com

The 'DNS - Answers' tab shows a message: 'No results found' with a sad face emoji.

At the bottom of the main area, there are 'Export' buttons for 'Raw' and 'Formatted' data.

Analisi file .raw delle query

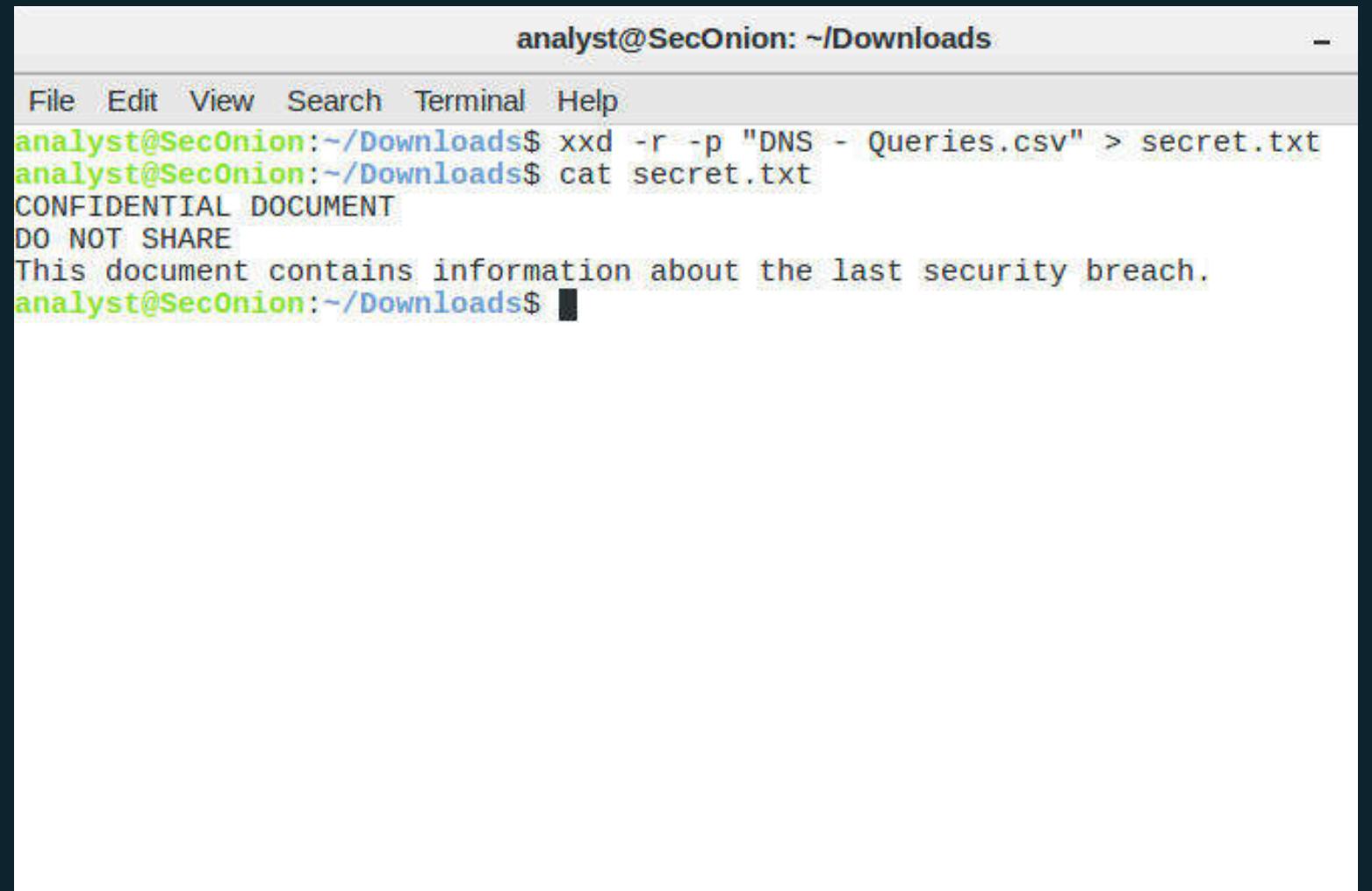
Andiamo poi a scaricare il file .raw delle query in questione. Un attaccante, per mascherare un dominio, potrebbe inserire del codice contenente caratteri codificati in formato esadecimale. Questa tecnica viene utilizzata per offuscare il contenuto e includere dati nascosti all'interno della richiesta.



```
Open File ~ /Downloads Save File
query,Count
"434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com",1
"484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com",1
"666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com",1
"697479206272656163682e0a.ns.example.com",1
```

Contenuto Nascosto

In un terminale utilizzando il comando xxd, siamo riusciti a decodificare il testo esadecimale in un testo leggibile e abbiamo salvato il contenuto in un file chiamato secret.txt. Abbiamo poi utilizzato il comando cat per visualizzare il contenuto del file. Quello che uscirà sarà quello mostrato in figura.



The screenshot shows a terminal window titled "analyst@SecOnion: ~/Downloads". The window contains the following text:

```
File Edit View Search Terminal Help
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~/Downloads$
```

Punto della situazione

Da un'attenta analisi siamo riusciti a risalire all'accaduto.

Siamo di fronte ad un attacco di DNS Tunneling ovvero una tecnica che viene utilizzata per bypassare i controlli di rete, per esfiltrare dati o per stabilire comunicazioni con un server esterno tramite il protocollo DNS.

In questo specifico attacco, il malintenzionato ha preso i dati da esfiltrare, li ha codificati in formato esadecimale e li ha divisi in piccoli pezzi (in quanto la lunghezza massima di una query DNS è di massimo 255 caratteri) e infine, li ha inviati come sottodomini all'interno delle query stesse.

Dall'altra parte il server DNS dell'attaccante riceve questa query, estrae i dati dai sottodomini e li decodifica per ricostruire il file. Queste query appaiono come normali risoluzioni DNS quindi il traffico passa spesso inosservato.



Bonus 3

07

BONUS 3

Dopo un attacco gli utenti non hanno più accesso al file confidential.txt. L'obiettivo è analizzare i logs e determinare come il file è stato compromesso. Lanciamo la macchina Security Onion e effettuiamo il login come analyst. Come step successivo apriamo sguil, effettuiamo il log in e mettiamo il flag su "seleziona tutti"



07

BONUS 3

Sguil è un software open-source utilizzato principalmente per analizzare e visualizzare i dati provenienti da un sistema di rilevamento intrusioni, come Snort o Suricata. In particolare, Sguil è progettato per supportare gli analisti della sicurezza informatica nella gestione di eventi di rete sospetti o attacchi informatici, centralizzando e semplificando la visualizzazione degli alert generati da questi strumenti.

07

BONUS 3

Guardando i vari eventi ce n'è uno che si nota subito per il nome che ha; **GPL_ATTACK_RESPONSE id check returned root**. Questo indica che qualcuno durante l'attacco ha avuto accesso ai privilegi root. Mettendo il flag su Show packet data otteniamo più dettagli.

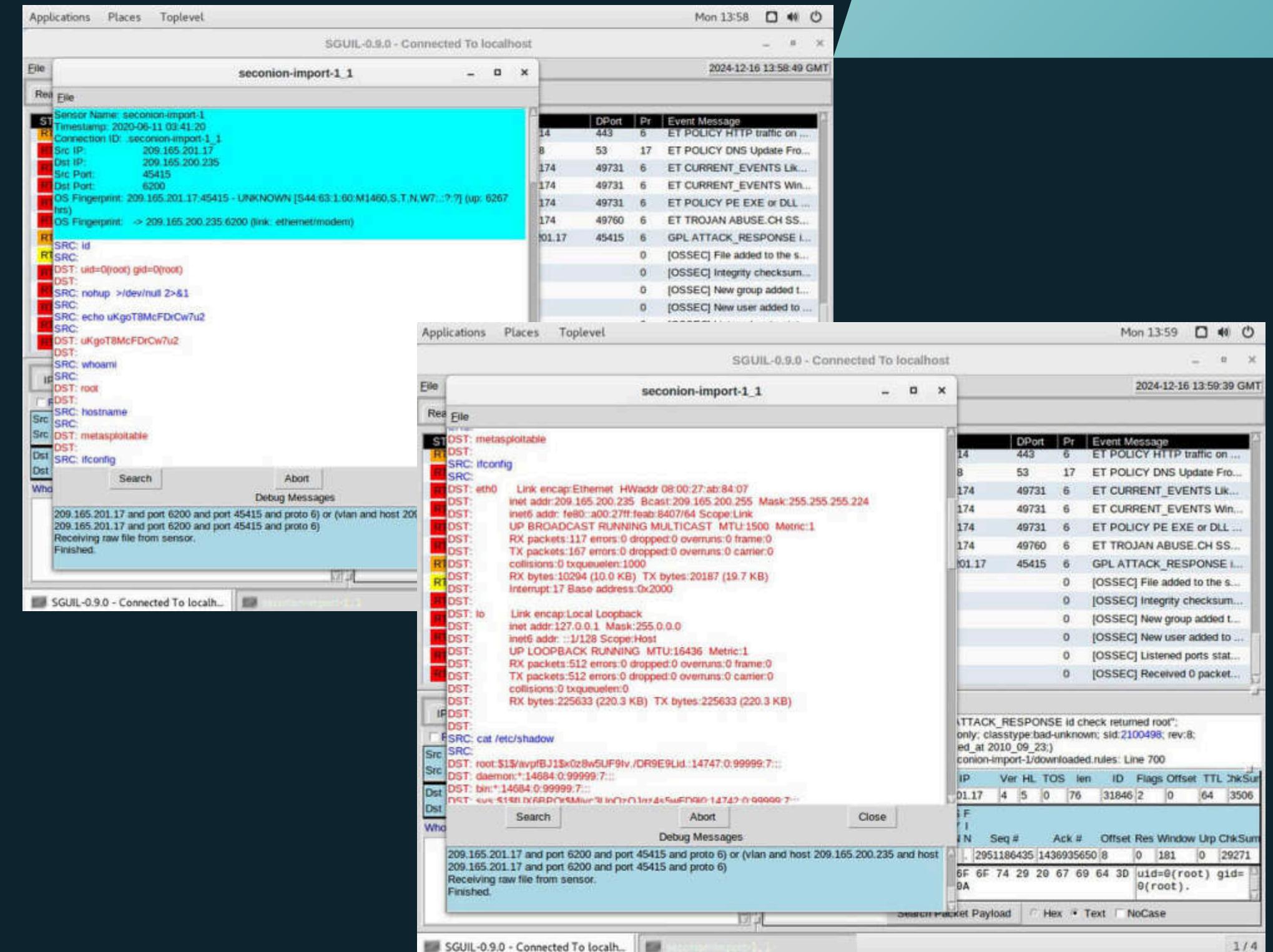
The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The event log table displays various security alerts, including several entries for 'GPL ATTACK_RESPONSE' events. One such entry is highlighted in yellow, indicating it's the current selection. The packet details pane shows a TCP connection between Source IP 209.165.200.235 and Dest IP 209.165.201.17, port 6200 to 45415. The payload shows a sequence of bytes corresponding to the rule definition: UAPRSF, RRRCSSYI, 10GKHTNN, 2951186435, 1436935650, 80181029271, followed by the rule content: alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;) /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 700.

07

BONUS 3

Se clicchiamo con il tasto destro nella colonna Alert ID e selezioniamo Transcript. Mostra le interazioni tra l'attaccante e il target durante l'attacco. L'attaccante come possiamo vedere sta eseguendo comandi linux.

Come possiamo notare l'attaccante ha ottenuto i privilegi di root e ha iniziato a navigare tra i file di sistema. Ha copiato shadow file e editato /etc/shadow e /etc/passwd.



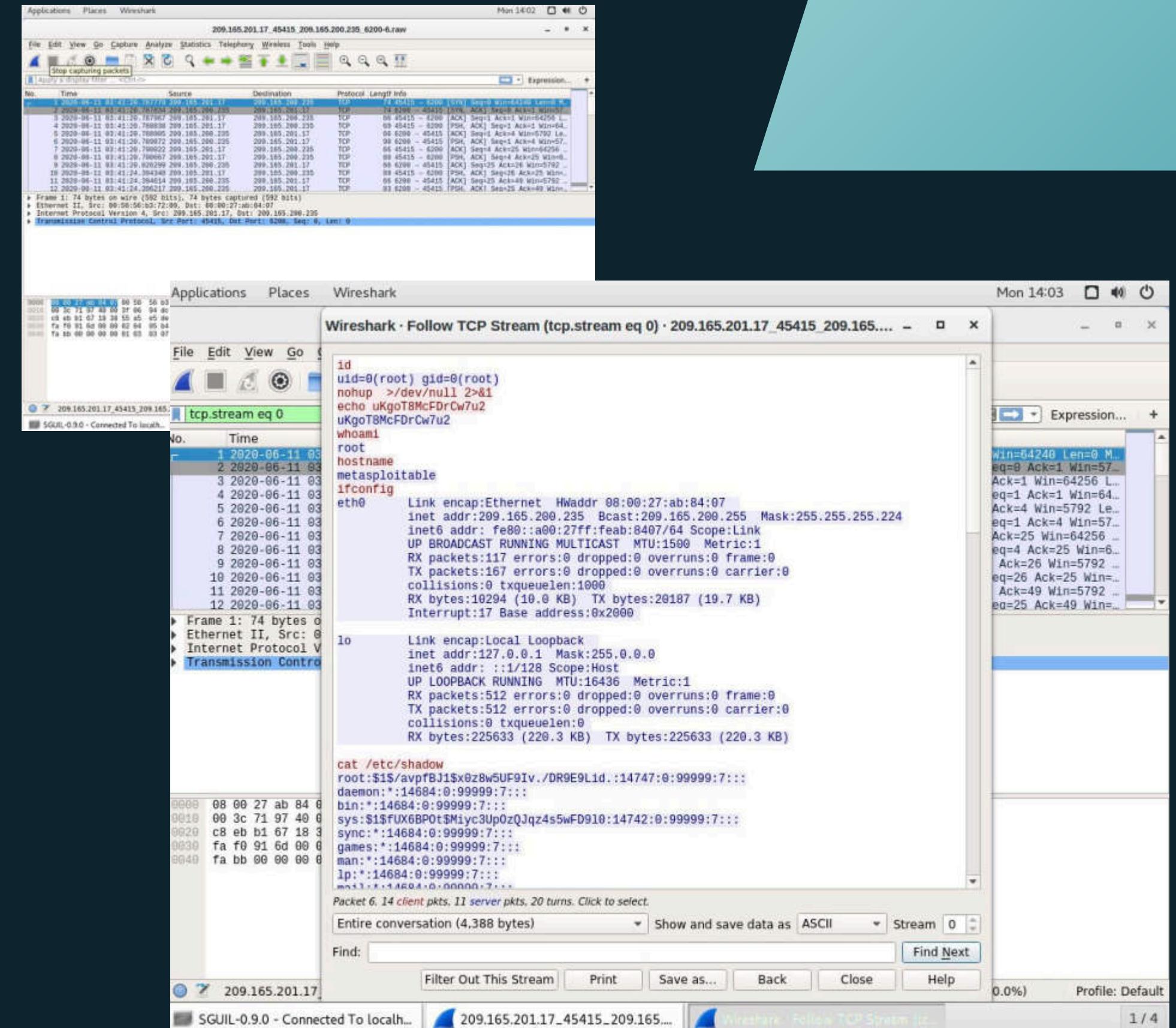
07

BONUS 3

Successivamente apriamo l'alert con wireshark

Per visualizzare tutti i pacchetti che formano la conversazione TCP, facciamo click destro su un qualsiasi pacchetto e selezioniamo follow -> TCP stream

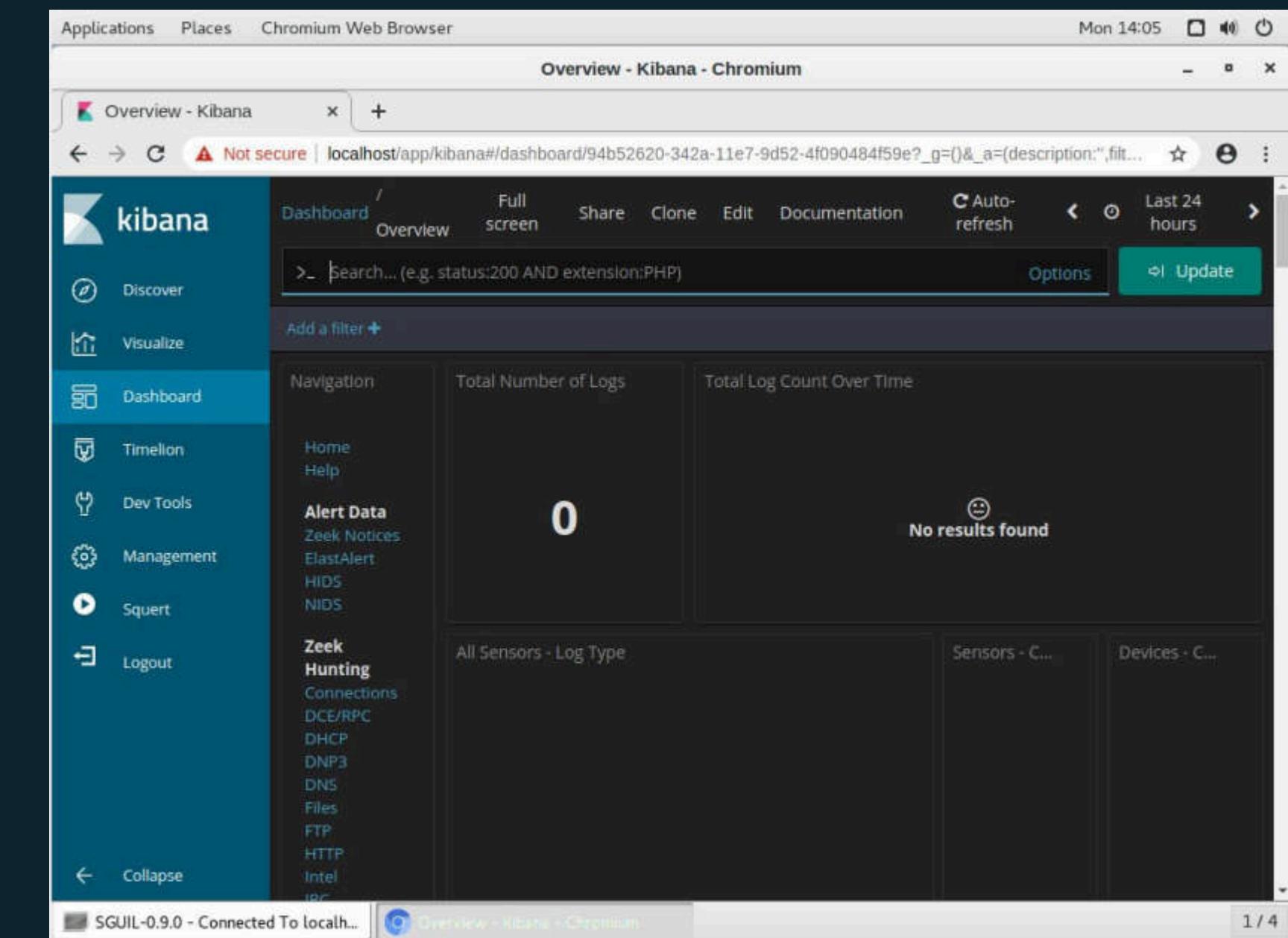
Questo mostra cosa ha scritto l'attaccante (rosso) e le risposte da parte del sistema (blu).



07

BONUS 3

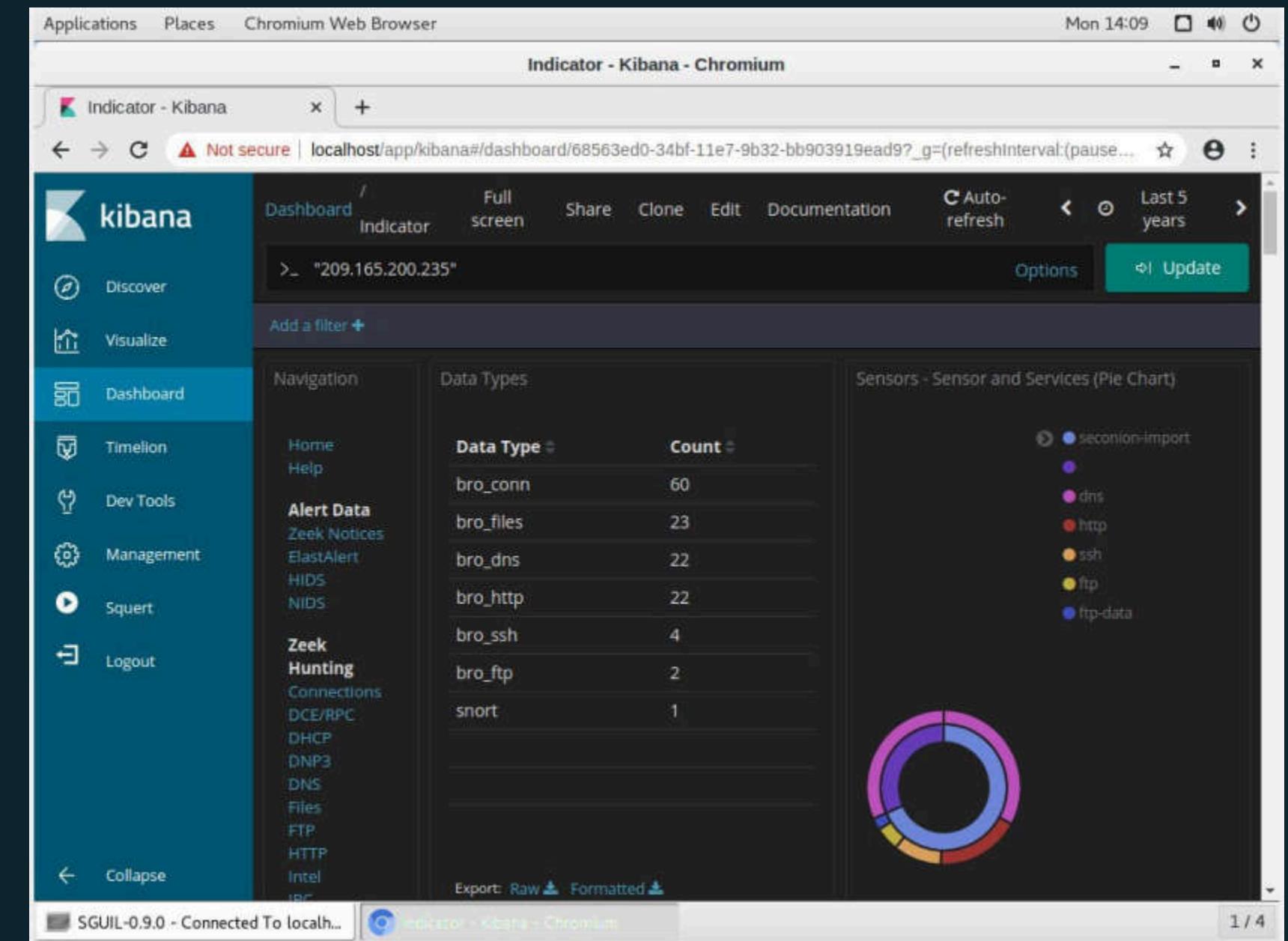
Ritornando su Sguil facciamo right click su source ip in questo caso 209.165.200.235 e clicchiamo su kibana IP Lookup. Kibana è uno strumento di visualizzazione e analisi dei dati che fa parte della Elastic Stack, precedentemente noto come ELK Stack (Elasticsearch, Logstash, Kibana). È utilizzato principalmente per esplorare, analizzare e visualizzare grandi volumi di dati in tempo reale, spesso da log o da altre fonti di dati non strutturati.



07

BONUS 3

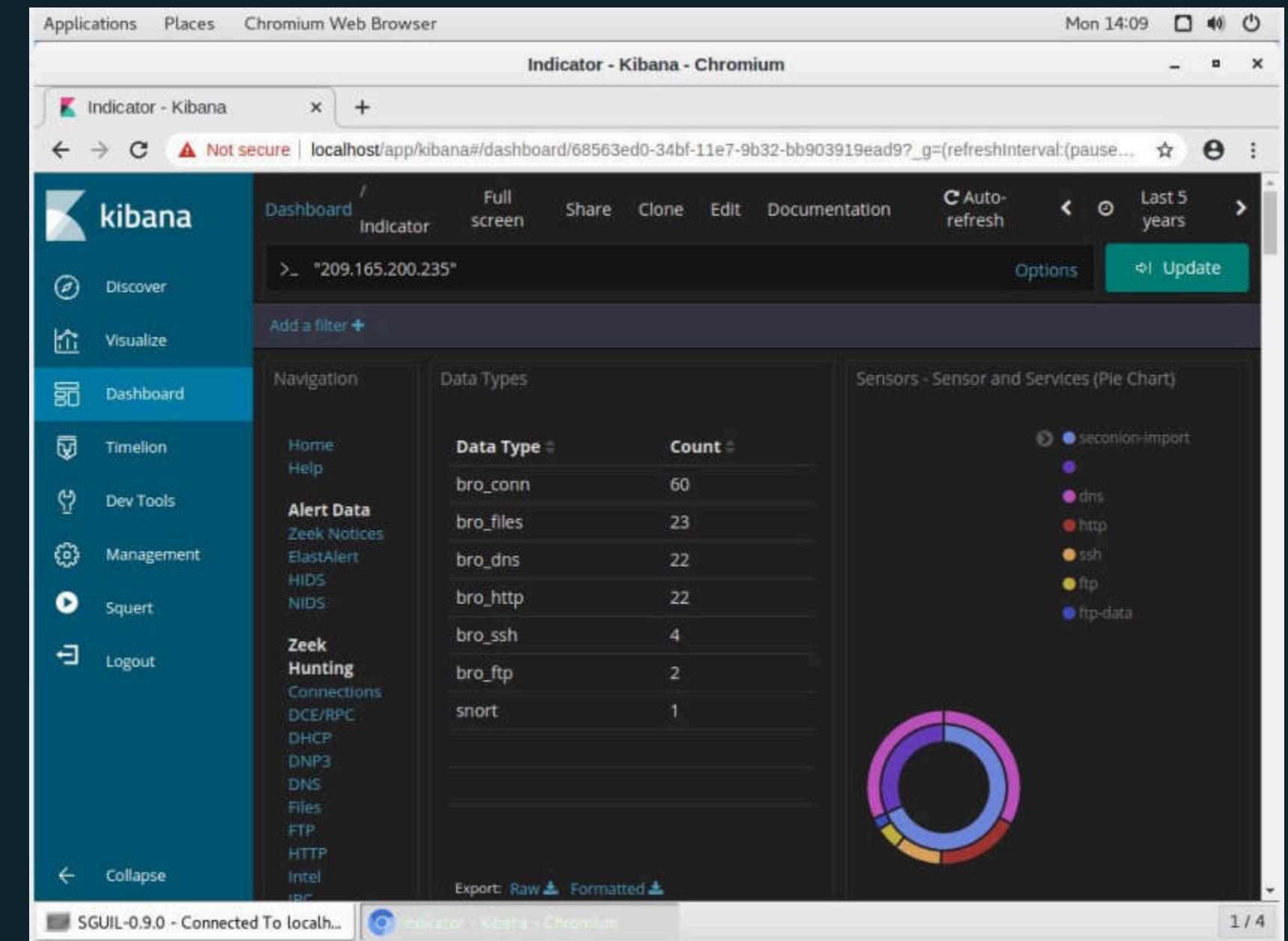
iP Lookup in Kibana è una funzionalità che consente di identificare informazioni aggiuntive riguardanti gli indirizzi IP presenti nei tuoi dati. Con l'IP Lookup, puoi ottenere dettagli come la posizione geografica, l'ISP, il paese, la città e altre informazioni relative all'indirizzo IP. cambiamo il time range in the last 5 years e mostra così una lista di tipi di dati differenti. Siccome il file confidential.txt non è più accessibile la prima cosa che andiamo a controllare l'FTP è stato usato per rubare il file. Aggiungiamo il filtro bro_ftp scrolliamo fino ad arrivare alla voce all logs



07

BONUS 3

iP Lookup in Kibana è una funzionalità che consente di identificare informazioni aggiuntive riguardanti gli indirizzi IP presenti nei tuoi dati. Con l'IP Lookup, puoi ottenere dettagli come la posizione geografica, l'ISP, il paese, la città e altre informazioni relative all'indirizzo IP. cambiamo il time range in the last 5 years e mostra così una lista di tipi di dati differenti. Siccome il file confidential.txt non è più accessibile la prima cosa che andiamo a controllare l'FTP è stato usato per rubare il file. Aggiungiamo il filtro bro_ftp scrolliamo fino ad arrivare alla voce all logs

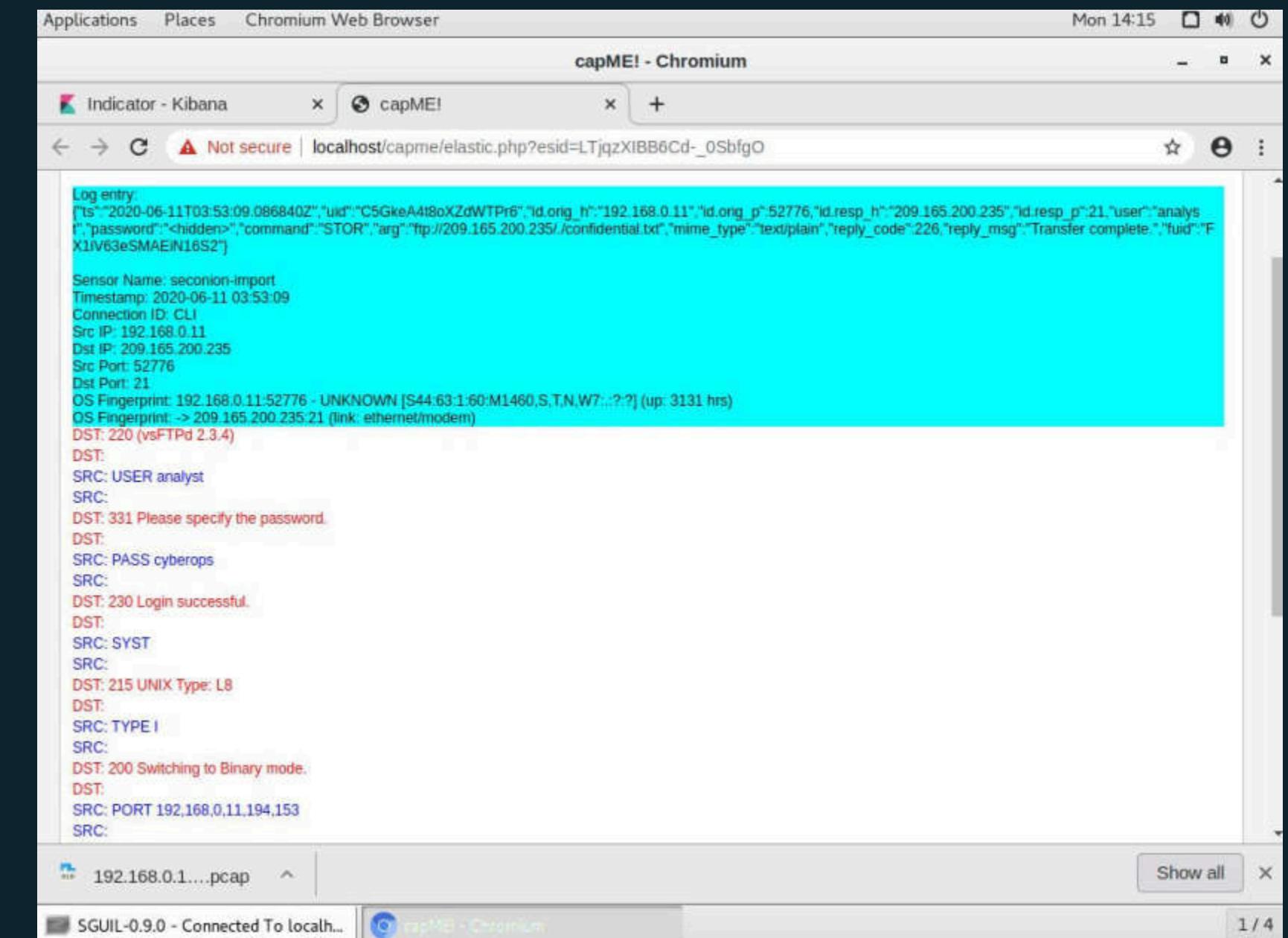


07

BONUS 3

In uno dei due log abbiamo un'entrata in `ftp://209.165.200.235/.confidential.txt`. Anch'esso mostra la conversazione tra attaccante e target. troviamo Che le credenziali usate per il log in sono state analyst and pass: cyberops.

Abbiamo capito da questo log che l'attaccante ha usato l'FTP per copiare il contenuto del file ed eliminarlo dal target.



The screenshot shows a Chromium browser window titled "capME! - Chromium" with the URL `localhost/capme/elastic.php?esid=LTjqzXIBB6Cd-_0SbfgO`. The page displays a log entry in JSON format:

```
Log entry:  
{"ts": "2020-06-11T03:53:09.086840Z", "uid": "C5GkeA4t8oXZdWTPr6", "id.orig_h": "192.168.0.11", "id.orig_p": 52776, "id.resp_h": "209.165.200.235", "id.resp_p": 21, "user": "analyst", "password": "<hidden>", "command": "STOR", "arg": "ftp://209.165.200.235/.confidential.txt", "mime_type": "text/plain", "reply_code": 226, "reply_msg": "Transfer complete.", "fuid": "F11V63eSMAEjN16S2"}  
Sensor Name: seconion-import  
Timestamp: 2020-06-11 03:53:09  
Connection ID: CLI  
Src IP: 192.168.0.11  
Dst IP: 209.165.200.235  
Src Port: 52776  
Dst Port: 21  
OS Fingerprint: 192.168.0.11:52776 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7...?:?] (up: 3131 hrs)  
OS Fingerprint: -> 209.165.200.235.21 (link: ethernet/modem)  
DST: 220 (vsFTPD 2.3.4)  
DST:  
SRC: USER analyst  
SRC:  
DST: 331 Please specify the password.  
DST:  
SRC: PASS cyberops  
SRC:  
DST: 230 Login successful.  
DST:  
SRC: SYST  
SRC:  
DST: 215 UNIX Type: L8  
DST:  
SRC: TYPE I  
SRC:  
DST: 200 Switching to Binary mode.  
DST:  
SRC: PORT 192.168.0.11,194.153  
SRC:
```

Below the browser window, the system tray shows "SGUIL-0.9.0 - Connected To localh..." and the taskbar shows "capME! - Chromium".

07

BONUS 3

Selezionando la voce file sotto la colonna Zeek Hunting troviamo 1 solo FTP_data scrollando fino in fondo nella voce alert id troviamo un link che se lo apriamo troviamo CONFIDENTIAL DOCUMENT DO NOT SHARE this document contains information about the last security breach.

Per far sì che ciò non si ripeti consiglio come minimo di utilizzare password e username più forti.

