



TABLE OF CONTENT



1. Malware analysis
2. Anyrun
3. Linux Filesystem
4. File PCAP
5. BONUS 1
6. BONUS 2
7. BONUS 3



MALWARE ANALYSIS

**Malware
Analysis**

Any.run

**Filesystem
Linux**

File PCAP

BONUS 1

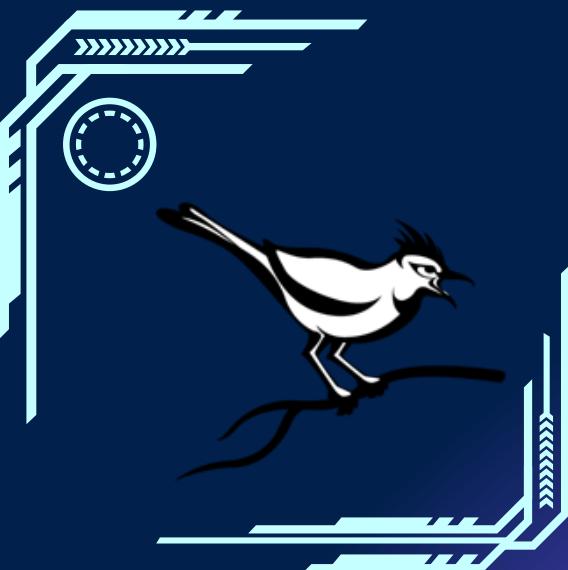
BONUS 2

BONUS 3

MALWARE ANALYSIS

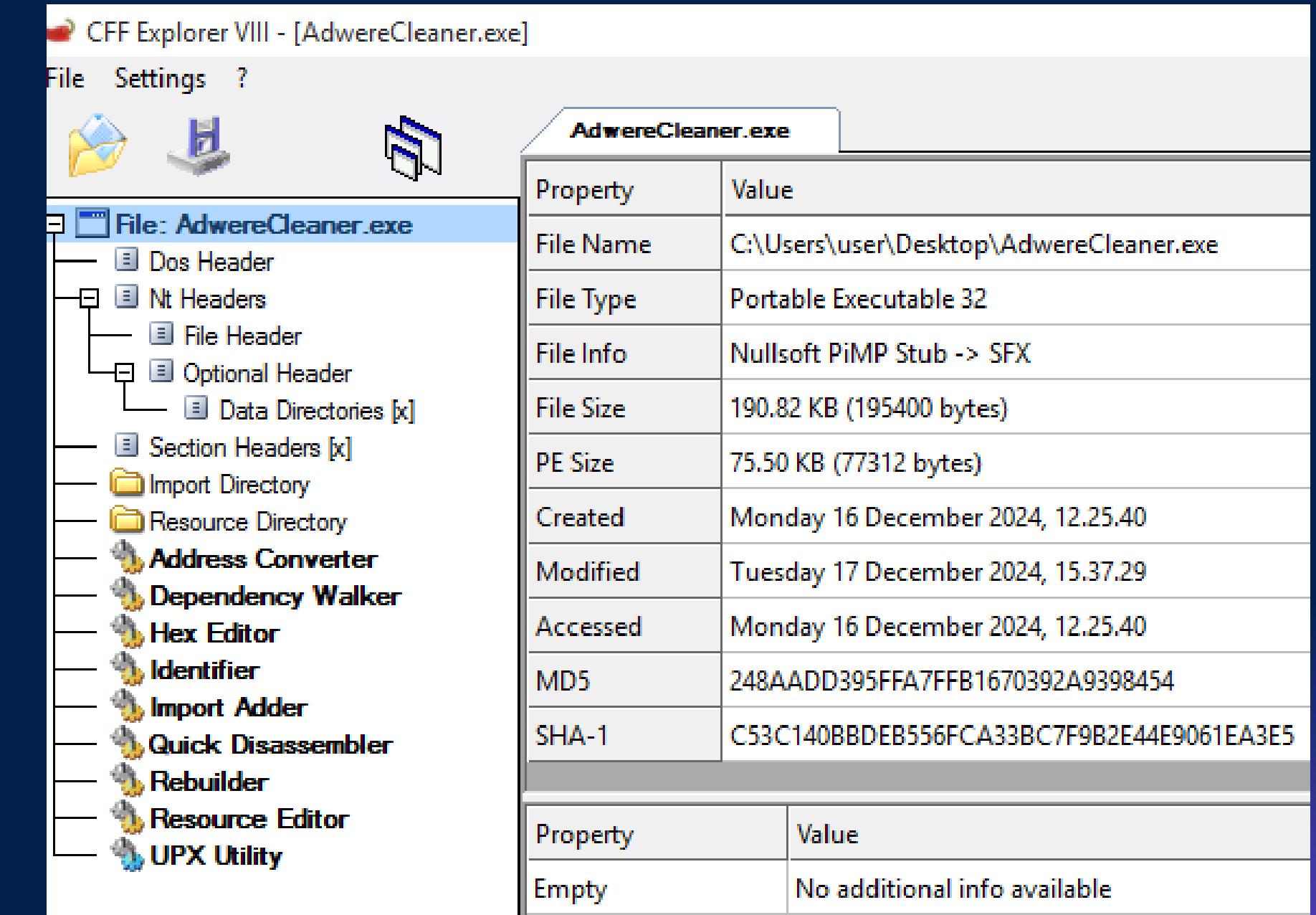
Introduzione:

È stata condotta un'analisi approfondita su un eseguibile potenzialmente dannoso, avvalendosi di diverse tecniche e strumenti per analisi statica e dinamica di un malware. L'obiettivo era identificare la natura del file, le sue funzionalità e le potenziali minacce associate.

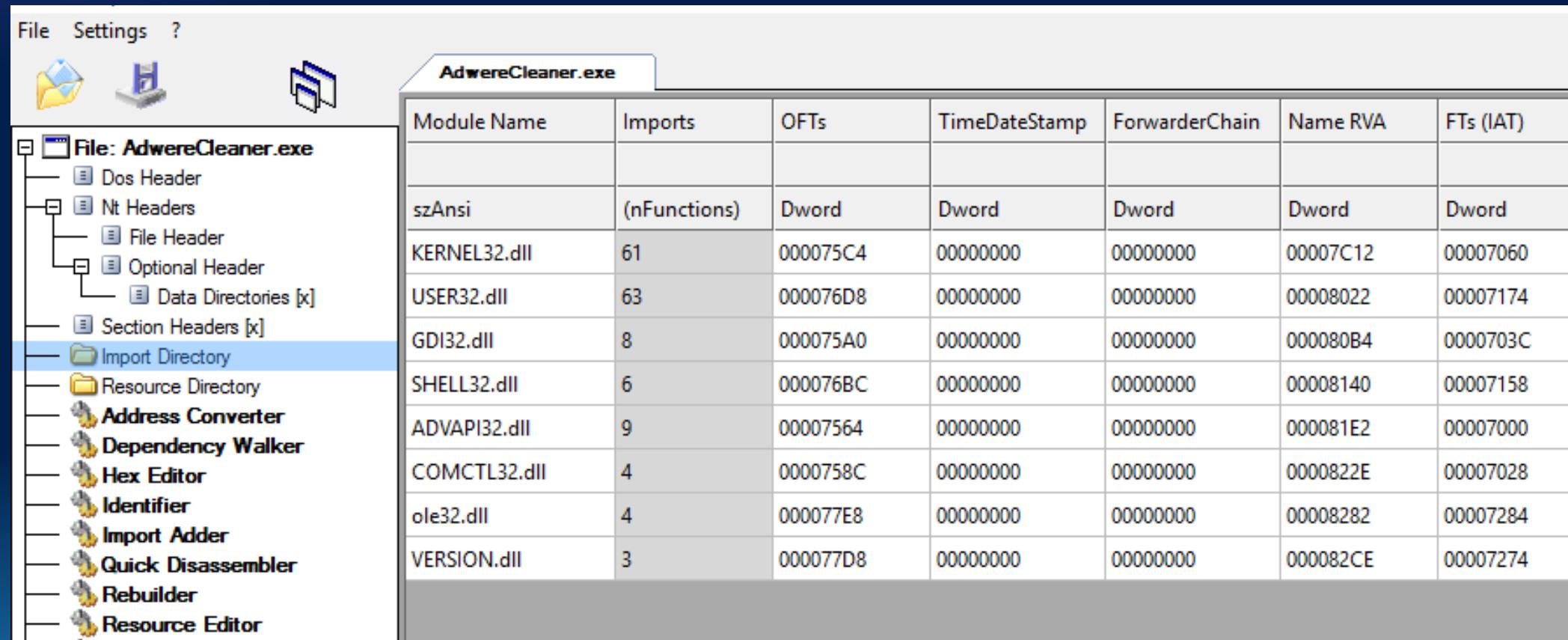


ANALISI STATICÀ

Abbiamo iniziato la nostra indagine del file eseguibile partendo da un'analisi statica utilizzando CFF Explorer. Questo software consente di esaminare in dettaglio le caratteristiche del file eseguibile, analizzandone il comportamento e il codice.



ANALISI STATICÀ



Inoltre è in grado di mostrarcì le funzioni che il file và a richiamare da determinate librerie presenti nel sistema.

Questo può fornirci un'indicazione sul suo comportamento.

ANALISI STATICÀ

Un altro tool utile nell'analisi statica è VirusTotal che ci permette di analizzare un file per rilevarne eventuali minacce e comportamenti dannosi.

Il suo funzionamento si basa sul confronto tra diversi motori antivirus, il che lo rende molto attendibile.

The screenshot shows the VirusTotal analysis interface for the file `AdwereCleaner.exe`. The file has a community score of **55 / 71**. A warning message indicates that **55/71 security vendors flagged this file as malicious**. The file size is **190.82 KB** and it was last analyzed **a moment ago**. The file type is identified as **EXE**. The analysis includes tags such as `peexe`, `nsis`, `persistence`, `checks-user-input`, `direct-cpu-clock-access`, `revoked-cert`, `overlay`, `runtime-modules`, `signed`, `detect-debug-environment`, and `executes-dropped-file`. Below the main summary, there are tabs for **DETECTION**, **DETAILS**, **RELATIONS**, **ASSOCIATIONS**, **BEHAVIOR**, and **COMMUNITY** (with 21+ entries). A green banner encourages users to join the community. The **Popular threat label** is `trojan.porcupine/mint`. Threat categories include `trojan` and `fakeav`. Family labels include `porcupine`, `mint`, and `boy2napig`. The **Security vendors' analysis** section lists findings from various engines:

Engine	Findings	Category	Notes
AhnLab-V3	Dropper/Win32.Dapato.R137988	Alibaba	Hoax:MSIL/Porcupine.e66e0e97
Antiy-AVL	HackTool[Hoax]/MSIL.Agent	Arcabit	Trojan.Mint.Porcupine.ED5D10
Avast	Win32:FakeAV-FLW [Trj]	AVG	Win32:FakeAV-FLW [Trj]
Avira (no cloud)	JOKE/Agent.rlham	BitDefender	Gen:Heur.Mint.Porcupine.luZ@bOy2NApig
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.fakeav

ANALISI STATICÀ

VirusTotal ci fornisce anche una panoramica sui dettagli del file e ci suggerisce dei risultati ottenuti dall'analisi dinamica da parte di alcune sandbox.

Dynamic Analysis Sandbox Detections ⓘ

- ⚠ The sandbox Dr.Web vxCube flags this file as: MALWARE
- ⚠ The sandbox Yomi Hunter flags this file as: MALWARE

Basic properties ⓘ

MD5	248aadd395ffa7ffb1670392a9398454
SHA-1	c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5
SHA-256	51290129cccc38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
Vhash	015056655d5c05709043z8003d7z47z62z3f03dz
Authentihash	8eb8f3a6371a77e2b5002de83a5955d4d5fb7f2cdb7d8642138bb20d243be578
Imphash	e160ef8e55bb9d162da4e266af9eeef3
Rich PE header hash	ecf81400e80e4d5ebc5ac2f7c2aacea3
SSDEEP	3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GID0g+ELqdSxo5XtIZjnvxRJggHaR:157TcfFPB6B3GL7g+me5aZjn5Vl9T/T17B1412524AF05AFFFB4384712AFDE1B9E7B7828C5274A9974B148E323B440D74F8611A
TLSH	
File type	Win32 EXE
	executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
TrID	NSIS - Nullsoft Scriptable Install System (92.7%) Win32 Executable MS Visual C++ (generic) (3.4%) Win64 Executable (generic) (1.1%) Win32 Dynamic Link Library (ge... PE32 Installer: Nullsoft Scriptable Install System (3.0a2) [zlib,solid] Compiler: Microsoft Visual C/C++ (12.20.9044) [C] Linker: Microsoft Linker (6.0) Tool: Visual St...
DetectItEasy	
Magika	PEBIN
File size	190.82 KB (195400 bytes)
F-PROT packer	NSIS, appended

ANALISI DINAMICA

Successivamente utilizzando la sandbox Cukoo abbiamo svolto l'analisi dinamica del file.

Questa analisi ci ha portato diversi risultati:

- Rilevamento multiplo: Il malware è stato identificato da 13 diversi motori antivirus, confermando la sua natura maliziosa.
- Diverse famiglie: I rilevamenti suggeriscono che il malware potrebbe appartenere a diverse famiglie o varianti, o presentare caratteristiche comuni a più famiglie, come Trojan e FakeAV.
- Comportamenti dannosi: Basandosi sulle regole Yara e sui rilevamenti antivirus, è emerso che il malware è in grado di:
 - Scalare i privilegi: Acquisire maggiori permessi nel sistema per eseguire azioni dannose.
 - Acquisire screenshot: Raccogliere informazioni visive sullo schermo dell'utente.
 - Modificare il registro di sistema: Persistere nel sistema e modificare il comportamento di altre applicazioni.
 - Manipolare i token di sistema: Impersonare altri utenti o processi.
 - Accedere a profili utente: Rubare informazioni sensibili o modificare le impostazioni del sistema.

Summary

Score

This file is very suspicious, with a score of 10 out of 10!

File AdwereCleaner.exe

Summary	
Size	190.8KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5	248aadd395ffa7ffb1670392a9398454
SHA1	c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5
SHA256	51290129cccc38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
SHA512	Show SHA512
CRC32	124412D7
ssdeep	None
Yara	<ul style="list-style-type: none">escalate_priv - Escalade privilegesscreenshot - Take screenshotwin_registry - Affect system registrieswin_token - Affect system tokenwin_private_profile - Affect private profilewin_files_operation - Affect private profile

Malware
Analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

Signatures

- ⓘ Yara rules detected for file (6 events)
- ⓘ Allocates read-write-execute memory (usually to unpack itself) (43 events)
- ⓘ Checks if process is being debugged by a debugger (2 events)
- ⓘ Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
- ⓘ Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- ⓘ The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)
- ⓘ Creates executable files on the filesystem (1 event)
- ⓘ Drops a binary and executes it (1 event)
- ⓘ Drops an executable to the user AppData folder (1 event)
- ⓘ Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
- ⓘ The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- ⚡ File has been identified by 13 AntiVirus engine on IRMA as malicious (13 events)
- ⚡ File has been identified by 55 AntiVirus engines on VirusTotal as malicious (50 out of 55 events)

ANALISI DINAMICA

Cukoo inoltre ci fornisce il dettaglio degli eventi che vengono a verificarsi durante l'esecuzione del malware.

CONCLUSIONI

Sulla base delle analisi effettuate, possiamo concludere che il campione analizzato rappresenta una seria minaccia per la sicurezza informatica. Il malware è in grado di eseguire diverse azioni dannose e di diffondersi rapidamente.



RACCOMANDAZIONI

Si consigliano le seguenti misure di sicurezza per mitigare i rischi associati a questo tipo di minacce:

- Mantenere aggiornati i sistemi: Installare regolarmente patch di sicurezza per sistema operativo e software applicativi.
- Utilizzare software antivirus affidabile: Scegliere un antivirus con un alto tasso di rilevamento e mantenerlo aggiornato.
- Evitare di aprire email sospette e cliccare su link non sicuri: La maggior parte delle infezioni da malware avviene tramite email o siti web compromessi.
- Effettuare backup regolari dei dati: In caso di infezione, un backup può permettere di ripristinare i dati persi.



ANY.RUN

The logo features the word "ANY.RUN" in a bold, white, sans-serif font. The letters are partially obscured by a futuristic, metallic frame with a glowing blue light effect. The frame has a circular hatch on the left side and vertical panels with horizontal arrows on the right side, suggesting a high-tech or industrial theme.

Malware
Analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

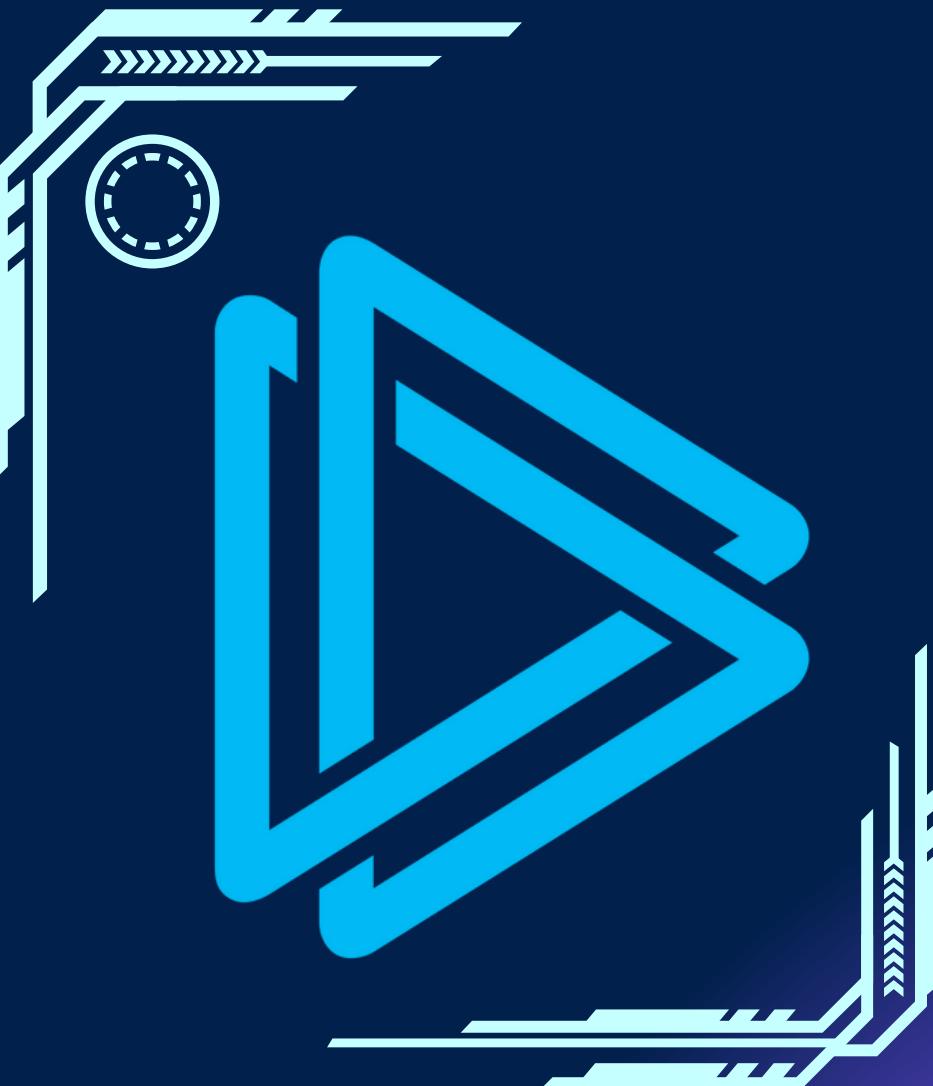
BONUS 2

BONUS 3

ANY.RUN

ANY.RUN è una piattaforma interattiva basata su cloud progettata per l'analisi dinamica di file sospetti, malware e URL.

Utilizzeremo questa piattaforma per analizzare 2 link diversi.



Abbiamo analizzato un file chiamato 66bddfcb52736_vidar.exe, che si è rivelato essere un malware, cioè un programma dannoso progettato per fare cose che non dovrebbero essere fatte su un computer.

Questo malware combina due tipi di minacce:

- **Vidar:** Un malware che ruba informazioni personali (come password, dati di carte di credito, o criptovalute).
- **Lumma:** Un programma che può essere usato dai criminali per rubare credenziali e altre informazioni sensibili.

The screenshot shows a Windows 10 desktop with several pinned icons: Recycle Bin, Microsoft Edge, iweekly.png, CCleaner, Skype, listingspac..., Adobe Acrobat, codegraphi..., metalsan..., Firefox, georgiauni..., sortsearch.rtf, Google Chrome, holiday.rsg..., websiteviewer..., VLC media player, hugemilf.ttf, 66bddfcb5..., and a file named 66bddfcb52736_vidar.exe. At the bottom, there's a network traffic analysis interface with tabs for Richieste HTTP, Connessioni, Richieste DNS, Minacce, and PCAP. The Minacce tab is active, showing a list of detected threats. One entry is highlighted: "7 millisecondi OTTENERE200: Va bene" with PID 5468, process svchost.exe, and URL http://ocsp.digicert.com/MFEwTzBNM... with a status of "471 anni ↓ binario". Other entries include "1 millisecondi OTTENERE200: Va bene" with PID 6908, process RegAsm.exe, and URLs http://147.45.44.104/prog/66cb2df8bd... and http://147.45.44.104/prog/66cb2df1d4... with statuses "321Kb di spazio ↓ eseguibile" and "193Kb ↓ eseguibile". A message at the bottom says "Pericolo [6340] RegAsm.exe È stato rilevato VIDAR (YARA)".

The screenshot shows a detailed analysis of the malware sample. At the top, it displays the file name 66bddfcb52736_vidar.exe, MD5 hash FEDB687ED23F77925B35623027F799BB, and the start time 25.08.2024, 22:11. The total duration is 60 s. Below this are sections for Vinci 10 64 bit Completare, Indicatori, Tracciatori, and various buttons like Ottieni un campione, CIO, MalConf, Riconcilia, Rapporto di testo, Grafico, ATTENZIONE, Riepilogo, and Exportare. The main pane is titled "Processi" and lists several processes, mostly RegAsm.exe, with details like PID, CPU usage, and memory usage. A specific entry for HCAEHJJKFC.exe is highlighted with the label "EDUCAZIONE FISICA". At the bottom, there are links for "Prova gratuitamente la versione community!" and "Registrati ora".

PRIMA ANALISI

Il malware che stiamo analizzando esegue queste operazioni.

Ruba informazioni:

- Legge le password salvate nei browser (Chrome, Firefox, Opera, ecc.).
- Cerca dati nei programmi come Telegram, Discord e Steam.
- Raccoglie dettagli del computer, come il nome del dispositivo, il sistema operativo, e altre informazioni tecniche.

Modifica il sistema:

- Crea nuovi file e modifica le impostazioni di sicurezza del computer.
- Elimina file importanti o legittimi per confondere chi cerca di analizzarlo.
- Cerca di nascondersi usando tecniche per evitare di essere scoperto.

Comunica con i criminali:

- Si collega a siti e server controllati dai cybercriminali (detti C2, o Commandand Control) per inviare le informazioni rubate o ricevere nuovi comandi.

PRIMA ANALISI

MALICIOUS

Actions looks like stealing of personal data

- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

VIDAR has been detected (YARA)

- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 6340)

Steals credentials from Web Browsers

- RegAsm.exe (PID: 6908)

LUMMA has been detected (SURICATA)

- RegAsm.exe (PID: 4704)

Stealers network behavior

- RegAsm.exe (PID: 4704)

LUMMA has been detected (YARA)

- RegAsm.exe (PID: 4704)

SUSPICIOUS

Reads security settings of Internet Explorer

- RegAsm.exe (PID: 6908)

Searches for installed software

- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

Drops the executable file immediately after the start

- 66bddfcb52736_vidar.exe (PID: 6780)
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 6340)

The process drops C-runtime libraries

- RegAsm.exe (PID: 6908)

The process drops Mozilla's DLL files

- RegAsm.exe (PID: 6908)

Checks Windows Trust Settings

- RegAsm.exe (PID: 6908)

Executable content was dropped or overwritten

- RegAsm.exe (PID: 6908)

Process drops legitimate windows executable

- RegAsm.exe (PID: 6908)

Reads the date of Windows installation

- RegAsm.exe (PID: 6908)

Starts CMD.EXE for commands execution

- RegAsm.exe (PID: 6908)

Uses TIMEOUT.EXE to delay execution

- cmd.exe (PID: 6284)

Potential Corporate Privacy Violation

- RegAsm.exe (PID: 6908)

[6780] 66bddfcb52736_vidar.exe C:\U

Verdetto della minaccia

100
SU 100

Malizioso

Il punteggio è un valore approssimativo calcolato dall'algoritmo ANY.RUN in base al processo e alle azioni dell'utente
Indicatori:

CONCLUSIONI

Dalla nostra analisi abbiamo osservato che questo malware compie le seguenti azioni:

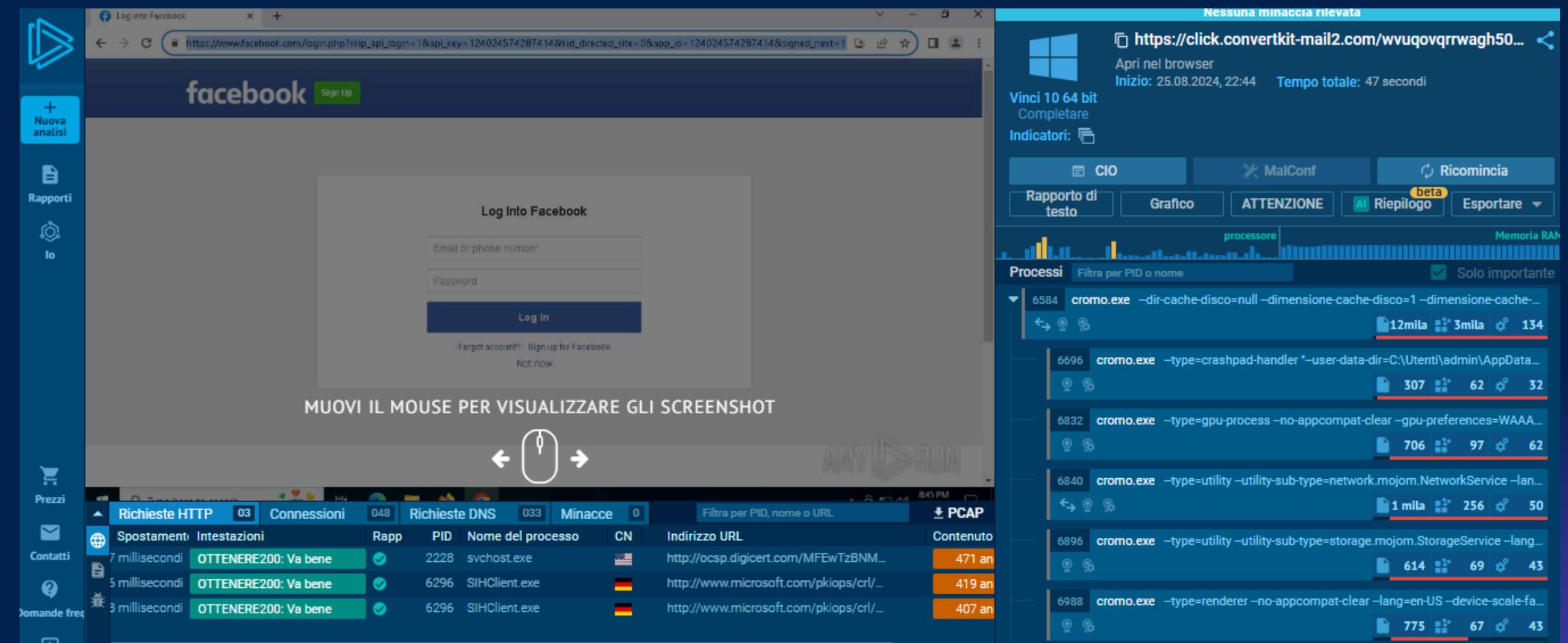
- Ruba dati personali: Password, informazioni bancarie, dati di applicazioni.
- Si nasconde bene: Usa tecniche avanzate per evitare di essere rilevato dagli antivirus.
- Compromette il sistema: Modifica file e impostazioni che potrebbero compromettere la sicurezza del computer anche dopo la rimozione del malware.

RACCOMANDAZIONI

Per evitare questo tipo di minacce, si consigliano le seguenti azioni:

- Isolare il computer: Spegni la connessione a internet per evitare che il malware continui a inviare dati ai criminali.
- Pulire il sistema: Usa un antivirus potente per eliminare i file infetti. Ripristina eventuali file di sistema modificati.
- Cambiare le password: Cambia tutte le password salvate sul computer infetto, specialmente quelle di servizi importanti come email e banche.
- Prevenire futuri attacchi: Non apri email sospette o file da fonti sconosciute. Usa programmi di sicurezza aggiornati.

Abbiamo analizzato un secondo file eseguibile. Il file non ha mostrato comportamenti sospetti o dannosi durante il test. Non sono state trovate attività che indicano la presenza di malware, come furto di dati, connessioni a server pericolosi o modifiche al sistema.



SECONDA ANALISI

Durante l'analisi è risultato che il file esaminato ha svolto le seguenti attività:

- Processi attivi: 139, ma nessuno sospetto o dannoso.
- Attività di rete: 48 connessioni TCP/UDP, tutte verso domini sicuri.
- Modifiche al sistema: Non sono state rilevate modifiche sospette.

Dettagli avanzati del processo

Informazioni principali

Firma del codice: **Valido**
Scarico del processo: 0

Eventi

Modifiche	Codice
File modificati	61
Modifiche al registro	18
Sincronizzazione	198
Richieste HTTP	0
Connessioni	2
Minacce di rete	0
...	...

[6584] chrome.exe C:\Programmi\Google\

Verdetto della minaccia

Nessun verdetto

Il punteggio è un valore approssimativo calcolato dall'algoritmo ANY.RUN in base al processo e alle azioni dell'utente

Indicatori: ↗

Informazioni sul processo

Nome utente: amministratore
SID: Numero di telefono: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIO
Inizio: 4,85 secondi

Informazioni sul file

Azienda: Google LLC
Descrizione: Google Chrome
Versione: 122.0.6261.70

Riga di comando AI

"C:\Programmi\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null
--disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache --di
sable-background-networking --disable-features=OptimizationGuideModelDo
wnloading OptimizationHintsFetching OptimizationTargetPrediction Optimizat

Processes

Total processes

139

Monitored processes

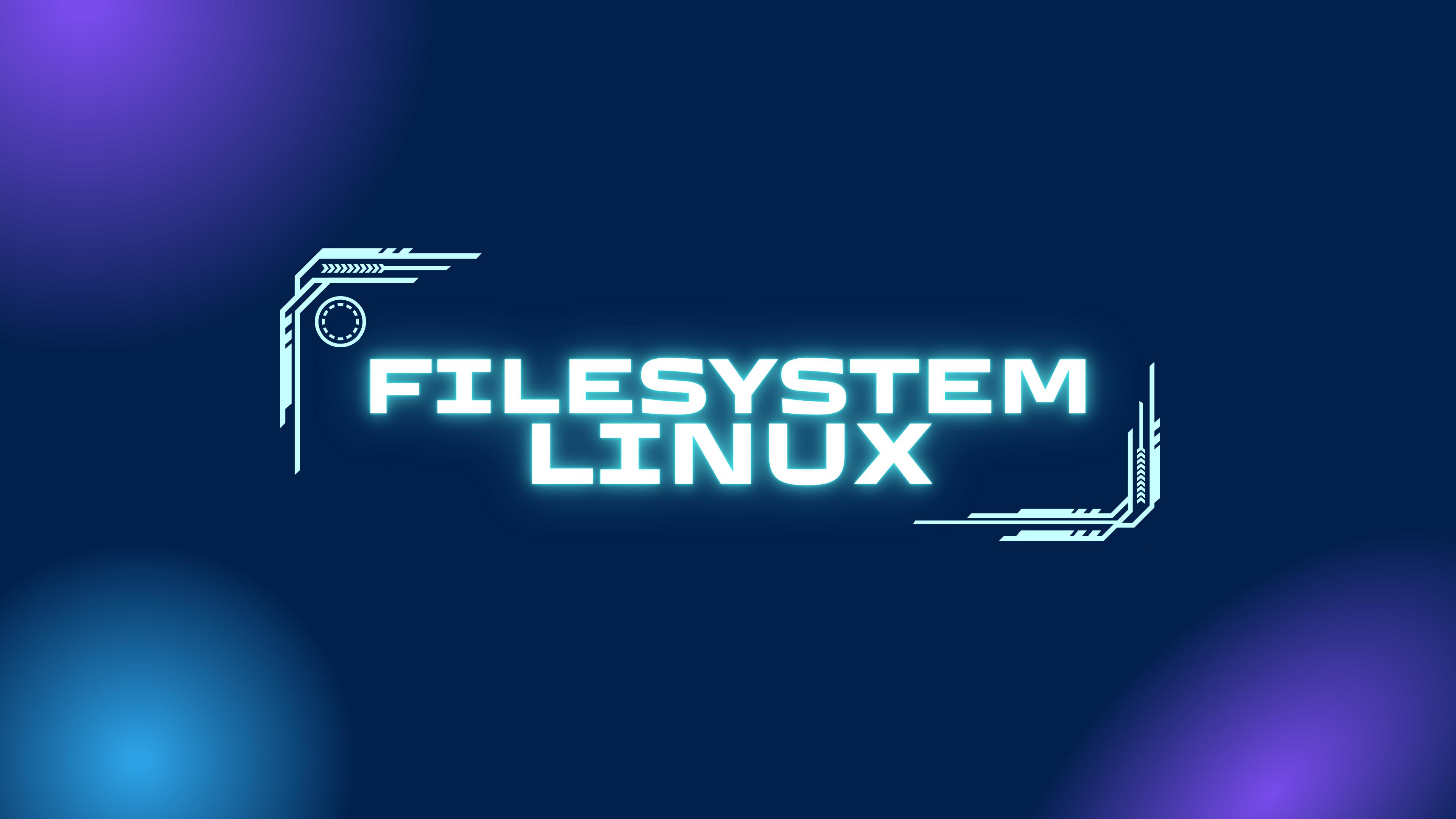
10

Malicious processes

0

Suspicious processes

0



FILESYSTEM

LINUX

Malware
Analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

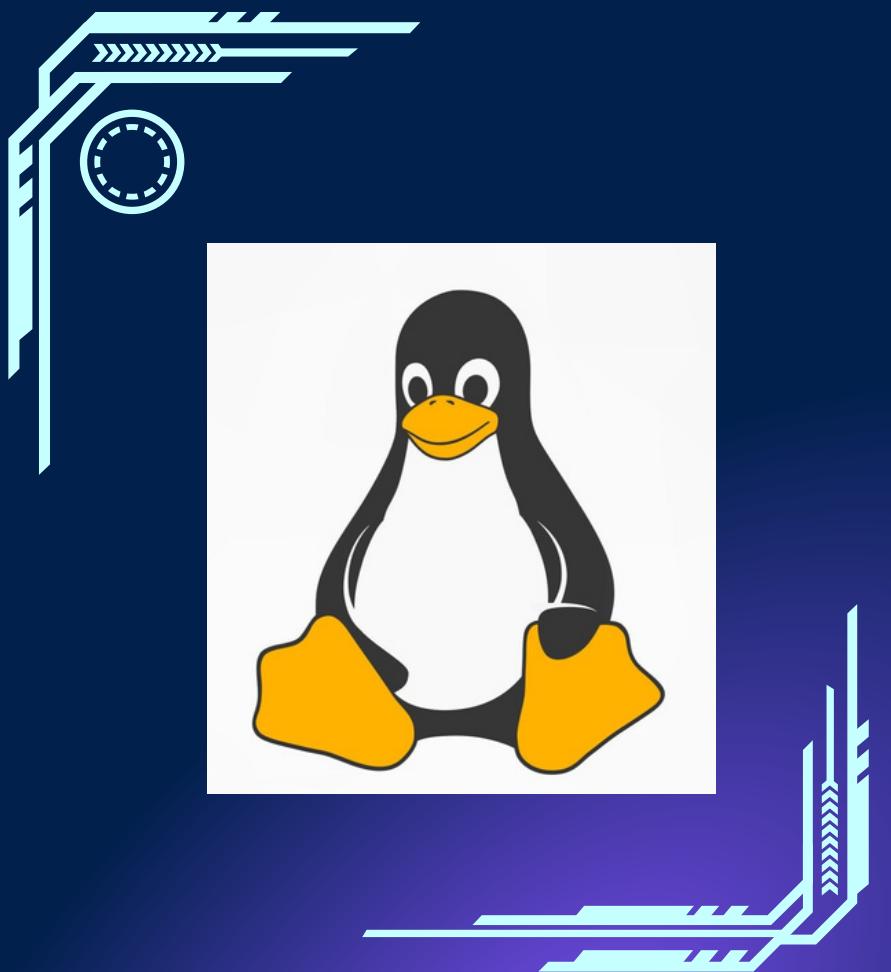
BONUS 2

BONUS 3

FILESYSTEM LINUX E IMPOSTAZIONI DEI PERMESSI

In questo laboratorio vedremo nel dettaglio:

- Esplorazione dei filesystem in linux
- Permessi dei file
- Collegamenti simbolici e altri tipi di file speciali

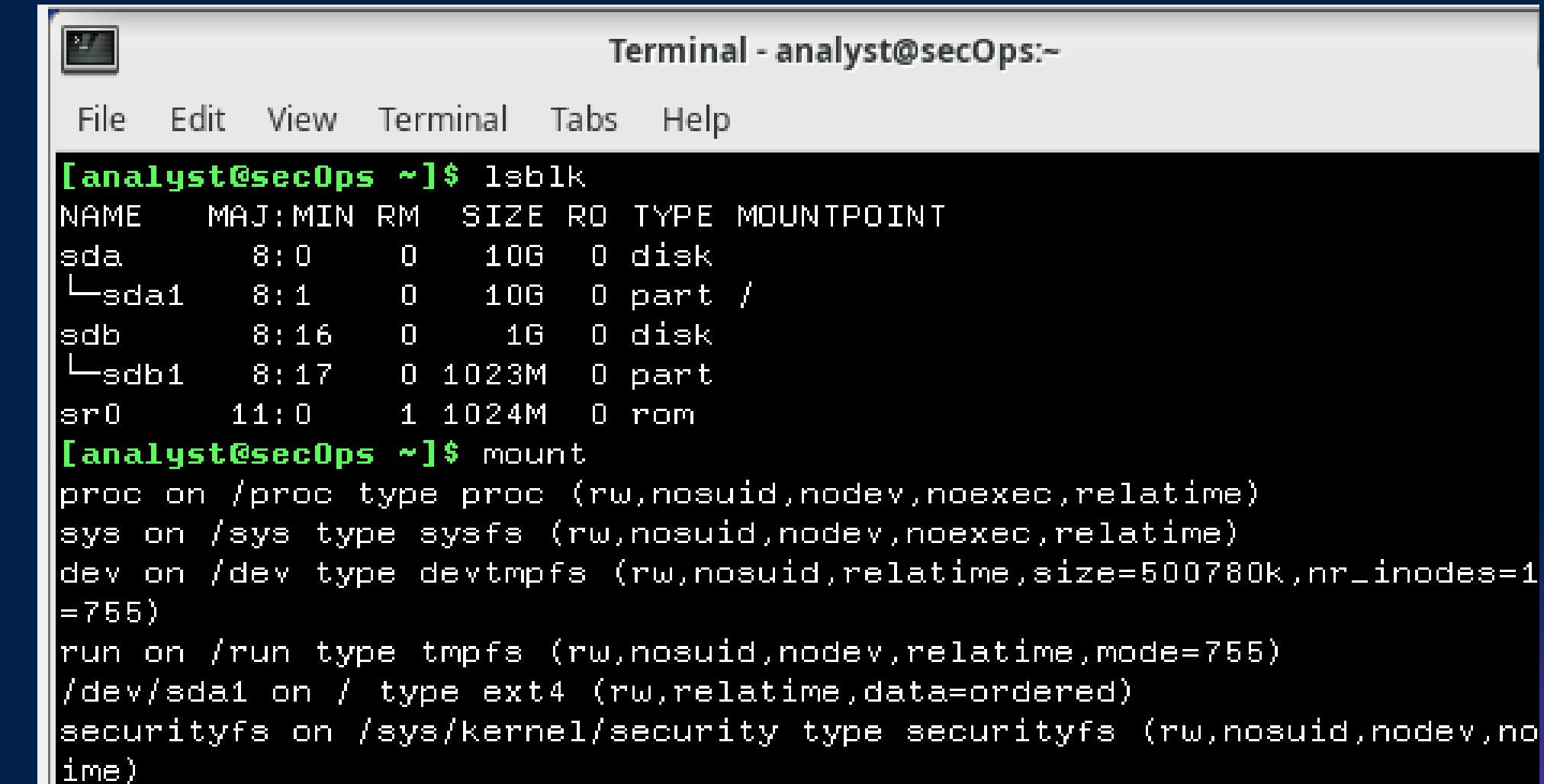


ESPLORAZIONE DEL FILESYSTEM LINUX

Per visualizzare i dispositivi a blocchi utilizziamo da terminale il comando `lsblk`.

Il filesystem su cui ci soffermeremo sarà `sda1`, poichè è il root filesystem (indicato con `/` nella colonna MOUNTPOINT)

Con il comando `mount`, invece, andiamo a visualizzare informazioni più dettagliate sui filesystem attualmente montati nella VM.



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

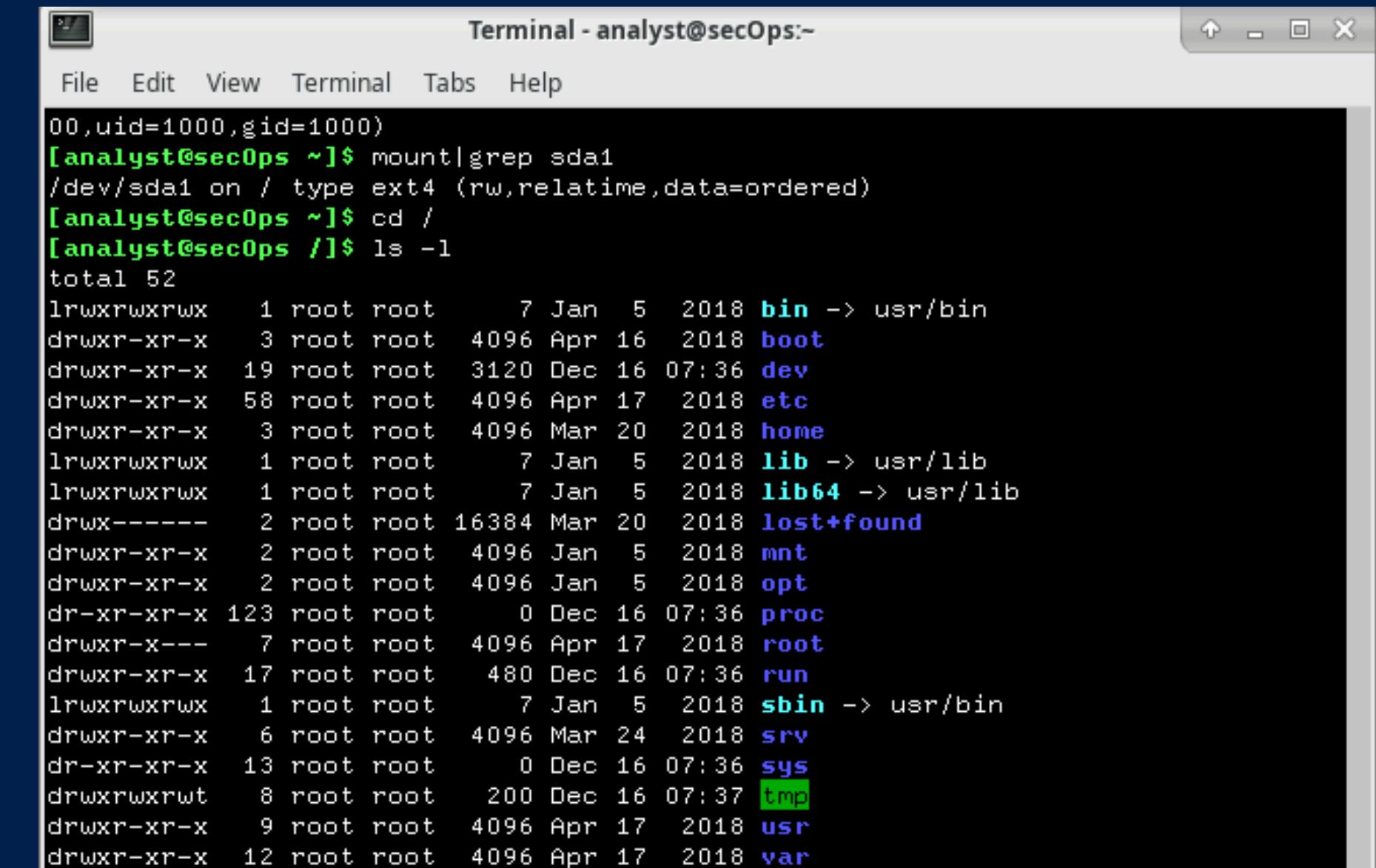
[analyst@secOps ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=500780k,nr_inodes=1
=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,no
ime)
```

ESPLORAZIONE DEL FILESYSTEM LINUX

Utilizziamo il comando

`mount | grep sda1` per filtrare l'output precedentemente ottenuto visualizzando unicamente il root filesystem.

Ci spostiamo nella directory root (con il comando `cd /`) e andiamo a visualizzare file e directory con i relativi permessi associati (con il comando `ls -l`).



```
[00,uid=1000,gid=1000)
[analyst@secOps ~]$ mount|grep sda1
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx  1 root root    7 Jan  5  2018 bin -> usr/bin
drwxr-xr-x  3 root root  4096 Apr 16  2018 boot
drwxr-xr-x 19 root root  3120 Dec 16 07:36 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 123 root root     0 Dec 16 07:36 proc
drwxr-x---  7 root root  4096 Apr 17  2018 root
drwxr-xr-x 17 root root   480 Dec 16 07:36 run
lrwxrwxrwx  1 root root    7 Jan  5  2018 sbin -> usr/bin
drwxr-xr-x  6 root root  4096 Mar 24  2018 srv
dr-xr-xr-x 13 root root     0 Dec 16 07:36 sys
drwxrwxrwt  8 root root  200 Dec 16 07:37 tmp
drwxr-xr-x  9 root root  4096 Apr 17  2018 usr
drwxr-xr-x 12 root root  4096 Apr 17  2018 var
```

ESPLORAZIONE DEL FILESYSTEM LINUX

Per tornare nella directory "analyst", utilizziamo il comando `cd`. Una volta nella directory corretta, eseguiamo il comando `ls -l` per elencare i contenuti e individuare la directory "second_drive". Dopo averla trovata, procediamo a montare il secondo disco (`sdb1`) all'interno della directory "second_drive" utilizzando il comando `sudo mount /dev/sdb1 ~/second_drive/`.

Successivamente, possiamo verificare i dischi montati eseguendo il comando `mount | grep /dev/sd`, che restituirà in output l'elenco dei dischi montati, evidenziando che in questo momento i dispositivi attivi sono due.

Per smontare il disco, utilizziamo il comando

`sudo umount /dev/sdb1`. Dopo aver smontato il disco, possiamo verificare che la directory "second_drive" sia vuota eseguendo il comando `ls -l second_drive/`, che restituirà un output pari a 0, confermando che la directory non contiene più alcun file o contenuto.

```
[analyst@secOps ~]$ cd
[analyst@secOps ~]$ mkdir second_drive
mkdir: cannot create directory 'second_drive': File exists
[analyst@secOps ~]$ ls -l
total 8616
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   8802879 Dec 13 07:11 httpdump.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
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwx----- 2 root   root   16384 Mar 26 2018 lost+found
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt
[analyst@secOps ~]$ mount | grep /dev/sd
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime,dat
[analyst@secOps ~]$ sudo umount /dev/sdb1
[sudo] password for analyst:
[analyst@secOps ~]$ ls -l second_drive/
total 0
```

PERMESSI DEI FILE

Con il comando `cd lab.support.files/scripts/` ci spostiamo nella directory specificata e visualizziamo i permessi dei file contenuti al suo interno utilizzando il comando `ls -l`.

Successivamente, proviamo a creare un file di testo vuoto all'interno della directory `/mnt` con il comando

`touch /mnt/myNewFile.txt`.

Tuttavia, l'operazione non sarà consentita, poiché solo l'utente root ha i permessi di scrittura nella directory `/mnt`. Questo può essere verificato tornando alla directory principale con il comando `cd` e controllando i permessi della directory `/mnt` tramite `ls -ld /mnt`.

Procediamo quindi rimontando il disco `sdb1` nella directory `second_drive`. Una volta fatto, visualizziamo i permessi del file `myFile.txt`. Per modificare tali permessi, utilizziamo il comando `sudo chmod 665 myFile.txt`.

```
[analyst@secOps ~]$ cd lab.support.files/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 3669 Mar 21 2018 cyberops_topo.py
-rw-r--r-- 1 analyst analyst 2871 Mar 21 2018 cyops.mn
-rwxr-xr-x 1 analyst analyst 458 Mar 21 2018 fw.rules
-rwxr-xr-x 1 analyst analyst 70 Mar 21 2018 mal_server_start.sh
drwxr-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_ELK.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_snort.sh
-rwxr-xr-x 1 analyst analyst 61 Mar 21 2018 start_tftpd.sh
[analyst@secOps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@secOps scripts]$ cd ..
bash: cd: too many arguments
[analyst@secOps scripts]$ cd
[analyst@secOps ~]$ ls -ld
drwx----- 14 analyst analyst 4096 Dec 16 07:37 .
[analyst@secOps ~]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan 5 2018 /mnt
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@secOps ~]$ cd ~/second_drive
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root root 16384 Mar 26 2018 lost+found
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt
[analyst@secOps second_drive]$ sudo chmod 665 myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root root 16384 Mar 26 2018 lost+found
-rw-rw-r-x 1 analyst analyst 183 Mar 26 2018 myFile.txt
```

PERMESSI DEI FILE

Il comando `sudo chown analyst:root myFile.txt` lo utilizziamo per cambiare proprietà e gruppo del file.

Ora che analyst è proprietario del file possiamo modificarlo aggiungendo la parola "test" alla fine di "myFile.txt" con il comando `echo test >> myFile.txt`.

```
analyst@secOps second_drive]$ sudo chown analyst:root myFile.txt
analyst@secOps second_drive]$ ls -l
total 20
rwx----- 2 root      root 16384 Mar 26  2018 lost+found
rw-rw-r-x  1 analyst    root   183 Mar 26  2018 myFile.txt
analyst@secOps second_drive]$ echo test >> myFile.txt
analyst@secOps second_drive]$ cat myFile.txt
his is a file stored in the /dev/sdb1 disk.
otice 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
est
```

PERMESSI DEI FILE

Rientrando nella directory `lab.support.files` ed elencando tutti i file con i dettagli, possiamo confrontare i permessi della directory malware con quelli del file `mininet_services`. Dal confronto, si nota che il primo carattere dei permessi di **malware** è una "d", che indica una directory, mentre per **mininet_services** è un "-", che specifica un file regolare.

```
[analyst@secOps second_drive]$ cd ~/lab.support.files/
[analyst@secOps lab.support.files]$ ls -l
total 580
drwxr-xr-x  4 analyst analyst    4096 Mar 21  2018 attack_scripts
-rw-r--r--  1 analyst analyst      649 Mar 21  2018 apache_in_epoch.log
-rw-r--r--  1 analyst analyst     126 Mar 21  2018 applicationX_in_epoch.log
-rw-r--r--  1 analyst analyst    4096 Mar 21  2018 confidential.txt
-rw-r--r--  1 analyst analyst     102 Mar 21  2018 cyops.mn
-rw-r--r--  1 analyst analyst      75 Mar 21  2018 elk_services
-rw-r--r--  1 analyst analyst     373 Mar 21  2018 h2_dropbear.banner
drwxr-xr-x  2 analyst analyst    4096 Apr  2  2018 instructor
-rw-r--r--  1 analyst analyst     255 Mar 21  2018 letter_to_grandma.txt
-rw-r--r--  1 analyst analyst  24464 Mar 21  2018 logstash-tutorial.log
drwxr-xr-x  2 analyst analyst    4096 Mar 21  2018 malware
-rw xr-xr-x  1 analyst analyst     172 Mar 21  2018 mininet_services
drwxr-xr-x  2 analyst analyst    4096 Mar 21  2018 openssl_lab
drwxr-xr-x  2 analyst analyst    4096 Mar 21  2018 pcaps
drwxr-xr-x  7 analyst analyst    4096 Mar 21  2018 pox
-rw-r--r--  1 analyst analyst 473363 Mar 21  2018 sample.img
-rw-r--r--  1 analyst analyst      65 Mar 21  2018 sample.img_SHA256.sig
drwxr-xr-x  3 analyst analyst    4096 Mar 21  2018 scripts
-rw-r--r--  1 analyst analyst   25553 Mar 21  2018 SQL_Lab.pcap
```

COLLEGAMENTI SIMBOLICI E FILE SPECIALI

Visualizzando i file della directory /dev possiamo notare che il primo carattere di ogni file rappresenta la natura dello stesso:

- c = file di dispositivo a caratteri
- b = file di blocco
- l = file di collegamento simbolico
- - = file regolari
- d = directory

```
[analyst@secOps lab.support.files]$ cd
[analyst@secOps ~]$ ls -l
total 8616
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     8802879 Dec 13 07:11 httpdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root   root     4096 Mar 26  2018 second-drive
[analyst@secOps ~]$ ls -l /dev/
total 0
crw-r--r-- 1 root   root      10, 236 Dec 16 07:36 autofs
                           140 Dec 16 07:36 block
                           100 Dec 16 07:36 bsg
                           10, 234 Dec 16 07:36 btrfs-control
                           60 Dec 16 07:36 bus
                           3 Dec 16 07:36 cdrom -> sr0
                           2800 Dec 16 07:36 char
                           5,  1 Dec 16 07:36 console
                           11 Dec 16 07:36 core -> /proc/kcore
                           10,  61 Dec 16 07:36 cpu-dma-latency
                           10,  203 Dec 16 07:36 cuse
                           120 Dec 16 07:36 disk
                           80 Dec 16 07:36 dri
                           29,  0 Dec 16 07:36 fb0
                           13 Dec 16 07:36 fd -> /proc/self/fd
                           1,   7 Dec 16 07:36 full
                           10,  229 Dec 16 07:36 fuse
                           245,  0 Dec 16 07:36 hidraw0
                           10,  228 Dec 16 07:36 hpet
                           0 Dec 16 07:36 hugepages
                           25 Dec 16 07:36 initctl -> /run/systemd/initctl/fifo
                           360 Dec 16 07:36 input
                           1,   11 Dec 16 07:36 kmsg
                           60 Dec 16 07:36 lightnvm
                           28 Dec 16 07:36 log -> /run/systemd/journal/dev-log
                           10,  237 Dec 16 07:36 loop-control
                           60 Dec 16 07:36 mapper
```

COLLEGAMENTI SIMBOLICI E FILE SPECIALI

Andiamo a creare due file, con il comando echo, inserendo al loro interno una parola:

- file1.txt conterrà la parola "simbolico"
- file2.txt conterrà la parola "difficile"

Questo ci servirà per creare un collegamento simbolico (con il comando ln -s) per file1.txt e un collegamento fisico (con il comando ln) per file2.txt.

```
[analyst@secOps ~]$ echo "simbolico" >file1.txt
[analyst@secOps ~]$ cat file1.txt
simbolico
[analyst@secOps ~]$ echo "difficile" > file2.txt
[analyst@secOps ~]$ cat file2.txt
difficile
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
```

COLLEGAMENTI SIMBOLICI E FILE SPECIALI

Esaminando l'elenco della directory, abbiamo osservato che file1symbolic è un collegamento simbolico che punta a file1.txt, mentre file2hard è un file normale, in quanto non punta a file2.txt ma condivide lo stesso inode sul disco rigido.

Successivamente, abbiamo rinominato i file utilizzando il comando mv, cambiando file1.txt in file1nuovo.txt e file2.txt in file2new.txt.

Aprendo i file con il comando cat, abbiamo notato che il collegamento simbolico file1symbolic non funziona più, mostrando un messaggio di errore relativo all'assenza del file o della directory, poiché il file a cui puntava è stato rinominato. Al contrario, apendo file2hard, il contenuto è rimasto accessibile e mostra la parola "difficile", presente nel file ora chiamato file2new.txt. Questo accade perché i collegamenti hard si riferiscono direttamente all'inode e non al nome del file.

```
[analyst@secOps ~]$ ls -l
total 8628
drwxr-xr-x 2 analyst analyst      4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst      4096 Mar 22  2018 Downloads
lrwxrwxrwx 1 analyst analyst      9 Dec 16 08:40 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst     10 Dec 16 08:37 file1.txt
-rw-r--r-- 2 analyst analyst     10 Dec 16 08:38 file2hard
-rw-r--r-- 2 analyst analyst     10 Dec 16 08:38 file2.txt
-rw-r--r-- 1 root   root    8802879 Dec 13 07:11 httpdump.pcap
drwxr-xr-x 9 analyst analyst      4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root   root      4096 Mar 26  2018 second_drive

[analyst@secOps ~]$ mv file1.txt file1nuovo.txt
[analyst@secOps ~]$ mv file2.txt file2new.txt
[analyst@secOps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@secOps ~]$ cat file2hard
difficile
[analyst@secOps ~]$
```



Malware
Analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

FILE PCAP

Introduzione:

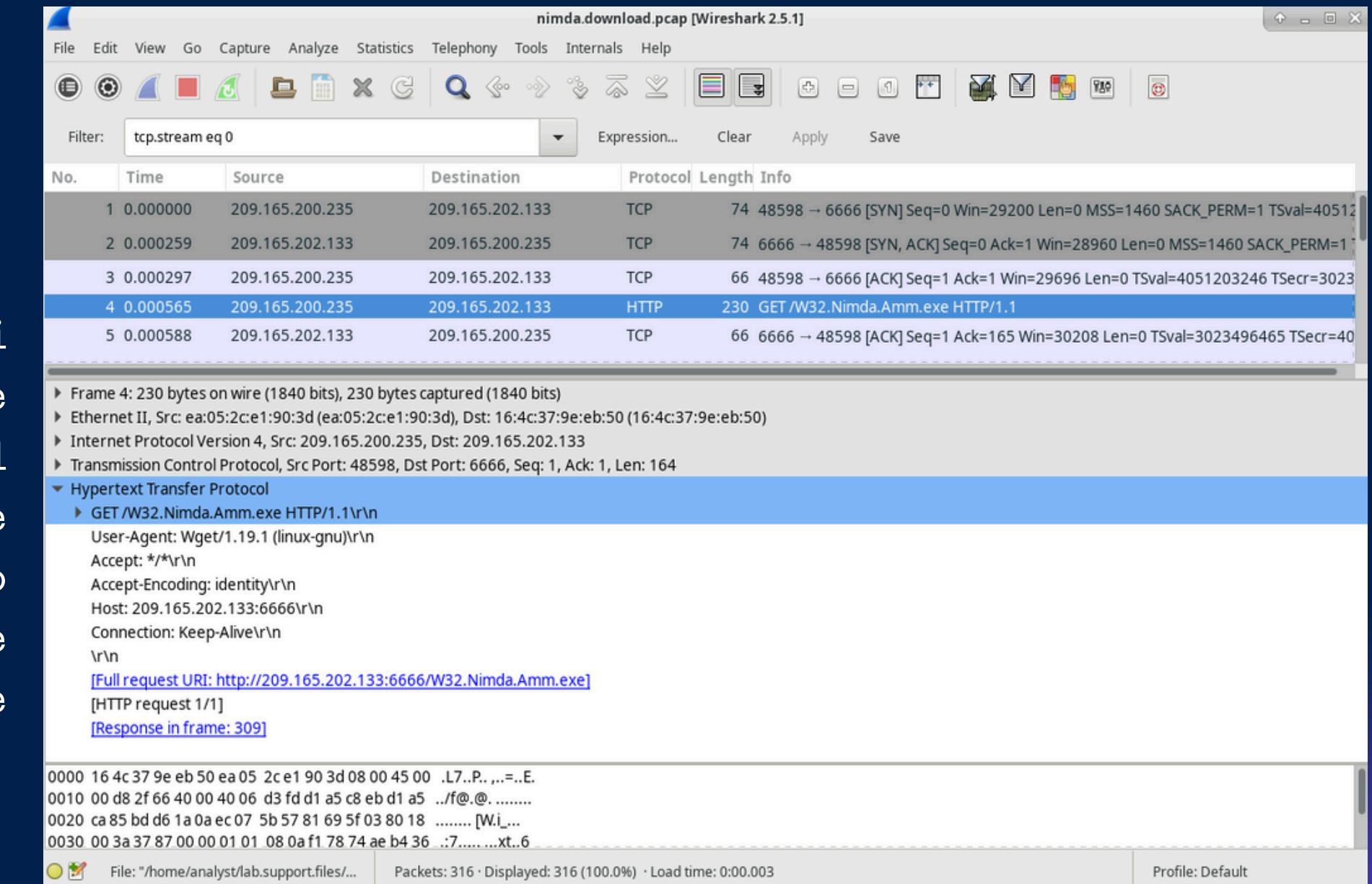
Analisi e Estrazione di un Eseguibile da un File PCAP

L'esercizio in oggetto si concentra sull'analisi di pacchetti di rete catturati in un file PCAP e sull'estrazione di un eseguibile scaricato durante una sessione HTTP. L'obiettivo principale è approfondire la comprensione delle transazioni di rete a livello di pacchetto e acquisire competenze nell'utilizzo di strumenti come Wireshark per analizzare e manipolare catture di rete. L'analisi dei log e delle catture di rete è fondamentale per identificare attività sospette e comprendere le dinamiche delle transazioni. Il laboratorio prevede l'analisi di un file PCAP contenente i dati relativi al download di un malware, chiamato Nimda.Amm.exe, e l'estrazione del file per successive attività di analisi. Il laboratorio utilizza file già acquisiti e archiviati nella directory della macchina virtuale CyberOps Workstation.



ANALISI DEI PACCHETTI CATTURATI

Dopo essersi spostati nella directory contenente i file PCAP, è stato avviato Wireshark per analizzare il file nimda.download.pcap. L'analisi è partita dal quarto pacchetto della cattura, identificato come una richiesta HTTP GET inviata dall'indirizzo 209.165.200.235 verso 209.165.202.133. Tale pacchetto contiene la richiesta per il file Nimda.Amm.exe.





Malware Analysis

Any.ru

Filesystem Linux

File PCAP

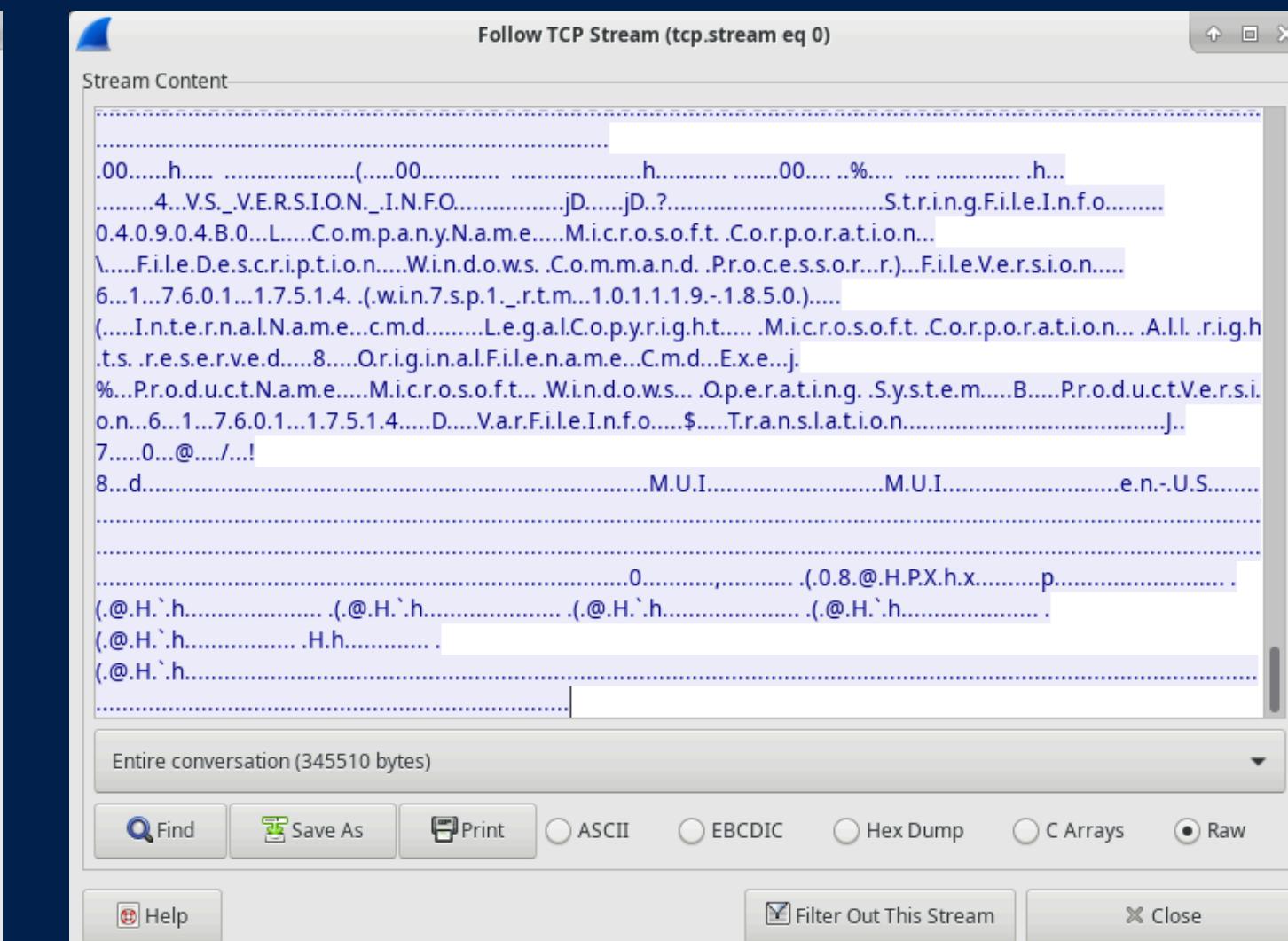
BONUS 1

BONUS 2

BONUS 3

ANALISI DEI PACCHETTI CATTURATI

È stato quindi utilizzato il comando "Follow TCP Stream" per ricostruire la transazione TCP completa. Il contenuto del file è apparso sotto forma di simboli, rappresentazione del codice binario che Wireshark non può decodificare direttamente. Tuttavia, alcune stringhe leggibili presenti tra i simboli hanno rivelato dettagli sul file eseguibile, suggerendo che si trattasse di cmd.exe di Windows.



Malware
Analysis

Any.run

Filesystem
Linux

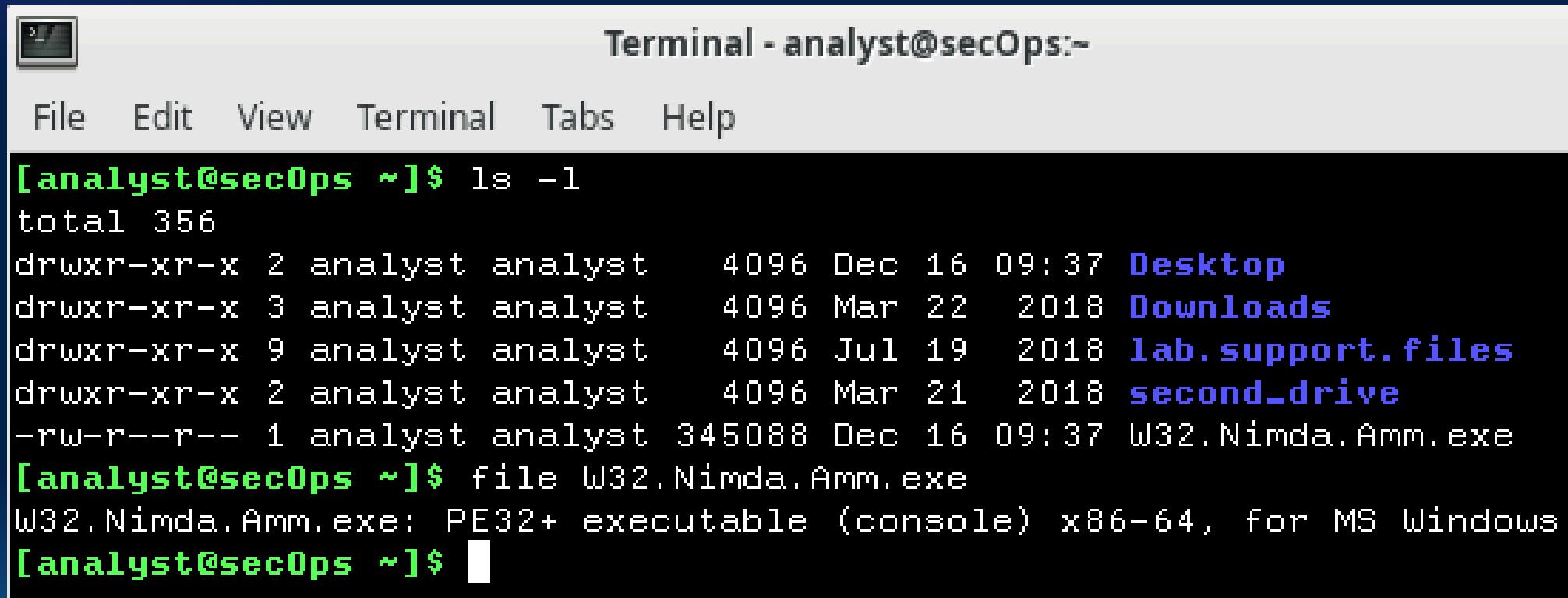
File PCAP

BONUS 1

BONUS 2

BONUS 3

ESTRAZIONE DEL FILE ESEGUIBILE



A terminal window titled "Terminal - analyst@secOps:~". The window shows a Linux command-line interface with the following output:

```
[analyst@secOps ~]$ ls -l
total 356
drwxr-xr-x 2 analyst analyst 4096 Dec 16 09:37 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Dec 16 09:37 W32.Nimda.Amm.exe
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

Successivamente, è stato utilizzato il menu "Esporta oggetti" di Wireshark per recuperare il file Nimda.Amm.exe dalla cattura. Il file è stato salvato nella directory "/home/analyst" della macchina virtuale e la sua presenza è stata verificata tramite il comando ls -l. Infine, il comando file ha confermato che si trattava di un eseguibile PE32+ per sistemi Windows.

Malware Analysis

Any.run

Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

VIRUSTOTAL

The screenshot shows the VirusTotal analysis interface for a file named Nimda.Amm.exe. The file is identified as a Cmd.Exe (337.00 KB) from Computernewb.com, last analyzed a moment ago. The analysis results show 0 detections out of 72, with a community score of 413. The file is categorized as EXE and has various tags: peexe, known-distributor, direct-cpu-clock-access, idle, 64bits, detect-debug-environment, legit, long-sleeps, attachment, assembly, runtime-modules, and via-tor. Below the main analysis, there is a section for security vendors' analysis, which shows results for Acronis (Static ML), AhnLab-V3, Alibaba, and AliCloud, all of which are undetected. A call-to-action button at the bottom encourages users to join the 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?
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
AliCloud	Undetected

Il laboratorio ha dimostrato come un file PCAP possa essere utilizzato per ricostruire e analizzare transazioni di rete, evidenziando l'importanza di strumenti come Wireshark per la sicurezza informatica. Dopo l'estrazione, il file Nimda.Amm.exe è stato identificato come un eseguibile di Windows.

Il passo successivo nell'analisi del malware consisterebbe nell'esecuzione controllata del file in un ambiente sandbox. Tale ambiente, basato su macchine virtuali, permette di monitorare il comportamento del malware senza rischiare danni a sistemi reali. Strumenti come VirusTotal possono essere utilizzati per un'analisi preliminare, mentre strumenti avanzati possono fornire dettagli approfonditi sul comportamento del malware, incluse le modifiche apportate al sistema operativo, le connessioni di rete e l'utilizzo delle risorse.

CONCLUSIONE E ANALISI EXTRA

File W32.Nimda.Amm.exe

Summary	
Size	337.0KB
Type	PE32+ executable (console) x86-64, for MS Windows
MD5	5746bd7e255dd6a8afa06f7c42c1ba41
SHA1	0f3c4ff28f354aede202d54e9d1c5529a3bf87d8
SHA256	db06c3534964e3fc79d2763144ba53742d7fa250ca336f4a0fe724b75aaff386
SHA512	Show SHA512
CRC32	D51795E3
ssdeep	None
PDB Path	cmd.pdb
Yara	<ul style="list-style-type: none">• DebuggerCheck_QueryInfo - (no description)• DebuggerException_SetConsoleCtrl - (no description)• anti_dbg - Checks if being debugged• disable_dep - Bypass DEP• win_registry - Affect system registries• win_token - Affect system token• win_files_operation - Affect private profile

Dopo aver estratto il file, il passo successivo per un analista di sicurezza è stato trasferire il malware in un ambiente controllato per una più approfondita analisi comportamentale. In questo caso, è stato suggerito l'utilizzo di strumenti come Cuckoo Sandbox, una piattaforma automatizzata di analisi malware.

L'analisi con Cuckoo Sandbox ha permesso di:

Osservare l'esecuzione del malware in un ambiente virtualizzato, isolato dal sistema reale per evitare danni.

Monitorare le connessioni di rete stabilite dal malware, i processi avviati e le modifiche al file system.

Generare un report dettagliato contenente informazioni sui comportamenti sospetti rilevati, come l'apertura di porte di rete o l'iniezione di codice in altri processi.

Questa analisi ha confermato che il file estratto, pur non essendo il worm Nimda originale, presentava un comportamento malevolo compatibile con un dropper utilizzato per scaricare ulteriori payload. Strumenti come VirusTotal possono fornire un'analisi complementare, confrontando il file con database di minacce noti.

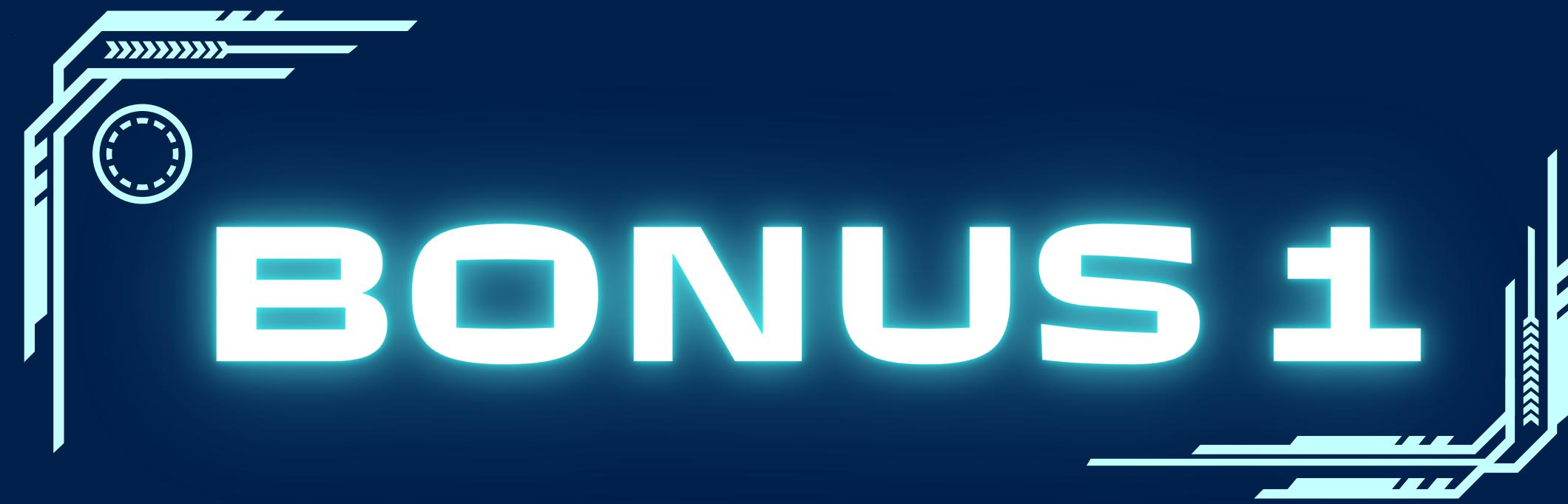
CONCLUSIONI

Durante questo laboratorio, sono stati esaminati i pacchetti di rete catturati nel file PCAP "nimda.download.pcap" per comprendere le transazioni di rete e individuare un file eseguibile. L'analisi ha rivelato che il file W32.Nimda.Amm.exe è stato scaricato tramite una richiesta HTTP GET e poi estratto utilizzando Wireshark. Successivamente, il file è stato analizzato con la sandbox Cuckoo per valutarne il comportamento e i potenziali impatti. L'utilizzo di un ambiente controllato ha permesso di evitare danni al sistema reale e di raccogliere informazioni dettagliate sulle attività del malware.

RACCOMANDAZIONI

Si consiglia di:

- Implementare sempre un ambiente di analisi isolato e sicuro, come una sandbox, per valutare il comportamento dei file sospetti.
- Utilizzare strumenti online, come VirusTotal, per confrontare i risultati ottenuti e verificare ulteriori indicatori di compromesso.
- Monitorare regolarmente le catture di rete per identificare tempestivamente attività anomale o sospette.
- Rafforzare le difese di rete implementando strumenti di rilevamento delle intrusioni (IDS) e firewall configurati adeguatamente.
- Fornire una formazione continua agli analisti per migliorare la capacità di riconoscere e rispondere alle minacce emergenti.



BONUS +1

The word "BONUS" is written in a large, white, sans-serif font with a bright blue glow around its edges. It is flanked by two vertical, light blue rectangular panels with a futuristic design. The left panel features a circular sensor-like element with a dashed line pattern. The right panel has a series of vertical arrows pointing upwards. The background is a dark blue gradient.

Malware analysis

Any.run

Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

BONUS 1

Nel laboratorio abbiamo analizzato il file eseguibile `Jvczfhe.exe` utilizzando la piattaforma AnyRun, identificando diversi Indicatori di Compromissione (IOC) associati a processi sospetti:

- `Jvczfhe.exe` (PID: 7492): Identificato come il file principale malevolo responsabile dell'infezione.
- `Muadnd.exe` (PID: 7824): Probabile copia o variante dello stesso malware.
- `WerFault.exe`: Utilizzato per alterare le impostazioni di sistema, probabilmente con intenti malevoli.

L'analisi ha evidenziato il comportamento anomalo di questi processi, suggerendo un'attività malevola.

ANYRUN
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information

General Info

URL:	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
Full analysis:	https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be inaccurate or incomplete. ANY.RUN does not guarantee maliciousness or safety of the content.

BONUS 1

Quello che abbiamo osservato è che il seguente file è stato identificato come malware e mostra diversi comportamenti sospetti e pericolosi:

- Raccolta di informazioni: Il malware legge dettagli sul sistema e controlla impostazioni di sicurezza
- Persistenza e nascondiglio: Il malware garantisce persistenza creando file nella directory dell'utente e sfrutta programmi legittimi come InstallUtil.exe per mascherarsi. Utilizza cmd.exe e timeout.exe per ritardare l'esecuzione, eludendo i sistemi di rilevamento.
- Modifiche al sistema: Cambia impostazioni di rete e sicurezza, disabilita i registri di traccia ed elimina file legittimi di windows
- Comunica con i server: sfrutta porte insolite per la connessione.

MALICIOUS

No malicious indicators.

SUSPICIOUS

- Reads security settings of Internet Explorer
 - Jvczfhe.exe (PID: 7492)
 - Muadnrd.exe (PID: 7824)
- Executes application which crashes
 - Jvczfhe.exe (PID: 7492)
 - Muadnrd.exe (PID: 7824)
- Uses TIMEOUT.EXE to delay execution
 - cmd.exe (PID: 7520)
 - cmd.exe (PID: 7876)
- Process drops legitimate windows executable
 - firefox.exe (PID: 6596)
- Checks Windows Trust Settings
 - Jvczfhe.exe (PID: 7492)
 - Muadnrd.exe (PID: 7824)
- Starts CMD.EXE for commands execution
 - Jvczfhe.exe (PID: 7492)
 - Muadnrd.exe (PID: 7824)
- Connects to unusual port
 - InstallUtil.exe (PID: 5152)
- Application launched itself
 - Muadnrd.exe (PID: 7824)

CONCLUSIONI

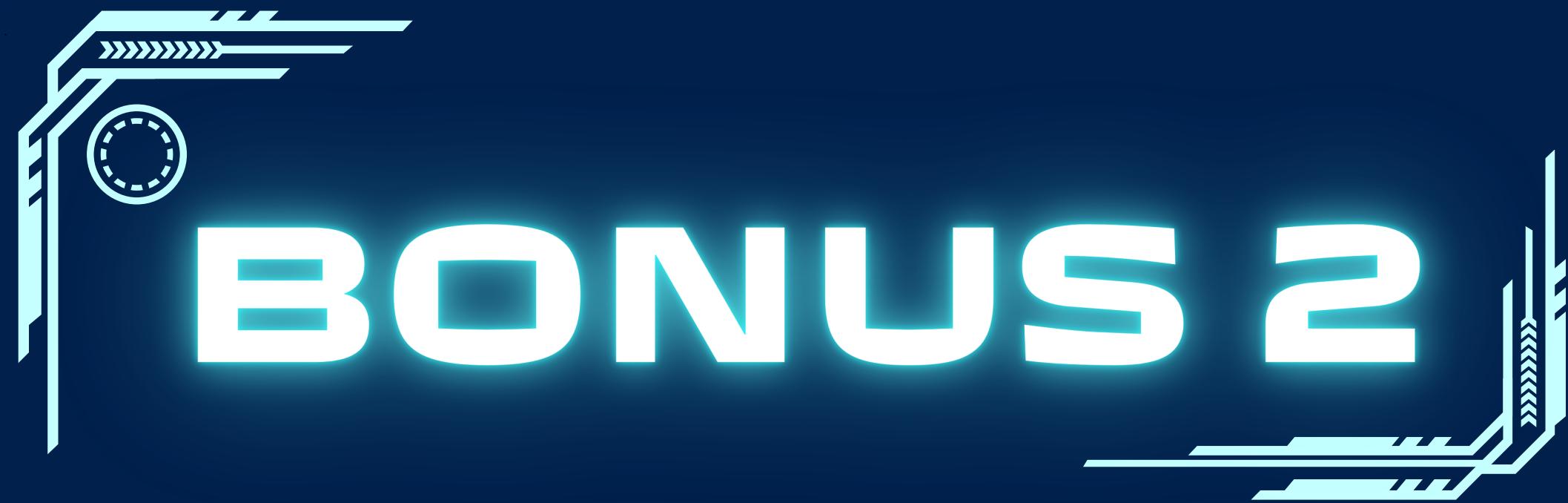
Da questa analisi siamo arrivati alla conclusione che questo malware è progettato per:

- Raccogliere informazioni personali e dati sensibili.
- Modificare il sistema operativo per garantire la sua presenza e nascondersi.
- Comunicare con server remoti per inviare dati rubati o ricevere comandi.

RACCOMANDAZIONI

In base all'analisi svolta consigliamo le seguenti operazioni:

- Isolare il sistema: Disconnettere immediatamente il computer dalla rete.
- Rimuovere il malware: Usare un antivirus avanzato o strumenti di rimozione specifici.
- Analisi approfondita: Controllare i log di rete e i file modificati per valutare eventuali compromissioni aggiuntive.
- Prevenzione futura: Aggiornare regolarmente software e sistemi operativi ed evitare di scaricare file da fonti non affidabili.
- Formazione: Fornire un'adeguata formazione al personale riguardo potenziali minacce.



BONUS 2

The logo features the words "BONUS 2" in a bold, white, sans-serif font. The letters are outlined in a bright blue color. The logo is set against a dark background and is framed by two vertical, glowing blue circuit board-like structures. On the left side, there is a circular component with a dashed border and internal lines, resembling a sensor or a small screen. On the right side, there are several parallel lines of varying lengths, creating a sense of depth or signal transmission.

Malware
Analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

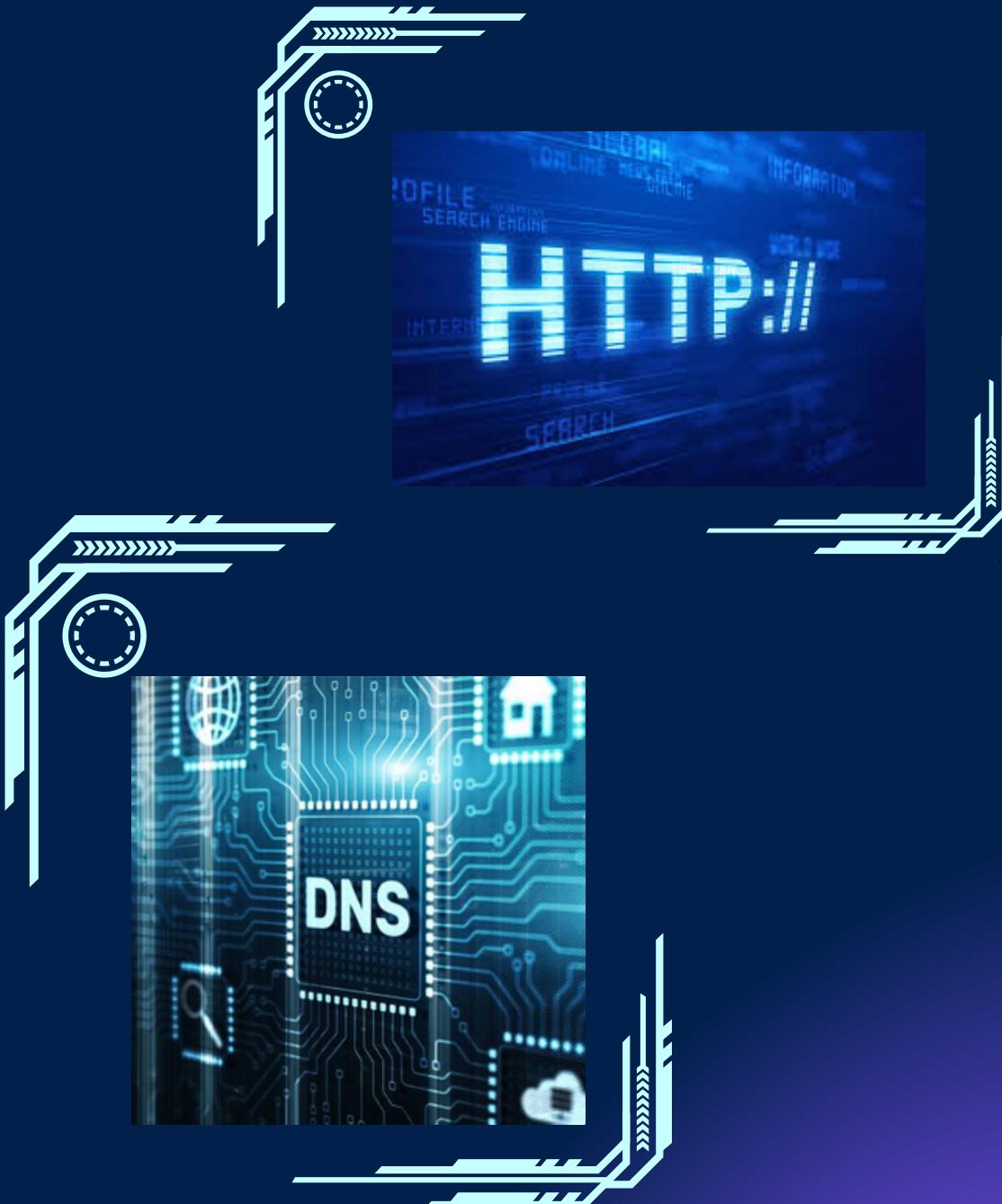
BONUS 2

BONUS 3

ANALISI DEI DATI HTTP E DNS PER IDENTIFICARE UN ATTORE DI MINACCIA

Introduzione: Il MySQL è un sistema di gestione di database relazionali ampiamente utilizzato nelle applicazioni web. Tra le tecniche più comuni di attacco a queste applicazioni, l'iniezione SQL è una delle più diffuse. Questa tecnica consente agli aggressori di eseguire comandi SQL dannosi, prendendo il controllo del server di database. Allo stesso tempo, i server DNS, responsabili della traduzione dei nomi di dominio in indirizzi IP, possono essere sfruttati per l'esfiltrazione di dati sensibili.

In questo laboratorio, verrà utilizzato Kibana per esaminare due scenari distinti di attacco: l'iniezione SQL e l'esfiltrazione dei dati tramite DNS. L'obiettivo è determinare se i dati sensibili, tra cui informazioni personali (PII), sono stati esposti durante gli attacchi.



The terminal window title is "analyst@SecOnion (10.0.2.15) - byobu". The window contains the following text:

```
Welcome to the light, powerful, text window manager, Byobu.  
You can toggle the launch of Byobu at login with:  
'byobu-disable' and 'byobu-enable'  
For tips, tricks, and more information, see:  
* http://bit.ly/byobu-help  
analyst@SecOnion:~} sudo so-status  
[sudo] password for analyst:  
Status: securityonion  
* sguil server  
Status: seconion-import  
* pcap_agent (sguil)  
* snort_agent-1 (sguil)  
* barnyard2-1 (spooler, unified2 format)  
Status: Elastic stack  
* so-elasticsearch  
* so-logstash  
* so-kibana  
* so-freqserver  
analyst@SecOnion:~}
```

At the bottom of the terminal window, there is a system status bar with the following information:

u_{EG} 16.04 0:- * 9m 2.18 2.8GHz 3.9G55% 2024-12-16 13:20:38

CONTROLLO DELLO STATO DEI SERVIZI E PREPARAZIONE DELL'AMBIENTE

Dopo aver verificato lo stato dei servizi con "sudo so-status", comando che permette di controllare se i servizi fondamentali per l'analisi, come quelli di raccolta e gestione dei log, sono attivi. Se un servizio fosse inattivo, potrebbe compromettere la capacità di raccogliere, analizzare e correlare dati, ostacolando l'indagine e lasciando potenziali minacce non rilevate. Questo controllo iniziale permette quindi di assicurare che l'ambiente sia pronto per un'analisi efficace e completa. La ricerca è stata poi impostata su Kibana per visualizzare i dati relativi al mese di giugno 2020.

Malware
Analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

IMPOSTAZIONE DEL PERIODO DI TEMPO PER L'ANALISI

Kibana, di default, visualizza solo i dati relativi alle ultime 24 ore. Tuttavia, per analizzare l'attacco SQL Injection che ha avuto luogo a giugno 2020, è stato necessario modificare l'intervallo temporale. Questo è un passaggio cruciale, poiché la corretta impostazione del periodo di tempo consente di visualizzare solo i log pertinenti all'incidente, evitando distrazioni da dati non rilevanti. Kibana ha quindi caricato i log specifici di giugno 2020, dove l'attacco è stato eseguito.

The screenshot shows the Kibana interface with the sidebar menu open. The 'Dashboard' option is selected. The main area displays the 'Time Range' configuration. The 'From' field is set to '2020-06-01 00:00:00.000' and the 'To' field is set to '2020-06-30 23:59:59.999'. Below the time range, a calendar for June 2020 is shown, with the dates from 01 to 30 visible. A 'Go' button is located at the bottom right of the time range section. The top navigation bar includes links for 'Dashboard', 'Overview', 'Full screen', 'Share', 'Clone', 'Edit', 'Documentation', and an 'Auto-refresh' button. The status bar at the bottom shows the URL 'http://127.0.0.1:5601/app/kibana#/discover?_t=1593311831111'.

Malware Analysis

Any.run

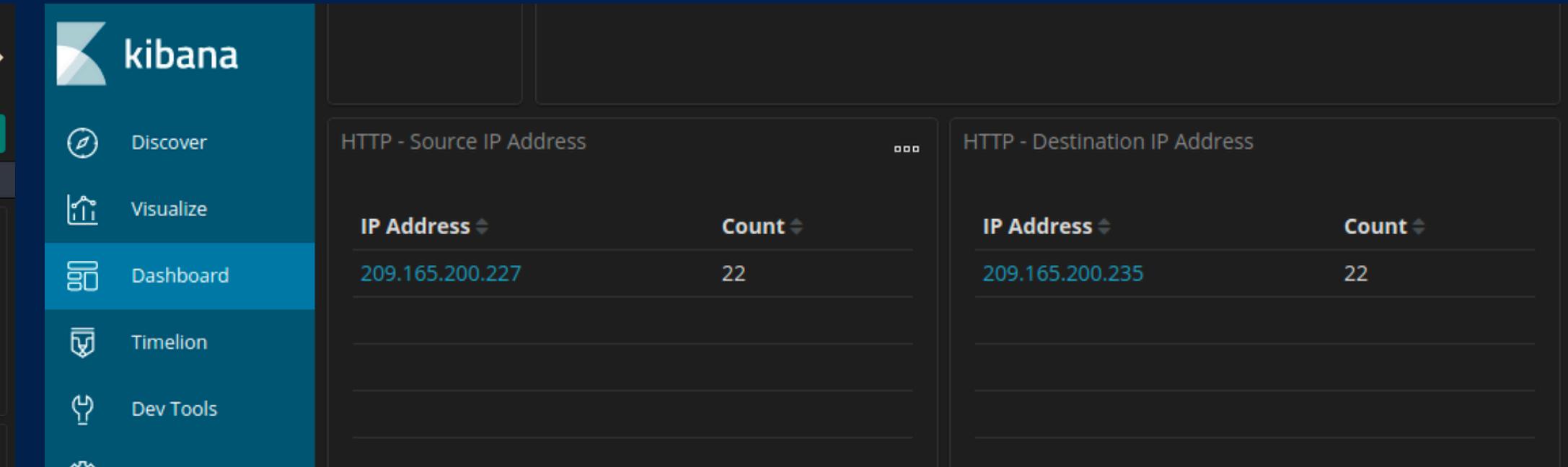
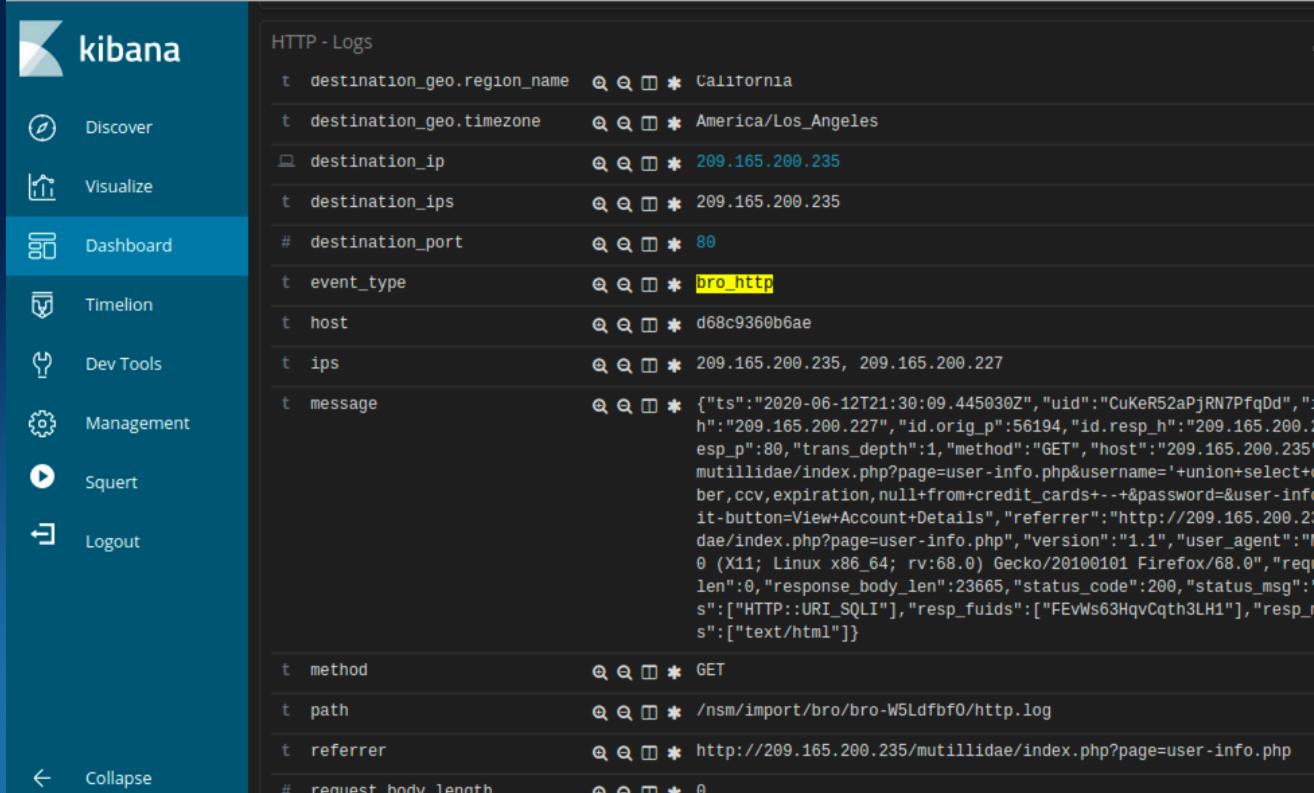
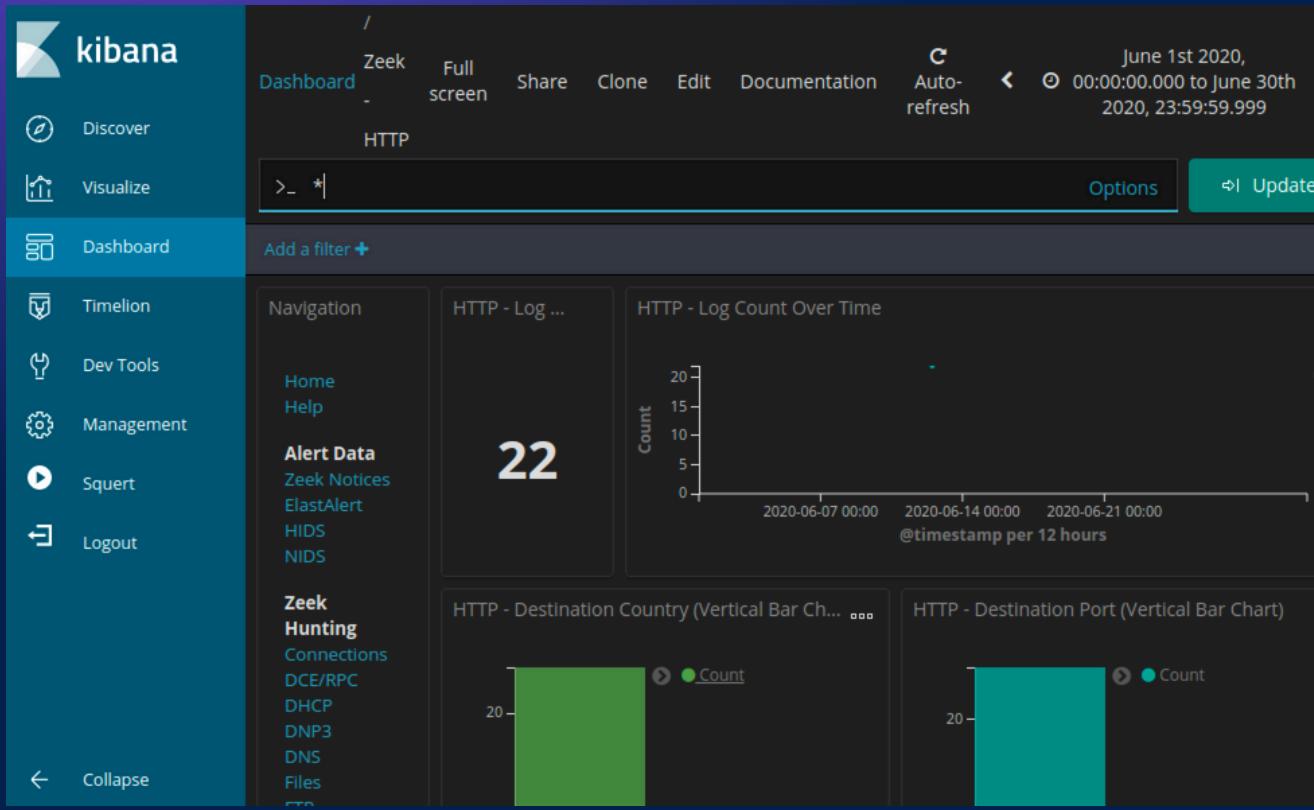
Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3



FILTRAGGIO E ANALISI DEI LOG HTTP

L'analisi dei log HTTP ha rivelato che un attore della minaccia aveva inviato richieste sospette dal client IP 209.165.200.227 verso il server IP 209.165.200.235 sulla porta 80. L'espansione dei dettagli dei log ha mostrato che il 12 giugno 2020, alle 21:30:09, un evento "bro_http" aveva registrato una richiesta HTTP GET contenente informazioni personali sensibili, come nomi utente, numeri di carta di credito, codici CCV e date di scadenza.

RISULTATI

Alcune delle informazioni nei log erano collegate tramite collegamenti ipertestuali ad altri strumenti. Facendo clic sul valore nel campo "alert_id", è stata visualizzata una pagina browser di CapME!, un'interfaccia web che consente di esaminare trascrizioni pcap. Il testo blu rappresentava le richieste HTTP inviate dalla sorgente (SRC), mentre il testo rosso indicava le risposte dal server Web di destinazione (DST). Nella sezione iniziale del registro, è stata individuata la stringa "username='+union+select+ccid,ccnumber,ccv,expiration,n ull+from+credit_cards+-+&password=". Questa stringa ha indicato un tentativo di attacco di iniezione SQL per aggirare l'autenticazione, utilizzando comandi SQL come "union" e "select" per accedere ai dati nel database. Una ricerca mirata nel registro ha rivelato un elenco di nomi utente e password, indicando che informazioni sensibili erano state effettivamente esposte.

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: ->209.165.200.235:80 (link: ethernet/modem)
SRC: GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+-+&password=&use r-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/mutillidae/index.php?page=user-info.php
SRC: Connection: keep-alive
SRC: Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb
SRC: Upgrade-Insecure-Requests: 1
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 12 Jun 2020 14:30:09 GMT
DST: Server: Apache/2.2.8 (Ubuntu) DAV/2
DST: X-Powered-By: PHP/5.2.4-2ubuntu5.10
DST: Expires: Thu, 19 Nov 1981 08:52:00 GMT
DST: Logged-In-User:
DST: Cache-Control: public

DST:
DST:
DST: 3a
DST: <p class="report-header">Results for . 5 records found.</p>
DST:
DST: 24
DST: Username=4444111122223333

DST:
DST: 17
DST: Password=745

DST:
DST: 22
DST: Signature=2012-03-01
<p>
DST:
DST: 24
DST: Username=7746536337776330

DST:
DST: 17
DST: Password=722

DST:
DST: 22
DST: Signature=2015-04-01
<p>
DST:
DST: 24
DST: Username=8242325748474749

DST:
DST: 17

username
3/10 | ^ v x

Malware
Analysis

Any.run

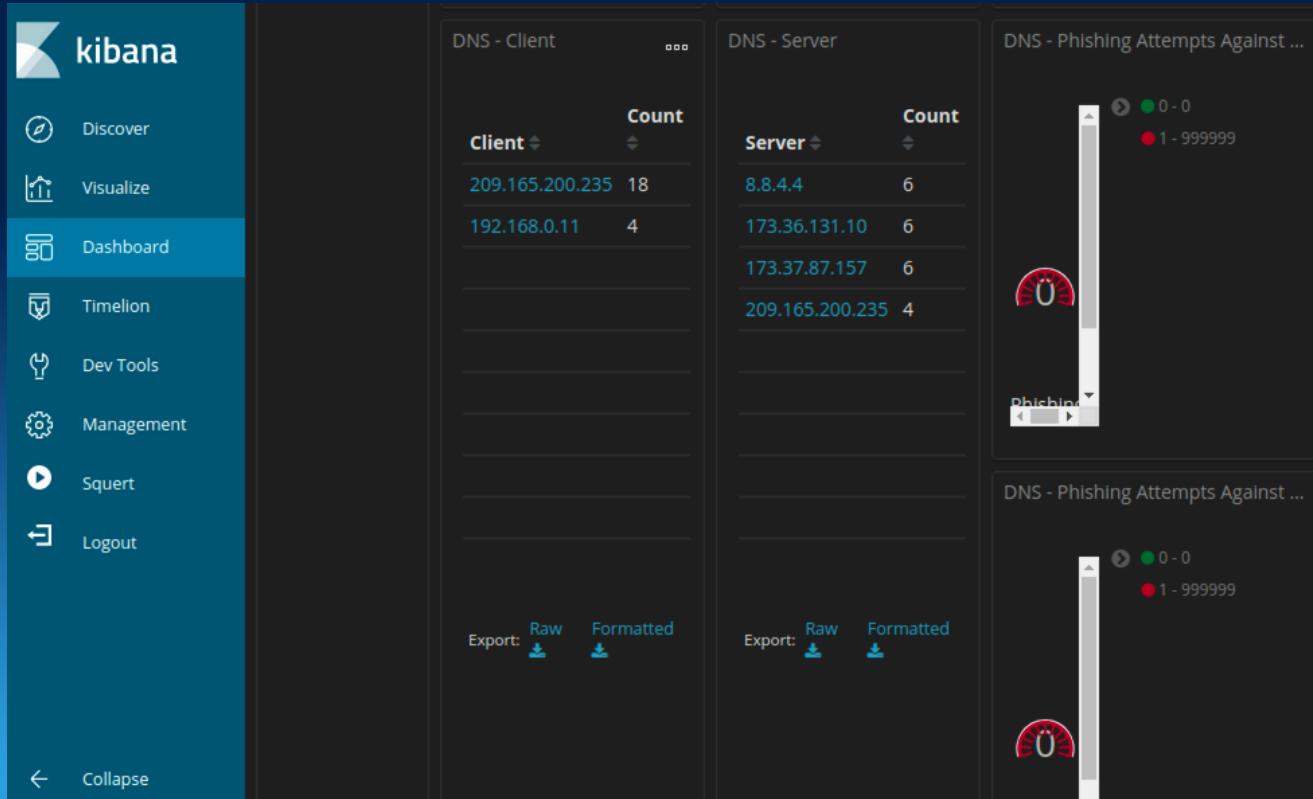
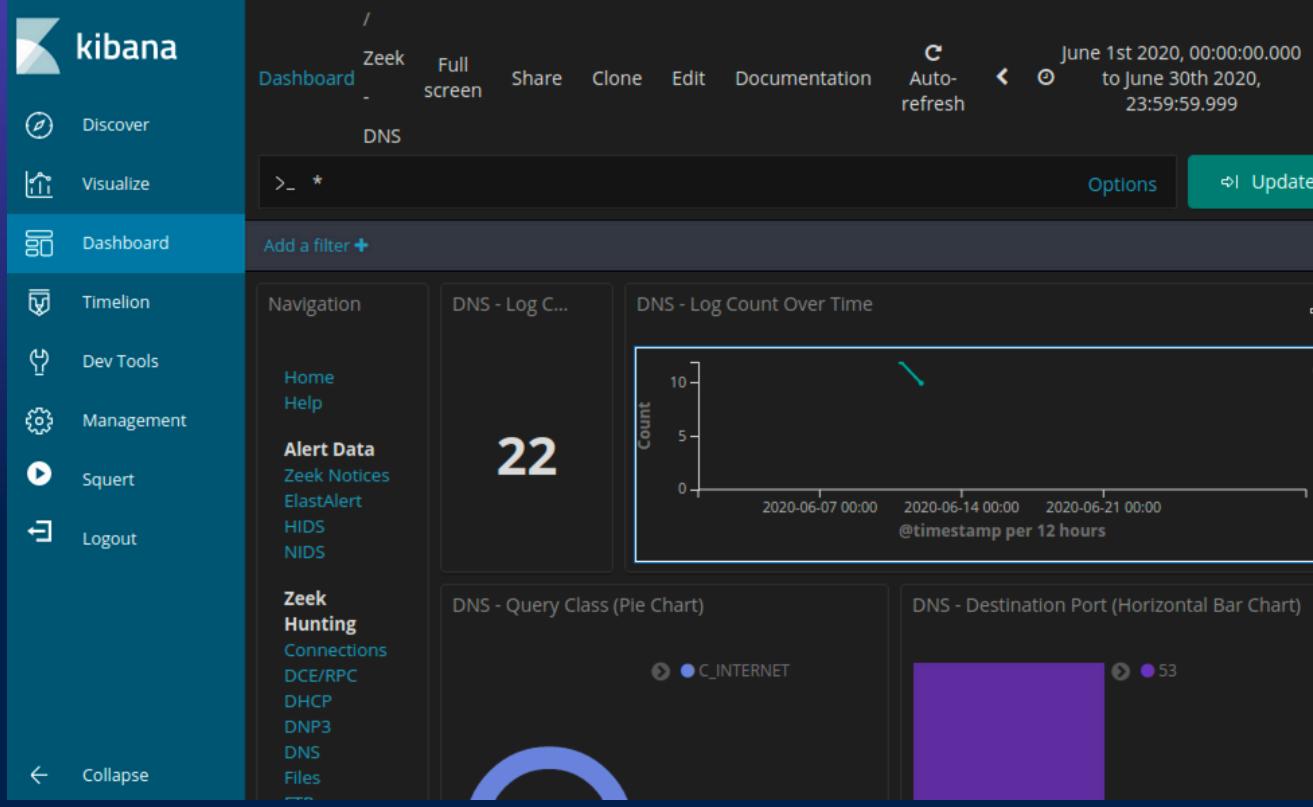
Filesystem
Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3



FILTRAGGIO TRAFFICO DNS

Filtrando i log DNS su Kibana nella sezione "Zeek Hunting", sono state visualizzate le metriche del conteggio dei registri DNS e un grafico a barre orizzontali che mostrava la distribuzione delle porte di destinazione. Scorrendo verso il basso, sono stati individuati diversi tipi di record DNS, tra cui record A (indirizzi IPv4), record AAAA (indirizzi IPv6), record NetBIOS (NB) e record PTR per la risoluzione degli hostname. Sono stati anche identificati codici di risposta DNS, insieme alle principali coppie di client e server DNS. È presente anche una metrica per il numero di tentativi di attacchi di phishing DNS, indicati come DNS pharming, spoofing o poisoning.

Malware Analysis

Any.run

Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

The screenshot shows the Kibana interface with the 'Discover' tab selected. On the left sidebar, there are links for 'Discover', 'Visualize', 'Dashboard', 'Timelion', and 'Dev Tools'. The main area displays a list of DNS queries under the heading 'DNS - Queries'. Some of the visible queries include: 17.201.165.209.in-addr.arpa, 434f4e464944454e5449414c20444f43554d454e540a444f, 484152450a5468697320646f63756d656e7420636f6e7461, 666f726d6174696f6e2061626f757420746865206c617374, and 697479206272656163682e0a.ns.example.com.

The screenshot shows the Kibana interface with the 'Discover' tab selected. On the left sidebar, there are links for 'Discover', 'Visualize', 'Dashboard', 'Timelion', 'Dev Tools', 'Management', 'Squert', and 'Logout'. The main area displays a visualization titled 'DNS - Log Count Over Time' showing the count of DNS logs over time from June 1st, 2020, to June 30th, 2020. A large number '4' is displayed above the chart, which has a y-axis labeled 'Count' ranging from 0 to 4 and an x-axis showing dates from 2020-06-07 to 2020-06-21.

VOCI RELATIVE AL DNS

Proseguendo l'analisi, un elenco delle query DNS ha rivelato sottodomini insolitamente lunghi associati a "ns.example.com", suggerendo possibili tentativi di esfiltrazione di dati. Filtrando i log per "example.com", il numero di voci è diminuito, indicando che la visualizzazione era ora limitata alle richieste al server specifico. È stato possibile individuare il client DNS con l'indirizzo IP 192.168.0.11 e il server DNS con l'indirizzo IP 209.165.200.235, evidenziando una possibile comunicazione sospetta. Questi dettagli hanno fornito indizi cruciali per comprendere l'estensione dell'attacco e la metodologia utilizzata dagli attori delle minacce.

The screenshot shows the Kibana interface with the 'Discover' tab selected. On the left sidebar, there are links for 'Discover', 'Visualize', 'Dashboard', 'Timelion', 'Dev Tools', 'Management', 'Squert', and 'Logout'. The main area displays two visualizations: 'DNS - Client' and 'DNS - Server'. The 'DNS - Client' visualization shows a table with one entry: Client 192.168.0.11 and Count 4. The 'DNS - Server' visualization shows a table with one entry: Server 209.165.200.235 and Count 4. Both tables have 'Client' and 'Count' as columns. At the bottom, there are 'Export' buttons for 'Raw' and 'Formatted' data.

The screenshot shows a Kibana interface with two panels: 'DNS - Queries' and 'DNS - Answers'. The 'DNS - Queries' panel lists several DNS query strings, including:

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

Below the Kibana interface is a terminal window titled 'analyst@SecOnion (10.0.2.15) - byobu'. The terminal shows the command 'xxd -r -p "/home/analyst/Downloads/DNS - Queries.csv" > secret.txt' being run, followed by the contents of 'secret.txt':

```
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
```

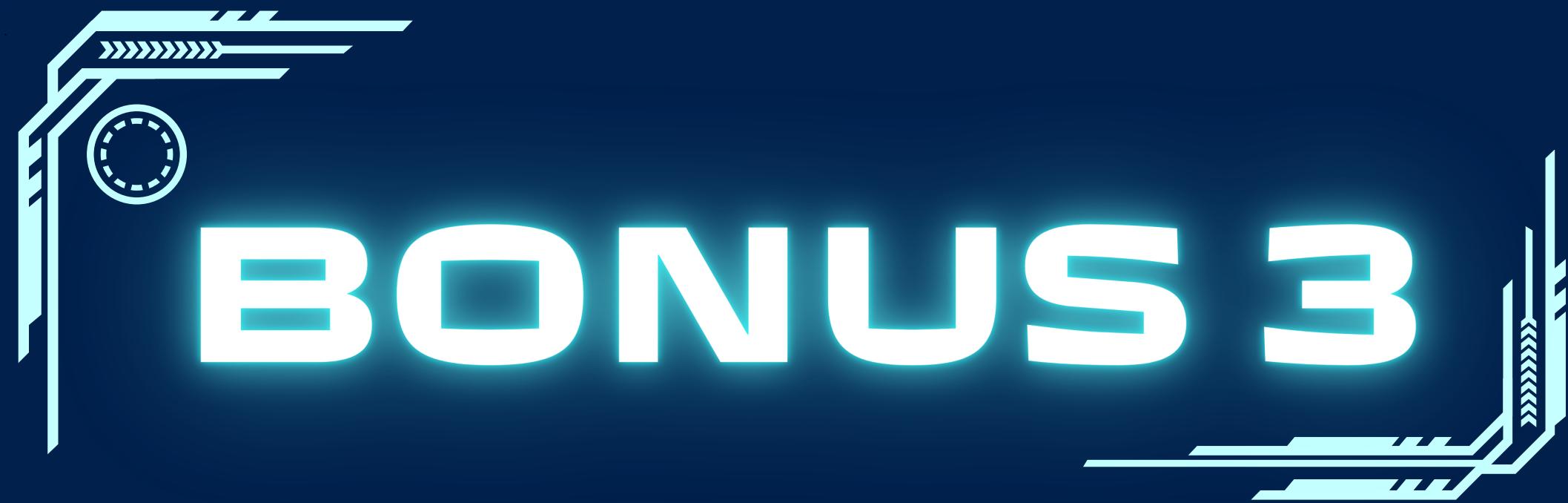
DETERMINAZIONE DEI DATI ESFILTRATI

La fase successiva dell'indagine si è concentrata su quattro voci relative a query DNS indirizzate a example.com. Le query erano dirette a sottodomini insolitamente lunghi associati a ns.example.com. Le stringhe di numeri e lettere presenti in questi sottodomini apparivano codificate in esadecimale (0-9, a-f), suggerendo un possibile tentativo di esfiltrazione di dati attraverso il protocollo DNS.

Per approfondire, le query sono state esportate in un file esterno in formato CSV facendo clic sull'opzione "Raw". Il file scaricato è stato salvato nella directory /home/analyst/Downloads. Successivamente, il file CSV è stato aperto utilizzando un editor di testo come gedit. Tutti i dati non pertinenti sono stati rimossi, lasciando solo le stringhe esadecimali sospette.

Per decodificare queste stringhe, è stato utilizzato il comando "xxd", che ha convertito i dati esadecimali in testo leggibile. Il file decodificato è stato salvato come "secret.txt" e visualizzato nel terminale tramite il comando "cat".

Questa procedura ha permesso di confermare che l'aggressore aveva effettivamente utilizzato query DNS codificate per trasmettere dati sensibili fuori dal sistema compromesso, evidenziando una tecnica di esfiltrazione sofisticata e difficile da rilevare senza un'analisi approfondita dei log DNS.



BONUS 3

Malware
analysis

Any.run

Filesystem
Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

BONUS 3

In questo laboratorio, verranno analizzati i log di un attacco informatico che ha sfruttato una vulnerabilità nota. L'obiettivo è identificare i dispositivi compromessi e il file sottratto, utilizzando strumenti avanzati come Sguil, Wireshark e Kibana. In particolare, un file denominato confidential.txt non è più accessibile agli utenti dopo l'attacco. Lo scopo è determinare come il file sia stato compromesso e sottratto, applicando il modello del 5-tuple, che considera IP sorgente e destinazione, porte sorgente e destinazione, e il protocollo utilizzato. Questa analisi consentirà di comprendere le tecniche utilizzate dall'attaccante e di proporre contromisure adeguate.



Malware analysis

Any.run

Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

BONUS 3

Effettuiamo l'accesso a sguil per esaminare i log e per determinare come il file confidential.txt sia stato compromesso. Possiamo notare in sguil l'evento denominato GPL ATTACK_RESPONSE id check returned root il quale indica che l'accesso root è stato ottenuto dal sistema attaccante sul target. Selezioniamo sull'evento la sezione Transcript che ci permette di esaminare le operazioni svolte dall'attaccante.

The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The main window displays a table of events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, DPort, Pr, and Event Message. One event is highlighted in yellow, showing details: Alert ID 5.1 from sensor seconion-... at 2020-06-11 03:41:20. The event message is "GPL ATTACK_RESPONSE id check returned root". A context menu is open over this event, listing options: Event History, Transcript, Transcript (force new), Wireshark, Wireshark (force new), NetworkMiner, NetworkMiner (force new), Bro, and Bro (force new). Below the table, there are sections for IP Resolution, Agent Status, and a packet list. The packet list shows a single TCP segment with source IP 209.165.200.235, destination IP 209.165.201.17, and port numbers 6200 and 45415. The payload contains the string "uid=0(root) gid=0(root)".

Malware analysis

Any.run

Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

BONUS 3

Analizzando la trascrizione si osserva che, l'attaccante (IP: 209.165.201.17) ha navigato nel file system del target (IP: 209.165.200.235).

Ha quindi verificato i privilegi ottenuti con il comando `whoami`, ricevendo come output "root". Avendo quindi i privilegi completi sul target ha potuto copiare e modificare file critici come `/etc/shadow` e `/etc/passwd`.

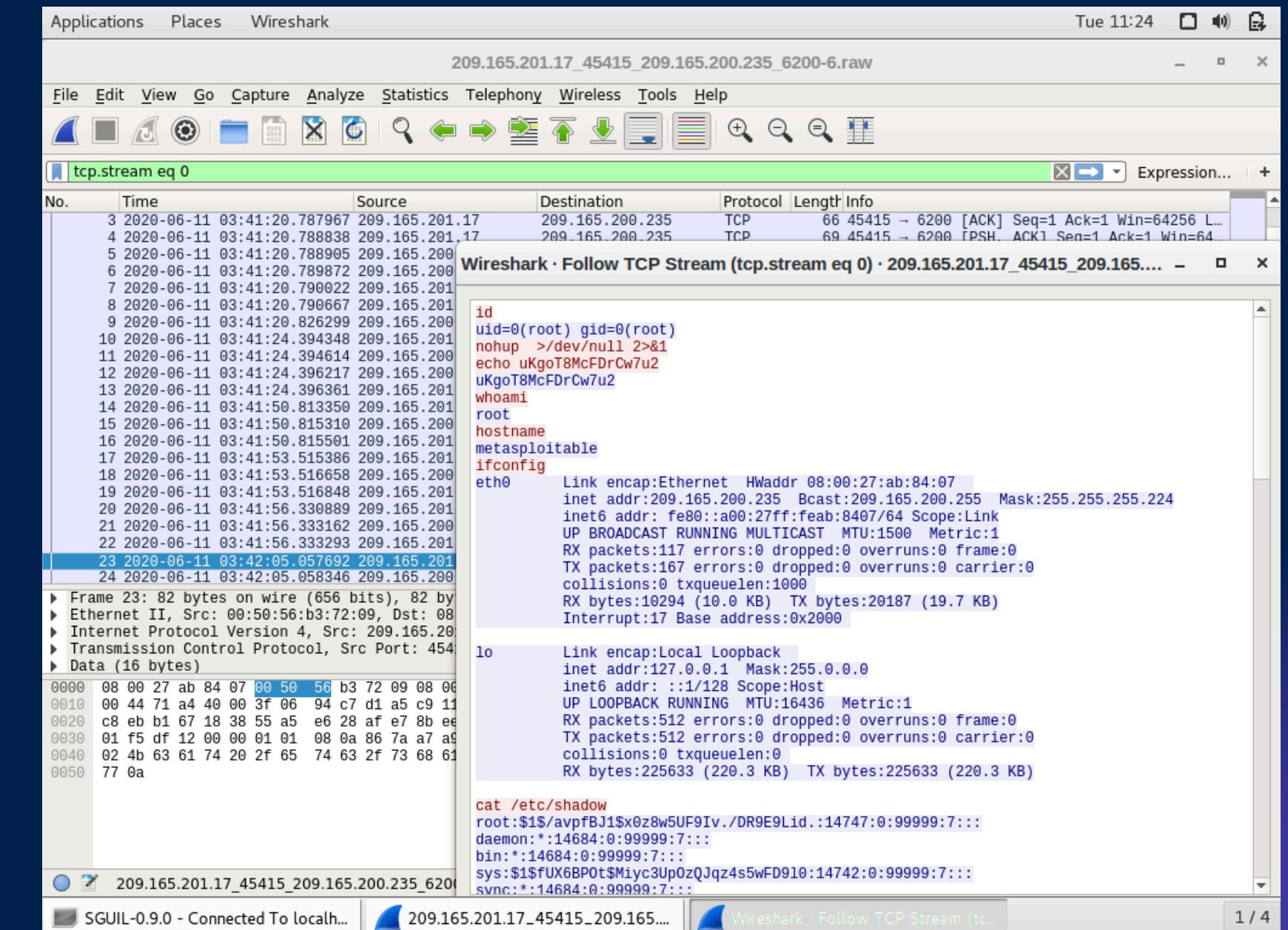
```
File
Sensor Name: seconion-import-1
Timestamp: 2020-06-11 03:41:20
Connection ID: .seconion-import-1_1
Src IP: 209.165.201.17
Dst IP: 209.165.200.235
Src Port: 45415
Dst Port: 6200
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7::?:?] (up: 6267 hrs)
OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)

SRC: id
SRC:
DST: uid=0(root) gid=0(root)
DST:
SRC: nohup >/dev/null 2>&1
SRC:
SRC: echo uKgoT8McFDrCw7u2
SRC:
DST: uKgoT8McFDrCw7u2
DST:
SRC: whoami
SRC:
DST: root
DST:
SRC: hostname
SRC:
DST: metasploitable
DST:
SRC: ifconfig

File
DST: bind:x:105:113::/var/cache/bind:/bin/false
DST: postfix:x:106:115::/var/spool/postfix:/bin/false
DST: ftp:x:107:65534::/home/ftp:/bin/false
DST: postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
DST: mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
DST: tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
DST: distcc:x:111:65534::/bin/false
DST: user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
DST: service:x:1002:1002,,,:/home/service:/bin/bash
DST: te
DST: inetd:x:112:120::/nonexistent:/bin/false
DST: proftpd:x:113:65534::/var/run/proftpd:/bin/false
DST: statd:x:114:65534::/var/lib/nfs:/bin/false
DST: analyst:x:1003:1003:Security Analyst,,,:/home/analyst:/bin/bash
DST:
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
SRC: exit
SRC:
```

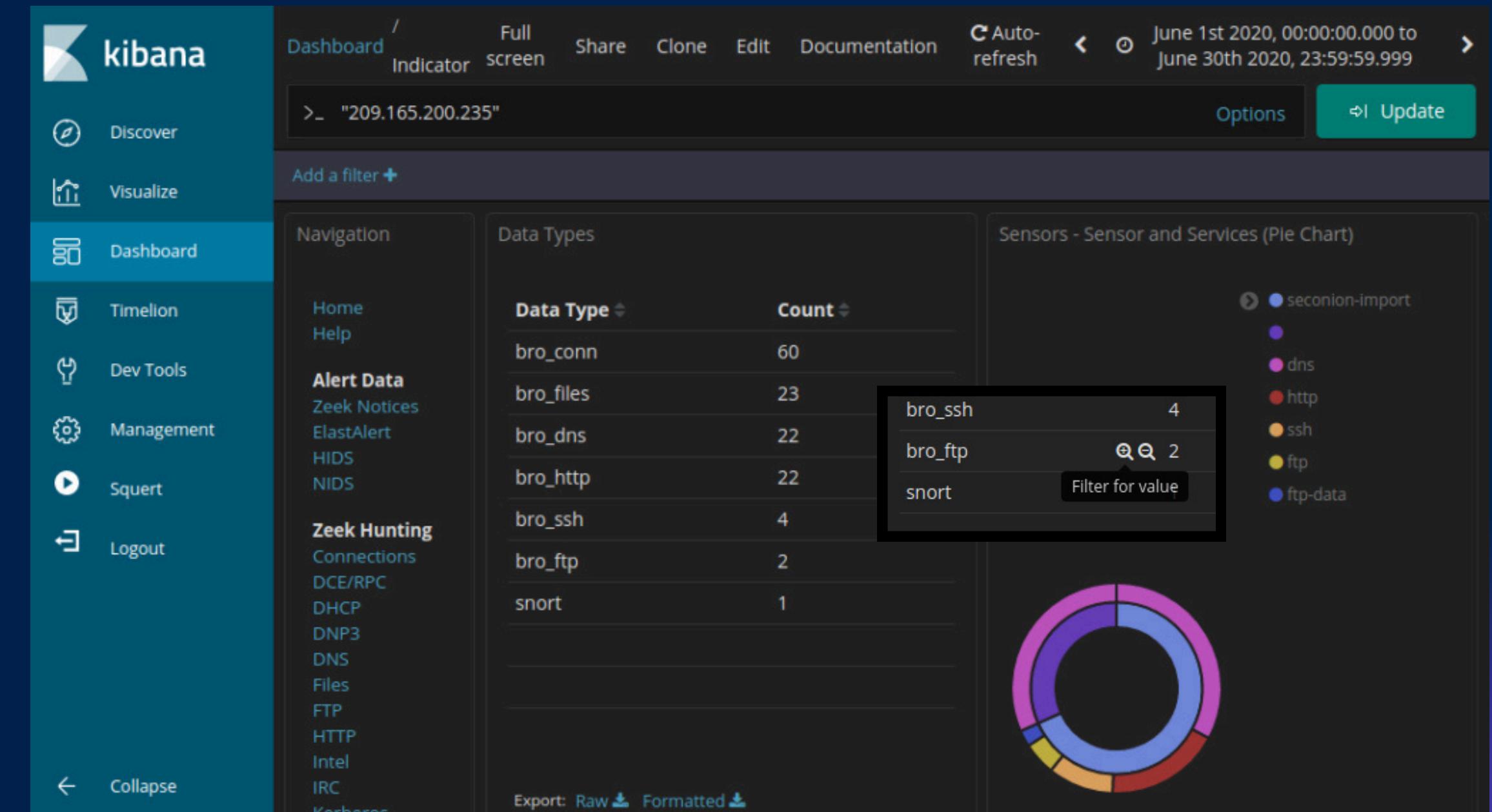
BONUS 3

Successivamente abbiamo utilizzato Wireshark per esaminare il traffico di rete associato all'evento che stiamo analizzando. Aprendo l'applicazione, ci siamo concentrati sulla visualizzazione completa del flusso TCP tra l'attaccante e il sistema target. Abbiamo notato che Wireshark evidenzia i dati trasmessi utilizzando il testo rosso per l'attaccante e il blu per il sistema target, facilitando la comprensione della direzione della comunicazione. Durante la revisione del flusso TCP, abbiamo riscontrato che le informazioni trasmesse corrispondevano a quelle presenti nella trascrizione precedente. Abbiamo identificato il nome host del sistema target come "metasploitable" e il suo indirizzo IP come 209.165.200.235.

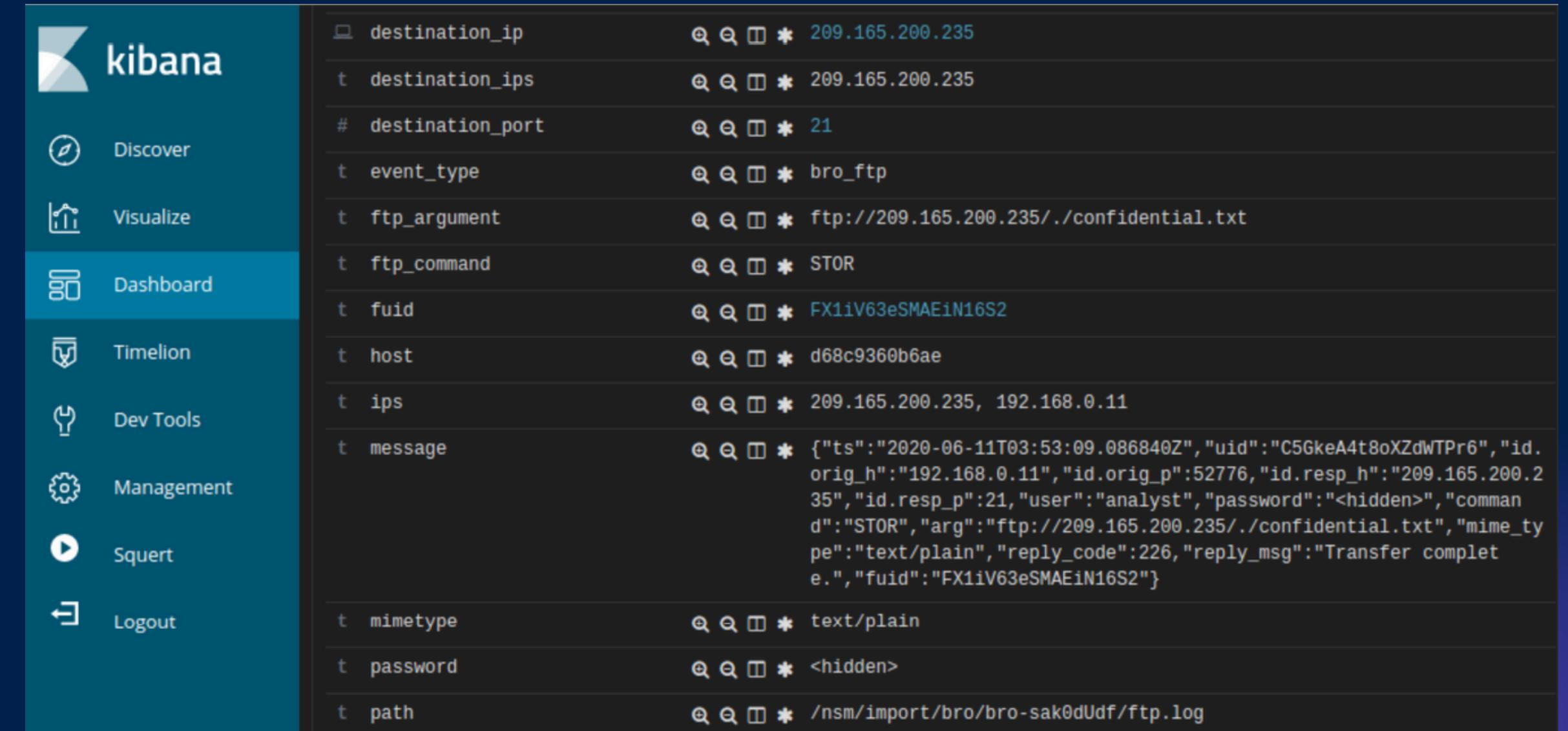


BONUS 3

Siamo passati a Kibana per approfondire i dati di rete relativi all'evento. Abbiamo impostato l'intervallo temporale su giugno 2020 per includere la data dell'attacco. Esaminando il grafico a torta "Sensors and Services" e l'elenco "Data Types", abbiamo notato la presenza dei servizi FTP e FTP-data, suggerendo un possibile utilizzo di questo protocollo per il trasferimento di file. Abbiamo ulteriormente filtrato selezionando solo il traffico FTP.



Tramite il filtro "bro_ftp", abbiamo individuato due voci di log. Analizzando queste voci, abbiamo scoperto che l'indirizzo IP di origine era 192.168.0.11 con la porta 52776, mentre l'indirizzo IP di destinazione era 209.165.200.235 con la porta FTP standard 21. Soffermandoci sulla voce "ftp_argument" si evidenzia l'operazione FTP che include il file "confidential.txt", dimostrando che è stato copiato e successivamente cancellato dal sistema compromesso.



destination_ip	Q Q D * 209.165.200.235	
destination_ips	Q Q D * 209.165.200.235	
destination_port	Q Q D * 21	
event_type	Q Q D * bro_ftp	
ftp_argument	Q Q D * ftp://209.165.200.235//confidential.txt	
ftp_command	Q Q D * STOR	
fuid	Q Q D * FX1iV63eSMAEiN16S2	
host	Q Q D * d68c9360b6ae	
ips	Q Q D * 209.165.200.235, 192.168.0.11	
message	Q Q D * {"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 completo.", "fuid": "FX1iV63eSMAEiN16S2"} <td></td>	
mimetype	Q Q D * text/plain	
password	Q Q D * <hidden>	
path	Q Q D * /nsm/import/bro/bro-sak0dUdf/ftp.log	

Malware analysis

Any.run

Filesystem Linux

File PCAP

BONUS 1

BONUS 2

BONUS 3

BONUS 3

All'interno della stessa voce di registro, nella sezione alert_id è presente un collegamento che ci permette di esaminare le transazioni tra attaccante e bersaglio.

Questo ci permette di osservare le credenziali utilizzate dal target per collegarsi al server FTP.

Time ▾	file_ip	destination_ip	source	uid	fuid	_id
▼ June 11th 2020, 03:53:09.088	192.168.0.1 1	209.165.200.235	FTP_DATA	C2Jv8MWV6 Xg4Ibb51	FX1IV63eSM AEIn16S2	KDjqzXIBB6Cd_0SVfiy

Table JSON [View surrounding documents](#) [View single document](#)

🕒 @timestamp ⓘ ⓘ ⓘ * June 11th 2020, 03:53:09.088
🕒 @version ⓘ ⓘ ⓘ * 1
🕒 _id ⓘ ⓘ ⓘ * KDjqzXIBB6Cd_0SVfiy
🕒 _index ⓘ ⓘ ⓘ * seconion:logstash-import-2020.06.11

Log entry:
{"ts":"2020-06-11T03:53:09.086482Z", "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":"PORT", "arg":"192.168.0.11,194,153", "reply_code":200, "reply_msg":"PORT command successful. Consider using PASV.", "data_channel_passive":false, "data_channel.orig_h":"209.165.200.235", "data_channel.resp_h":"192.168.0.11", "data_channel.resp_p":49817}

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.

Malware analysis

Any.run

Filesystem Linux

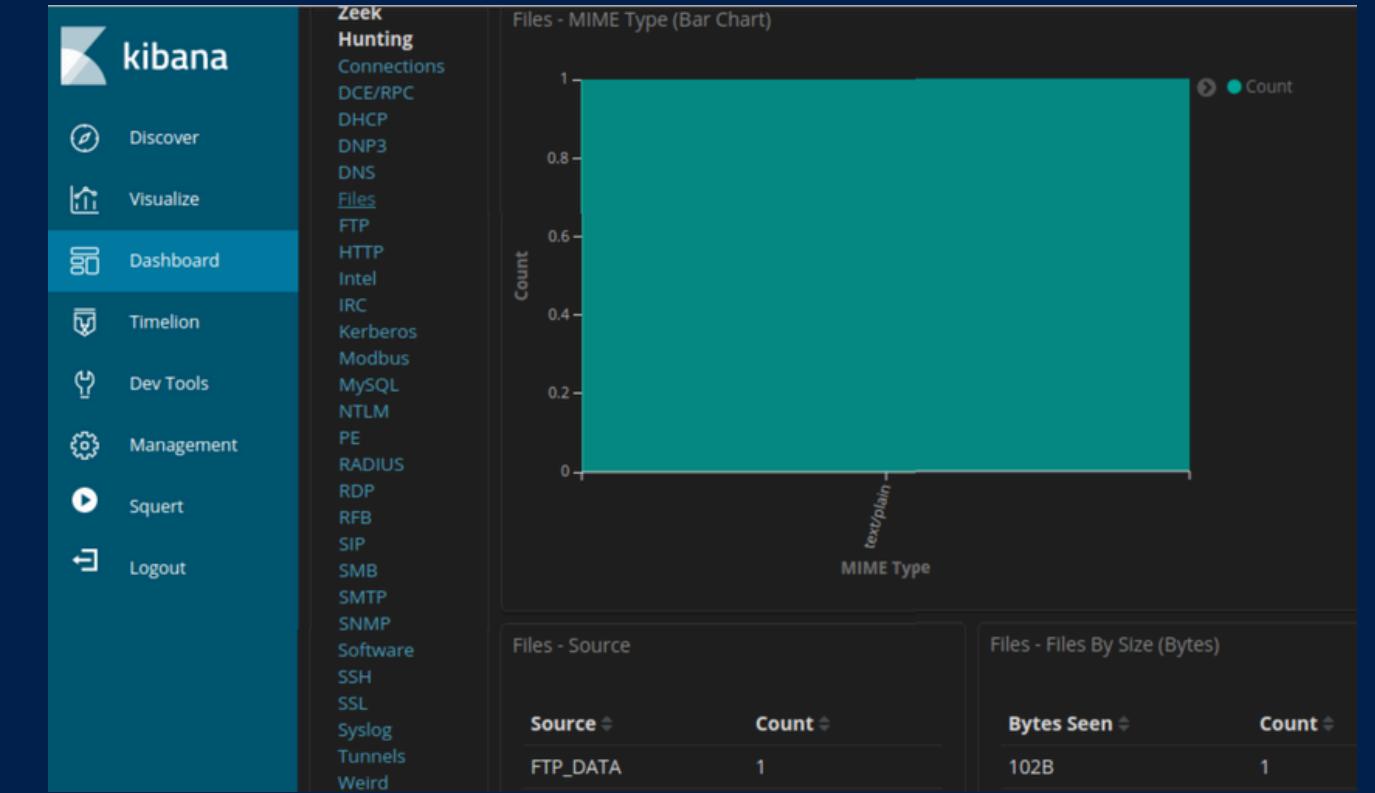
File PCAP

BONUS 1

BONUS 2

BONUS 3

Infine, entrando nella sezione file sotto la voce "Zeek Hunting", possiamo vedere tutti i tipi di file. Abbiamo poi filtrato per FTP_DATA e otteniamo un file di testo trasferito l'11 giugno 2020 alle 3:53. dall' IP 192.168.0.11 all'IP 209.165.200.235. Aprendo il collegamento associato avviso_id possiamo vedere il contenuto del file testuale trasferito tramite FTP.



Log entry:
{"ts": "2020-06-11T03:53:09.088773Z", "fuid": "FX1iV63eSMAEiN16S2", "tx_hosts": ["192.168.0.11"], "rx_hosts": ["209.165.200.235"], "conn_uids": ["C2Jv8MWV6Xg4lbb51"], "source": "FTP_DATA", "depth": 0, "analyzers": ["SHA1", "MD5"], "mime_type": "text/plain", "duration": 0.0, "is_orig": false, "seen_bytes": 102, "missing_bytes": 0, "overflow_bytes": 0, "timedout": false, "md5": "e7bc9c20bfd5666365379c91294d536b", "sha1": "f7f54acee0342f6161f8e63a10824ee11b330725"}
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: 49817
Dst Port: 20
OS Fingerprint: 209.165.200.235:20 - Linux 2.6 (newer, 1) (up: 1 hrs)
OS Fingerprint: -> 192.168.0.11:49817 (distance 0, link: ethernet/modem)
SRC: CONFIDENTIAL DOCUMENT
SRC: DO NOT SHARE
SRC: This document contains information about the last security breach.
SRC:

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817_209.165.200.235:20-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent_type='pcap' LIMIT 1
CAPME: Processed transcript in 0.74 seconds: 0.23 0.32 0.00 0.20 0.00

BONUS 3

TEAM



Stefano Fiori
Beatrice Mastrella
Daniel Gabriel Costeanu
Sara Larizza
Edoardo Mucci



THANK
YOU

