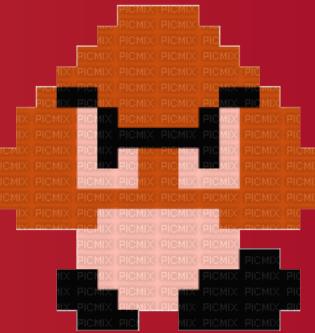




By Panthercriptz

BUILD WEEK III



FELIDRON OMBRAFUSA

Name of Project:
BW3

Presented By:
Panthercript

Presented To:
Epicode



🐾 **INSERT COIN – BEGIN INFILTRATION** ⚡

MENU

START

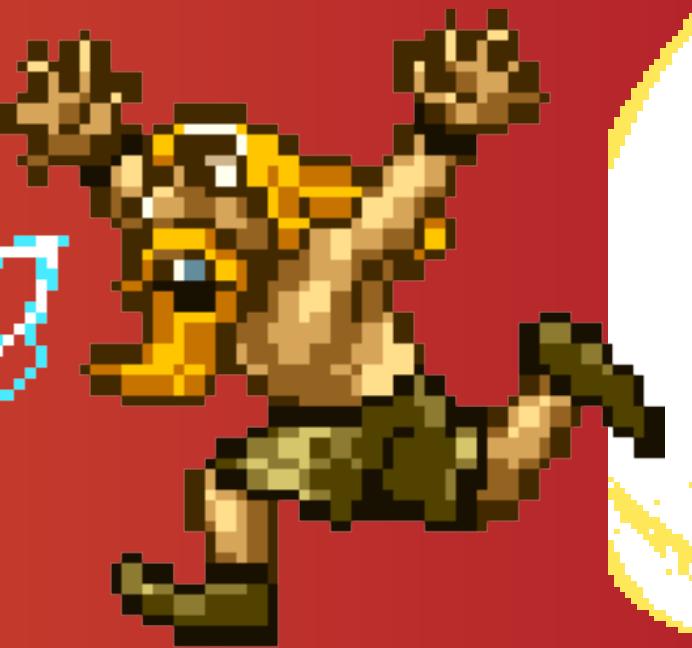
Our team



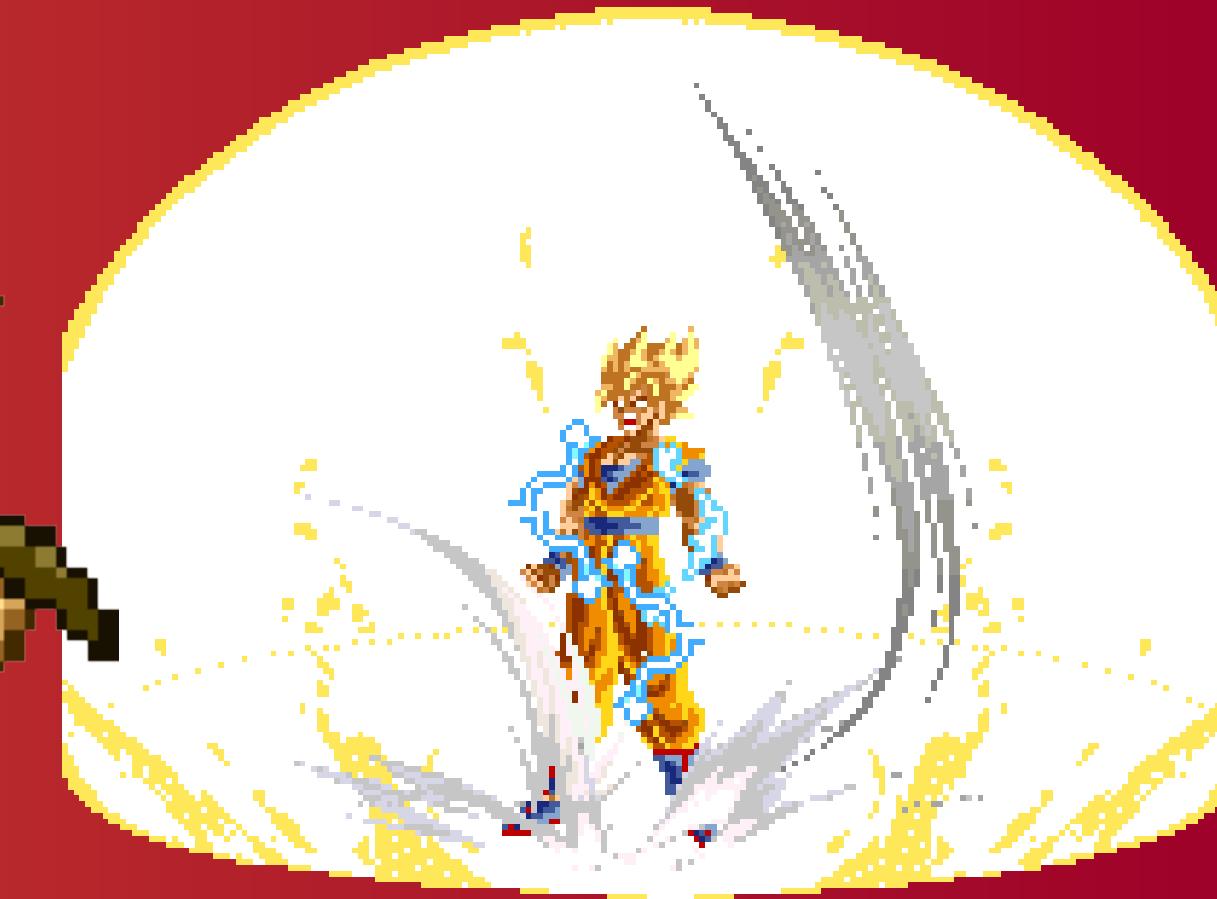
Luca Tavani



Diego Turturo



Ettore Njah

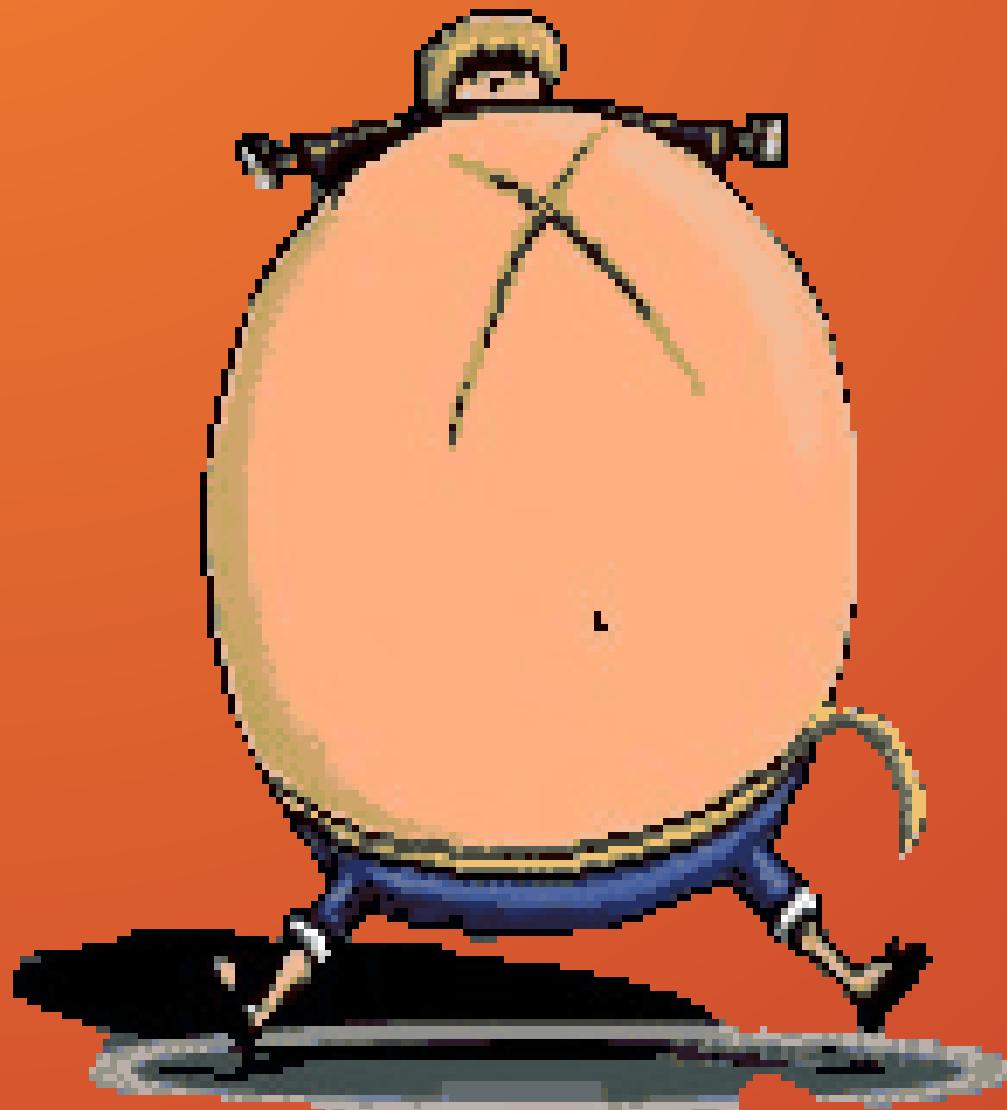


Manuel Pavia



Scarabaffa Torcicorno

Our team



Ritish Bhantooa



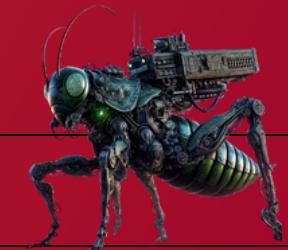
Salvatore La Pira



Christian Pezzella



Felipe Soria



Balzatore Corazzato

Agenda

Malware analysis

Anyrun

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

Lab - Extract an Executable from a PCAP

BONUS 1

BONUS 2

BONUS 3



Ranamandrillo

Giorno 1

Malware analysis

Indagine su AdwareCleaner.exe

Ci siamo trovati di fronte a un file chiamato AdwareCleaner.exe. Il nome suggerisce uno strumento di pulizia, ma era attendibile? Il nostro obiettivo era chiaro: capire la sua vera natura (sicuro, adware o malware?) e proteggere i nostri sistemi.

Cosa Nasconde?

Abbiamo esaminato la "carta d'identità" del file con CFF Explorer. Scoperta chiave: è "impacchettato" con NSIS, una tecnica spesso usata per nascondere codice malevolo dentro installazioni apparentemente innocue.

Leggendo il "testo nascosto" al suo interno (strings), abbiamo trovato comandi sospetti (API Windows e riferimenti a parti delicate del sistema – primi campanelli d'allarme.



FLARE-VM 14/04/2025 12:21:42,70

C:\Users\FlareVM\Downloads>strings AdwereCleaner.exe > strings.txt

Strings v2.54 – Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999–2021 Mark Russinovich
Sysinternals – www.sysinternals.com



Brickzilla

Giorno 1

Malware analysis

Il Comportamento Sotto Osservazione

Abbiamo eseguito il file in un ambiente sicuro, spiando ogni sua mossa con Process Monitor

Abbiamo osservato che:

- Modifica il Sistema: Interviene pesantemente sulle impostazioni "nascoste" di Windows (Registro).
- Tenta la Persistenza: Prova a manipolare la barra di "Avvio Rapido" (Quick Launch), forse per restare attivo o ingannare l'utente.
- Accede ai Dati: Esplora le cartelle con i file personali dell'utente.

Chiediamo alla Community: La Reputazione Online

Per una conferma esterna, abbiamo consultato VirusTotal. Il risultato è stato netto: ben 56 sistemi antivirus su 72 lo identificano come MINACCIA CONCRETA. Le etichette parlano chiaro: Dropper, FakeAV, Trojan – tutte classificazioni di malware.

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:57:...	I sass.exe	688	QueryNameInfo	C:\Users\FlareVM\AppData\Local\Temp\...	SUCCESS	Name: \Users\Flar...
11:57:...	I sass.exe	688	QueryNameInfo	C:\Users\FlareVM\AppData\Local\Temp\...	SUCCESS	Name: \Users\Flar...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
11:57:...	Explorer.EXE	4620	RegCloseKey	HKCU	SUCCESS	
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	QueryOpen	C:\Users\FlareVM\AppData\Local\Temp\...	SUCCESS	Creation Time: 14/0...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
11:57:...	Explorer.EXE	4620	RegCloseKey	HKCU	SUCCESS	
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
11:57:...	Explorer.EXE	4620	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85...	NAME NOT FOUND	Desired Access: R...

Giorno 1

Malware analysis

Il Quadro Completo: Le Prove Portano a una Conclusione

Mettendo insieme tutti i pezzi:

- La struttura mascherata (NSIS).
- Gli indizi interni (stringhe API).
- Il comportamento attivo sul sistema (modifiche al registro, accesso ai dati).
- Il riconoscimento quasi unanime come minaccia (VirusTotal).
- Conclusione: AdwareCleaner.exe è senza dubbio software malevolo mascherato da utility.

Parte 2

prima abbiamo guardato "dentro" il file (AdwareCleaner.exe), poi abbiamo osservato cosa è successo realmente sul sistema quando questo tipo di adware è attivo (basandoci sui log del secondo report), scoprendo anche il coinvolgimento di Word.



Giomo 1

Malware analysis

- Abbiamo analizzato il file sospetto **AdwareCleaner.exe** stesso (come è fatto, cosa contiene).
- Inoltre, abbiamo esaminato i log di attività di un sistema infetto da adware simile (**AdwereCleaner.exe**, **6AdwCleaner.exe**), osservando le azioni reali.
- Obiettivo: Avere un quadro completo della minaccia, unendo l'analisi del "codice" a quella del "comportamento".

Comportamento Osservato: Manipolazione del Sistema

- Cosa Fa sul PC? Modifiche alle Impostazioni Internet
- Cambia le regole di Internet: Modifica le impostazioni di connessione (Registro: ZoneMap, Proxy) per controllare il traffico web, bypassare sicurezze o spiarti.
- Cerca di nascondersi: Cancella la cronologia dei file recenti e dati di recupero per non lasciare tracce.

Security vendor	Detection	Family	Notes
AhnLab-V3	Dropper/Win32.Dapato.R137988	Alibaba	Hoax/MSIL/Porcupine.e66ee97
Anti-AVL	HackTool/Hoax/MSIL.Agent	Arcabit	Trojan.Mint.Porcupine.ED5010
Avast	Win32:FakeAV-FLW [Trj]	AVG	Win32:FakeAV-FLW [Trj]
Avira (no cloud)	JOKE/Agent.Lrham	BitDefender	Gen:Heur.Mint.Porcupine.luZ@bOy2NApi
Bkav Pro	w32.Common.sF08E2E4	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Eve.trojan.fakesav	Cylance	Unsafe
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
DrWeb	Trojan.FakeAV.17850	Elastic	Malicious (high Confidence)
Emissisoft	Gen:Heur.Mint.Porcupine.luZ@bOy2NApi...	eScan	Gen:Heur.Mint.Porcupine.luZ@bOy2NApi
ESET-NOD32	MSIL/Hoax.Agent.NBD	Fortinet	W32/Agent.GDCItr
GData	Gen:Heur.Mint.Porcupine.luZ@bOy2NApi	Google	Detected
Gridinsoft (no cloud)	Fake.Win32.Gen.vII	Huorong	Rogue/FakeAV.j
Ikarus	Trojan.Fakesav	K7GWVirus	Trojan (U05863041)

```
##u
^[
%r@
%xr@
%tr@
RichEdit
RichEdit20A
RichEd32
RichEd20
.DEFAULT\Control Panel\International
Control Panel\Desktop\ResourceLocale
Software\Microsoft\Windows\CurrentVersion
Microsoft\Internet Explorer\Quick Launch
#+3;CScs
!1Aa
MulDiv
DeleteFileA
FindFirstFileA
FindNextFileA
FindClose
SetFilePointer
WriteFile
GetPrivateProfileStringA
WritePrivateProfileStringA
MultiByteToWideChar
```

Giomo 1

Malware analysis

Comportamento Osservato: SCOPERTA CRITICA - Il Ruolo di Word

- Fatto Gravissimo: Dai log emerge che anche WINWORD.EXE (Microsoft Word) esegue azioni dannose!
- Azione Specifica: Modifica le stesse identiche impostazioni Internet cambiate dall'adware.
- Azione Specifica: Cancella i file di recupero e la cronologia dei documenti recenti, proprio come l'adware.
- Conclusione: Questo è altamente sospetto e indica quasi certamente che Word è stato compromesso (infettato da macro o altro) e viene usato dall'adware.

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3752	6AdwCleaner.exe	GET	-	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/paymore.php	DE	-	-	malicious
3752	6AdwCleaner.exe	GET	-	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/paymore.php	DE	-	-	malicious
3752	6AdwCleaner.exe	GET	-	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/paymore.php	DE	-	-	malicious
3752	6AdwCleaner.exe	GET	403	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/status.php?action=clean&id=0	DE	html	146 b	malicious
3752	6AdwCleaner.exe	GET	200	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/paydefault.ph p?id=0	DE	html	1.32 Kb	malicious
3752	6AdwCleaner.exe	GET	403	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/get_data.php?id=0	DE	html	146 b	malicious
3752	6AdwCleaner.exe	GET	200	185.53.177.53:80	http://www.vikingwebscanner.com/scripts/paydefault.ph p?id=0	DE	html	1.32 Kb	malicious
3752	6AdwCleaner.exe	GET	200	185.53.177.53:80	http://www.vikingwebscanner.com/track.php?domain=vikingwebscanner.com&toggel=browserjs&uid=MTY40DE0MTUyNS4wMzQyOmEwZDMzY2E2TZJNmZhOGJmNTkyOWNlODQ0ODY00Dg4ZTMxOGEzMGFInjl2M WyWmzNIOGY4ZDlxNWNjOWQxNjU6NjQ5ZWIZDUwOD U4Mg%3D%3D	DE	binary	20 b	malicious
3752	6AdwCleaner.exe	GET	403	208.91.196.46:80	http://ifdnzact.com/?dn=vikingwebscanner.com&pid=9P0755G95	VG	html	272 b	suspicious
3752	6AdwCleaner.exe	GET	200	18.66.121.190:80	http://d38psrni17bxv.cloudfront.net/scripts/js3.js	US	text	1.07 Kb	suspicious

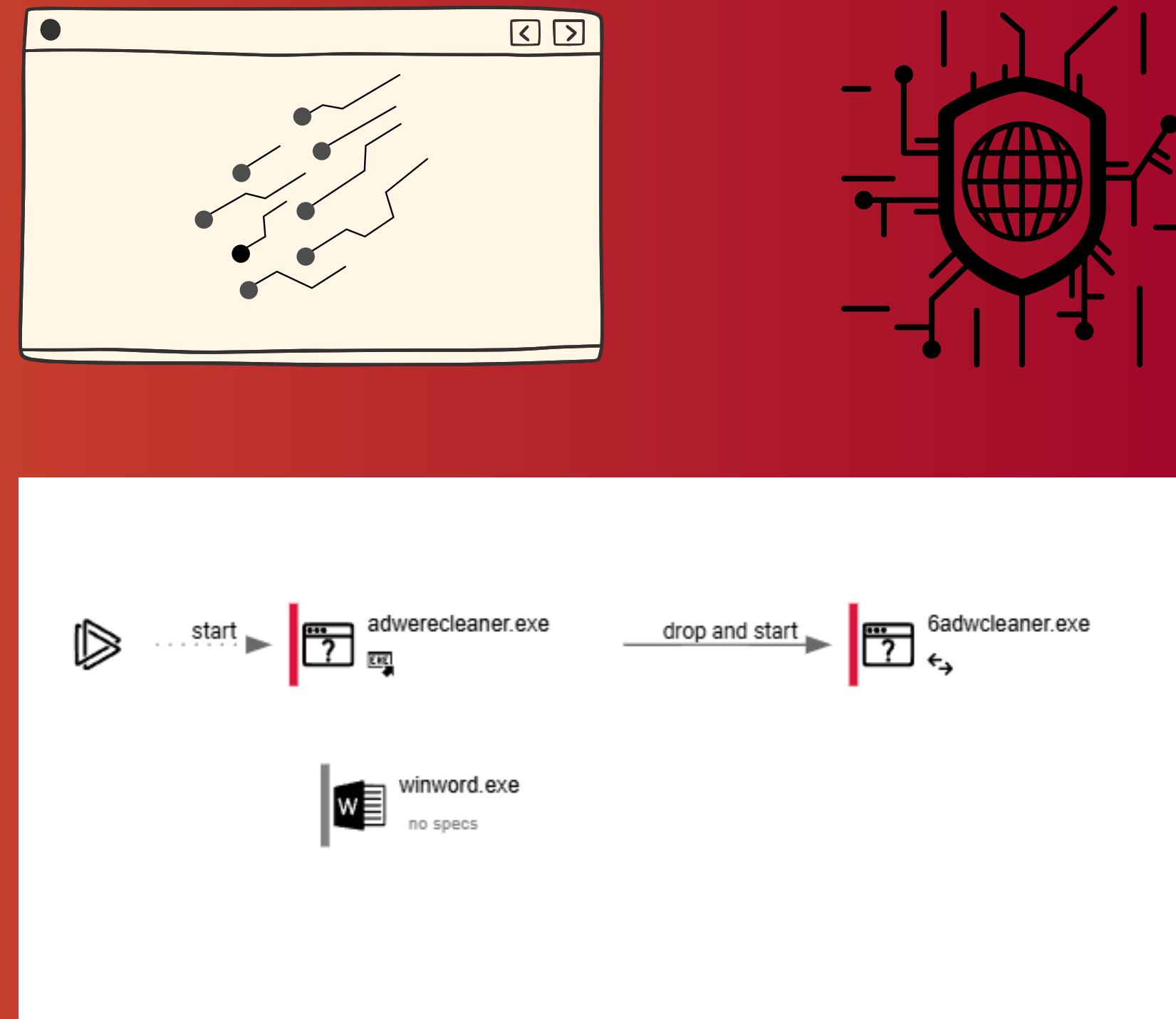
Analisi Dettagliata delle Richieste HTTP:

- Processo Sorgente: Tutte le richieste HTTP registrate provengono da **6AdwCleaner.exe** (PID 3752).
- Destinazioni Sospette/Malevoli:
 - **www.vikingwebscanner.com** (IP: 185.53.177.53 - Germania): Questo dominio è stato contattato ripetutamente. Il nome stesso ("viking web scanner") è indicativo di software potenzialmente indesiderato o scareware. Le richieste puntano a script PHP (paymore.php, paydefault.php, status.php, get_data.php, track.php, ls.php) i cui nomi suggeriscono funzioni legate a pagamenti, controllo dello stato, recupero dati, tracciamento e licenze/registrazione. Molte di queste comunicazioni sono classificate come malicious.
 - **ifdnzact.com** (IP: 208.91.196.46 - Isole Vergini Britanniche): Questo dominio, classificato come suspicious, è stato contattato passando il dominio vikingwebscanner.com come parametro, indicando un possibile servizio di reindirizzamento, tracciamento o affiliazione.
 - **d38psrni17bxv.cloudfront.net** (IPs: 18.66.121.190, 18.66.121.138 - USA): È stato scaricato uno script (js3.js) da una distribuzione **CloudFront** (un servizio CDN legittimo spesso abusato per distribuire malware). Questa attività è classificata come suspicious.
- **Codici di Risposta:** Sono stati osservati codici 200 OK (successo), 201 Created (risorsa creata/registrata), 403 Forbidden (accesso negato) e richieste senza codice (probabilmente fallite o bloccate). Questa varietà indica tentativi attivi di comunicazione con i server di comando e controllo (C&C).

Punti Chiave

Mitigation e Remediation:

- È confermato che si tratta di malware pericoloso. Non solo modifica il PC e si nasconde, ma l'aspetto più allarmante è che sembra aver compromesso Microsoft Word, rendendo l'infezione più profonda e difficile da rimuovere completamente.
- **Rischi Concreti:** I pericoli principali sono: violazione della privacy (tracciamento), truffe online, maggiore esposizione ad altri virus, possibili problemi di funzionamento del PC e di Office. La pulizia è complicata dal coinvolgimento di Word.
- **Azioni Prioritarie :** Scansione Totale: Pulire il sistema con un buon antimalware.
- **FOCUS SU WORD:** Controllare e bonificare Microsoft Word con massima attenzione.
- Ripristino: Correggere le impostazioni Internet/Proxy modificate.
- Blocco: Bloccare i siti web malevoli identificati.
- Aggiornamento: Mantenere tutto aggiornato.



Giorno 2

Analisi Malware Vidar Stealer



Questo documento fornisce un'analisi dettagliata del malware identificato come Vidar Stealer
(file: [66bddfcb52736_vidar.exe](#)).

L'analisi si basa su un'esecuzione in sandbox e include informazioni statiche, comportamentali e di rete, con raccomandazioni per la remediation.

Vidar Stealer: An In-depth Analysis of an Information-Stealing Malware

Identificazione e Classificazione



- **File analizzato:** 66bddfcb52736_vidar.exe
- **Tipologia:** Stealer (Malware per furto credenziali e dati sensibili)
- **Data analisi:** 20 gennaio 2025
- **Metodo di diffusione:** Phishing
- **Obiettivi del malware:**
 - Credenziali account
 - Wallet di criptovalute
 - Dati personali
- **Azione raccomandata:**
Quarantena e rimozione immediata



Comportamento Osservato (Sandbox)

- Creazione di mutex malevoli
- Furto di credenziali da browser
- Avvio di cmd.exe per auto-eliminazione
- Accesso a impostazioni di sicurezza IE
- Comunicazione sospetta con Telegram (uso come server C2)
- La comunicazione con Telegram indica un'esfiltrazione attiva di dati verso l'attaccante.



Analisi Statica

- Tipo file: PE32 .NET Executable
- Hash:
 - MD5: FEDB687ED23F77925B35623027F799BB
 - SHA1: 7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
 - SHA256:
325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1

Questi hash vanno inseriti nelle blacklist di antivirus e firewall.

Attività di Rete

Domini contattati:

- **steamcommunity.com** → Possibile furto credenziali Steam
- **t.me** → Canale Telegram per esfiltrazione
- **arpdabl.zapto.org** → Possibile server C2
- Domini Microsoft (per validazione certificati)



Modifiche al Registro

- Lettura info di sistema e software installato
- Modifica cache e impostazioni IE



File Creati e Processi Coinvolti

- File HTML sospetto in INetCache IE
- Processi osservati:
 - **RegAsm.exe** → Caricamento codice .NET
 - **Cmd.exe** → Esecuzione comandi
 - **Timeout.exe** → Delay nei comandi



Conclusioni e Raccomandazioni Finali

1. Eliminare il file infetto
2. Effettuare una scansione antivirus completa
3. Inserire in blacklist hash e IP/domini associati
4. Monitorare la rete per traffico sospetto
5. Controllare integrità dei file RegAsm.exe e Cmd.exe



Analisi di Sicurezza URL : Instagram

Analisi di sicurezza su un URL di Instagram effettuata con ANY.RUN, con evidenza di attività sospette a livello di software, registro, file e rete per valutarne la potenziale pericolosità.

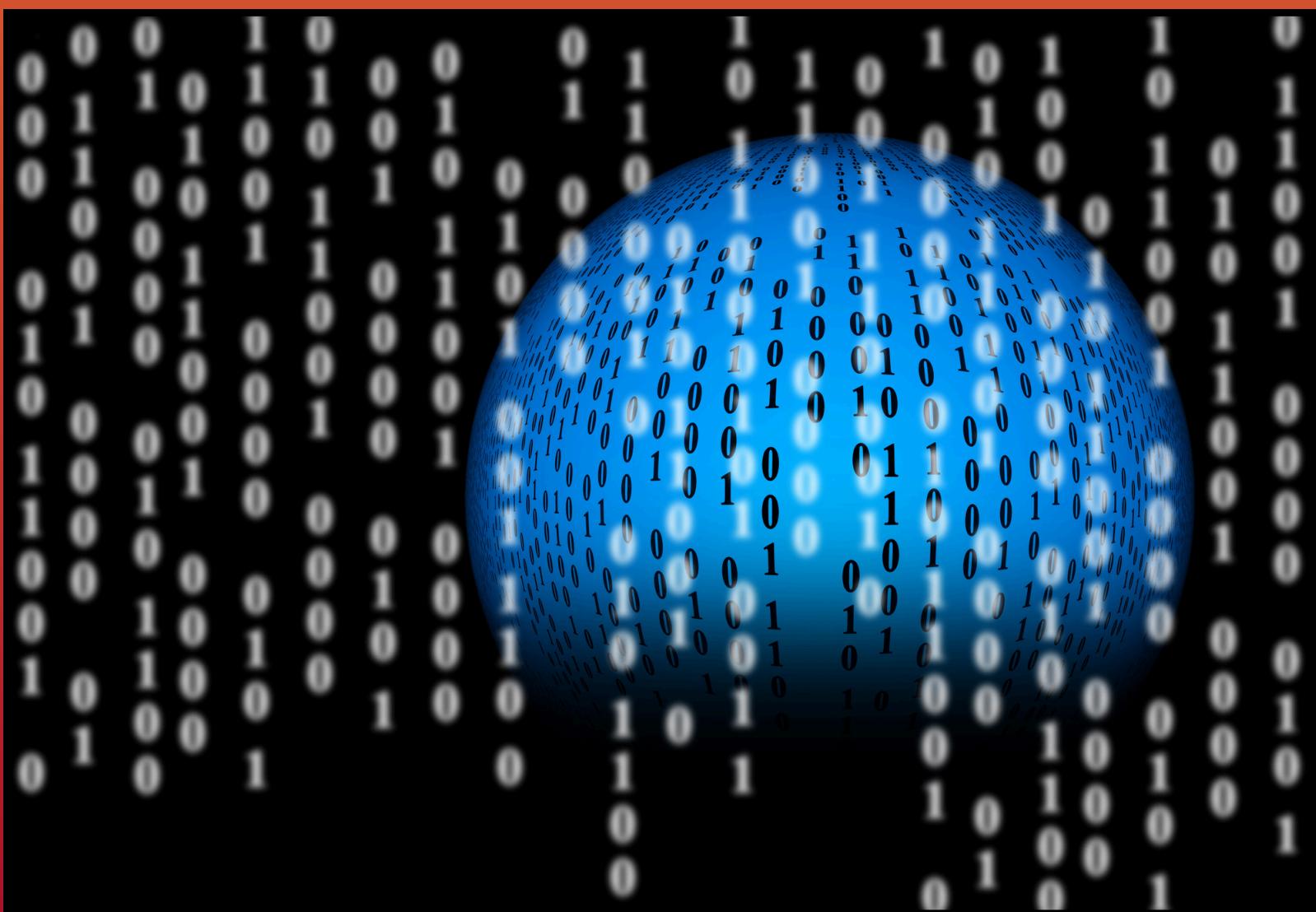


Riepilogo dell'Analisi

L'analisi dell'URL (eseguita il 25 agosto 2024 su Windows 10) non ha rilevato minacce, ma consiglia di esaminare eventuali comportamenti sospetti. Sono stati usati browser e software comuni.

Analisi e Ambiente Software

L'analisi, della durata totale di 540 secondi, è stata eseguita con rete attiva e impostazioni di privacy pubbliche, senza l'uso di tecniche avanzate come "Heavy Evasion" o "MITM proxy". L'ambiente includeva software comuni come browser, Office, Java e Adobe, per simulare un contesto realistico e facilitare l'individuazione di comportamenti sospetti.



Attività Comportamentali e del Registro di Sistema

L'ANALISI COMPORTAMENTALE NON HA RILEVATO ATTIVITÀ SOSPETTE O DANNOSE. SONO STATE OSSERVATE ATTIVITÀ INFORMATIVE, COME LA LETTURA DI CHIAVI DEL REGISTRO DI SISTEMA DI MICROSOFT OFFICE DA PARTE DI CHROME.EXE E IL SUO AVVIO AUTONOMO.

SONO STATI REGISTRATI 4567 EVENTI DEL REGISTRO, PRINCIPALMENTE LETTURE (4549) E POCHE SCRITTURE (18), RIGUARDANTI CHIAVI LEGATE A GOOGLE CHROME (ES. BLBEACON, THIRDPARTY, UPDATE). QUESTE MODIFICHE SONO NORMALI PER IL FUNZIONAMENTO DEL BROWSER E NON INDICANO COMPORTAMENTI MALEVOLI.



Attività dei File e di Rete



SONO STATI RILEVATI 30 FILE SOSPETTI (TEMPORANEI E DI LOG CREATI DA CHROME IN APPDATA) E 18 FILE DI TESTO. ANCHE SE NON RISULTANO DANNOSI, È CONSIGLIATA UN'ULTERIORE ANALISI IN CASO DI SOSPIETTA INFESTAZIONE.

L'ATTIVITÀ DI RETE HA INCLUSO RICHIESTE HTTP(S), CONNESSIONI TCP/UDP E DNS VERSO DOMINI LEGITTIMI COME MICROSOFT, GOOGLE, FACEBOOK E CONVERTKIT. TUTTE LE RICHIESTE HTTP SONO STATE WHITELISTATE E NON COSTITUISCONO UNA MINACCIA.

Conclusioni e Raccomandazioni

L'ANALISI DELL'URL DI INSTAGRAM NON HA RILEVATO MINACCIE IMMEDIATE, MA NON GARANTISCE LA TOTALE SICUREZZA. COMPORTAMENTI SOSPETTI POTREBBERO EMERGERE IN SEGUITO E L'ANALISI RIFLETTE SOLO IL MOMENTO IN CUI È STATA ESEGUITA. SI CONSIGLIA DI MONITORARE REGOLARMENTE L'URL, FARE NUOVE ANALISI IN CASO DI CAMBIAMENTI SOSPETTI E SEGUIRE BUONE PRATICHE DI SICUREZZA, COME USARE UN ANTIVIRUS AGGIORNATO E NAVIGARE IN MODO SICURO.



Comportamento Osservato (Sandbox)

- Creazione di mutex malevoli
- Furto di credenziali da browser
- Avvio di cmd.exe per auto-eliminazione
- Accesso a impostazioni di sicurezza IE
- Comunicazione sospetta con Telegram (uso come server C2)
- La comunicazione con Telegram indica un'esfiltrazione attiva di dati verso l'attaccante.



- Tipo file: PE32 .NET Executable
- Hash:
 - MD5: FEDB687ED23F77925B35623027F799BB
 - SHA1: 7F27D0290ECC2C81BF2B2DOFA1026F54FD687C81
 - SHA256:
325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1

Questi hash vanno inseriti nelle blacklist di antivirus e firewall.



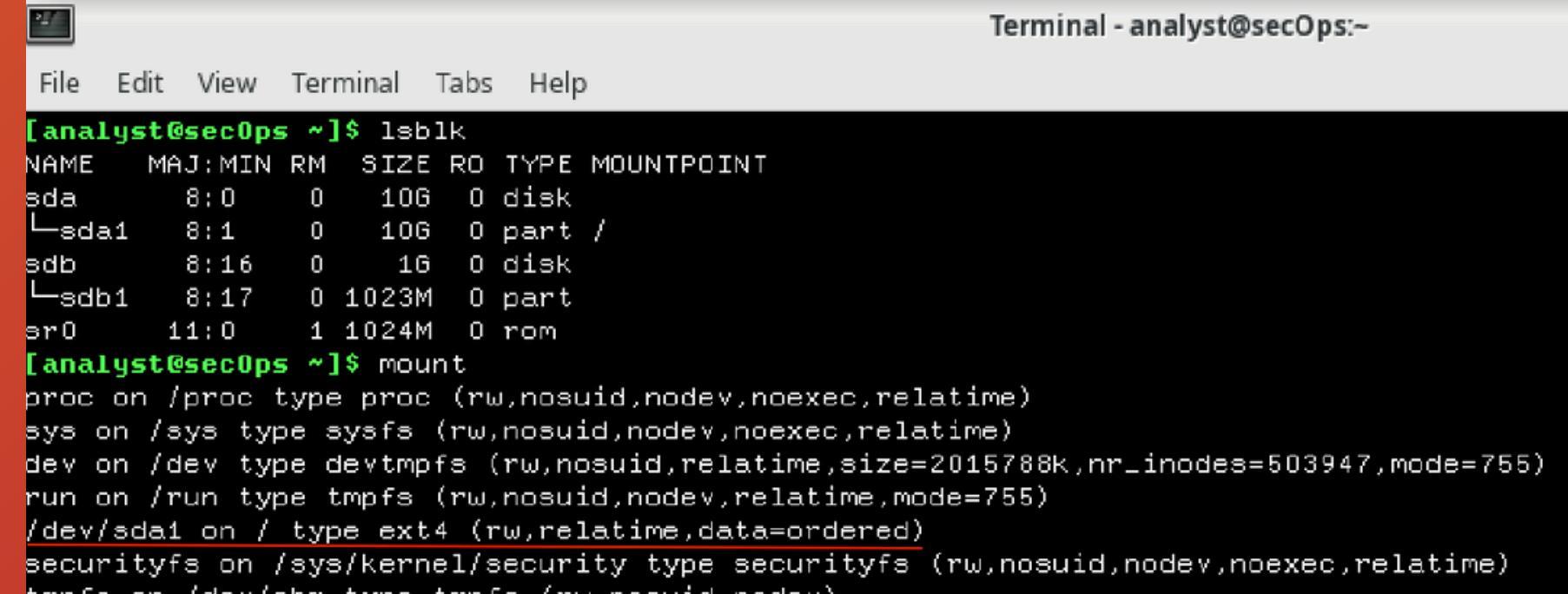
Giorno 3

Lab - Navigating the Linux Filesystem and Permission Settings

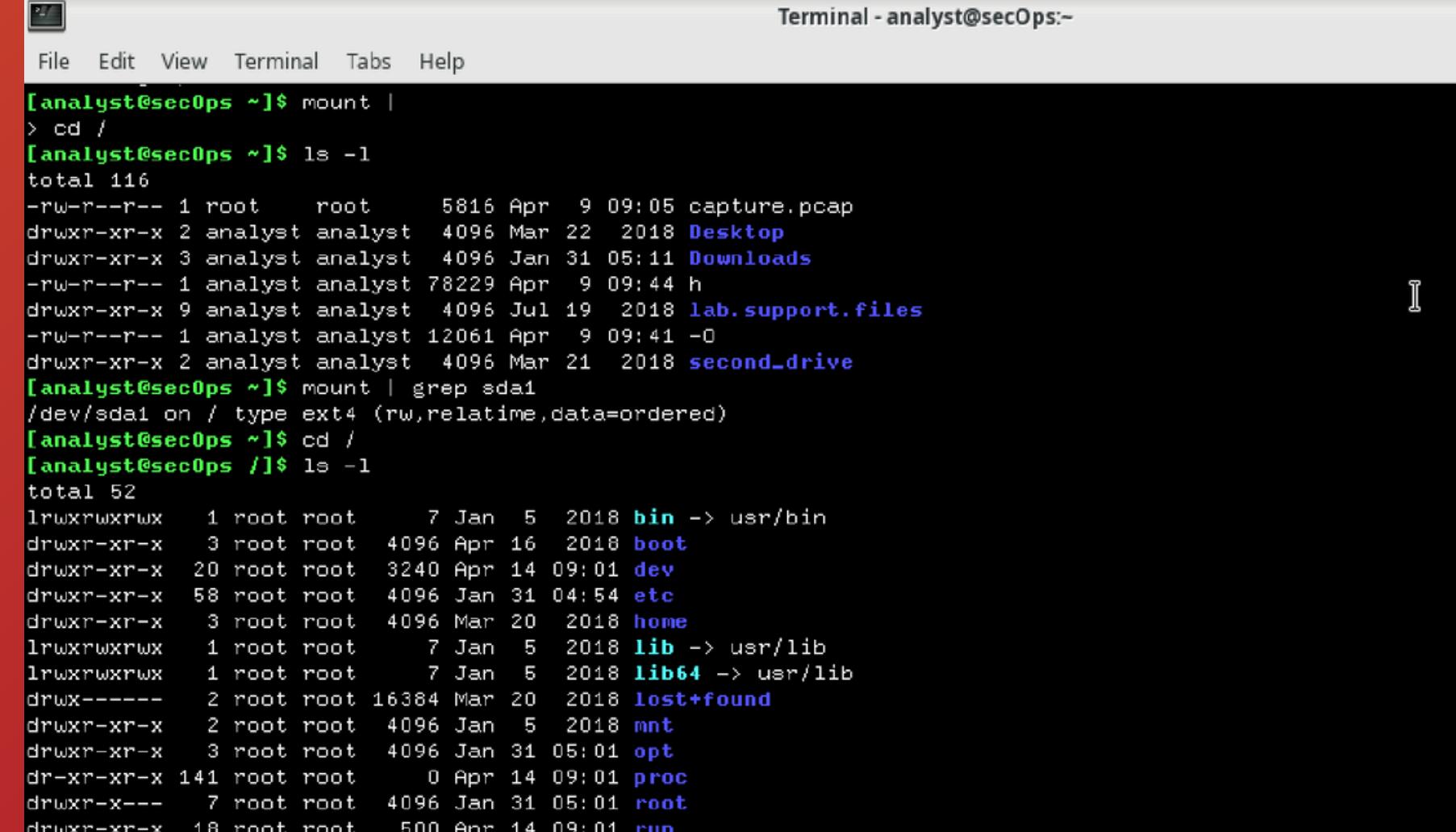
PART 1:

EXPLORING FILESYSTEMS IN LINUX

- **LSBLK:** MOSTRA I DISPOSITIVI DI ARCHIVIAZIONE E LE LORO PARTIZIONI.
- **MOUNT:** MOSTRA I FILE SYSTEM EFFETTIVAMENTE MONTATI E DOVE SONO ACCESSIBILI NEL SISTEMA.
- **MOUNT | GREP SDA1:** FILTRA L'OUTPUT DI MOUNT PER MOSTRARE SOLO LE RIGHE CHE CONTENGONO "SDA1", VERIFICANDO SE IL DISPOSITIVO /DEV/SDA1 È MONTATO.



```
Terminal - analyst@secOps:~  
[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    16  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=2015788k,nr_inodes=503947,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)
```



```
Terminal - analyst@secOps:~  
[analyst@secOps ~]$ mount |  
> cd /  
[analyst@secOps ~]$ ls -l  
total 116  
-rw-r--r-- 1 root root 5816 Apr  9 09:05 capture.pcap  
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop  
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads  
-rw-r--r-- 1 analyst analyst 78229 Apr  9 09:44 h  
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files  
-rw-r--r-- 1 analyst analyst 12061 Apr  9 09:41 -0  
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive  
[analyst@secOps ~]$ mount | grep sda1  
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)  
[analyst@secOps ~]$ cd /  
[analyst@secOps /]$ ls -l  
total 52  
lrwxrwxrwx 1 root root 7 Jan  5 2018 bin -> usr/bin  
drwxr-xr-x 3 root root 4096 Apr 16 2018 boot  
drwxr-xr-x 20 root root 3240 Apr 14 09:01 dev  
drwxr-xr-x 58 root root 4096 Jan 31 04:54 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 3 root root 4096 Jan 31 05:01 opt  
dr-xr-xr-x 141 root root 0 Apr 14 09:01 proc  
drwxr-x--- 7 root root 4096 Jan 31 05:01 root  
drwxr-xr-x 18 root root 500 Apr 14 09:01 run
```

Lab - Navigating the Linux Filesystem and Permission Settings



Terminal - analyst@sec0ps

```
File Edit View Terminal Tabs Help
[analyst@sec0ps ~]$ ls -l
total 52
lrwxrwxrwx 1 root root 7 Jan 5 2018 bin -> usr/bin
drwxr-xr-x 3 root root 4096 Apr 16 2018 boot
drwxr-xr-x 20 root root 3240 Apr 14 09:01 dev
drwxr-xr-x 58 root root 4096 Jan 31 04:54 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 3 root root 4096 Jan 31 05:01 opt
dr-xr-xr-x 139 root root 0 Apr 14 09:01 proc
drwxr-x--- 7 root root 4096 Jan 31 05:01 root
drwxr-xr-x 18 root root 500 Apr 14 09:01 run
lrwxrwxrwx 1 root root 7 Jan 5 2018 sbin -> usr/bin
drwxr-xr-x 6 root root 4096 Mar 24 2018 srv
dr-xr-xr-x 13 root root 0 Apr 14 09:01 sys
drwxrwxrwt 8 root root 200 Apr 14 09:02 tmp
drwxr-xr-x 9 root root 4096 Jan 31 04:53 usr
drwxr-xr-x 12 root root 4096 Jan 31 04:54 var
[analyst@sec0ps ~]$ mkdir second_drive
mkdir: cannot create directory 'second_drive': Permission denied
[analyst@sec0ps ~]$ sudo mount /dev/sdb1 ~/second_drive
[sudo] password for analyst:
mount: /home/analyst/second_drive: special device /dev/sdb1/ does not exist
[analyst@sec0ps ~]$ ls -l second_drive/
ls: cannot access 'second_drive/': No such file or directory
[analyst@sec0ps ~]$ mkdir second_drive
mkdir: cannot create directory 'second_drive': Permission denied
[analyst@sec0ps ~]$ cd ~
[analyst@sec0ps ~]$ ls -l
total 116
-rw-r--r-- 1 root root 5816 Apr 9 09:05 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads
-rw-r--r-- 1 analyst analyst 78229 Apr 9 09:44 h
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 12061 Apr 9 09:41 -0
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
```

```
[analyst@sec0ps ~]$ mkdir second_drive
mkdir: cannot create directory 'second_drive': File exists
[analyst@sec0ps ~]$ ls -l second_drive/
total 0
[analyst@sec0ps ~]$ sudo mount /dev/sdb1 ~/second_drive
mount: /home/analyst/second_drive: special device /dev/sdb1/ does not exist (a path prefix is not a directory).
[analyst@sec0ps ~]$ ls -l
total 116
-rw-r--r-- 1 root root 5816 Apr 9 09:05 capture.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads
-rw-r--r-- 1 analyst analyst 78229 Apr 9 09:44 h
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 12061 Apr 9 09:41 -0
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
[analyst@sec0ps ~]$ ls -l second_drive/
total 0
[analyst@sec0ps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[analyst@sec0ps ~]$ ls -l second_drive/
total 20
drwx----- 2 root root 16384 Mar 26 2018 lost+found
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt
[analyst@sec0ps ~]$ 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: umount: command not found
[analyst@sec0ps ~]$ sudo umount /dev/sdb1
[analyst@sec0ps ~]$ ls -l second_drive/
total 0
```

PART 1:

EXPLORING FILESYSTEMS IN LINUX

- **CD ~:** CAMBIA LA DIRECTORY NELLA HOME DELL'UTENTE ATTUALE.
- **SUDO UOUNT /DEV/SDB1:** SIGNIFICA CHE STAI SMONTANDO LA PARTIZIONE /DEV/SDB1 DAL TUO SISTEMA, UTILIZZANDO I PRIVILEGI DI AMMINISTRATORE. QUESTO È UTILE QUANDO VUOI RIMUOVERE O MODIFICARE LA PARTIZIONE IN MODO SICURO.

Lab - Navigating the Linux Filesystem and Permission Settings

```
[analyst@sec0ps ~]$ cd lab.support.files/scripts/  
[analyst@sec0ps 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@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:  
[analyst@sec0ps scripts]$ cd ~/second_drive  
[analyst@sec0ps second_drive]$ ls -  
ls: cannot access '-': No such file or directory  
[analyst@sec0ps second_drive]$ ls -l  
total 20  
drwxr-xr-x 2 root root 16384 Mar 26 2018 lost+found  
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt  
[analyst@sec0ps second_drive]$ sudo chmod 665 myFile.txt  
[analyst@sec0ps second_drive]$ ls -l  
total 20  
drwxr-xr-x 2 root root 16384 Mar 26 2018 lost+found  
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt  
[analyst@sec0ps second_drive]$ sudo chown analyst myFile.txt
```

- **D LAB.SUPPORT.FILES/SCRIPTS/:** CAMBIA LA DIRECTORY CORRENTE NELLA DIRECTORY SCRIPTS, CHE SI TROVA ALL'INTERNO DELLA DIRECTORY LAB.SUPPORT.FILES.
- **TOUCH /MNT/MYNEWFILE.TXT:** CREA UN NUOVO FILE VUOTO CHIAMATO MYNEWFILE.TXT NELLA DIRECTORY /MNT/.
- **SUDO MOUNT /DEV/SDB1 ~/SECOND_DRIVE/:** MONTA LA PARTIZIONE /DEV/SDB1 NELLA DIRECTORY ~/SECOND_DRIVE/.
- **SUDO CHMOD 665 MYFILE.TXT:** MODIFICA I PERMESSI DEL FILE MYFILE.TXT PER CONSENTIRE LETTURA E SCRITTURA AL PROPRIETARIO E AL GRUPPO, E SOLO LETTURA AGLI ALTRI.
- **SUDO CHOWN ANALYST MYFILE.TXT:** CAMBIA IL PROPRIETARIO DEL FILE MYFILE.TXT A ANALYST.
- **ECHO TEST >> MYFILE.TXT:** AGGIUNGE LA PAROLA "TEST" ALLA FINE DEL FILE MYFILE.TXT.

```
[analyst@sec0ps second_drive]$ sudo chown analyst myFile.txt  
[analyst@sec0ps second_drive]$ ls -l  
total 20  
drwxr-xr-x 2 root root 16384 Mar 26 2018 lost+found  
-rw-r--r-- 1 analyst analyst 183 Mar 26 2018 myFile.txt  
[analyst@sec0ps second_drive]$ echo test >> myFile.txt  
[analyst@sec0ps second_drive]$ cat myFile.txt  
This is a file stored in the /dev/sdb1 disk.  
Notice that even though this file has been sitting in this disk for a while, it  
test  
[analyst@sec0ps second_drive]$ cd ~/lab.support.files/  
[analyst@sec0ps 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
```

Lab - Navigating the Linux Filesystem and Permission Settings

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ ls -l /dev/  
total 0  
crw-r--r-- 1 root root 10, 235 Apr 14 09:01 autofs  
drwxr-xr-x 2 root root 140 Apr 14 09:01 block  
drwxr-xr-x 2 root root 100 Apr 14 09:01 bsg  
crw----- 1 root root 10, 234 Apr 14 09:01 btrfs-control  
drwxr-xr-x 3 root root 60 Apr 14 09:01 bus  
lrwxrwxrwx 1 root root 3 Apr 14 09:01 cdrom -> sr0  
drwxr-xr-x 2 root root 2960 Apr 14 09:01 char  
crw----- 1 root root 5, 1 Apr 14 09:01 console  
lrwxrwxrwx 1 root root 11 Apr 14 09:01 core -> /proc/kcore  
crw----- 1 root root 10, 61 Apr 14 09:01 cpu-dma-latency  
crw----- 1 root root 10, 203 Apr 14 09:01 cuse  
drwxr-xr-x 6 root root 120 Apr 14 09:01 disk  
drwxr-xr-x 3 root root 100 Apr 14 09:01 dri  
crw-rw--- 1 root video 29, 0 Apr 14 09:01 fb0  
lrwxrwxrwx 1 root root 13 Apr 14 09:01 fd -> /proc/self/fd  
crw-rw-rw- 1 root root 1, 7 Apr 14 09:01 full  
crw-rw-rw- 1 root root 10, 229 Apr 14 09:01 fuse  
crw----- 1 root root 245, 0 Apr 14 09:01 hidraw0  
crw----- 1 root root 245, 1 Apr 14 09:01 hidraw1  
crw----- 1 root root 245, 2 Apr 14 09:01 hidraw2  
crw-rw--- 1 root audio 10, 228 Apr 14 09:01 hpet  
drwxr-xr-x 2 root root 0 Apr 14 09:01 hugepages  
crw----- 1 root root 10, 183 Apr 14 09:01 hwring  
lrwxrwxrwx 1 root root 25 Apr 14 09:01 initctl -> /run/systemd/initctl/fifo  
drwxr-xr-x 4 root root 260 Apr 14 09:01 input  
crw-r--r-- 1 root root 1, 11 Apr 14 09:01 kmsg  
drwxr-xr-x 2 root root 60 Apr 14 09:01 lightnvm  
  
[analyst@secOps ~]$ echo "symbolic" > file1.txt  
[analyst@secOps ~]$ cat file1.txt  
symbolic  
[analyst@secOps ~]$ echo "hard" > file2.txt  
[analyst@secOps ~]$ cat file2.txt  
hard  
[analyst@secOps ~]$ ln -s file1.txt file1symbolic  
[analyst@secOps ~]$ ln file2.txt file2hard  
[analyst@secOps ~]$ ls -l  
total 128  
-rw-r--r-- 1 root root 5816 Apr 9 09:05 capture.pcap  
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop  
drwxr-xr-x 3 analyst analyst 4096 Jan 31 05:11 Downloads  
lrwxrwxrwx 1 analyst analyst 9 Apr 14 09:50 file1symbolic -> file1.txt  
-rw-r--r-- 1 analyst analyst 9 Apr 14 09:49 file1.txt  
-rw-r--r-- 2 analyst analyst 6 Apr 14 09:50 file2hard  
-rw-r--r-- 2 analyst analyst 5 Apr 14 09:50 file2.txt  
-rw-r--r-- 1 analyst analyst 78229 Apr 9 09:44 h  
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files  
-rw-r--r-- 1 analyst analyst 12061 Apr 9 09:41 -0  
drwxr-xr-x 3 root root 4096 Mar 26 2018 second_drive  
[analyst@secOps ~]$ mv file1.txt file1new.txt  
[analyst@secOps ~]$ mv file2.txt file2new.txt  
[analyst@secOps ~]$ cat file1symbolic  
cat: file1symbolic: No such file or directory  
[analyst@secOps ~]$ cat file2hard  
hard
```

PART 3:

- **LS -L /DEV/**: VISUALIZZA I DISPOSITIVI NEL DIRECTORY /DEV/.
- **ECHO "SYMBOLIC" > FILE1.TXT**: CREA O SOVRASCRIVE FILE1.TXT CON IL TESTO "SYMBOLIC".
- **LN -S FILE1.TXT FILE1SYMBOLIC**: CREA UN LINK SIMBOLICO A FILE1.TXT.
- **LN FILE2.TXT FILE2HARD**: CREA UN LINK DURO A FILE2.TXT.

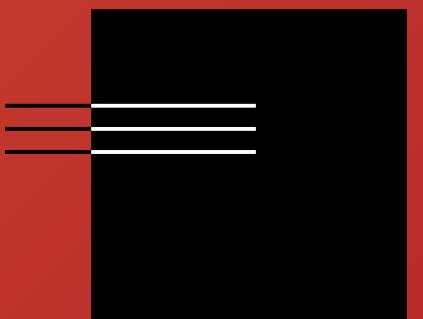
Relazione Tecnica - Analisi e Estrazione di Malware da File PCAP



ANALISI DEL TRAFFICO

PASSAGGI PRINCIPALI

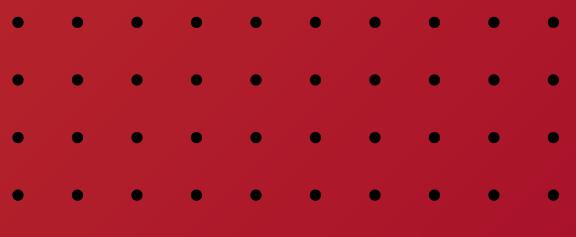
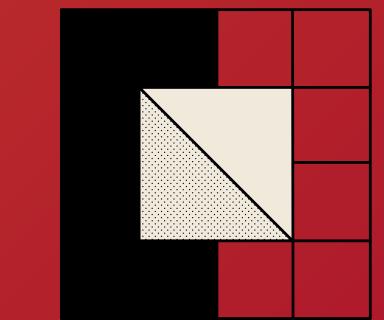
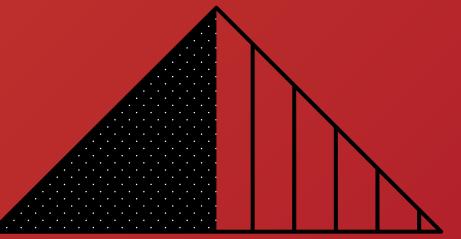
- ACCESSO ALLA DIRECTORY: CD /HOME/ANALYST/LAB.SUPPORT.FILES/PCAPS
- APERTURA DEL FILE CON WIRESHARK
- IDENTIFICAZIONE DELLA RICHIESTA HTTP GET TRA DUE IP
- VISUALIZZAZIONE DEL FLUSSO TCP COMPLETO (FOLLOW TCP STREAM)



INTERPRETAZIONE DEL FLUSSO

COSA SI OSSERVA NEL FLUSSO TCP:

- SIMBOLI STRANI → CONTENUTO BINARIO DEL FILE ESEGUITIBILE
- STRINGHE LEGGIBILI → FRASI O NOMI DI FUNZIONE NEL FILE
- IDENTITÀ DEL FILE: NON È UN MALWARE VERO, MA IL CMD.EXE DI WINDOWS (RINOMINATO)



The screenshot shows the Wireshark interface with the following details:

- Panels:** Top-left: Applications (pcaps - File Manager), Top-right: Terminal - analyst@secOps... (05:57).
Main: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help; Filter, Expression..., Clear, Apply, Save.
- Packet List:** nimda.download.pcap [Wireshark 2.5.1]. Shows 15 entries from 0.000000 to 0.004614. The 4th entry is highlighted in green, showing an HTTP GET request for "W32.Nimda.Amm.exe".
- Details:** Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 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: 0, Len: 0
- Bytes:** Hex dump of the captured data, showing the raw binary content of the frames.
- Stream Content:** Displays the raw hex and ASCII data of the captured session, showing the structure of the captured data, including the initial SYN and subsequent ACKs, and the HTTP GET request for "W32.Nimda.Amm.exe".
- Bottom Buttons:** Find, Save As, Print, ASCII, EBCDIC, Hex Dump, C Arrays, Raw, Help, Filter Out This Stream, Close.

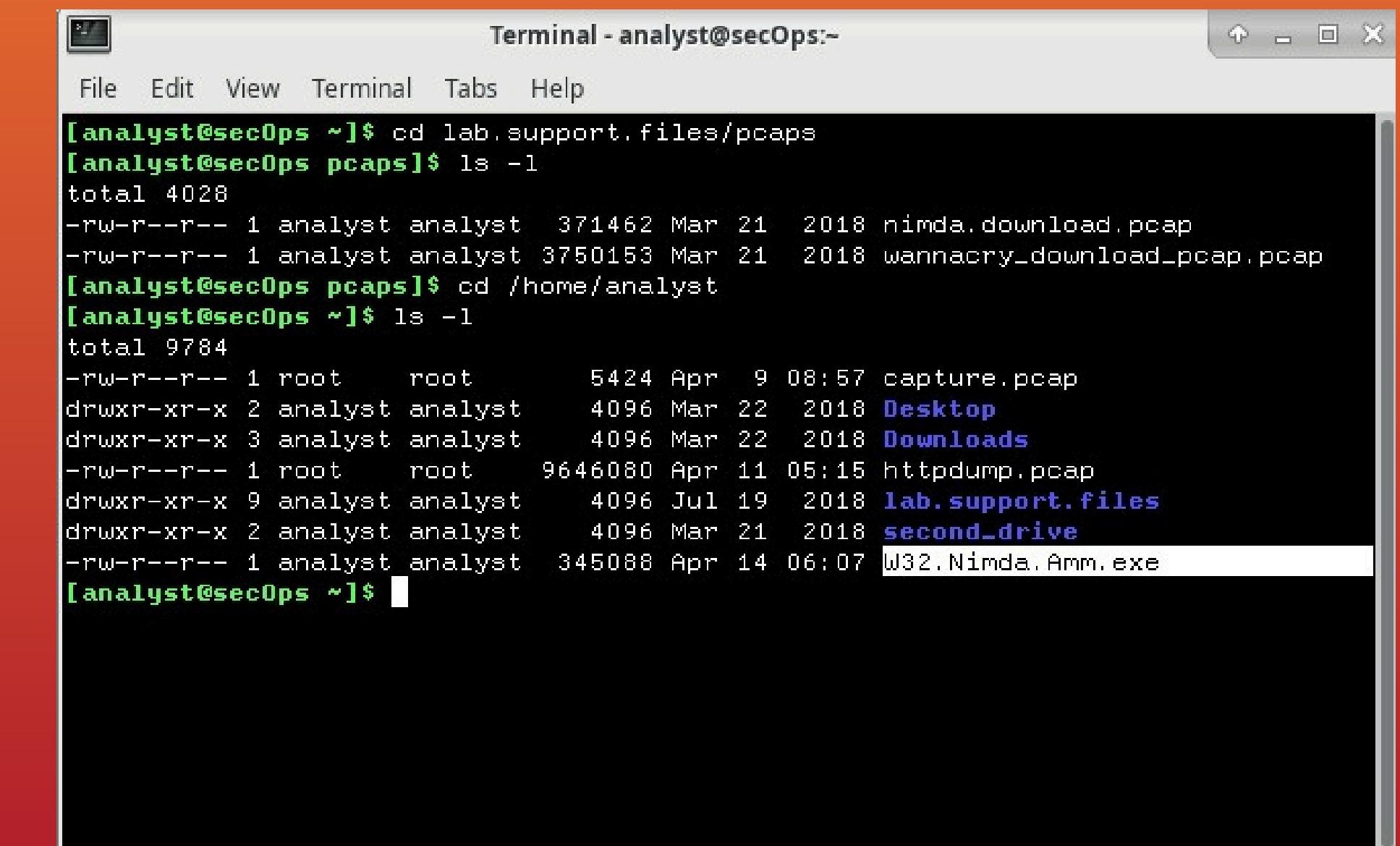
ESTRAZIONE DEL FILE

PROCEDURA:

- ESPORTAZIONE OGGETTO HTTP DAL PACCHETTO GET
- SALVATAGGIO FILE: NIMDA.AMM.EXE
- MOTIVO PER CUI C'È SOLO UN FILE: CATTURA LIMITATA AL SOLO DOWNLOAD
- VERIFICA TIPO FILE CON FILE W32.NIMDA.AMM.EXE
- RISULTATO: PE32+ EXECUTABLE FOR WINDOWS

CONCLUSIONI

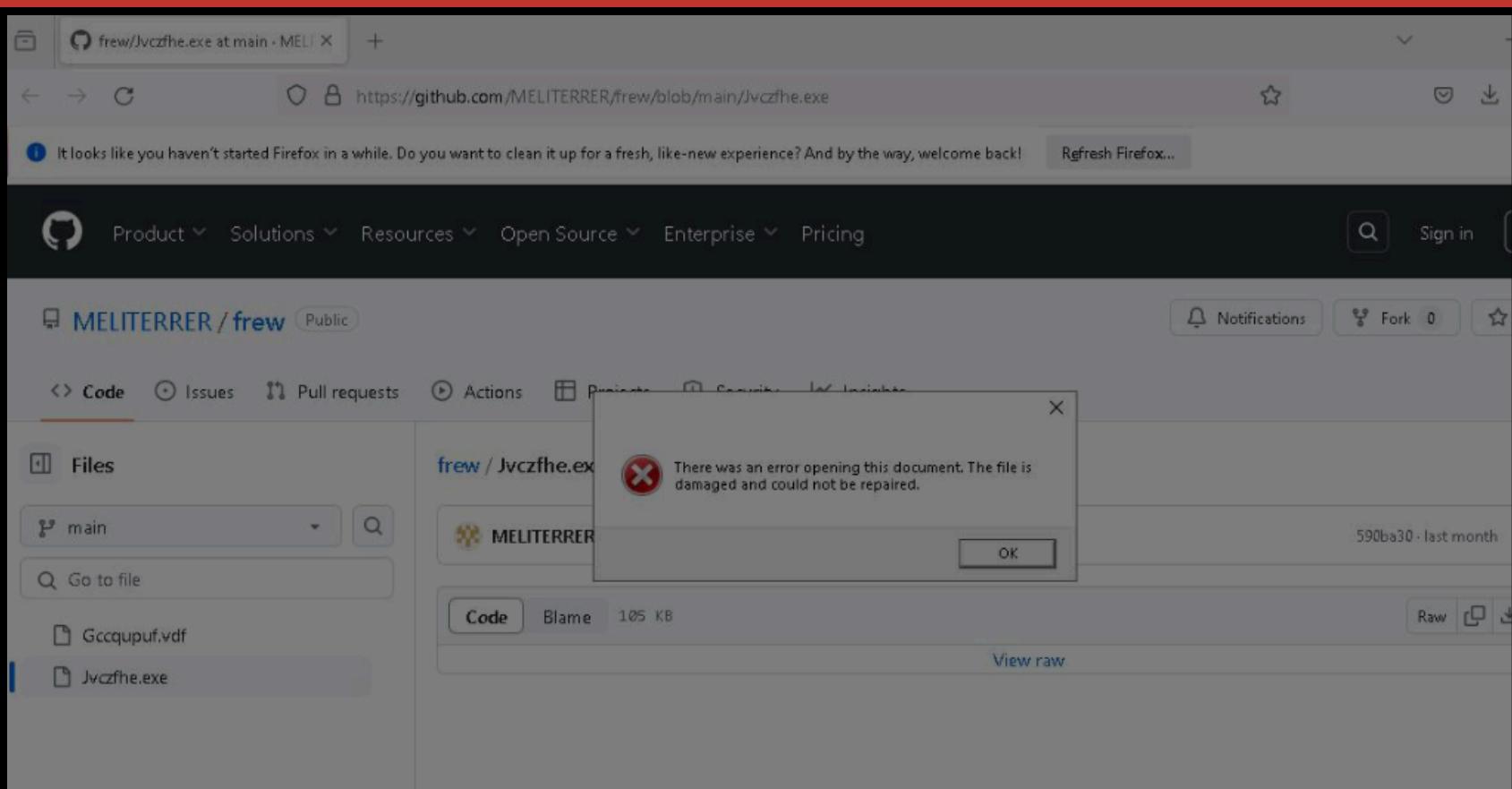
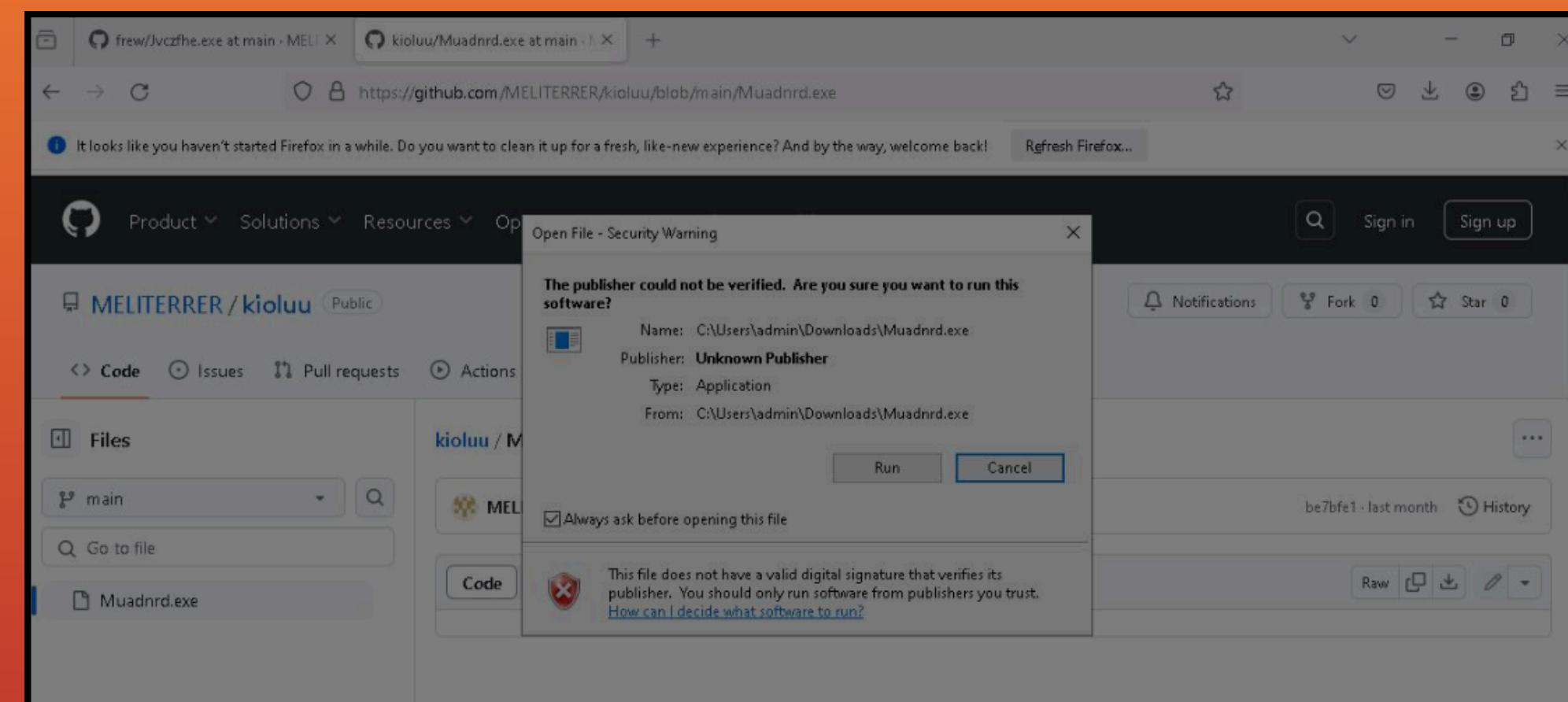
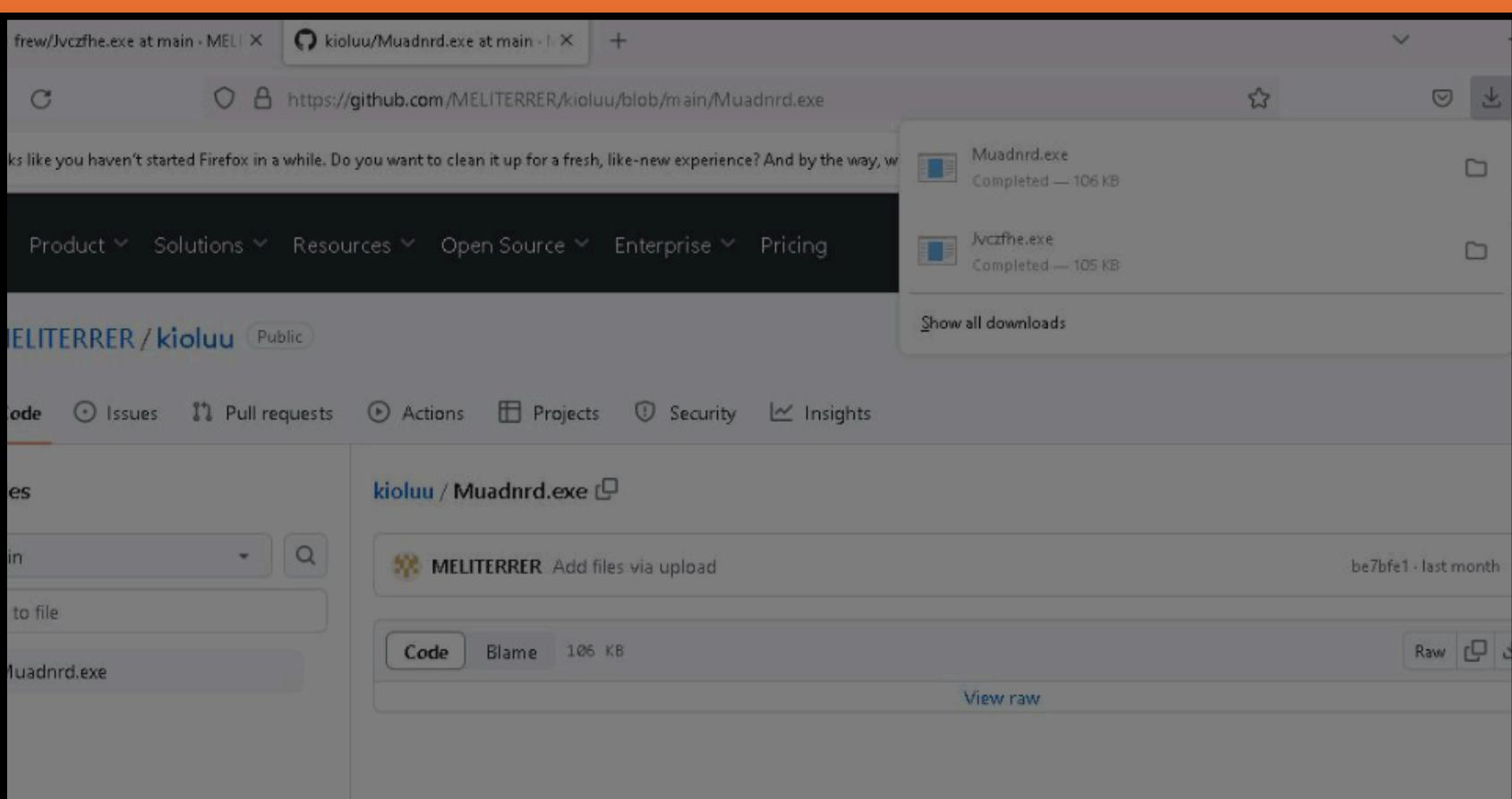
- IL LABORATORIO HA DIMOSTRATO COME:
- INTERCETTARE UN FILE DA UNA SESSIONE HTTP
- ANALIZZARE IL TRAFFICO A LIVELLO DI PACCHETTO
- RICOSTRUIRE UN FLUSSO TCP
- ESPORTARE E IDENTIFICARE UN FILE ESEGUIBILE
- COMPETENZE ACQUISITE UTILI PER ATTIVITÀ DI MALWARE ANALYSIS E INVESTIGAZIONE FORENSE.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The terminal is running on a Linux system. The user has navigated to the directory "/lab.support.files/pcaps" and run the command "ls -l" to list files. The output shows several files, including "nimda.download.pcap", "wannacry_download_pcap.pcap", and "W32.Nimda.Amm.exe". The file "W32.Nimda.Amm.exe" is highlighted with a red rectangle.

```
[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]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 9784
-rw-r--r-- 1 root root 5424 Apr  9 08:57 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 9646080 Apr 11 05:15 httpdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Apr 14 06:07 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

Bonus 1

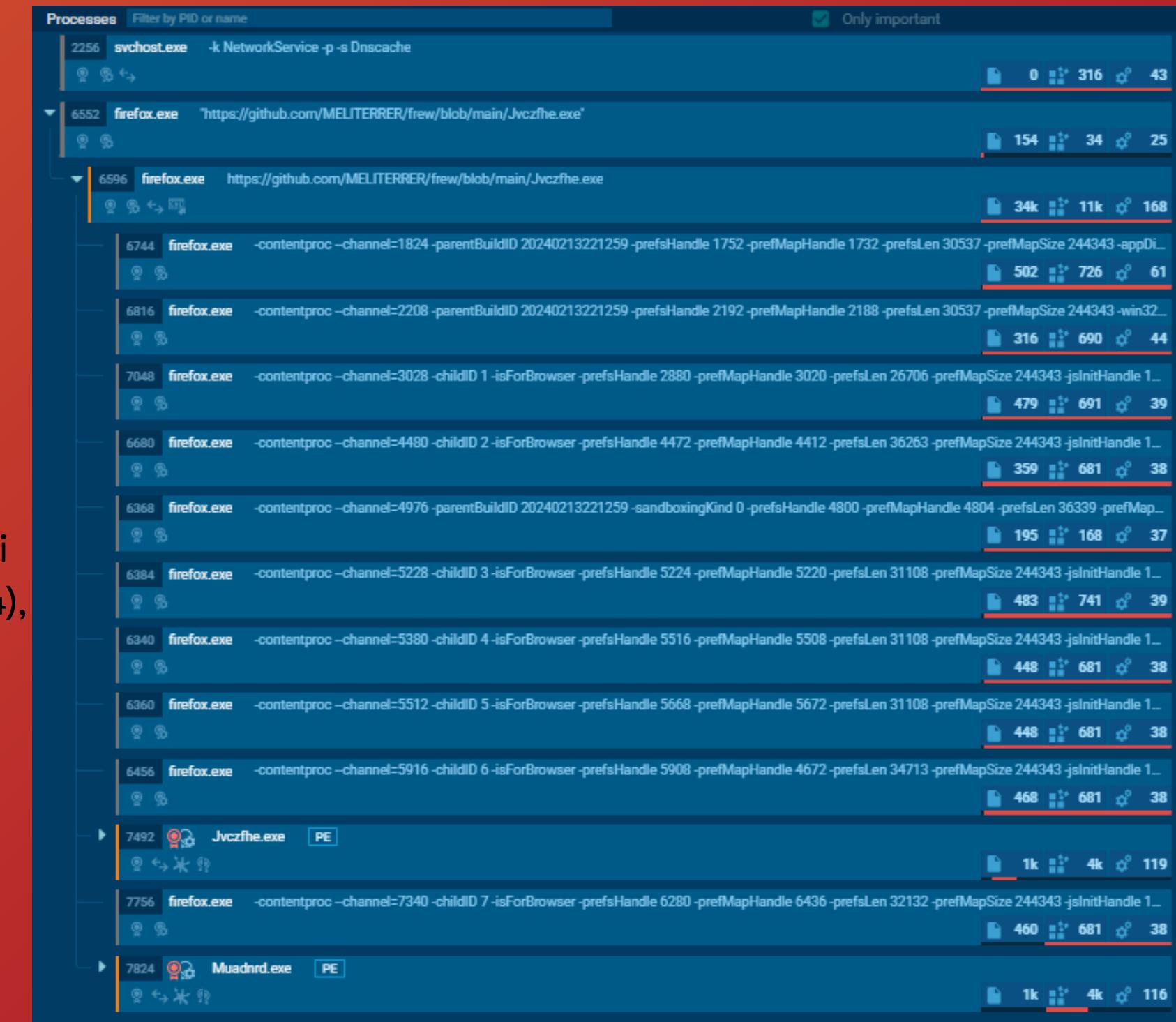


-Avvio di Firefox
-Inizio del malware
-Github
-Scaricamento automatico dei due malware
-Visualizzazione delle notifiche di sicurezza

Attività Comportamentali Sospette

L'analisi comportamentale del malware "Jvczfhe.exe" ha rivelato diverse attività sospette che indicano un comportamento potenzialmente dannoso:

- Processo rilascia un eseguibile Windows legittimo: firefox.exe (PID: 6596), suggerendo un tentativo di mascherare l'attività malevola
- Avvio di CMD.EXE per l'esecuzione di comandi: Jvczfhe.exe (PID: 7492) e Muadnrd.exe (PID: 7824), indicando l'esecuzione di comandi potenzialmente dannosi.
- Utilizzo di TIMEOUT.EXE per ritardare l'esecuzione: cmd.exe (PID: 7520) e cmd.exe (PID: 7876), suggerendo tecniche di evasione per sfuggire al rilevamento.
- Verifica delle impostazioni di attendibilità di Windows e lettura delle impostazioni di sicurezza di Internet Explorer: Jvczfhe.exe (PID: 7492) e Muadnrd.exe (PID: 7824), indicando un tentativo di manipolare le impostazioni di sicurezza.
- Esecuzione di applicazioni che si arrestano in modo anomalo: Jvczfhe.exe (PID: 7492) e Muadnrd.exe (PID: 7824), suggerendo instabilità o tecniche di offuscamento.
- Connessione a porte insolite: InstallUtil.exe (PID: 5152), indicando una potenziale comunicazione con server di comando e controllo (C2).
- Applicazione che si avvia autonomamente: Muadnrd.exe (PID: 7824), suggerendo persistenza sul sistema



Attività di Rete e Minacce Rilevate

L'analisi del traffico di rete ha rivelato diverse connessioni e richieste HTTP(S) che meritano attenzione:

- Richieste HTTP a detectportal.firefox.com: Utilizzate da Firefox per rilevare la connettività a Internet.
- Richieste POST a r11.o.lencr.org e r10.o.lencr.org: Probabilmente correlate alla validazione dei certificati Let's Encrypt.
- Richieste POST a o.pki.goog: Utilizzate per il recupero di certificati intermediari di Google.
- Richieste POST a ocsp.sectigo.com: Utilizzate per la verifica dello stato di revoca dei certificati (OCSP) di Sectigo
- Connessioni a github.com: Utilizzate per scaricare il file malevolo Jvczfhe.exe

HTTP requests

PID	Process	Method	HTTP Code	IP	URL
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/
6596	firefox.exe	POST	200	184.24.77.74:80	http://r11.o.lencr.org/
6596	firefox.exe	POST	200	172.64.149.23:80	http://ocsp.sectigo.com/
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2
6596	firefox.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2

ⓘ Download PCAP, analyze network streams, HTTP content and a lot more at the [full report](#) ↗

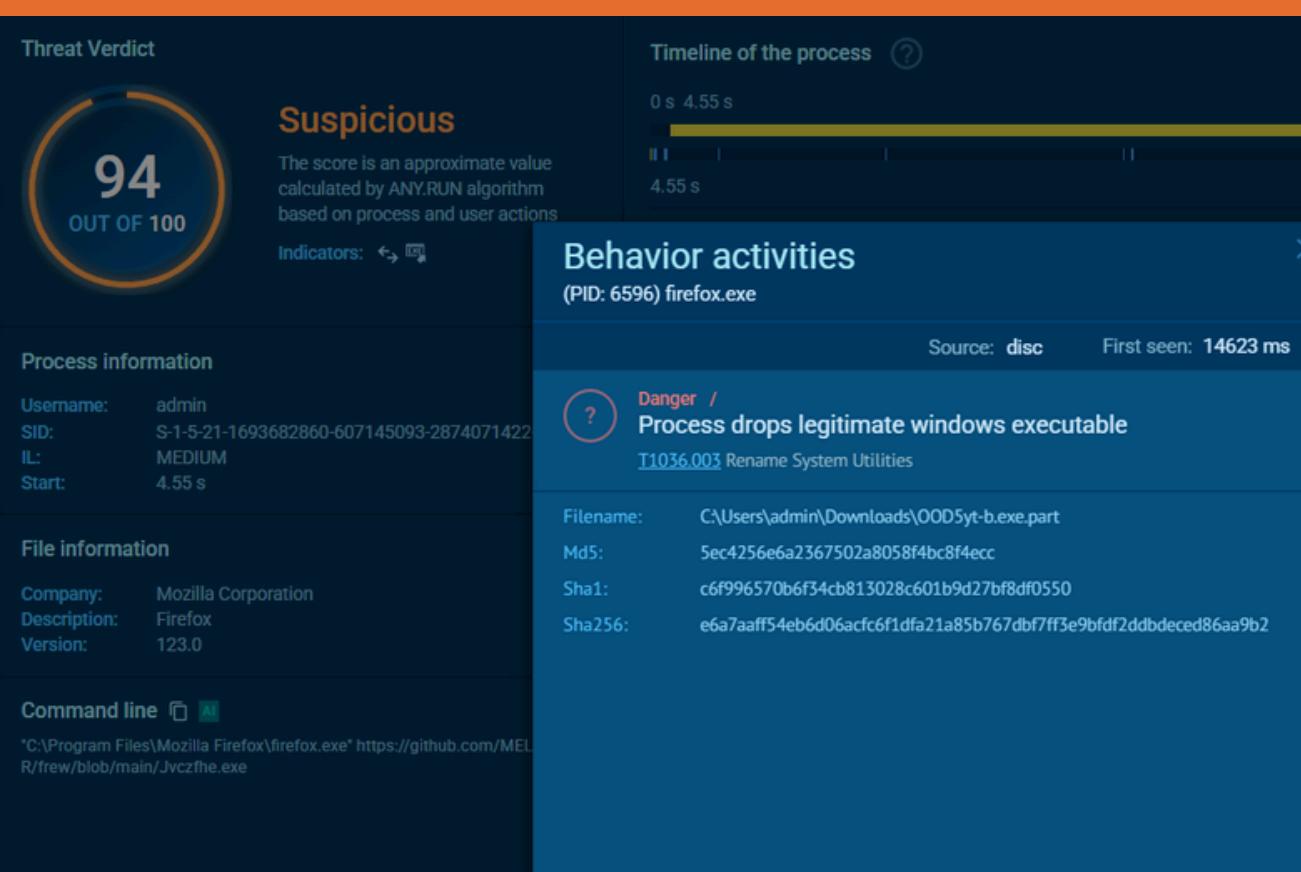
Attività del Registro di Sistema e dei File

L'attività del registro di sistema ha registrato un totale di 35.308 eventi, con una predominanza di eventi di lettura (35.167) rispetto a quelli di scrittura (140) e cancellazione (1). Tra gli eventi di modifica, si segnalano quelli relativi a Firefox, indicando una possibile manipolazione delle impostazioni del browser.

L'analisi dell'attività dei file ha rilevato 6 file eseguibili, 190 file sospetti, 40 file di testo e 5 tipi sconosciuti. Tra i file rilasciati, si segnalano quelli relativi a Firefox, indicando la possibile memorizzazione di dati nella cache o la modifica delle preferenze del browser.

Total events	Read events	Write events	Delete events
35 308	35 167	140	1
Modification events			
(PID) Process: (6552) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe\Launcher
			Value: 84B995F900000000
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe\Browser
			Value: 63DA97F900000000
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe\Progress
			Value: 0
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe\Progress
			Value: 1
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Installer\308046B0AF4A39CB	Operation: delete value	Name: installer.taskbarpin.win10.enabled
			Value:
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe\Telemetry
			Value: 0
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\DllPrefetchExperiment	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe
			Value: 0
(PID) Process: (6596) firefox.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings	Operation: write	Name: C:\Program Files\Mozilla Firefox\firefox.exe\Theme
			Value: 1

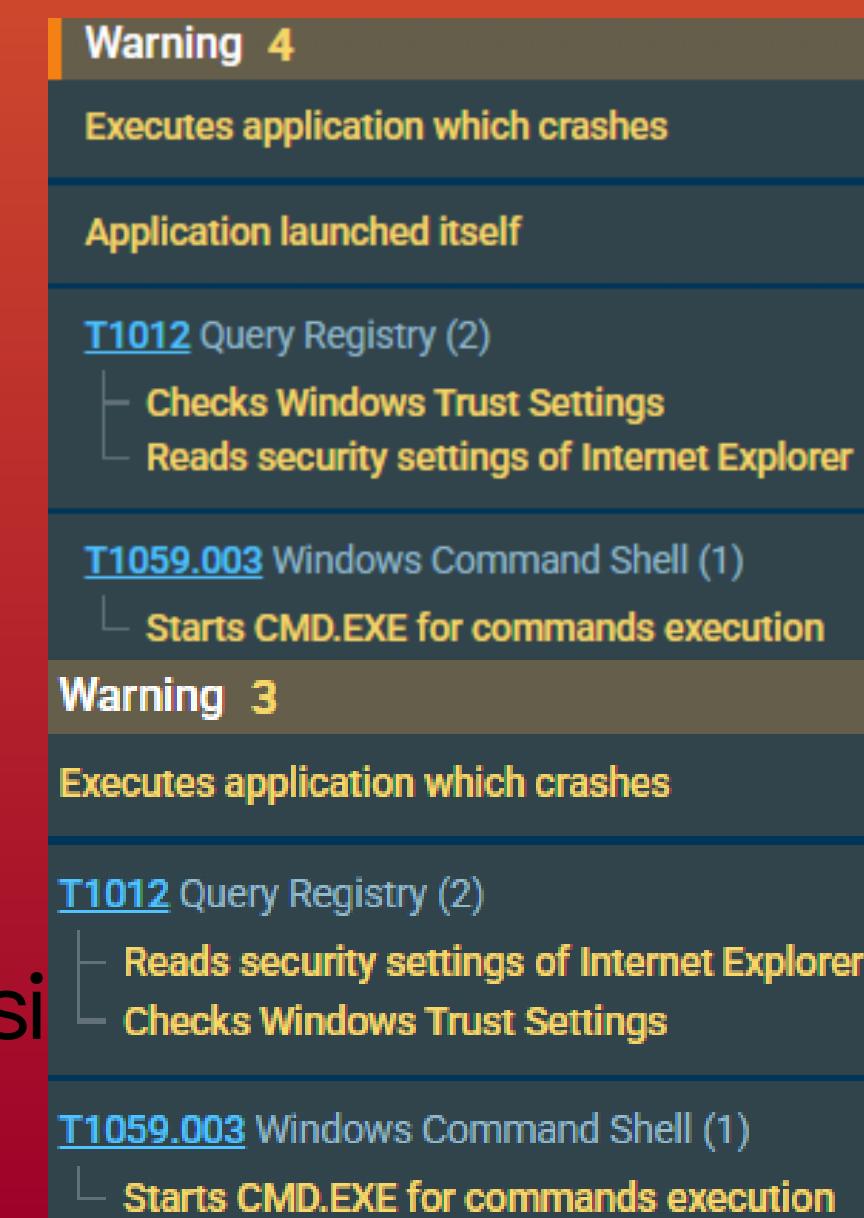
Analisi dei Processi



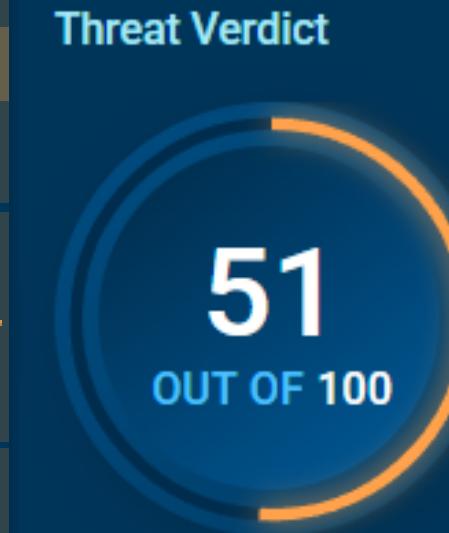
Warning 1
T1036.003 Rename System Utilities (1)
└ Process drops legitimate windows executable

Come vediamo dall'analisi a destra, vi sono altre due attività sospette, le quali sono i due malware installati automaticamente, entrambi seguite dalle rispettive notifiche si attenzione

Dopo un'attenta analisi, abbiamo notato il primo processo firefox con un'attività sospetta del 94 su 100, inoltre viene data anche una notifica in questa schermata in cui viene esplicitamente detto che il processo è un eseguibile di Windows



Suspicious
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators: ↗ *



Suspicious
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators: ↗ *

Analisi dei Processi

46 / 72
Community Score

46 security vendors flagged this file as malicious

File Hash: SHA256: 00
Jvczfhe.exe

Size: 104.05 KB | Last Analysis Date: 1 month ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Popular threat label: trojan-msil/injoke

Threat categories: trojan

Family labels: null, jalapeño, injoke

Security vendor's analysis (46)

Vendor	Detection	Family
Alibaba	Trojan-MSIL/Injoke.DhMildci	AIYac
Arcabit	Trojan-Jalapeño.D459G	Asust
AVG	Win32-PWSX-gen [Tr]	Avira [no cloud]
BitDefender	Gen:Variant:jalapeño.17798	Bitn Pro
CrowdStrike Falcon	Minymalicious_confidence_100% (M)	CTI
Cylance	Unsafe	Deepinfect
Elastic	Malicious (high confidence)	Elastic
eScan	Gen:Variant:jalapeño.17798	ESET-NOD32
Fortinet	MSIL/Kryptik.ALT10	Forti
Google	Detected	Ikarus
K7AntiVirus	Trojan (002beb291)	K7GW
Kaspersky	HEUR:Trojan-MSIL-HTA.gen	Kingssoft
Lionic	Trojan-Win32.Injoke.MKz	Malwarebytes
McAfee	Trojan-Malware-384903-origen	McAfee Scanner
Microsoft	Trojan-MSIL/Injoke.SEAUMT0	Palo Alto Networks
Panda	TryGoGoku4	QuickHeal
Rising	Trojan-Kryptik.BB (CLOUD)	Sangfor Engine Zero
SecureAge	Malicious	SentinelOne (Static ML)
Sophos	Mal/Generic-3	Symantec
Tencent	Malware:Win32-Gencirc.11pc280	Trend (TNS)
Trellix (XDR)	Gen:Variant:jalapeño.17798	Vardec
VBA32	Downloaded MSIL/PureCryptor.Mal	WIPRE
WishSecure	Trojan-TR/Kryptik.cba	Zillya

Riportando l'hash del processo iniziale in cui abbiamo un'attività sospetta di 94 su 100, siamo riusciti a capire che il malware installato è un trojan, riportandolo su VirusTotal, viene mostrato che sulla community 46 fornitori di sicurezza su 72 contrassegnano questo file come malevole

Conclusioni

L'analisi del malware "Jvczfhe.exe" tramite ANY.RUN ha rivelato un comportamento sospetto e potenzialmente dannoso. Il campione esaminato presenta caratteristiche tipiche di malware progettato per eludere il rilevamento, manipolare le impostazioni di sicurezza e stabilire persistenza sul sistema.

Si raccomanda di intraprendere le seguenti azioni:

Isolare il sistema infetto: Per prevenire l'ulteriore diffusione del malware.

- Eseguire una scansione completa del sistema: Utilizzando un software antivirus aggiornato per rilevare ed eliminare eventuali file malevoli.
- Monitorare l'attività di rete: Per identificare eventuali comunicazioni con server di comando e controllo (C2).
- Analizzare ulteriormente il malware: Per comprendere appieno le sue capacità e sviluppare contromisure efficaci.

Introduzione all'analisi

Durante questo laboratorio abbiamo analizzato un attacco informatico simulato con due tecniche principali: la **SQL Injection** e la esfiltrazione di dati tramite DNS.

L'indagine è stata condotta all'interno della piattaforma Security Onion, utilizzando Kibana per visualizzare e interpretare il traffico di rete.

L'obiettivo era identificare l'attività malevola e isolare l'attore della minaccia, analizzando i dati raccolti tramite i protocolli **HTTP** e **DNS**.

Bonus 2

Attacco SQL Injection

L'attacco inizia con una vulnerabilità su un'applicazione web che permette a un attore esterno di eseguire una **SQL Injection**.

In particolare, l'attaccante utilizza una richiesta **HTTP** con la clausola **UNION SELECT**, che consente di accedere a tavelli contenenti dati sensibili.

Attraverso l'analisi dei log **HTTP** in Kibana, si nota la trasmissione di numeri di carte di credito, CVV e date di scadenza, esfiltrati nella risposta del server.

Questo dimostra quanto sia pericolosa la mancanza di validazione dell'input lato server.

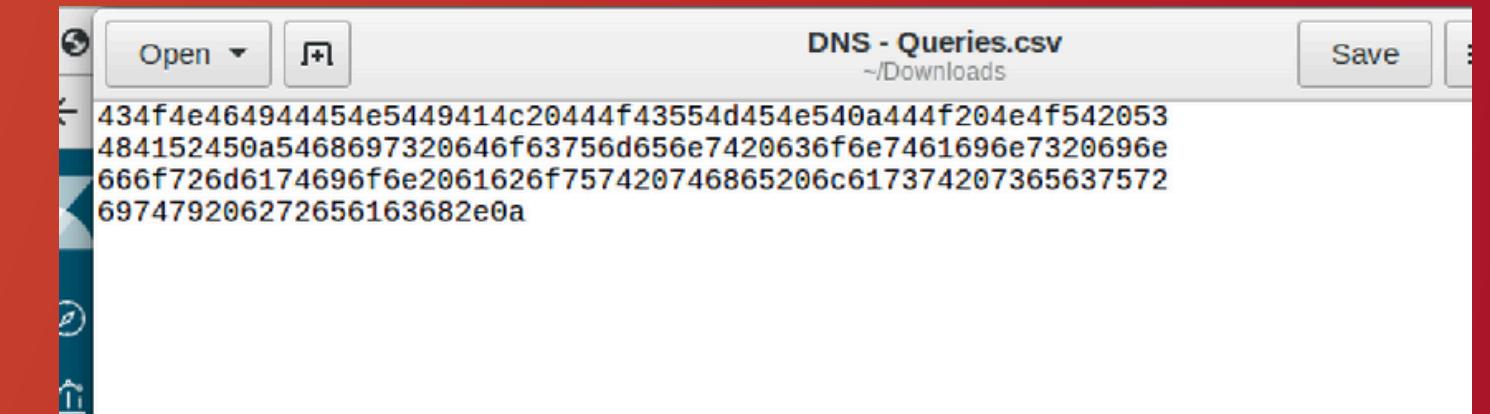
```
{"ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfqDd", "id.orig_h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "id.resp_p": 80, "trans_depth": 1, "method": "GET", "host": "209.165.200.235", "uri": "/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards++&password=&user-info-php-submit-button=View+Account+Details", "referrer": "http://209.165.200.235/mutillidae/index.php?page=user-info.php", "version": "1.1", "user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "request_body_len": 0, "response_body_len": 23665, "status_code": 200, "status_msg": "OK", "tags": ["HTTP::URI_SQLI"], "resp_fuids": ["FEvWs63Hqvcqth3LH1"], "resp_mime_types": ["text/html"]}
```

```
DST: 24
DST: <b>Username=</b>4444111122223333<br>
DST: 24
DST: <b>Password=</b>745<br>
DST: 22
DST: <b>Signature=</b>2012-03-01<br><p>
DST: 24
DST: <b>Username=</b>7746536337776330<br>
DST: 17
DST: <b>Password=</b>722<br>
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST: 24
DST: <b>Username=</b>8242325748474749<br>
DST: 17
DST: <b>Password=</b>461<br>
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST: 24
DST: <b>Username=</b>7725653200487633<br>
DST: 17
DST: <b>Password=</b>230<br>
DST: 22
DST: <b>Signature=</b>2017-06-01<br><p>
DST: 24
DST: <b>Username=</b>1234567812345678<br>
DST: 17
DST: <b>Password=</b>627<br>
```

Esfiltrazione dati via DNS

Dopo aver acquisito i dati, l'attaccante sfrutta il protocollo DNS per esfiltrarli:

- Il client compromesso (IP 192.168.0.11) invia una serie di richieste DNS verso un server esterno controllato dall'attaccante (IP 209.165.200.235).
- I nomi di dominio nelle richieste contengono stringhe molto lunghe in esadecimale, che rappresentano i dati rubati.
- Tramite strumenti come xxd, è possibile ricostruire il contenuto originale dei dati esfiltrati.
- Questa tecnica evidenzia come anche protocolli apparentemente innocui, come DNS, possano essere usati per attività malevole se non adeguatamente monitorati.



```
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~/Downloads$
```

Tips & Tricks per la difesa

- 🔎 È fondamentale registrare tutti i log, anche quelli relativi a protocolli apparentemente innocui come HTTP e DNS
- 🏭 Ogni input proveniente dall'utente deve essere rigorosamente validato, per evitare query SQL non controllate
- 💡 È utile saper riconoscere pattern sospetti, come l'uso di UNION SELECT o richieste DNS con nomi molto lunghi e codificati
- 👓 Una corretta analisi deve correlare eventi su protocolli diversi: un attacco può iniziare su HTTP e proseguire via DNS
- 🔍 Si consiglia di configurare alert per anomalie DNS, ad esempio in base alla frequenza o alla lunghezza delle query
- 🛡️ La segmentazione della rete riduce la superficie di attacco e isola eventuali compromissioni
- 🛡️ L'uso di strumenti come Kibana, Zeek e Suricata consente di automatizzare e velocizzare l'analisi
- 💡 È importante non sottovalutare protocolli considerati "sicuri": anche il DNS può essere usato per esfiltrare dati

Bonus 3 Lab - Isolate Compromised Host Using 5-Tuple

- Obiettivi del laboratorio:

Analizzare i log di rete per identificare un attacco informatico.

Utilizzare il metodo delle 5 tuple per isolare l'host compromesso.

Esaminare l'esfiltrazione di un file sensibile.

- Strumenti utilizzati:

Security Onion (VM)

Sguil

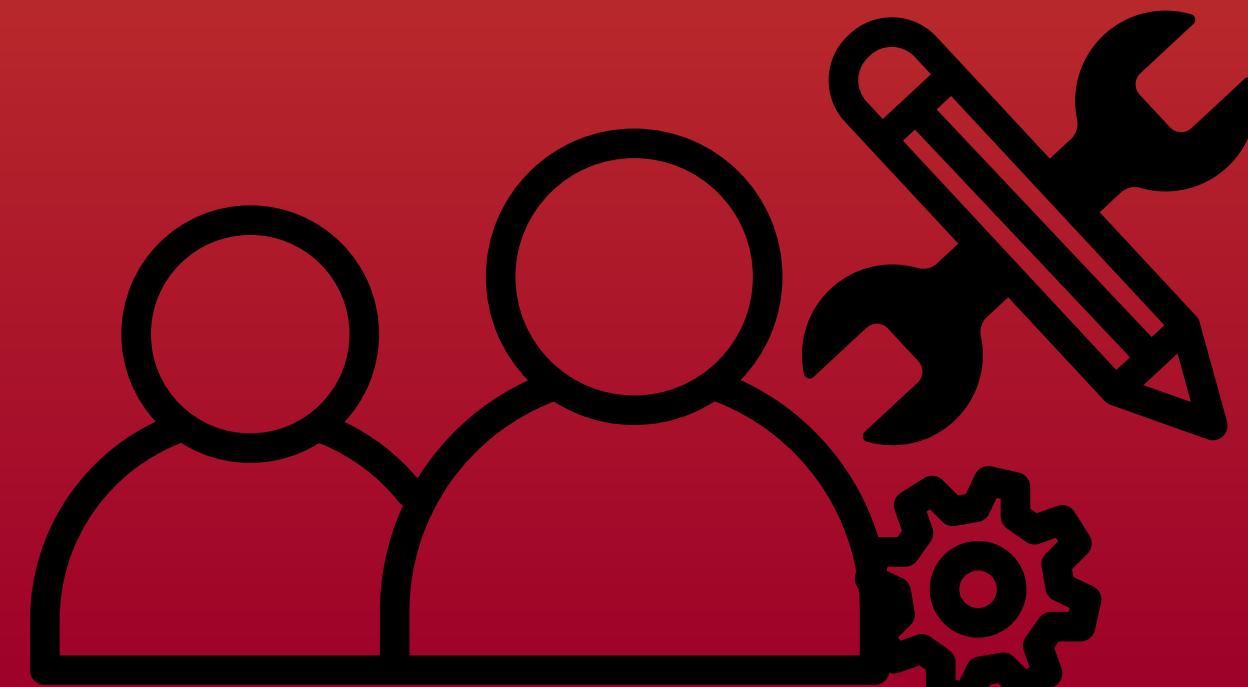
Wireshark

Kibana



Analisi degli Alert in Sguil

- Accesso a Sguil:
Login con utente: analyst, password: cyberops.
- Identificazione dell'alert:
Messaggio: GPLATTACK_RESPONSE id check returned root.
Indica che l'host 209.165.200.235 ha restituito accesso root a 209.165.201.17.
- Analisi del transcript:
L'attaccante ha eseguito comandi Linux sul target, come:
whoami, cat /etc/passwd, cat /root/confidential.txt.
Conferma dell'accesso root da parte dell'attaccante.



Sguil.tk

Tue 08:04

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2025-04-15 08:04:35 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
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 Fro...
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 Lik...
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 Win...
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 ...
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 SS...
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 i...
RT	351	seconion...	1.1	2020-06-19 18:09:28	0.0.0.0				0	[OSSEC] File added to the s...
RT	23	seconion...	1.2	2020-06-19 18:09:29	0.0.0.0				0	[OSSEC] Integrity checksum...
RT	7	seconion...	1.4	2020-06-19 18:10:04	0.0.0.0				0	[OSSEC] New group added t...
RT	7	seconion...	1.5	2020-06-19 18:10:04	0.0.0.0				0	[OSSEC] New user added to ...
RT	2	seconion...	1.18	2020-06-19 18:14:41	0.0.0.0				0	[OSSEC] Listened ports stat...
RT	1	seconion...	1.19	2020-06-19 18:18:41	0.0.0.0				0	[OSSEC] Received 0 packet...

IP Resolution Agent Status Snort Statistics System Msg

Show Packet Data Show Rule

Reverse DNS Enable External DNS

Src IP: Src Name: Dst IP: Dst Name:

Whois Query: None Src IP Dst IP

IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum

TCP Source Dest R R C S S Y I Port Port 1 0 G K H T N N Seq # Ack # Offset Res Window U rp ChkSum

DATA

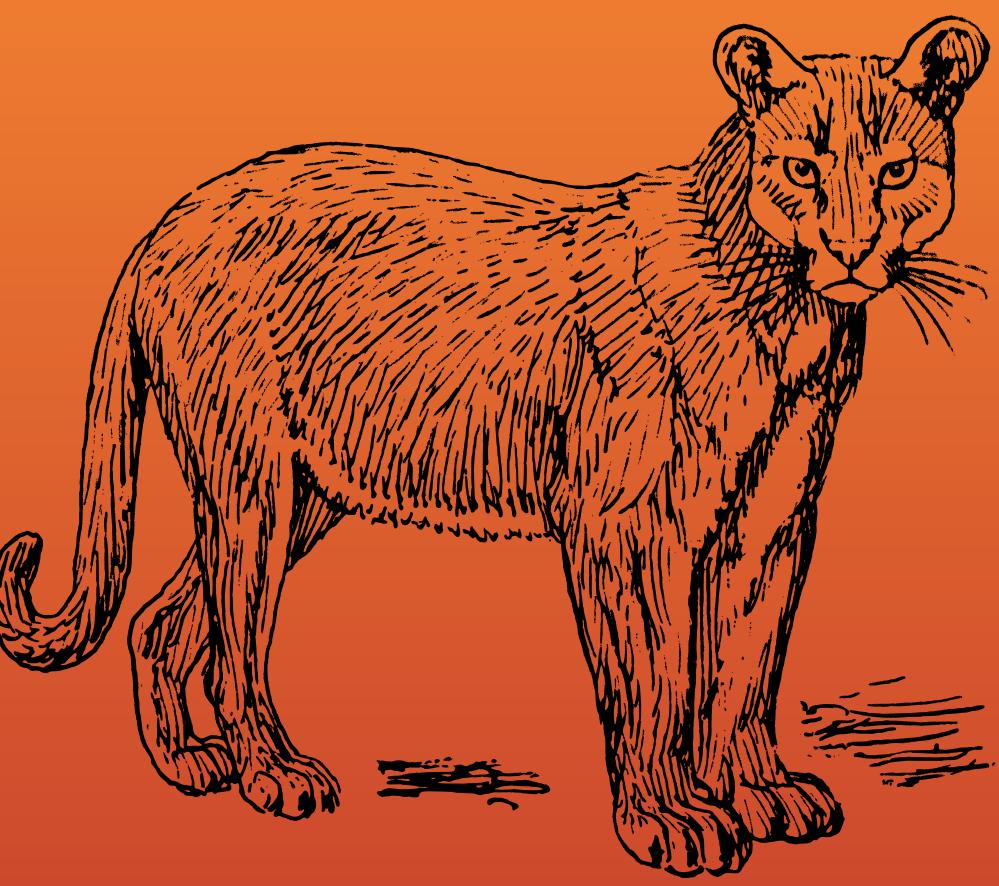
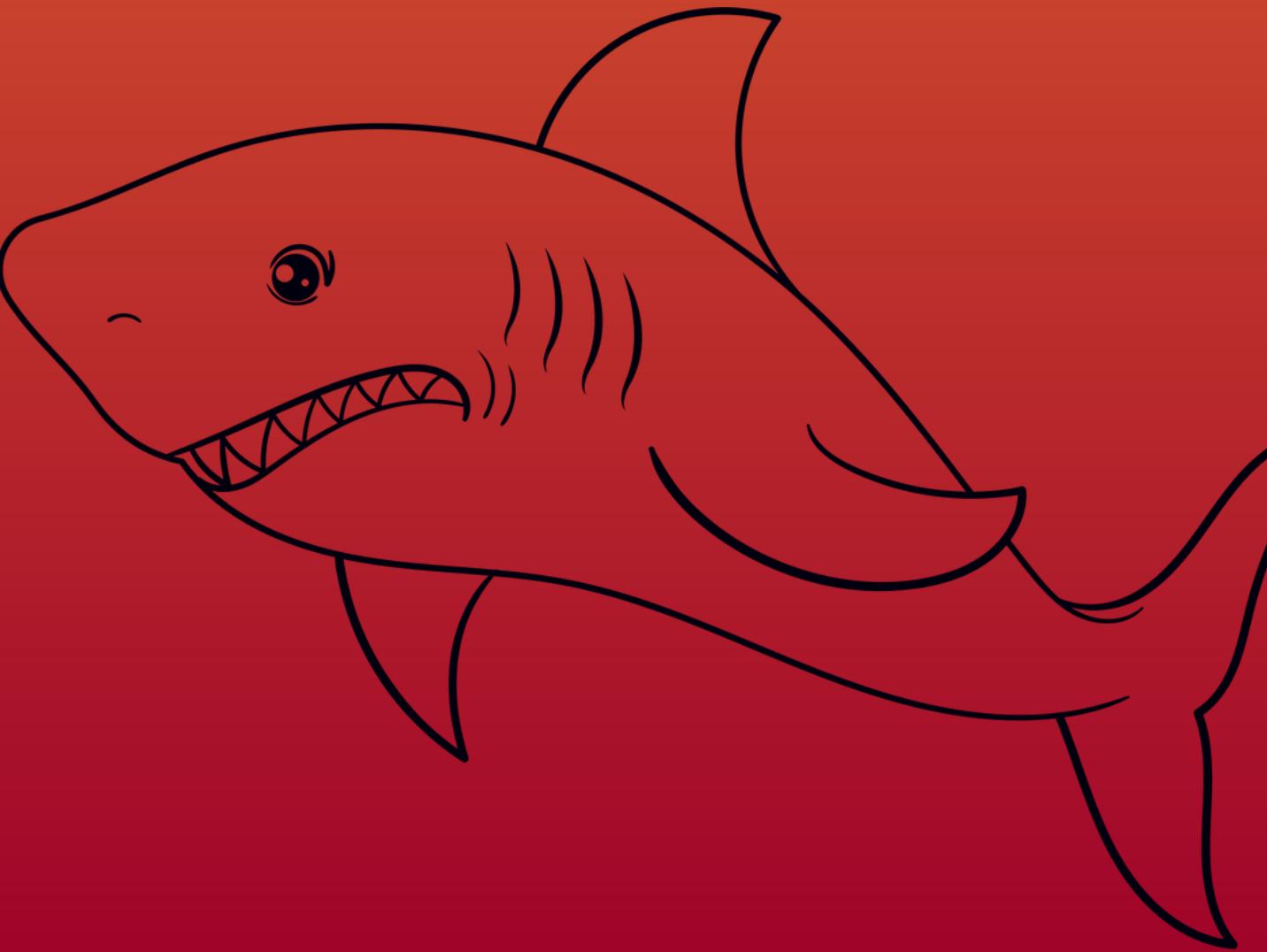
Search Packet Payload Hex Text NoCase

SGUIL-0.9.0 - Connected To localhost

1 / 4

Esame del Traffico con Wireshark

- Analisi del flusso TCP:
Visualizzazione delle comunicazioni tra attaccante (rosso) e target (blu).
L'attaccante ha eseguito comandi per accedere a informazioni sensibili.
- Osservazioni:
L'attaccante ha letto file contenenti informazioni sugli account utente.
Conferma dell'accesso completo al sistema da parte dell'attaccante.

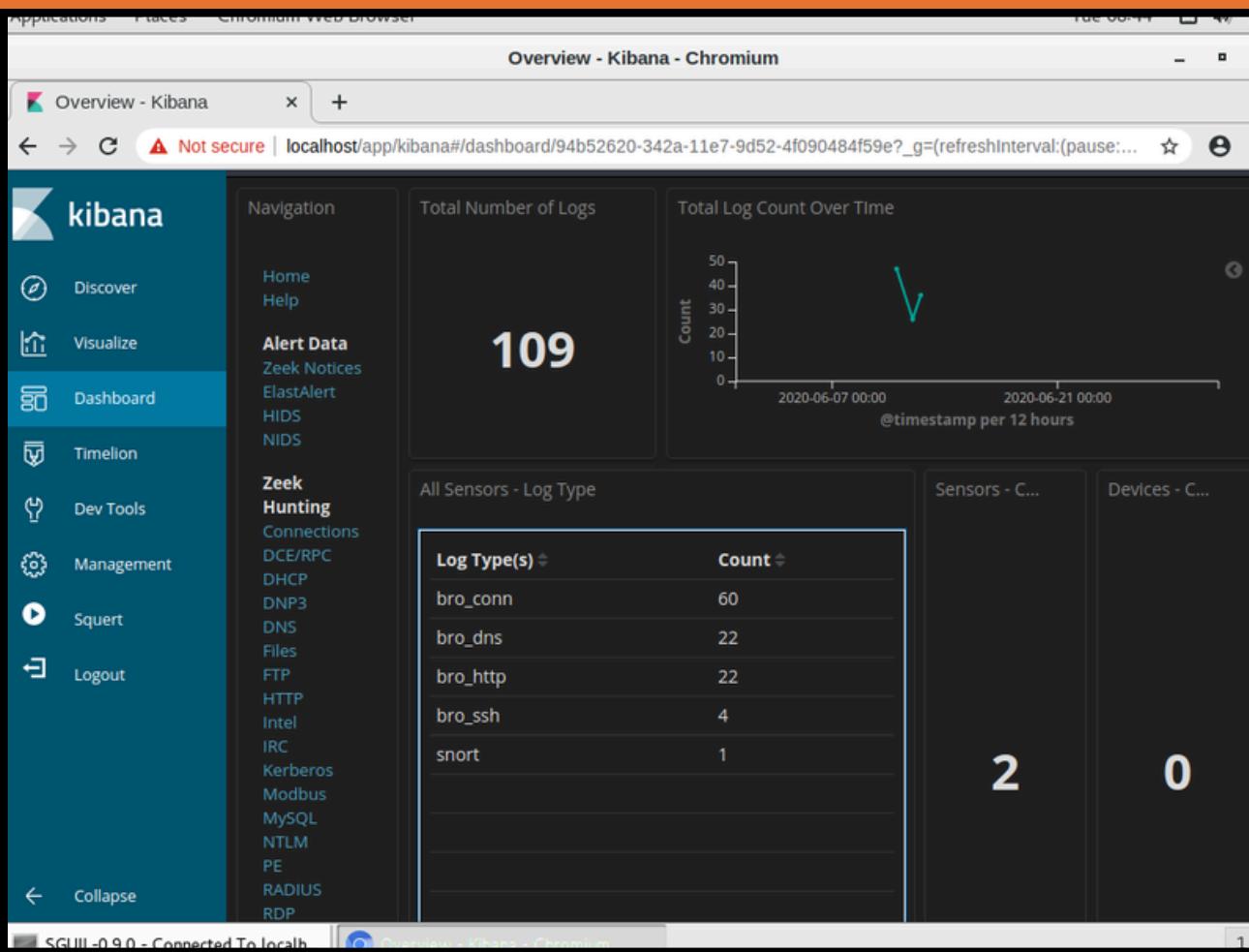


```
Tue 08:16 Applications Places Wireshark
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17_45415_209.165.200.235_6200-6.raw

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:255.255.255.252
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
eth0
10 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:$1$avpfBJ1$x0z8w5UF9IV./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX6BPot$MiyC3Up0zQJqz4s5wFD910:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7...
14 client pkts, 11 server pkts, 20 turns.

Entire conversation (4,388 bytes) Show and save data as ASCII
Find: 209.165.200.235
Filter Out This Stream Print Save as... Back Close Find Next
SGUIL-0.9.0 - Connected To localhost 209.165.201.17_45415_209.165... Wireshark · Follow TCP Stream [tc...
1 / 4
```

Investigazione con Kibana



- Analisi del traffico FTP:
Fonte: 192.168.0.11:52776
Destinazione: 209.165.200.235:21
File trasferito: confidential.txt
- Contenuto del file:
"CONFIDENTIAL DOCUMENT DO NOT SHARE. This document contains information about the last security breach."

The screenshot shows the Kibana Discover interface. A log entry is selected: @timestamp: June 11th 2020, 03:53:09.086, @version: 1, _id: LTjrzXIBB6Cd-_0SbfgO (circled in red), _index: seconion:logstash-import-2020.06.11, _score: -. The right side shows the log fields: @timestamp, @version, _id, _index, and _score.

- Raccomandazioni:
Cambiare la password dell'utente analyst su tutti i sistemi.
Implementare misure di sicurezza per prevenire accessi non autorizzati futuri.

Syslog Tunnels Weird X.509 Host Hunting Autoruns Beats OSSEC	Source	Count	Bytes Seen
	HTTP	22	99.685KB
	FTP_DATA	1	70.19KB
		Filter for value	55.912KB
			50.438KB

GRAZIE PER
AVER GIOCATO!

Si

No