COrtana Security

PROGETTO SETTIMANALE

S9/L5

Presented by: Gabriele Arcelli, Giammarco Iorio, Stefano Cesaroni & Valerio Zampone

GIORNO 1

Nell’esercizio di oggi vedremo come la presenza di un firewall riesca ad impattare considerevolmente sulla sicurezza di un sistema operativo. In effetti, nonostante Windows XP sia un sistema operativo piuttosto obsoleto in termini di sicurezza, la presenza di un firewall riesce comunque a limitare le azioni che un dispositivo può compiere da remoto sulla macchina e quindi ne aumenta sensibilmente la sicurezza.

OGGETTO: Ingaggio da parte del Sig. Rossi per la messa in sicurezza rete aziendale

Il Sig. Rossi si è rivolto alla nostra azienda, la “C0rtana Security” per valutare la sicurezza della propria rete aziendale.
Il primo step sarà quello di mettere in evidenza l’importanza di un firewall, pertanto verrà mostrata la risposta del dispositivo del sig. Rossi con e senza firewall.
Il dispositivo utilizza la versione di windows XP, e perciò non risulta essere propriamente aggiornato.

FIREWALL DISATTIVATO

Abbiamo configurato gli IP delle macchine secondo quanto segue:
Kali Linux : 192.168.240.100/24
Windows XP: 192.168.240.150/24
Effettueremo dei test sulla macchina windows XP con nmap prima con il firewall disattivato e poi con il firewall attivato per mettere in evidenza le implementazioni che in firewall apporta in termini di sicurezza.

```
┌──(kali㉿kali)-[~]
└─$ ping  192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.736 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.677 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.395 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.457 ms
^C
── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.395/0.566/0.736/0.143 ms
```

Dalla macchina di Kali effettuiamo prima un ping per assicurarci che le macchine comunichino tra loro.

Dalla macchina di Kali effettuiamo prima una scansione dei servizi e delle relative versioni con il comando di nmap “-sV”.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:29 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o
:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.99 seconds
```

Possiamo notare che nmap ha trovato 3 porte aperte con i rispettivi servizi e versioni.

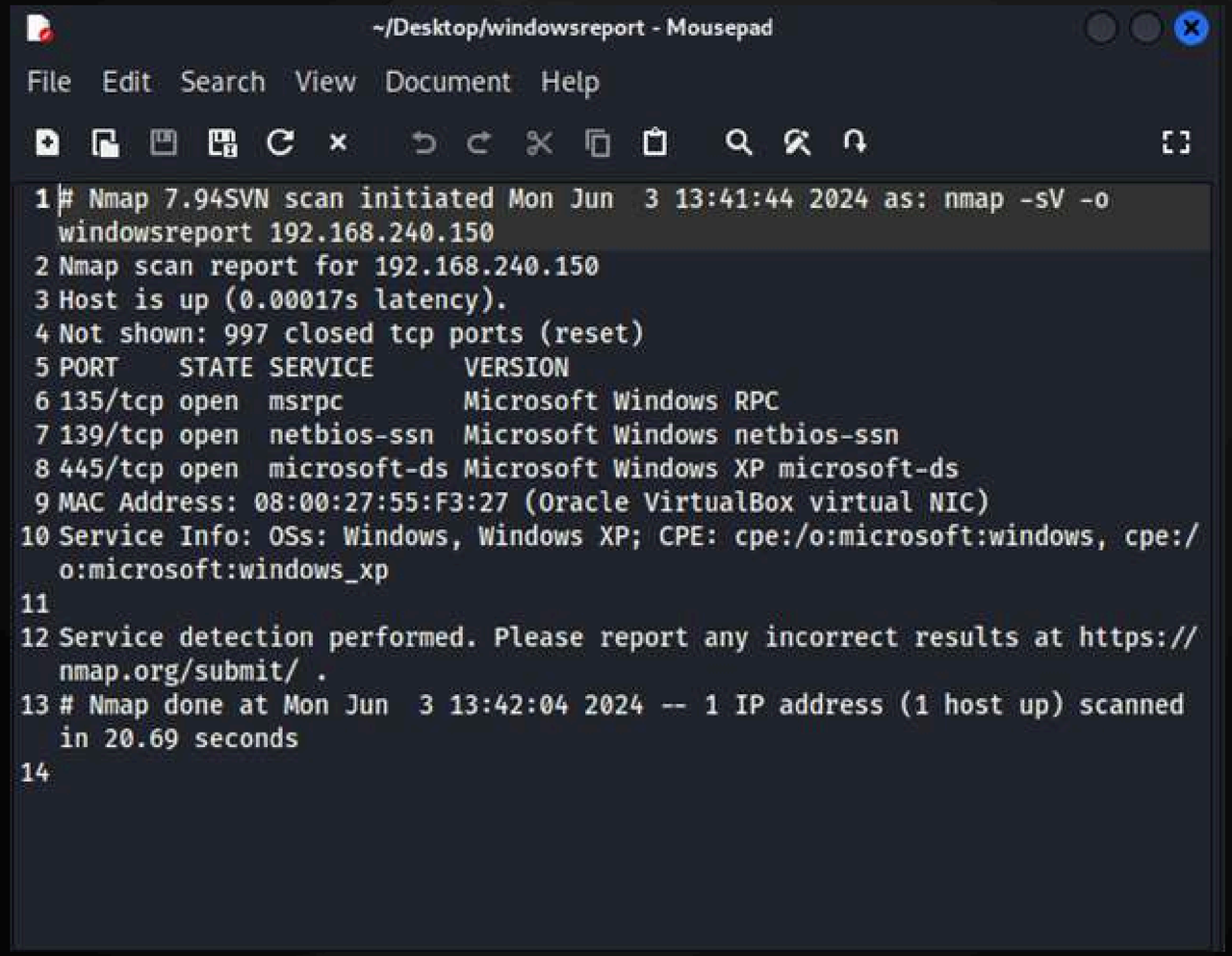
Porta 135 (msrpc): Utilizzata per le chiamate di procedura remota di Microsoft (RPC). È una porta critica per le funzionalità di rete di Windows e può essere un vettore di attacco se non adeguatamente protetta.

Porta 139 (netbios-ssn): Utilizzata dal servizio NetBIOS per sessioni di rete su TCP/IP. Tipicamente usata per condivisioni di file e stampanti.

Porta 445 (microsoft-ds): Utilizzata per la condivisione di file e stampanti tramite SMB (Server Message Block) su TCP/IP. Sostituisce la funzionalità del NetBIOS sulle reti più moderne.

Possiamo salvare direttamente i risultati ottenuti in un file di testo che chiameremo “windowsreport”; dopodichè ci spostiamo nella directory dove è contenuto il file di testo, apriamo il terminale (come root) e aggiungiamo alla scansione precedente il comando “-o” seguito dal nome del file di testo.

I risultati verranno inseriti e salvati direttamente all’interno del file di testo.



FIREWALL ATTIVO

Proviamo nuovamente ad effettuare un ping tra le due macchine; possiamo già notare delle differenze rispetto a quando il firewall era disattivato.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
^C
── 192.168.240.150 ping statistics ──
54 packets transmitted, 0 received, 100% packet loss, time 54813ms
```

La macchina sembra essere irraggiungibile tramite ping. Possiamo ipotizzare che il firewall stia bloccando le richieste ICMP (quindi anche i pacchetti inviati da noi tramite ping).

Proviamo dunque un comando meno invasivo per provare ad aggirare il firewall e vedere se riceviamo risposta dalla macchina di windows XP: diamo in input il comando “nmap –PN” seguito dall’IP della macchina di windows XP.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -Pn 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 14:00 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.83 seconds
```

Anche questa volta non siamo riusciti ad ottenere molte informazioni sulla macchina; tuttavia, ci viene restituito il MAC Address della macchina di windows XP e scopriamo anche che il sistema operativo è in esecuzione all’interno di una macchina virtuale.

Proviamo con un metodo più invasivo. Il comando “nmap –A” è il metodo di scansione più completo. Questo comando unisce in un'unica soluzione le seguenti scansioni:

-OS fingerprint: Rilevamento del sistema operativo

-Version detection: analisi delle porte aperte, servizi attivi sulle porte e relative versioni (corrispondente al comando “nmap –sV”).

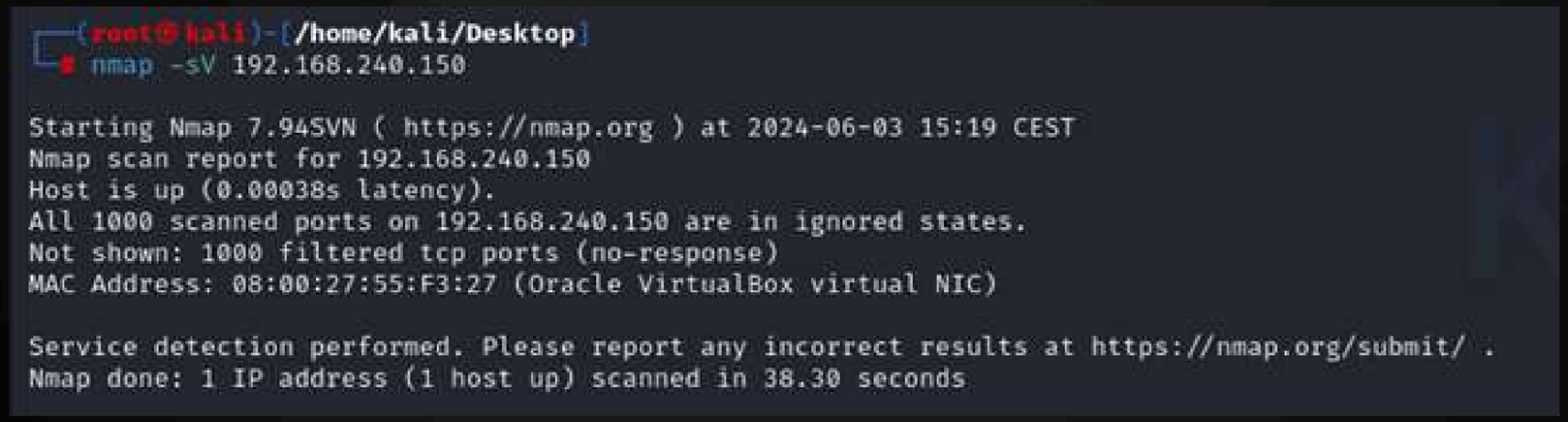
-Script scanning: Raccolta informazioni aggiuntive per identificare vulnerabilità (corrispondente al comando “nmap --script=default”).

-Traceroute: tenta di identificare il percorso preso dai pacchetti per raggiungere il target (corrispondente al comando “nmap –traceroute”).

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -A 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 13:58 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:55:F3:27 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 192.168.240.150

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.42 seconds
```

Otteniamo qualche informazione aggiuntiva sulla macchina, ovvero il numero di HOP (cioè quanti dispositivi di rete sono stati attraversati dai pacchetti da noi inviati) e il RTT (Tempo di andata e ritorno, cioè il tempo di risposta della macchina al pacchetto inviato).

Effettuiamo nuovamente la scansione con il comando“nmap -sV“ delle porte e versione dei servizi presenti su di esse e possiamo osservare come nessuna porta sia raggiungibile.



In conclusione, possiamo affermare che il firewall incrementa sensibilmente la sicurezza di una macchina, anche se questa presenta servizi obsoleti e quindi poco sicuri, rendendo più difficile per un attaccante sfruttarne le vulnerabilità.

COrtana Security

Fattura

- Costo Manodopera = 100$/h
  x 8h = 800$
- Sopralluogo = 200 $

Tot: 1000$

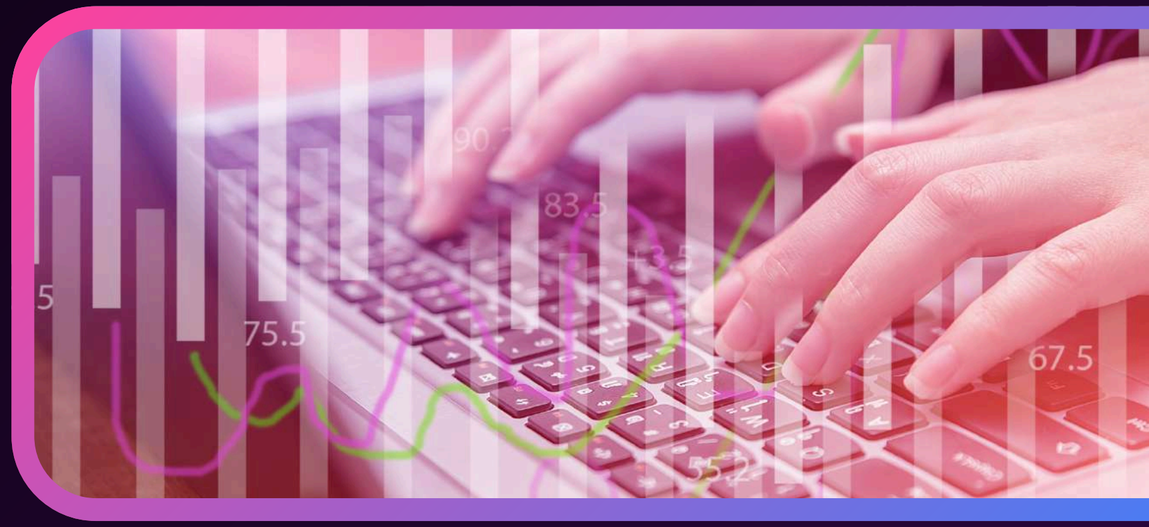
GIORNO 2

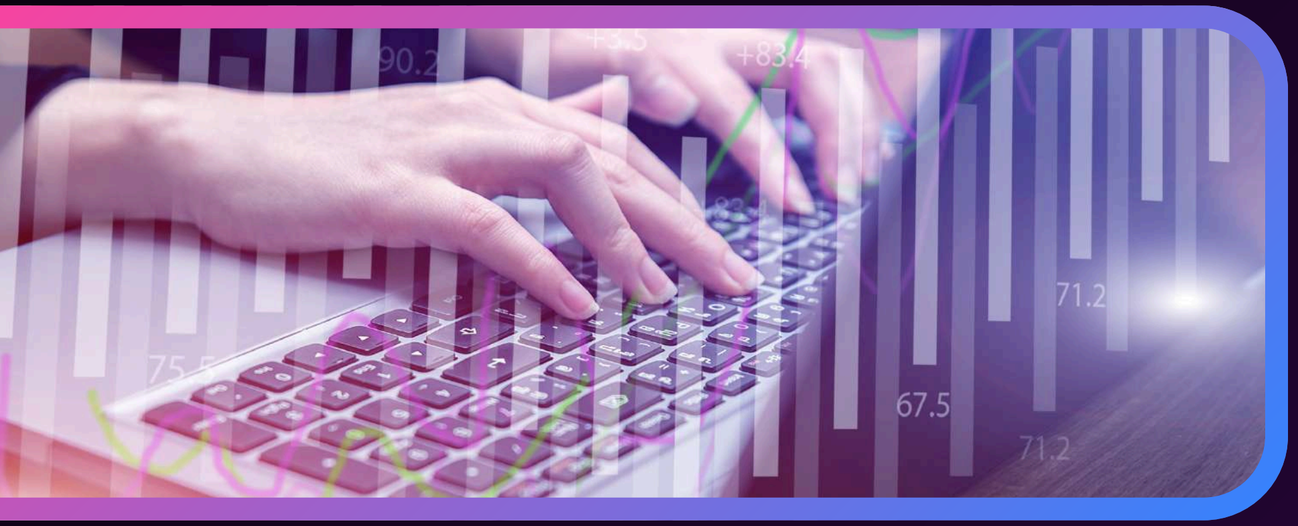
COrtana Security

BUSINESS CONTINUITY & DISASTER RECOVERY

Business Continuity Plan

La **business continuity plan** (BCP) è un piano strategico che mira a garantire la continuità delle operazioni aziendali in caso di interruzioni dovute a vari rischi, come disastri naturali (terremoti, incendi, inondazioni), guasti tecnologici, attacchi informatici o altre emergenze.
Nell'ambito della cybersecurity, il BCP è fondamentale per proteggere gli asset informatici e garantire che i dati e i sistemi critici rimangano operativi o possano essere ripristinati rapidamente.





Il BCP per la cybersecurity comprende una serie di processi e procedure progettati per ridurre al minimo l'impatto di interruzioni e garantire il ripristino rapido e sicuro delle operazioni. Questo piano include l'identificazione degli asset critici, l'analisi dei rischi e la predisposizione di strategie di mitigazione.

Per valutare i danni provocati ai vari asset dai diversi rischi, si utilizza spesso una combinazione di metriche finanziarie e probabilistiche. Due concetti chiave in questo contesto sono il **Single Loss Expectancy** (SLE) e l'**Annualized Rate of Occurrence** (ARO).

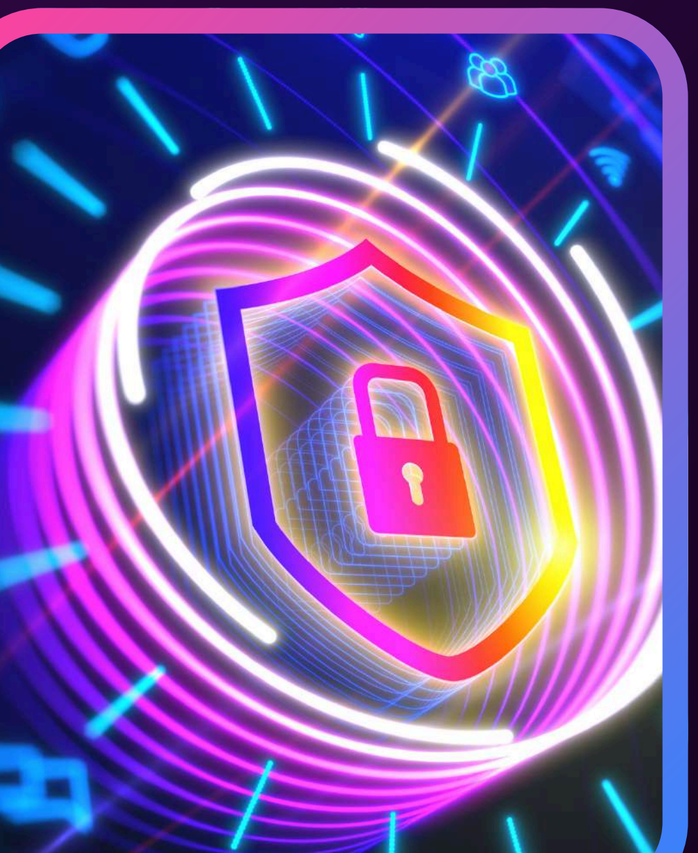
SINGLE LOSS EXPECTANCY

L'SLE rappresenta il costo finanziario stimato di una singola occorrenza di un rischio specifico. È calcolato utilizzando la formula:

SLE=Asset Value (AV) * Exposure Factor (EF)

- Asset Value (AV): Il valore dell'asset in termini finanziari.
- Exposure Factor (EF): La percentuale di perdita che si prevede l'asset subisca in caso di evento rischioso. Questo valore è espresso come una frazione o percentuale.

ANNUALISED RATE OF OCCURRENCE



L'**ARO** rappresenta la frequenza annua con cui si prevede che un particolare evento rischioso si verifichi. Questo tasso è solitamente stimato basandosi su dati storici e analisi delle tendenze.

Se, per esempio in una determinata zona si verificano terremoti con una frequenza di una volta ogni trenta anni, il valore di ARO sarà 1/30.

ANNUALISED LOSS EXPECTANCY

Una volta calcolati l'SLE e l'ARO, si può determinare l'**Annualized Loss Expectancy** (ALE), che stima la perdita finanziaria annua prevista a causa di un rischio specifico. La formula per calcolare l'ALE è:

ALE=SLE * ARO

In conclusione, l'integrazione di SLE e ARO nel processo di valutazione dei rischi consente alle aziende di quantificare in termini economici l'impatto potenziale dei vari rischi. Questo approccio aiuta a prendere decisioni informate su quali misure di mitigazione implementare, garantendo una protezione efficace degli asset e la continuità delle operazioni aziendali in caso di eventi avversi.

In data odierna il Sig. Rossi ci ha fornito dei dati riguardanti i suoi asset e ci ha chiesto di calcolare la perdita potenziale che potrebbe subire l'azienda in caso di disastro naturale.

Traccia: Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery. Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia. Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- *Inondazione sull'asset «edificio secondario»*
- *Terremoto sull'asset «datacenter»*
- *Incendio sull'asset «edificio primario»*
- *Incendio sull'asset «edificio secondario»*
- *Inondazione sull'asset «edificio primario»*
- *Terremoto sull'asset «edificio primario»*

Dati Degli Asset

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

SVOLGIMENTO

RICORDIAMO LE FORMULE:

SLE=AV * EF

ALE=SLE * ARO

SIGLE DEI FATTORI:

SLE: Single Loss Expectancy
AV: Asset value
EF: Exposure factor
ARO: Annualized Rate of Occurrence
ALE: Annualized loss expectancy

SOLUZIONE

1) Inondazione sull’asset «edificio secondario»

150.000€ * 40% = 60.000 * (1/50) = 1200€/anno

2) Terremoto sull’asset «datacenter»

100.000€ * 95% = 95.000 * (1/30) = 3.166,66€/anno

3) Incendio sull’asset «edificio primario»

350.000€ * 60% = 210.000 * (1/20) = 10.500€/anno

4) Incendio sull’asset «edificio secondario»

150.000€ * 50% = 75.000 * (1/20) = 3750€/anno

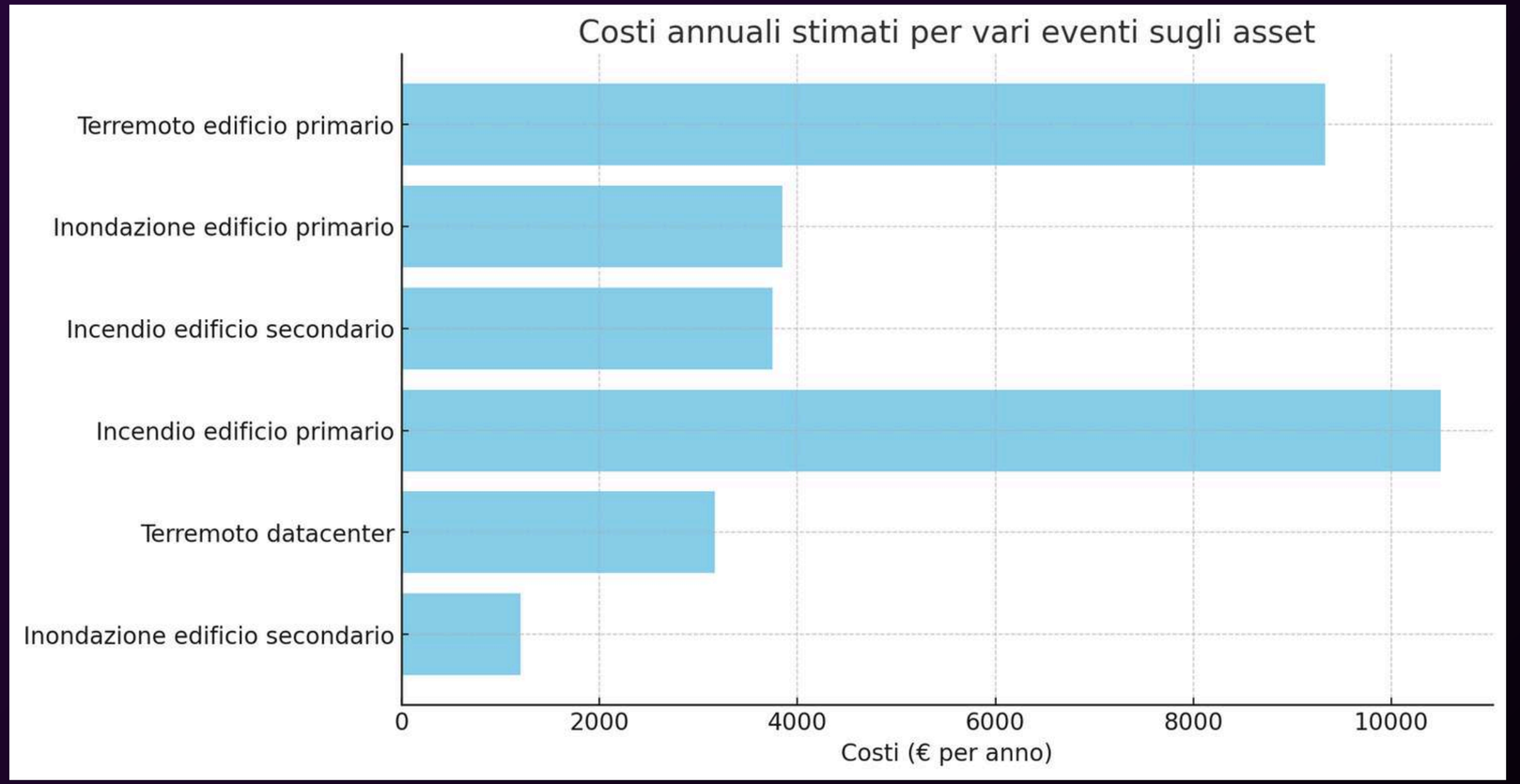
5) Inondazione sull’asset «edificio primario»

350.000€ * 55% = 192.500 * (1/50) = 3850€/anno

6) Terremoto sull’asset «edificio primario»

350.000€ * 80% = 280.000 * (1/30) = 9.333,33€/anno

Di seguito vediamo i danni(in termini economici) che deriverebbero da questi incidenti



GIORNO 3

IOC & THREAT INTELLIGENCE

In data odierna, il Sig. Rossi ci ha chiesto di verificare la sicurezza della rete verificando se sono presenti **Indicatori di compromissione** (IOC).

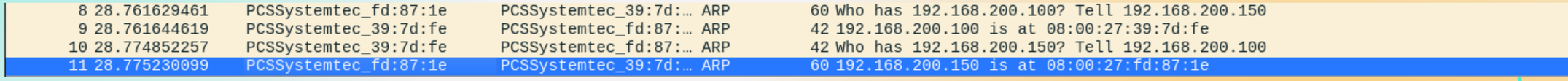
Decidiamo di effettuare subito una scansione di rete ed avviamo “**Wireshark**”.

Notiamo, intanto che tra la riga 1 e 4 abbiamo delle richieste TCP. Ci viene detto che la richiesta viene da una macchina di **Metasploitable**.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server,
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	http(80) → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64

Sebbene la richiesta sia inusuale, non abbiamo ancora sufficienti informazioni su cosa stia avvenendo, poiché questo protocollo è utilizzato per molti scopi differenti.

Tra la riga 8 e 11 osserviamo la presenza di pacchetti ARP associati al dispositivo "PCSSystemtec" nel traffico di rete. Questi potrebbero indicare un potenziale attacco di tipo **Man-In-The-Middle** (MITM), specialmente se le richieste ARP non sono usuali o sospette. Gli attacchi MITM spesso sfruttano l'ARP spoofing per intercettare e reindirizzare il traffico di rete.



8	28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:…	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:…	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:…	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:…	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Questo tipo di richieste vengono effettuate dall’attaccante per associare all’indirizzo IP della vittima il corrispondente indirizzo MAC del dispositivo.

Nei casi peggiori possiamo sospettare che qualcuno voglia effettuare un **ARP Poisoning**.

arp spoofing

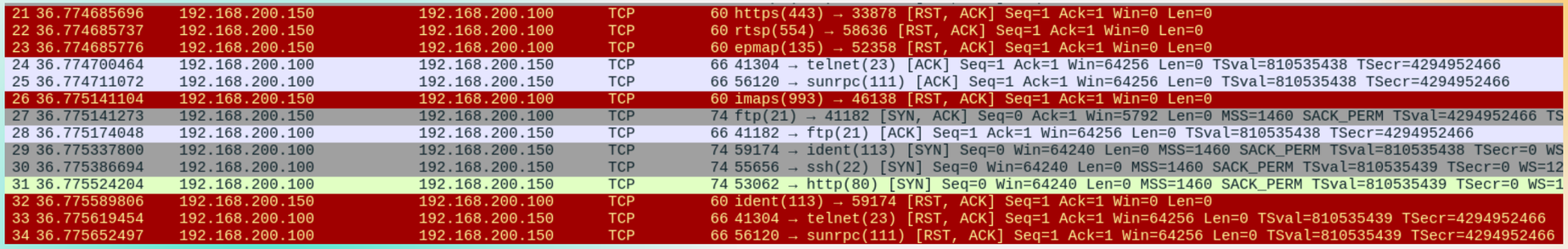
Cos'è?

Gli attacchi MITM che utilizzano ARP spoofing consistono nell'inviare risposte ARP falsificate per associare il proprio indirizzo MAC all'indirizzo IP di un altro dispositivo sulla rete. Questo permette all'attaccante di intercettare e manipolare il traffico tra due dispositivi legittimi.

Come difendersi?

Abilitare funzionalità di sicurezza come ARP inspection sui dispositivi di rete per prevenire l'ARP spoofing. Configurare static ARP entries per dispositivi critici, se possibile.

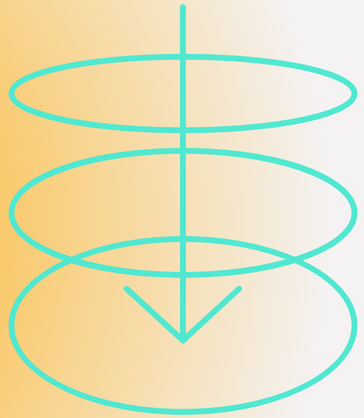
Un fattore molto importante è dato dalla presenza di molteplici richieste (quelle evidenziate in rosso) da parte dello stesso IP su servizi/porte differenti.
Le porte delle richieste evidenziate bloccano subito la richiesta tramite reset(RST).



21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 https(443) → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 rtsp(554) → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 epmap(135) → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → telnet(23) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → sunrpc(111) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 imaps(993) → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 ftp(21) → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TS
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → ftp(21) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → ident(113) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → ssh(22) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=12
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=1
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 ident(113) → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → telnet(23) [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → sunrpc(111) [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Si può ipotizzare che qualcuno stia effettuando una scansione di rete con strumenti tipo **nmap**.

Un altro elemento molto interessante è dato dalla presenza di pacchetti **SYN ACK**(riga 27). questi tentano di sfruttare il processo “Three way handshake”, senza tuttavia concluderlo.



```
27 36.775141273    192.168.200.150          192.168.200.100      TCP        74 ftp(21) → 41182 [SYN, ACK]
```

SUGGERIMENTI

Continuare a monitorare l’Host “PCSSystemtec” e l’Host “192.168.200.150” ed eventualmente, bloccarli .

Creare delle sotto-reti divise per area di lavoro, in modo che l’attaccante non possa muoversi agilmente all’interno della rete aziendale.

Installare e configuare un firewall in modo da bloccare richieste sospette.

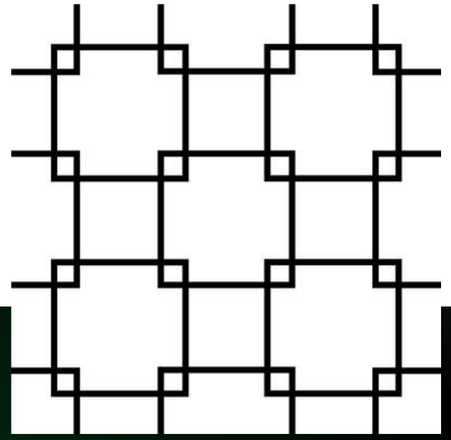
Cifrare, se non ancora fatto, i dati sensibili

GIORNO 4

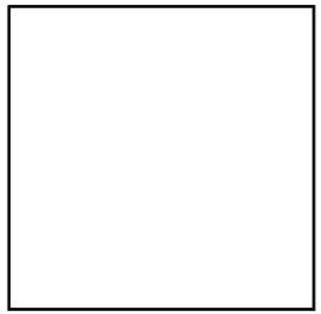
INCIDENT RESPONSE

In data odierna, il Sig. Rossi ha subito un attacco e ci ha chiesto di intervenire tempestivamente per gestire la criticità e ripristinare il sistema in modo da renderlo nuovamente utilizzabile e sicuro.

Modalità di gestione di un sistema compromesso



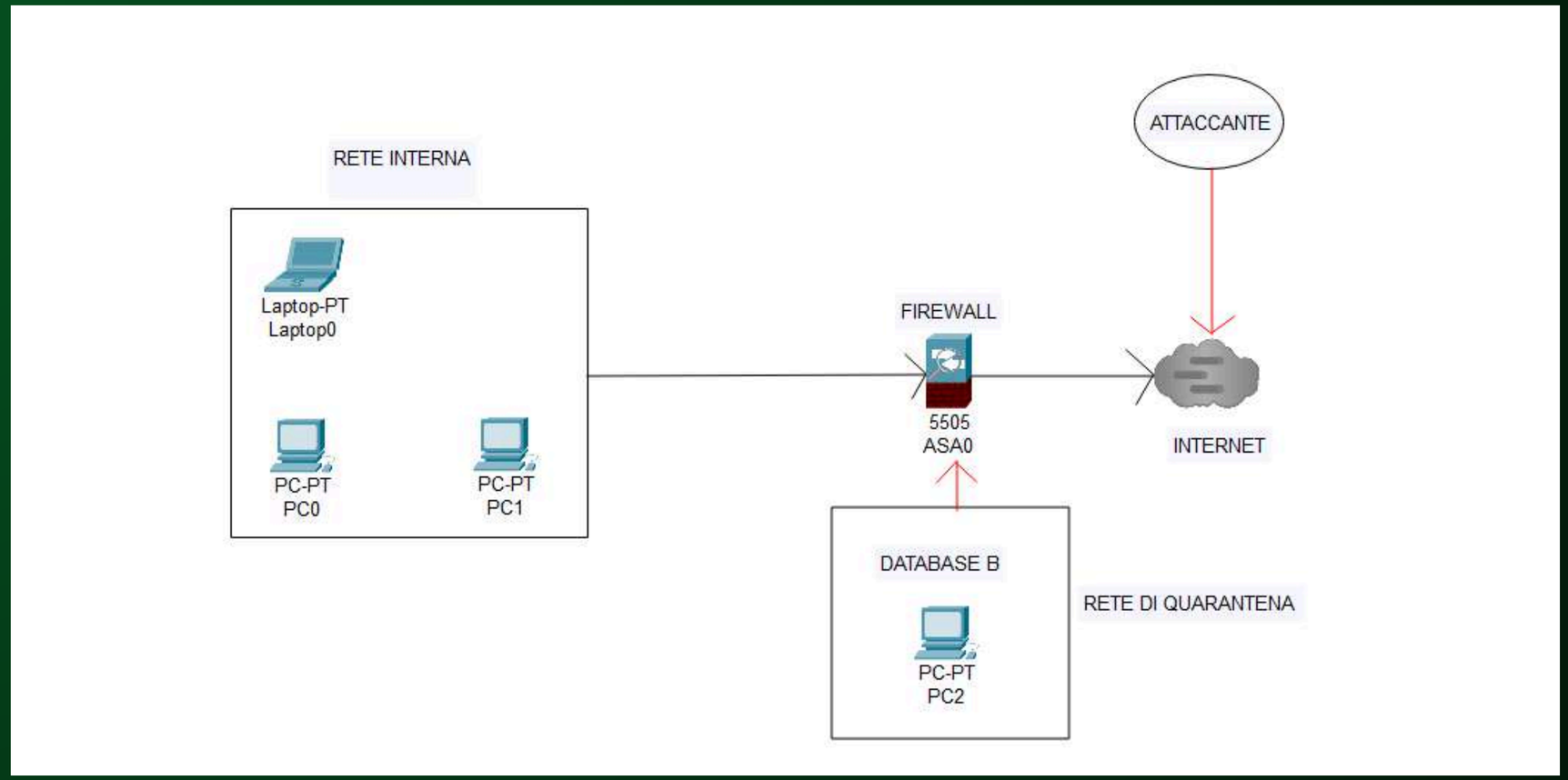
Segmentazione



isolamento

Segmentazione

Se avviene un incidente, è possibile isolare il sistema compromesso (nel nostro caso il sistema B) creando una **VLAN,** in modo da contenere la diffusione del malware e impedire all'attaccante di muoversi per l'intera rete aziendale. Tuttavia, è buona pratica effettuare la segmentazione prima che avvenga un incidente.

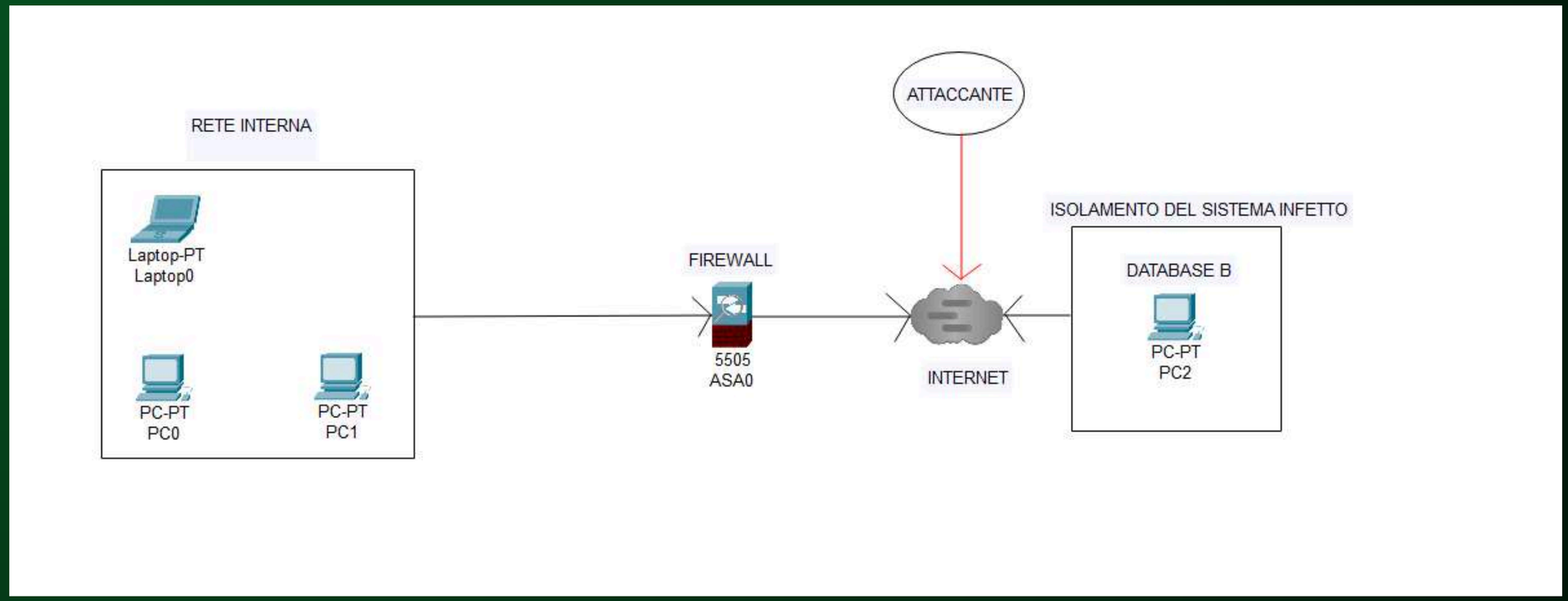


Creiamo una VLAN dedicata al sistema compromesso, chamata “**rete di quarantena**” (come in figura). Questo avrà una doppia utilità:

- Evitare che l’attaccante arrivi ai sistemi della rete non ancora compromessi
- Creare un ambiente sicuro dove poter analizzare, anche in un secondo momento, il malware (per esempio all’interno di una **sandbox**)

Isolamento

Questa tecnica prevede la **disconnessione fisica** del dispositivo dalla rete; sebbene impedisca il propagarsi del malware o il funzionamento delle backdoor, annienta l’accessibilità ai dati, creando disagi al business aziendale.



Abbiamo 2 opzioni (scegliamo in base alle policy aziendali):

- Isolare il sistema B dalla rete aziendale, ma permettergli di collegarsi comunque ad internet (come in figura)
- Isolare completamente il sistema B da internet, ma ciò impedirà ai dipendenti di avere accesso rapido alle risorse aziendali

Rimozione dell’incidente

Non basta aver isolato il sistema infetto; bisogna anche mettere in sicurezza ciò che più vale all’interno di un’azienda: i **dati.** La diffusione di dati sensibili, infatti, può causare (oltre ad un enorme perdita finanziaria) anche delle ripercussioni legali.

RECUPERO DATI

Esistono 2 approcci per il recupero di dati da dischi compromessi :

- Reconstruction: se il sistema non è stato interamente compromesso, possiamo recuperare le parti non intaccate ed eliminare quelle compromesse

- Rebuilding: se il sistema è stato interamente compromesso oppure non conosciamo appieno la gravità del danno, dovremo ricostruire interamente il sistema

Distruzione dei File/Dispositivi compromessi

Esistono 3 principali modalità per distruggere file o dispositivi non più sicuri:

Clear

I dati presenti sul dispositivo vengono sovrascritti più volte con tecniche “logiche” per essere sicuri che non rimanga traccia dei dati malevoli. Si tratta di un ripristino dati di fabbrica.

Purge

Oltre all’approccio logico, si utilizzano magneti per la rimozione dei dati.

Destroy

Si tratta dell’eliminazione “fisica” del dispositivo su cui sono presenti i dati. Questo approccio può avvalersi anche di sofisticate tecnologie di laboratorio.

GIORNO 5

COrtana Security

PROJECT S9/L5

Participants: Gabriele Arcelli, Giammarco Iorio, Stefano Cesaroni, Valerio Zampone

PART 1

XSS AND SQL ATTACK PREVENTION

XSS AND SQL ATTACKS

Xss and Sql attacks are among the most frequent attacks on websites. The difference is that in Xss attacks the user's session is exploited, while the Sql attack attempts to exploit an input vulnerability to retrieve sensitive information from a database. Xss-type attacks are divided into:

- Xss stored: if a malicious code is inserted on the page and every time a user visits the page in question information (especially the session cookie) will be sent to the attacker's listening server (typically “netcat”).
- Xss Reflected: the attacker manages to make the victim click a LINK to which he has “attached” a malicious code, which will be executed along with the opening of the LINK, if the site is not properly configured. Again, data will be sent to the attacker's listening server.

PREVENTION OF XSS ATTACKS

1. Sanitization of input: Remove or replace dangerous characters from user input before using it in web pages.
2. Escaping: Use proper escaping in HTML, JavaScript, CSS and URL contexts to ensure that special characters are not interpreted as executable code.
   - o HTML: &, <, >, “, ', /
   - o JavaScript: \, ', “
   - o CSS: \, ', “
   - o URL: %
3. Content Security Policy (CSP): Implement CSP to limit the sources from which the browser can load resources, reducing the risk of malicious code execution.
4. Input Validation: Validate user input to ensure that it matches expected formats.
5. HttpOnly and Secure Cookie Attributes: Set HttpOnly and Secure attributes for cookies to protect them from scripted access and ensure they are transmitted only over secure connections.
6. Update Libraries: Ensure that all libraries and frameworks used are up-to-date and free of known vulnerabilities.

PREVENTION OF SQL INJECTION ATTACKS

1. Parameterized Queries (Prepared Statements): Use parameterized queries instead of directly concatenating user input into SQL queries.
2. ORM (Object-Relational Mapping): Use an ORM that automatically handles sanitization and parameter binding.
3. Stored Procedures: Use stored procedures that accept parameters, thus avoiding the dynamic construction of SQL queries.
4. Input Validation: Validate and sanitize user input to ensure that it contains only the expected data.
5. Minimum Privilege Principle: Assign database accounts the minimum privileges necessary to perform the required operations.
6. Escape Characters: Use special character escaping in cases where parameterized queries cannot be used.
7. Database Firewall: Implement a database firewall that can monitor and block suspicious queries.
8. Software Update: Keep the database and management system up-to-date with the latest security patches.

Also, for both types of attacks it is advisable to implement a WAF. In our case we will insert it between the firewall protecting the DMZ and the DMZ itself (in our case it is the e-commerce).

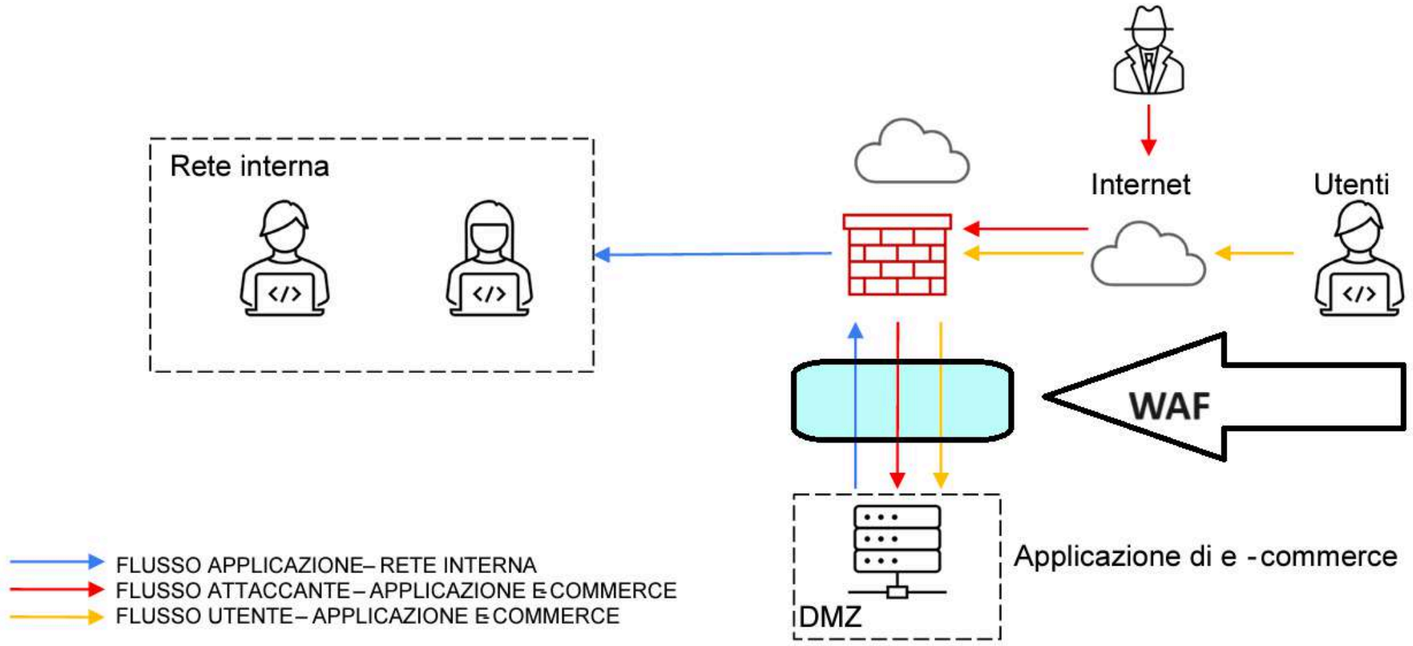
Functions of the WAF:

- A WAF monitors and filters HTTP/HTTPS traffic directed to a web application, detecting and blocking attacks such as SQL injection, cross-site scripting (XSS), and other common vulnerabilities.
- Protection from Attacks: Blocks common attacks such as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and other OWASP Top 10 vulnerabilities.
- Monitoring and Logging: Provides visibility into web traffic and logs suspicious or malicious activity for analysis and auditing.
- Data Theft Prevention: Prevents exfiltration of sensitive data by intercepting malicious requests seeking access to confidential information.
- DDoS Attack Mitigation: Helps protect web applications from Distributed Denial of Service (DDoS) attacks that aim to overload the system.
- Access Control: Implements access policies to ensure that only authorized users can access certain application resources or features.
- In addition, WAF can also act as IDS(Intrusion System Detection).

Figure implemented by adding a WAF

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



PART 2

PREVENTION & BUSINESS IMPACT

In the second part, we are asked to estimate the amount of damage the company would suffer if it were attacked and rendered inactive for 10 minutes, considering that 1,500 euros are spent on the site every minute; we are, in addition, asked to develop strategies against the attack.

Preventive actions

- **Implementing a Web Application Firewall (WAF)**: A WAF filters and monitors HTTP/HTTPS traffic, blocking suspicious requests and DDoS attacks.
  Examples: AWS WAF, Sucuri, Imperva.
- **Automatic Scalability:** Use cloud hosting services that offer automatic scalability to increase resources during an attack.
  Examples: AWS Auto Scaling, Google Cloud Autoscaler.
- **Limit Rate of Requests**: Configure limits on the number of requests a single IP can make in a given time interval.
  Tools: Server configurations (Nginx, Apache) or services such as Cloudflare Rate Limiting.
- **Monitoring and Alerting**: Implement monitoring systems to quickly detect abnormal traffic spikes and alert administrators.
  Tools: Nagios, Zabbix, New Relic.

Preventive actions

- **Block Malicious IPs**: Use blacklists to block IPs known to be part of botnets or sources of malicious traffic.
  Tools: Firewall configurations, threat intelligence services.
- **Diversify the Network:** Use multiple Internet service providers (ISPs) to provide redundancy and distribute traffic load.
  Benefits: Increases resilience against DDoS attacks targeted at a single ISP.
- **Planning an Incident Response Plan**: Develop and document a response plan to address DDoS attacks, including team roles and responsibilities.
  Benefits: Improves readiness and speed of response.
- **Resiliency Testing**: Perform periodic resilience testing and mock DDoS attacks to identify weaknesses and improve defense.
  Tools: Internal testing, DDoS simulation services.

It is important to make decisions in advance to protect against various attacks in order to limit economic damage.

In our case, where the application was unreachable for 10 minutes and there was a loss of 1,500 euros per minute, we would suffer a loss of as much as 15,000 euros.

PART 3

RESPONSE

In this part we will see how to behave where there is an attack in progress.
We suppose that our corporate network provides an e-commerce service, which is located on a DMZ; however, the latter communicates with the internal network, and this could allow malware to pass from the DMZ to the internal network.

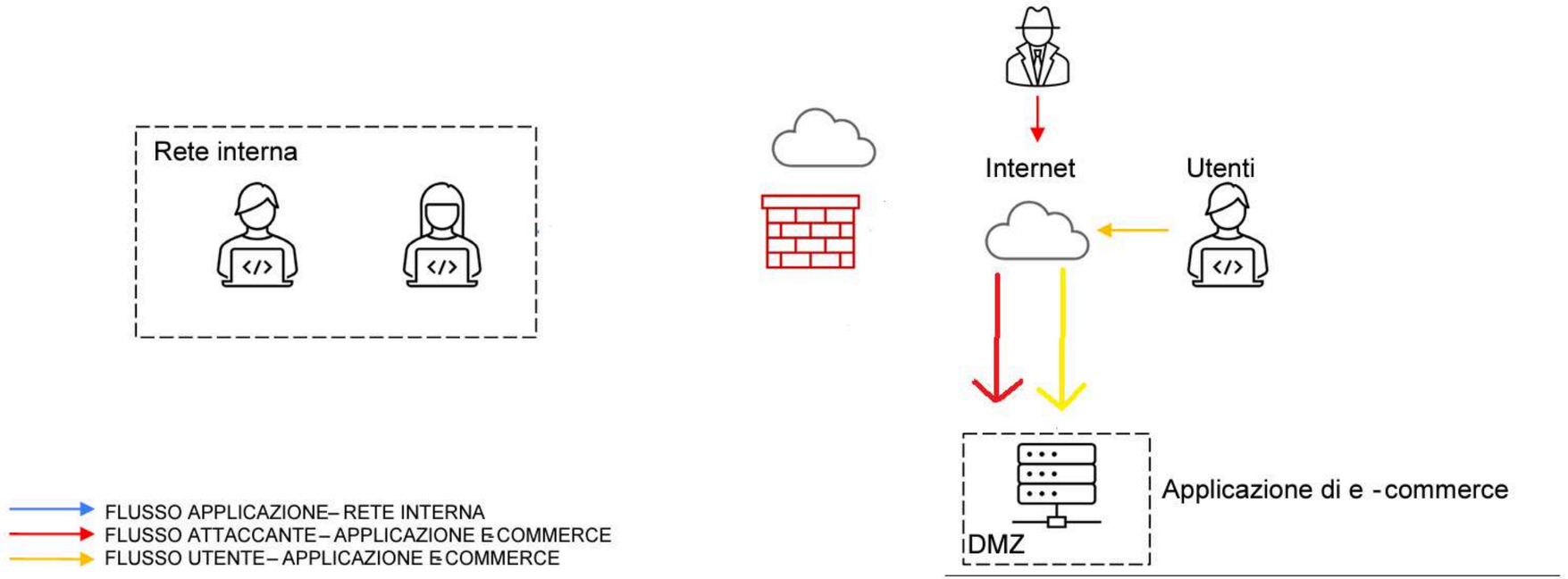
Generally, there are two approaches when a system is infected:

- **Quarantine**: the system remains on the same corporate network, but the network is segmented. Segmentation includes all activities that allow a network to be divided into different LANs or VLANs. In doing so, the infected system remains isolated.
- **Isolation**: the system is removed completely from the corporate network with the aim of preventing the infected machine from propagating to the internal network.

In our case, since we know that a malware is present on the e-commerce system, we decide to isolate it to avoid compromise of other devices.

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



We chose the **isolation method**; this way both users and attackers will still be able to access the DMZ, however it will be impossible for them to get to the internal corporate network.

Immediate Actions:

Isolate the Server: Disconnect the infected server from the network to prevent the spread of malware.

Place Server in Quarantine: Set up the server in an isolated network where it can be scanned without risking other parts of the infrastructure.

Isolation prevents malware from propagating to other systems and reduces the risk of further compromise or data breach.Also, it is advisable to move to a sandbox to analyze the malware and see how it behaves.

- **Antivirus/Malware Scan**: Perform a full scan with up-to-date security tools to identify and remove malware.

- **Log Analysis**: Examine system logs to trace the origin and behavior of malware.Rationale: Understanding how the malware entered the system and what damage it caused is crucial to preventing future infections.

- **Secure Backup and Integrity Verification**: Use a verified backup, made before the infection, to restore the system and ensure that backups are free of malware before restoring them.

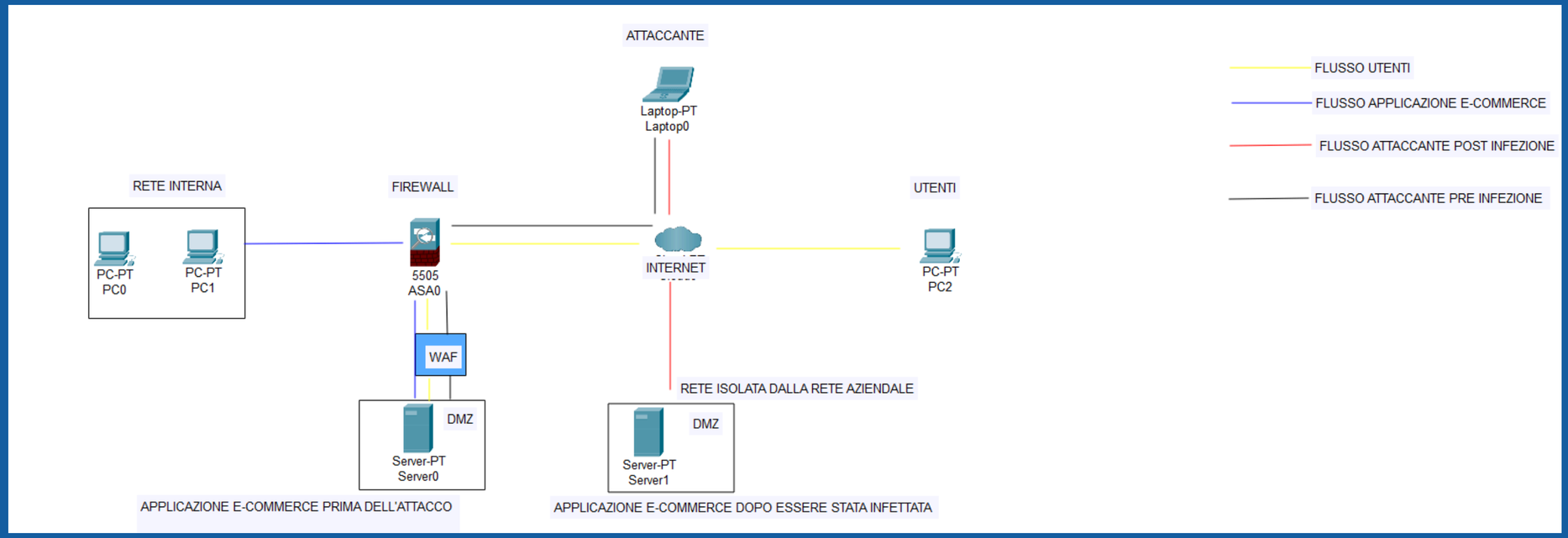
- **Software Reinstallation**: If there are no reliable backups, completely reinstall the operating system and applications.

- **Updates and Patches**: Apply all available security patches for the operating system and applications. Restoring the system to a clean state ensures that the malware has been completely removed.
- Add **WAF** and **IDS/IPS**: Implement a Web Application Firewall (WAF) and Intrusion Detection/Prevention (IDS/IPS) systems to monitor and block suspicious activities.
- **Restricted Access**: Reduce user privileges and restrict access to critical systems.
- Implement Security Information and Event Management (SIEM) systems to continuously monitor network activity and detect anomalies.

PART 4
COMPLETE SOLUTION

Let's see what would be the best solution for our case.

In our case, the best solution is the union of the solutions seen in step 1 and step 3



we divided the structure into 2 phases: the before and after attack. in the upper right corner we can observe a legend with the various types of flows.

PART 5

AGGRESSIVE MODIFICATION OF NETWORK STRUCTURE

To make the structure even more secure, we can integrate other security elements:

- Adding a **Next Generation Firewall:** an advanced network security appliance that offers protection against a wide range of modern threats by combining traditional firewall capabilities with advanced traffic inspection, intrusion prevention, application control, and more. It is used to improve network security, reduce the complexity of security management, and ensure compliance with applicable regulations.

- Dividing the network into **VLAN (Virtual Local Area Network):** a network configuration that allows a physical network to be segmented into multiple logical subnets. Each VLAN functions as a separate LAN, even though the devices are physically in the same network. VLANs are a powerful tool for logically segmenting networks, improving security, performance, and network management. They offer flexibility and scalability, allowing organizations to easily adapt their network infrastructure to changing needs. Using VLANs can help optimize network resources, ensure data security, and improve operational efficiency.

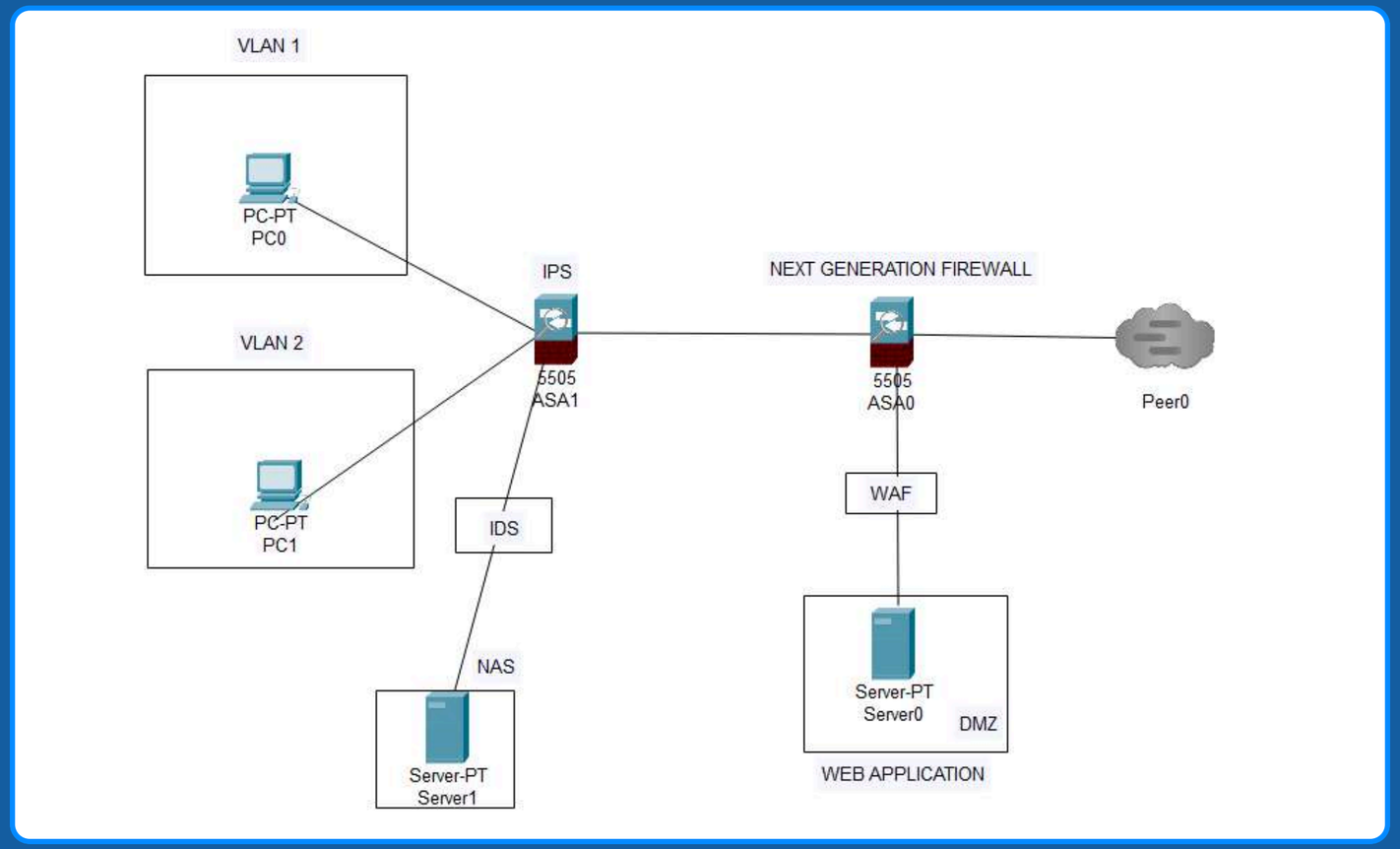
- We used an **Intrusion Detection System (IDS)** to protect a NAS; this is an effective strategy for improving security and preventing unauthorized access and attacks. An IDS provides constant visibility into network traffic and system activity, generating real-time alerts and maintaining detailed logs for forensic analysis. This helps not only to prevent potential threats, but also to ensure compliance with security regulations, thereby protecting sensitive and critical data stored on the NAS.

- We added an **IPS (Intrusion Prevention System),** a network security device or software designed to monitor network traffic in real time to detect and prevent malicious activity. It works by analyzing data flowing through the network and comparing it to signatures of known attacks or behavioral anomalies. When an IPS identifies a potential attack, it can take several actions to mitigate the threat, such as blocking suspicious traffic, terminating dangerous connections, or sending alerts to system administrators. The main goal of an IPS is to prevent cyber attacks before they can cause damage to the network or computer systems.

Advantages of using an IPS in conjunction with a next generation firewall

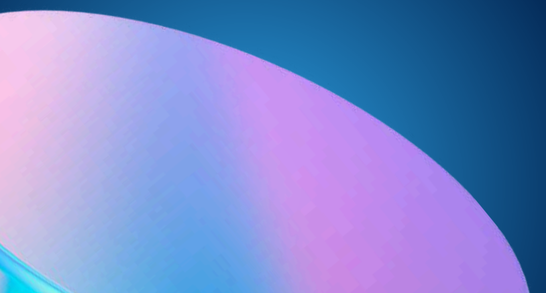
Deploying an **IPS** along with a **Next Generation Firewall** is a recommended practice to achieve more robust and comprehensive protection against malware. Although NGFWs offer many advanced features, a dedicated IPS can provide an additional layer of specialized security, enhancing the ability to detect and prevent sophisticated attacks. This combination of security technologies helps create defense in depth, reducing the overall risk to the network infrastructure.

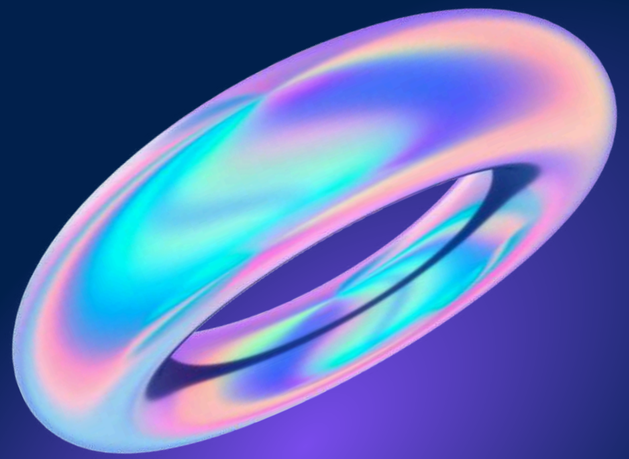
Here’s a look at the modified infrastructure:



Analysis Reports on ANY.RUN

We will look in detail at two reports uploaded to anyrun to understand both the types of attacks and how to prevent them in the future.
Before we begin, let's briefly look at what anyrun is and what it is used for.





ANY.RUN is an interactive cloud-based malware analysis tool. It is designed to enable cyber security analysts to examine and understand the behavior of suspicious files in a controlled environment.
Let's look at its utilities:

Rapid Threat Identification:

Analysts can quickly determine if a file is malicious and understand its behavior without having to manually configure complex testing environments.

Education and Training:

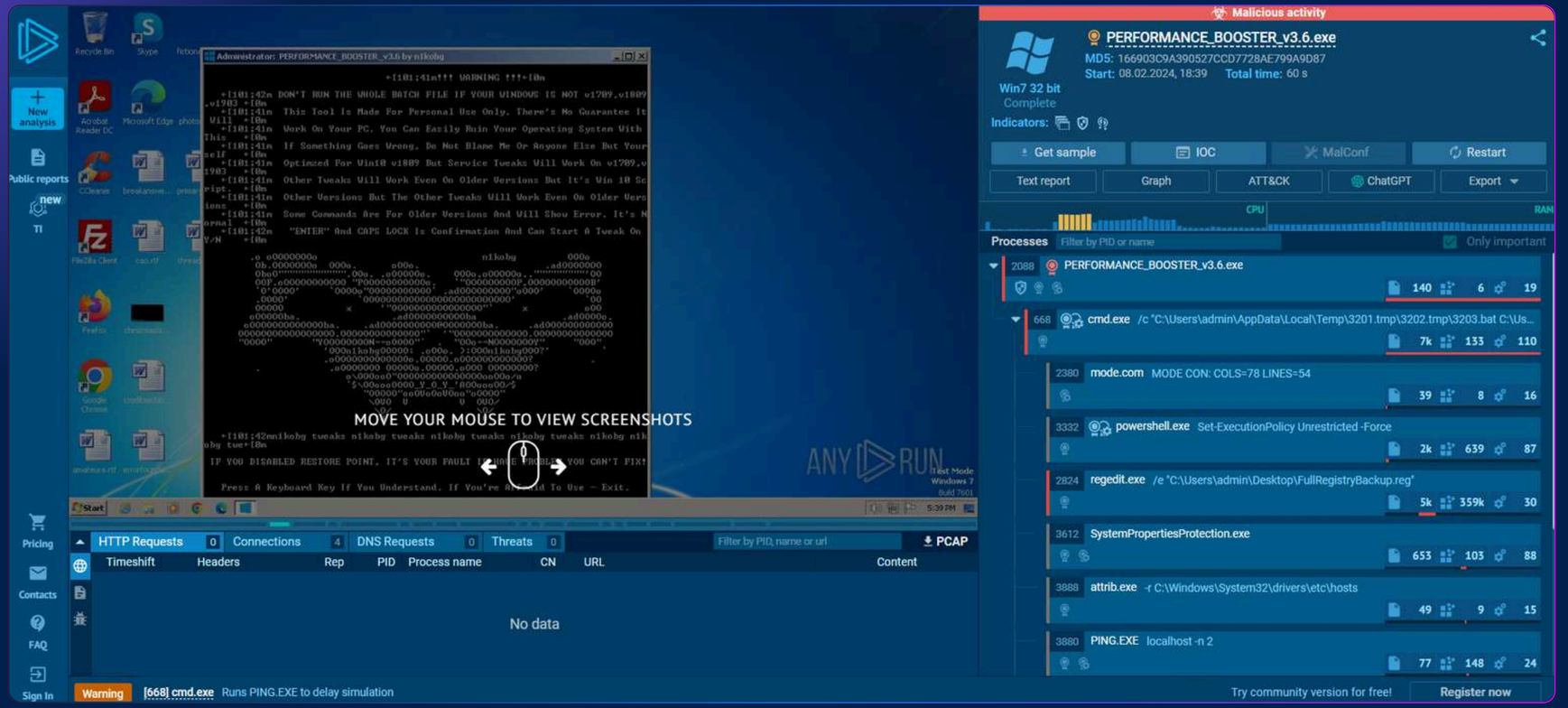
ANY.RUN is also a useful educational tool for cybersecurity training, allowing students and professionals to see how malware works in a secure environment.

Security Investigation Support:

Companies can use ANY.RUN to investigate security incidents by analyzing suspicious files found in their networks and better understanding how they were compromised.

In conclusion, ANY.RUN is a powerful tool for interactive malware analysis that helps security experts quickly identify and understand threats, improving response and protection against cyber attacks.

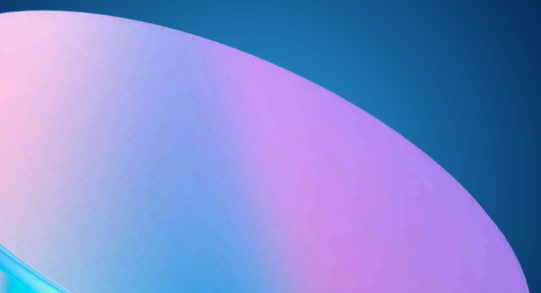
First Report

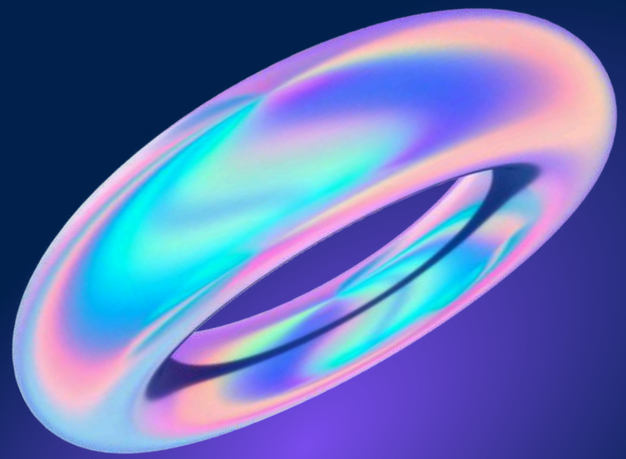


The first report uploaded on anyrun refers to a suspicious file called “**PERFORMANCE_BOOSTER_v3.6.exe.**”

Since this file has been identified as malicious, we will now explain in a simple way what it means and how we can protect ourselves from such threats in the future.

Damaging Actions





We found that this file, when executed, performs a number of malicious actions on our computer:

Changing Security Settings:

Changes the settings of PowerShell, a Windows tool used to automate tasks. Normally, these settings prevent the execution of unauthorized scripts, but the file changes them to run anything without restrictions.

Running Commands:

Starts the program cmd.exe, also known as “Command Prompt,” and powershell.exe to execute various commands. These tools are similar to an interpreter that receives and executes instructions.

Editing Files:

Use ATTRIB.EXE, a tool that can change the properties of files, such as hiding them or making them read-only. This can be used to hide malicious files or manipulate important system files.

Sensitive Information Collection:

It reads various information from our computer, such as network settings, Microsoft Outlook installation paths, and remote connection history. This information can be used for further attacks.

Preventive Actions

To prevent such threats from compromising our security, we can take some simple preventive measures:

Use Antivirus Software:

Install and keep updated a good antivirus program that can detect and block malicious files.

Update Software:

Make sure that the operating system and all applications are always updated with the latest security patches.

Limit User Permissions:

Use user accounts with limited permissions for day-to-day tasks and reserve administrative accounts only for tasks that require high privileges.

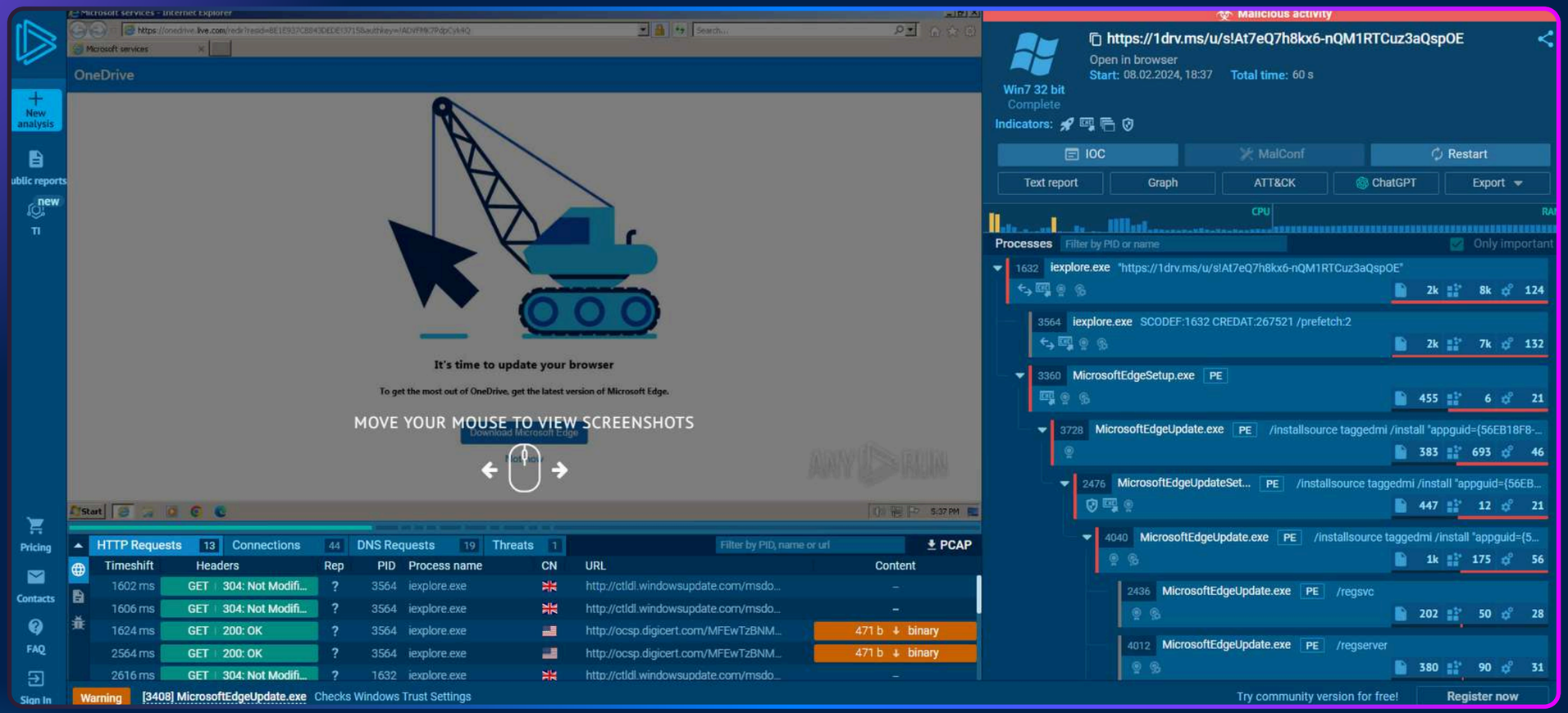
Monitor System Activities:

Implement monitoring solutions that can detect suspicious activity and alert us immediately.

Train Staff:

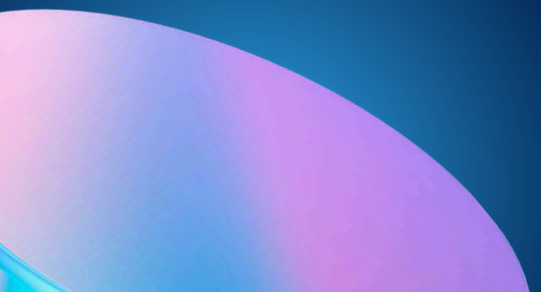
Educate all users about the risks of downloading and running files from untrusted sources and teach them to recognize signs of possible attacks.

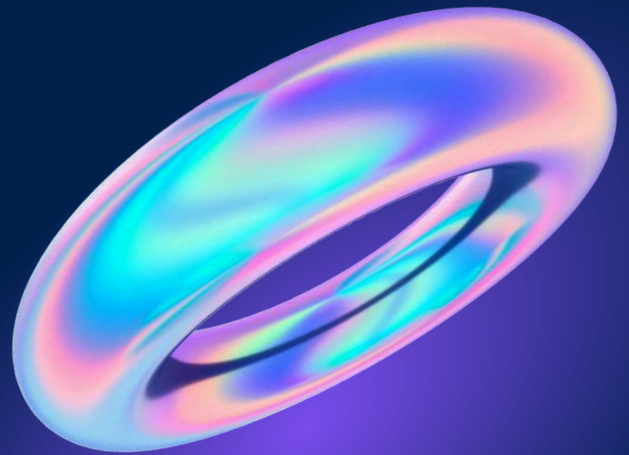
Second Report



Any.Run analysis report indicates attack is **malware** masquerading as legitimate Microsoft Edge updates. Malware is a malicious software designed to infiltrate or damage a computer system without the user's consent.

Observed Behaviors





Executable Drops:

Malware drops executables such as MicrosoftEdgeSetup.exe and MicrosoftEdgeUpdateSetup.exe to masquerade as legitimate updates. An executable is a type of file that contains a program capable of being executed by the computer. Files with the .exe extension are common examples of executables.

Execution from Unusual Paths:

Processes are executed from nonstandard paths, a typical behavior of malware attempting to avoid detection.

Disabling SEHOP:

Disabling SEHOP (Structured Exception Handler Overwrite Protection), a Windows security measure, to execute its code without being blocked.

Modifying COM Objects and Creating Uninstall Entries:

Malware creates or modifies COM (Component Object Model) objects in the Windows task scheduler to allow malicious processes to run automatically and adds uninstall entries to appear legitimate. COM is a Microsoft technology that allows different software to communicate with each other.

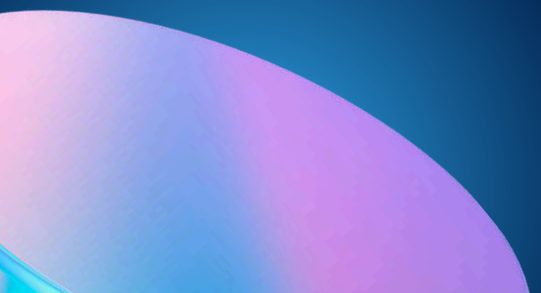
Running as a Windows Service:

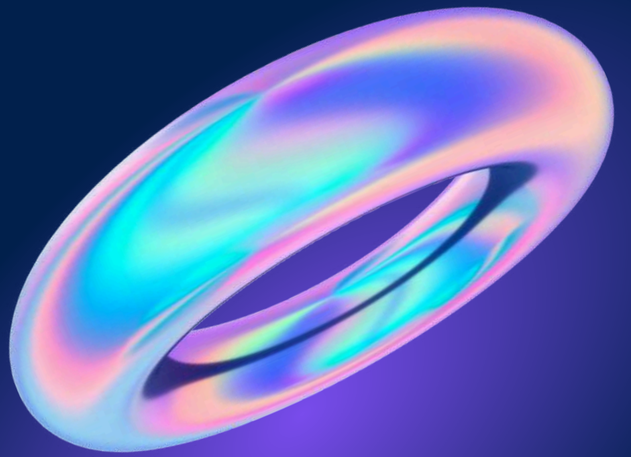
Malware runs as a Windows service to achieve persistence on the system.

Suspicious Behaviors:

- **Reading of security and system settings**
- **Creating files in temporary and program directories** (indicative of malicious activity)
- **Checking proxy settings and environment values** to better understand the system it is running on

Preventive Actions





Software Updates:

Keep all software updated with the latest security patches.

Advanced Security Solutions:

Use up-to-date and reliable antivirus and antimalware that include detection features based on abnormal behavior.

Controlling Attachments and Downloads:

Do not open email attachments or download software from untrusted sources. Always verify the authenticity of the source.

Implementation of Execution Restrictions:

Use tools such as AppLocker or Software Restriction Policies to restrict the execution of unauthorized executables.

Staff Training.

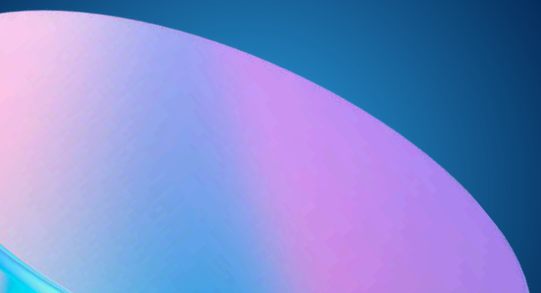
Regular Backups.

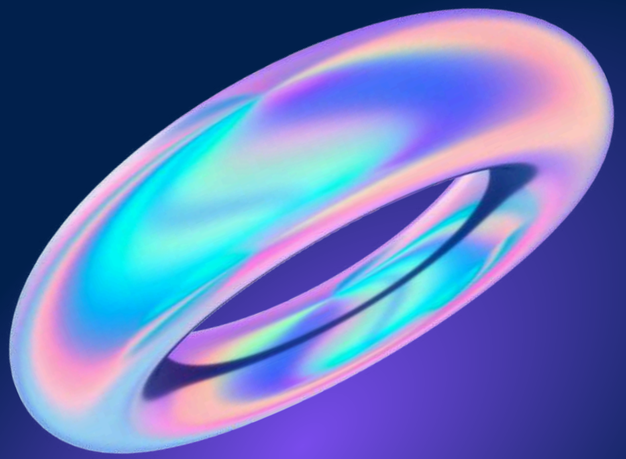
Monitoring and Logging
to detect suspicious activity and respond quickly to security incidents.

Security Patch Management
to reduce vulnerabilities.

Critical Systems Isolation and Network Segmentation
to reduce the impact of an infection.

Final Considerations





In conclusion, cybersecurity is a crucial aspect of our business.

It is important that all of us, users and managers, understand the risks and the preventive measures needed to protect our data and systems.

By remaining vigilant and adopting good security practices, we can significantly reduce the risk of cyber attacks.

OUR TEAM

Valerio Zampone

Giammarco Iorio

Gabriele Arcelli

Stefano Cesaroni

Thanks for your attention