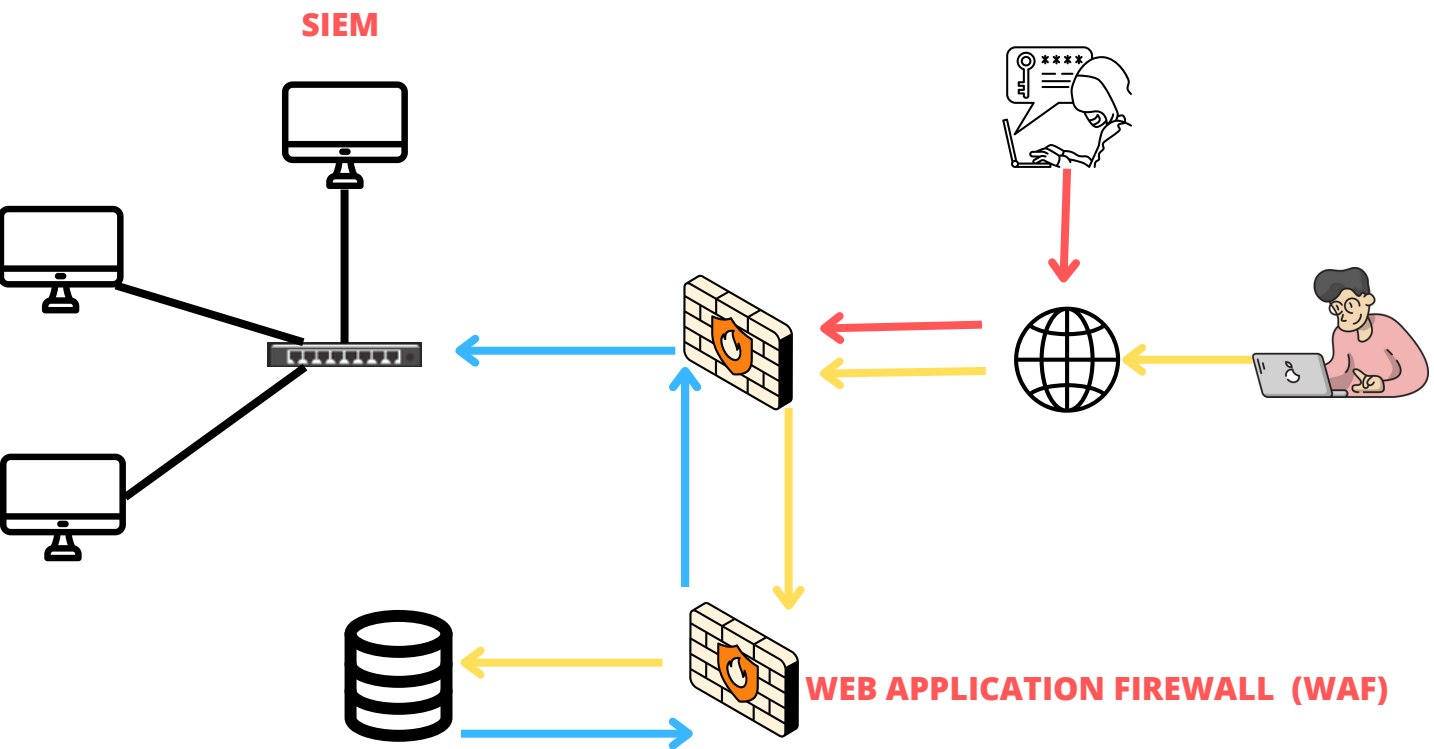


Esercizio 1

Eseguire azioni preventive per difendere l'app web da XSS e SQLi



Flusso applicazione - rete interna

Flusso attaccante - app e-commerce

Flusso utente - app e-commerce-

Per prevenire attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS) in un'applicazione e-commerce si può inserire un WAF per filtrare e bloccare attività sospette.

Si può inserire anche SIEM per tenere traccia di tutti i log.

Analisi dei link: <https://tinyurl.com/linklosco1> <https://tinyurl.com/linklosco2> 1) <https://tinyurl.com/linklosco1>

Analizzando la prima URL vado ad inserirla su Virus total

https://tinyurl.com/linklosco1

0 / 90

No security vendors flagged this URL as malicious

Reanalyze Search Graph API

Status: 200 Last Analysis Date: 29 minutes ago

Community Score

DETECTION DETAILS COMMUNITY

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

Security vendors' analysis Do you want to automate checks?

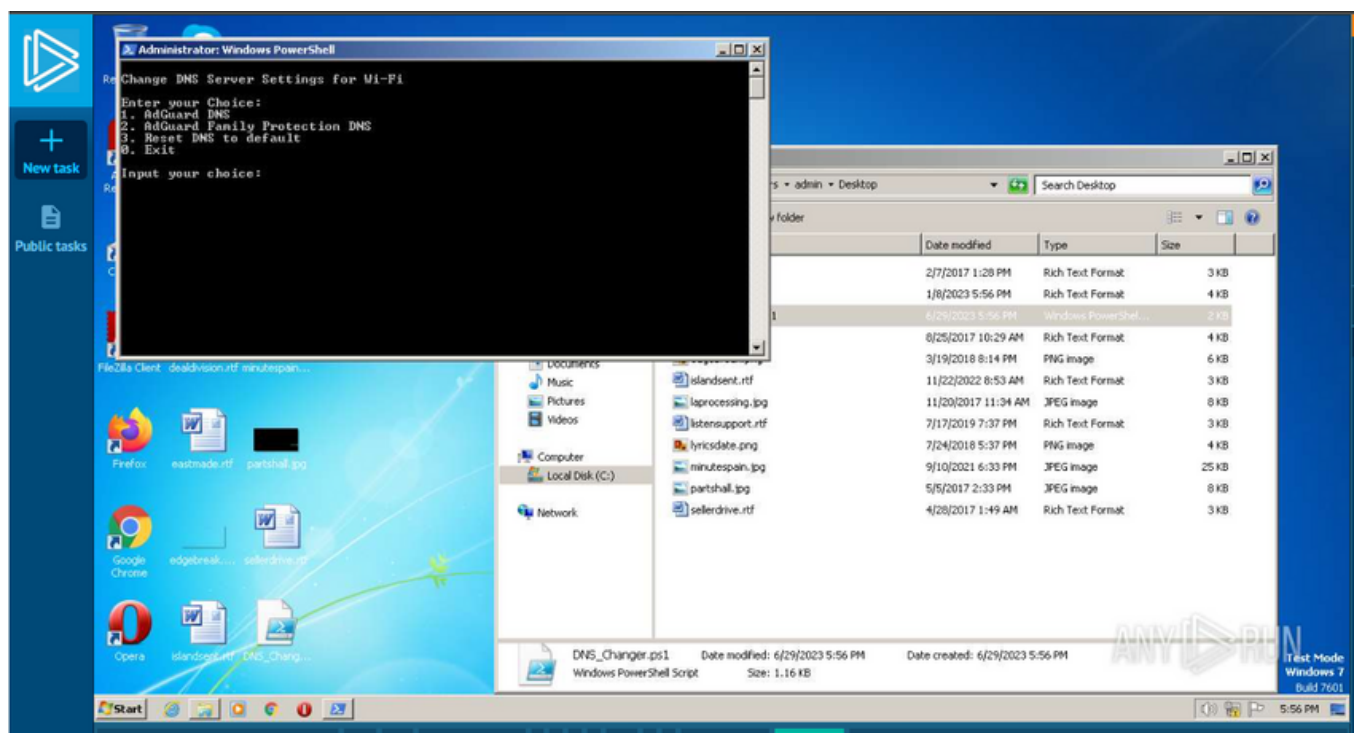
ArcSight Threat Intelligence Suspicious Abusix Clean

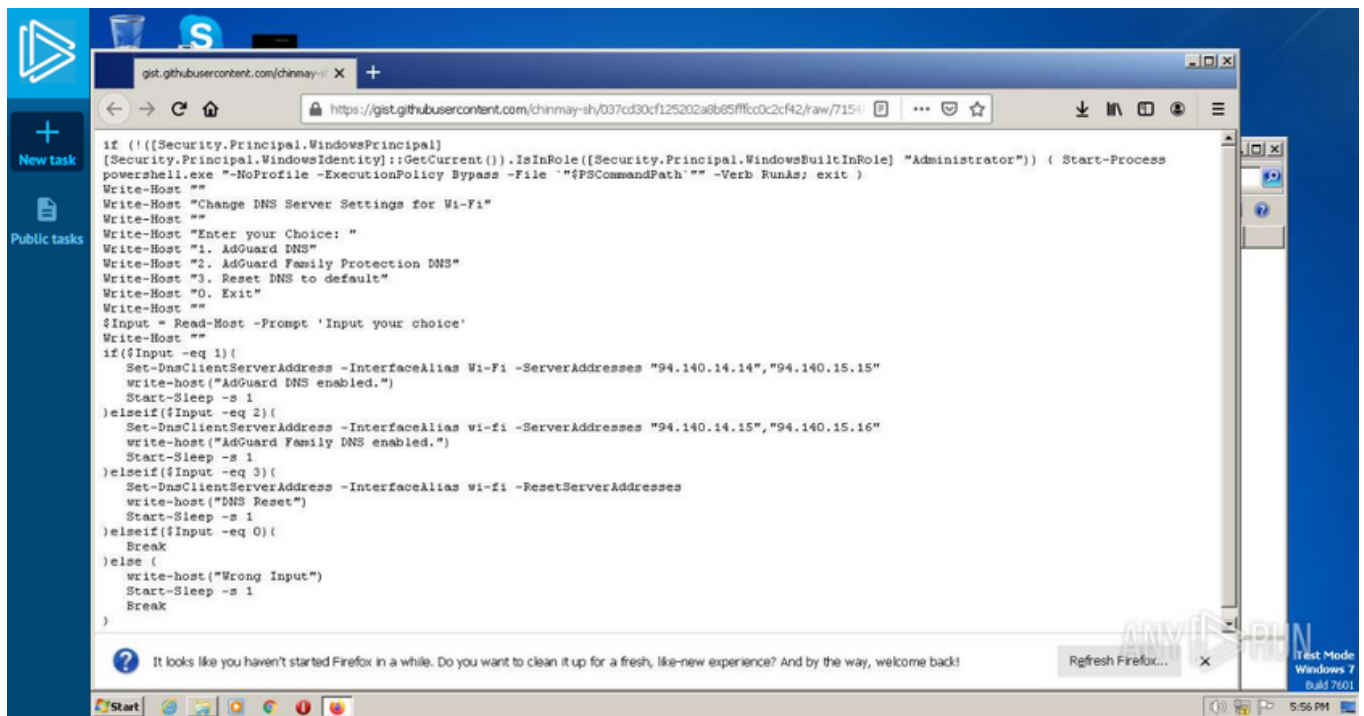
Virus total ci dice che è un link sospetto. Avverto i dipendenti di non aprire quel determinato link. Se è già stato aperto consiglio loro di cambiare tutte le password per una sicurezza preventiva.

Apro il link e mi ritrovo su anyrun dove posso analizzare l'eventuale minaccia.

Il primo link si tratta di una PowerShell che gestisce le impostazioni del server DNS..

Questa PoweShell ha un menù a scelta come si vede nella figura seguente.





Come si può vedere nella figura precedente digitando 1 o 2 cambierà il dns in "94.140.14.15" o "94.140.14.16"

Facendo un'analisi approfondita inserisco l'indirizzo ip su <https://talosintelligence.com/>

LOCATION DATA

📍 Cyprus

OWNER DETAILS

IP ADDRESS	94.140.14.15
FWD/REV DNS MATCH	Yes
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	adguard software limited

CONTENT DETAILS

📄 CONTENT CATEGORY No established content categories

Think these category details are incorrect?

[Submit Content Categorization Ticket](#)

REPUTATION DETAILS

📊 SENDER IP REPUTATION ● Neutral [Submit Sender IP Reputation Ticket](#)

📊 WEB REPUTATION ? Unknown [Submit Web Reputation Ticket](#)

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
📧 EMAIL VOLUME	0.0	0.0
📈 VOLUME CHANGE	0%	
📧 SPAM LEVEL	Medium	

BLOCK LISTS

Block List	Status
BL-SPAMCOPNET	Not Listed
CBLABUSEAT.ORG	Not Listed
PBL-SPAMHAUS.ORG	Not Listed
SBL-SPAMHAUS.ORG	Not Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST No

ADDITIONAL INFORMATION

[IP ADDRESSES](#) [WHOIS](#) [EMAIL VOLUME HISTORY](#)

Top IP Addresses used to send emails in 94.140.14.15 /24

IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
94.140.14.33	94-140-14-33.adguard.com	No	1.9	0.5	0	● Neutral

<https://talosintelligence.com/> dice che l'indirizzo ip è neutrale ovvero non ha rilevato alcuna minaccia.

ANALIZZARE IL MALWARE

» Enorme database di campioni e IOC
 » Configurazione personalizzata della VM
 » Inviati illimitati

Approccio interattivo

Iscriviti, è gratis

Informazioni generali

URL:

https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc0c2cf42/raw/7154ff6746be8626495a6ee7073889972c4580df/DNS_Changer.ps1

Analisi completa:

https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a

Verdetto:

Attività sospetta

Data di analisi:

29 giugno 2023 alle 18:56:12

Sistema operativo:

Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Indicatori:

MDS:

7CD193E2B9F15030CA538B924B4498C

SHA1:

07A04D3C4279FFE62968A4F76133B1AC71B490F

SHA256:

3B9E727C56BFA9A16E5311FBD17472B9DCBE2F1E149FA2924EDA013611076D039

SSDEEP:

3N81MCMEd2NM0YVVqJ3ERXM7JuqET+hdSedSXG2dzKhYMN:21MEgNMOYVUOadyfjSNWYMN

QUALSIASI RUN è un servizio interattivo che fornisce pieno accesso al sistema ospite. Le informazioni in questo rapporto potrebbero essere distorte dalle azioni dell'utente e sono fornite per il riconoscimento dell'utente così com'è. [QUALSIASI RUN](#) non garantisce la malizia o la sicurezza del contenuto.

Set di ambienti software e opzioni di analisi

Attività comportamentali

MALIZIOSO

Ignora la politica di esecuzione per eseguire i comandi
 • powershell.exe (PID: 3300)

SOSPETTO

Il processo esegue script Powershell
 • powershell.exe (PID: 2272)
 Il processo ignora il caricamento delle impostazioni del profilo di PowerShell
 • powershell.exe (PID: 2272)
 Legge le impostazioni Internet
 • powershell.exe (PID: 2272)
 • powershell.exe (PID: 3300)
 L'applicazione si è avviata da sola
 • powershell.exe (PID: 2272)
 Utilizzo di PowerShell per operare con gli account locali
 • powershell.exe (PID: 3300)
 Avvia POWERSHELL.EXE per l'esecuzione dei comandi
 • powershell.exe (PID: 3300)

INFORMAZIONI

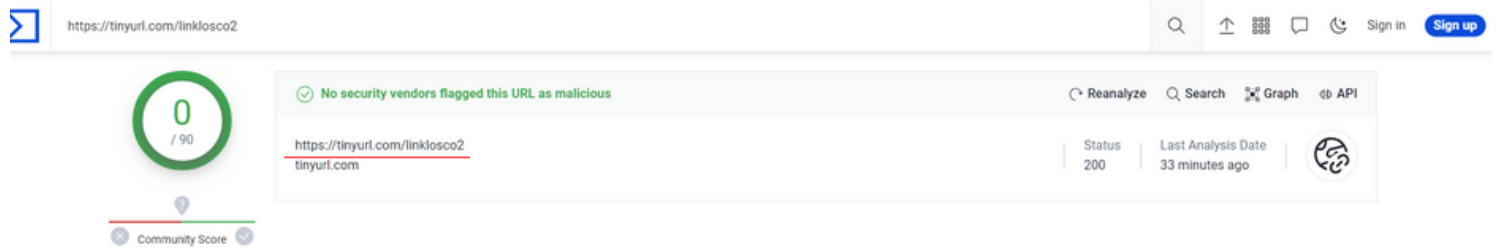
L'applicazione si è avviata da sola
 • firefox.exe (PID: 2976)
 • firefox.exe (PID: 3384)
 Il processo utilizza il file scaricato
 • powershell.exe (PID: 2272)
 • firefox.exe (PID: 3384)
 Esecuzione manuale da parte di un utente
 • powershell.exe (PID: 2272)

Any run ci dice che è un attività sospetta infatti essa può essere eseguita in automatico ma soprattutto comunicare con gli account locali

Fase di contenimento, rimozione e recupero

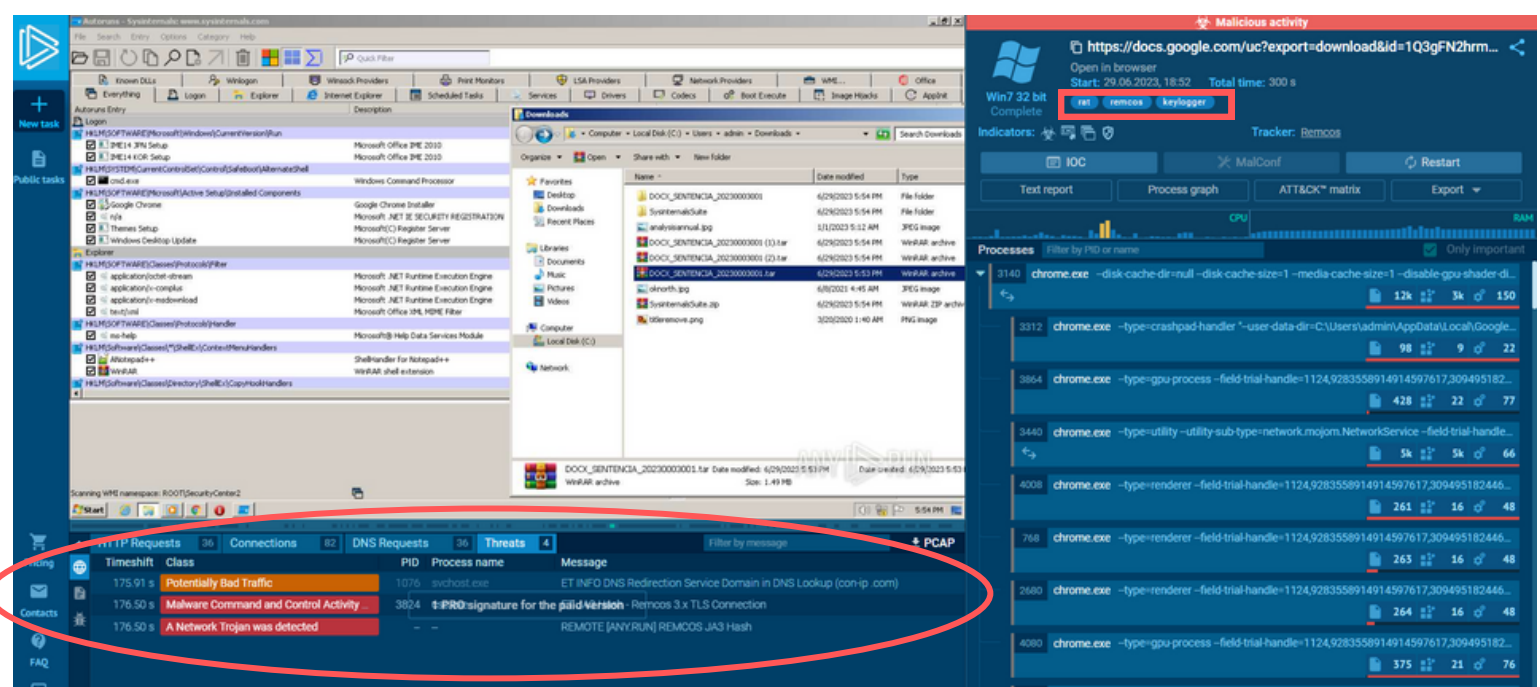
- 1) Se un dipendente ha aperto il link dividere la rete in diverse Vlan
- 2) Avvertire l'azienda
- 3) Recupero dati causati da eventuali danni
- 4) Ripulire completamente il dispositivo danneggiato

2) <https://tinyurl.com/linklosco2>



Virus total ci dice che è un link sospetto. Avverto i dipendenti di non aprire quel determinato link. Se è già stato aperto consiglio loro di cambiare tutte le password per una sicurezza preventiva.

Apro il link e mi ritrovo su anyrun dove posso analizzare l'eventuale minaccia,



Analizzando l'eventuale minaccia Anyrun ci dice che siamo di fronte ad un malware chiamato Remocs.

- 1)Potenziale traffico cattivo
- 2)Un keylogger
- 3)Ha rilevato un trojan

ANYRUN

ANALIZZARE IL MALWARE

» Enorme database di campioni e IOC

» Configurazione personalizzata della VM

» Invii illimitati

Approccio interattivo

Iscriviti, è gratis

ANYRUN

INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Aggiungi per la stampa

URL:

https://docs.google.com/uc?export=download&id=1Q3gFN2hmBADT0BymgtAG_apwYt60Ys

Analisi completa:

https://app.any.run/tasks/685ba854-4644-4140-9ea5-be9057161248

Verdetto:

Attività dannosa

Minacce:

Remcos

Remcos è un malware di tipo RAT che gli aggressori utilizzano per eseguire azioni su macchine infette da remoto. Questo malware è aggiornato in modo estremamente attivo con aggiornamenti in uscita quasi ogni mese.

Data di analisi:

29 giugno 2023 alle 18:52:04

Sistema operativo:

Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tag:

ratto remcos registratore di tasti

Indicatori:

MD5:

F227842BC5D29AC82A82C40B6325B9E3

SHA1:

E5AA130B362D68AD2010540C0DE6BE3372DA3375

SHA256:

B24023DF44B0A1074B5D6BB8A66DA16FA4C10918C5C21E0100C4B12CAE056C49

SSDEEP:

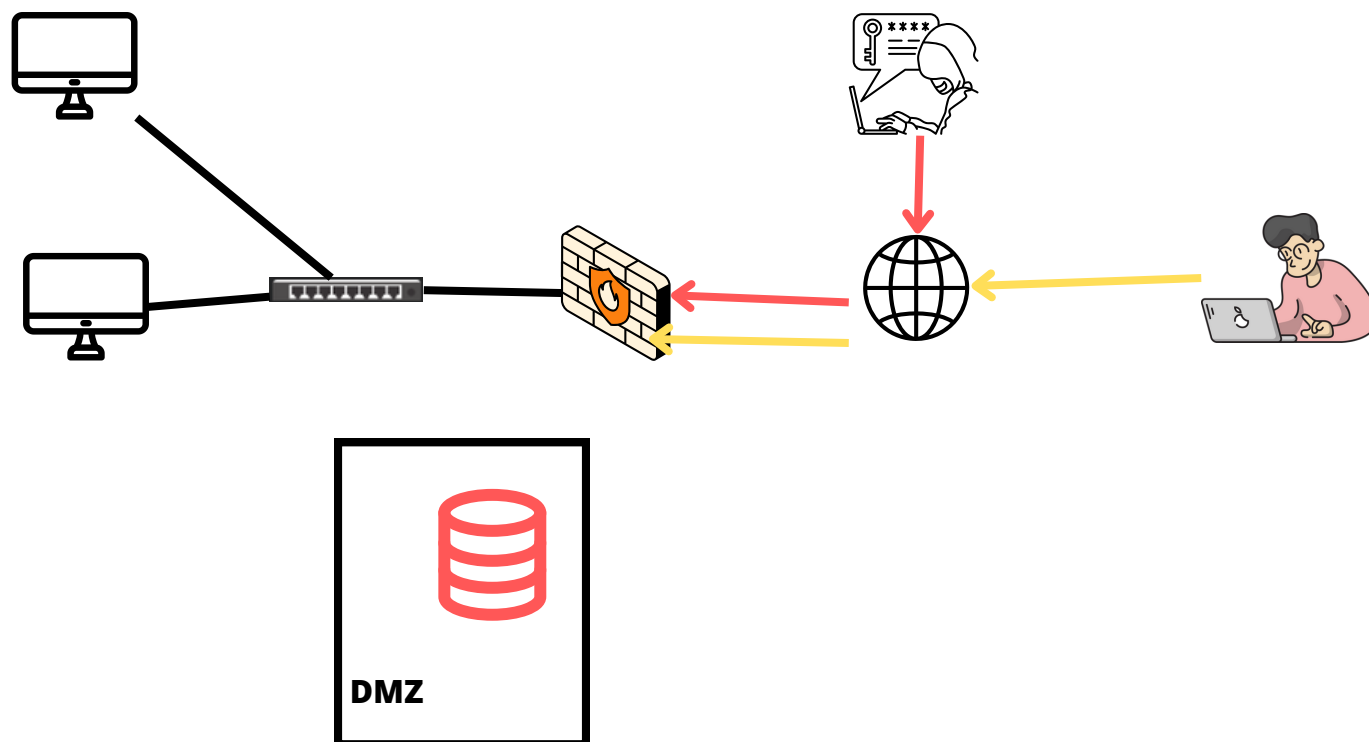
3.NBSP9uZNAaBrC20ZrVhG0NZT2n2Sm2BB+2oxvc5in

Fase di contenimento, rimozione e recupero

- 1) Se un dipendente ha aperto il link dividere la rete in diverse Vlan
- 2) Avvertire l'azienda
- 3) Recupero dati causati da eventuali danni
- 4) Ripulire completamente il dispositivo danneggiato

Esercizio 3

L'applicazione Web è stata infettata da un malware. Il malware non si deve propagare sulla rete e non devono essere divulgate info sensibili.

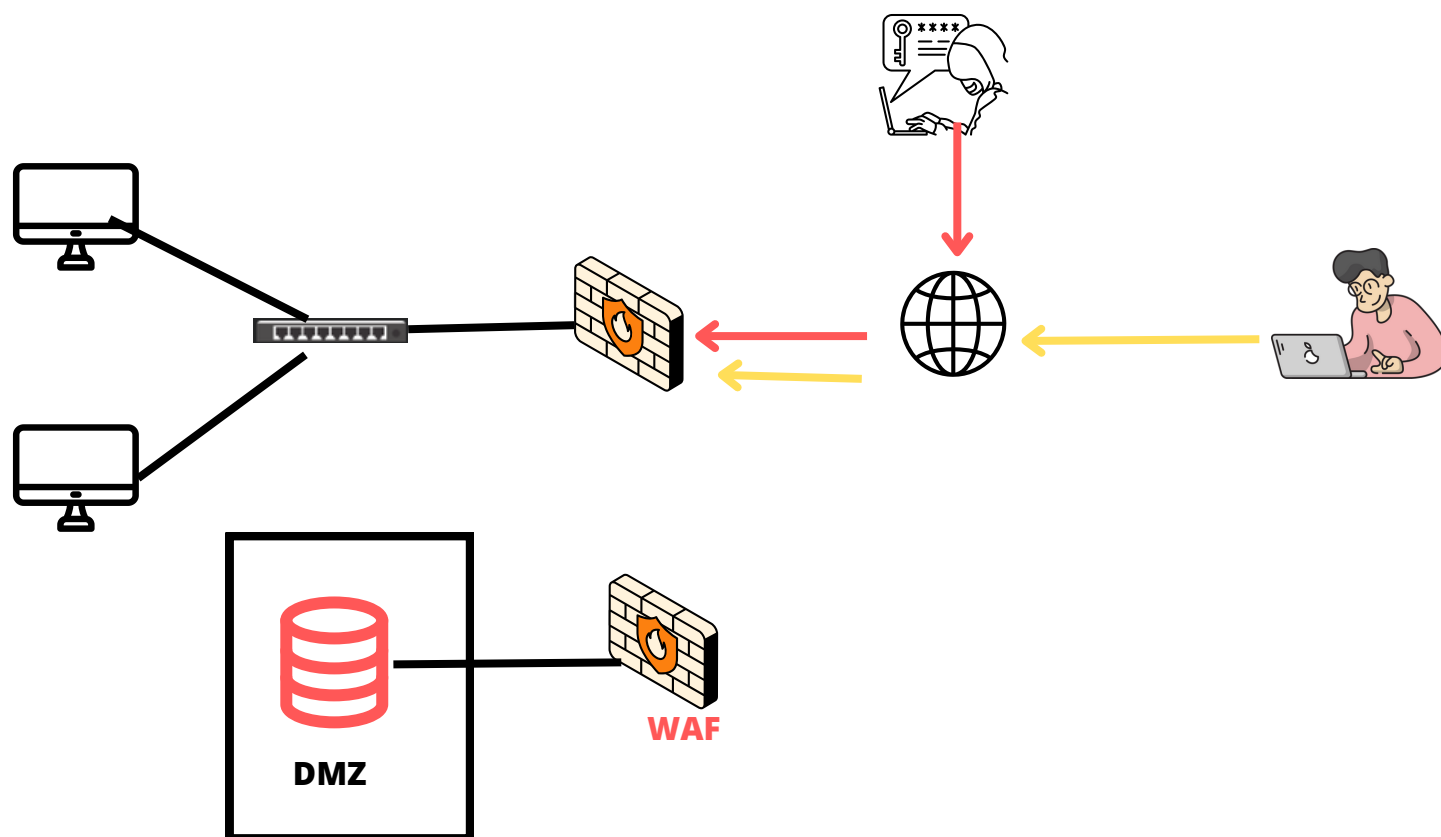


La priorità è che il malware non si propaghi sulla nostra rete, dopo l'attacco e non divulgare dati sensibili, quindi andiamo bloccare la web app rendendola inaccessibile.

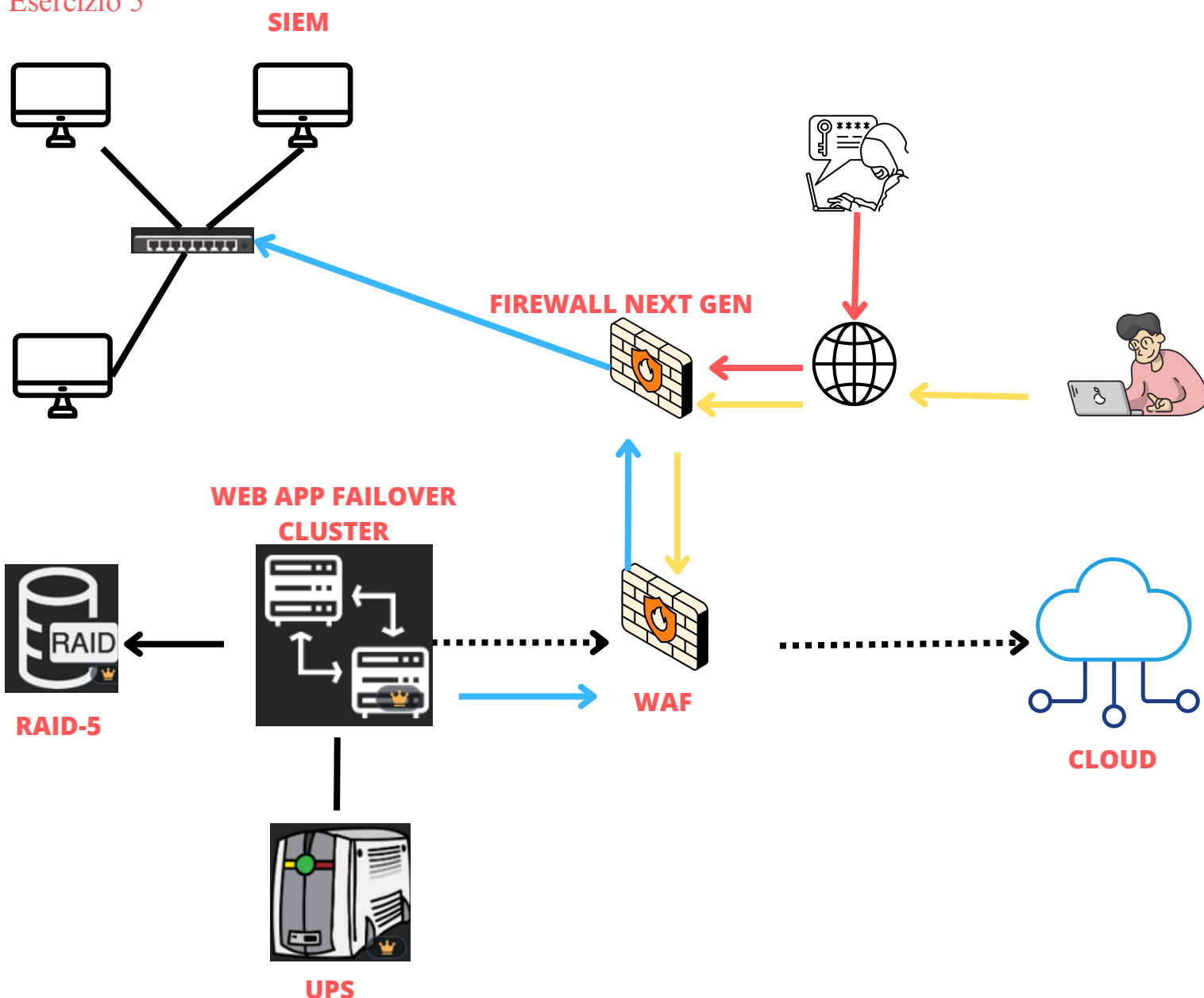
Andiamo a creare una zona di quarantena dove ci sarà la nostra Web App.

Esercizio 4

Unisco le azioni preventive e la response



Esercizio 5



Per implementare la sicurezza dell'infrastruttura di seguito sono riportati alcuni consigli

Piano di disaster recovery

- Creazione di un EXECUTIVE SUMMARY
- Configurazione di un RAID-5
- Acquisto di un UPS per il servizio critico
- Acquisto di un Cloud
- Backup
- In questo modo si ha una triplice copia, due locazioni per il backup e una off-site

Acquisto di ulteriori hardware/software

- Firewall next gen effettua un'analisi su tutti i livelli iso/osi. Include un ids per il filtraggio di connessioni malevoli.
- Acquisto di un software SIEM per il continuo monitoraggio dei log (SPLUNK)
- Ridondanza di un applicativo e-commerce, utile se la web app principale è infettata da un malware.