Architettura di rete

Traccia

Traccia:

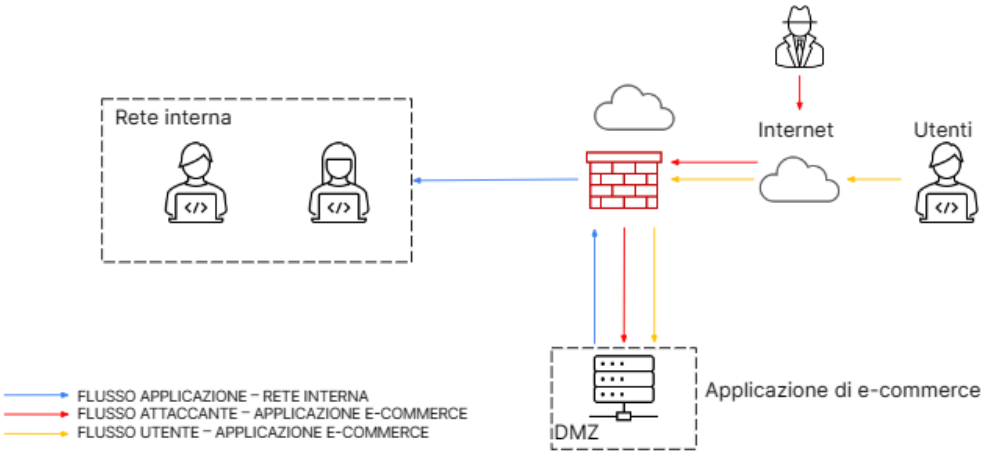
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
   Modificate la figura in modo da evidenziare le implementazioni
2. **Analisi attacco**: analizzare i seguenti link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco https://tinyurl.com/linklosco1 https://tinyurl.com/linklosco2
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, ma è altrettanto importante non divulgare informazioni sensibili verso Internet.
   Modificate la figura in slide 2 con la soluzione proposta.
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. **Modifica «più aggressiva» dell'infrastruttura:** integrando eventuali altri elementi di sicurezza

Rete

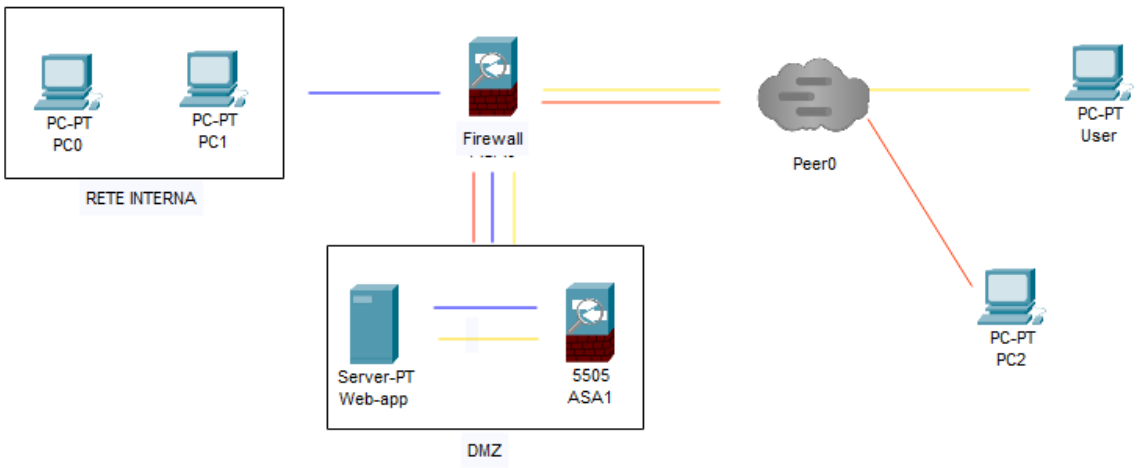
Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

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.



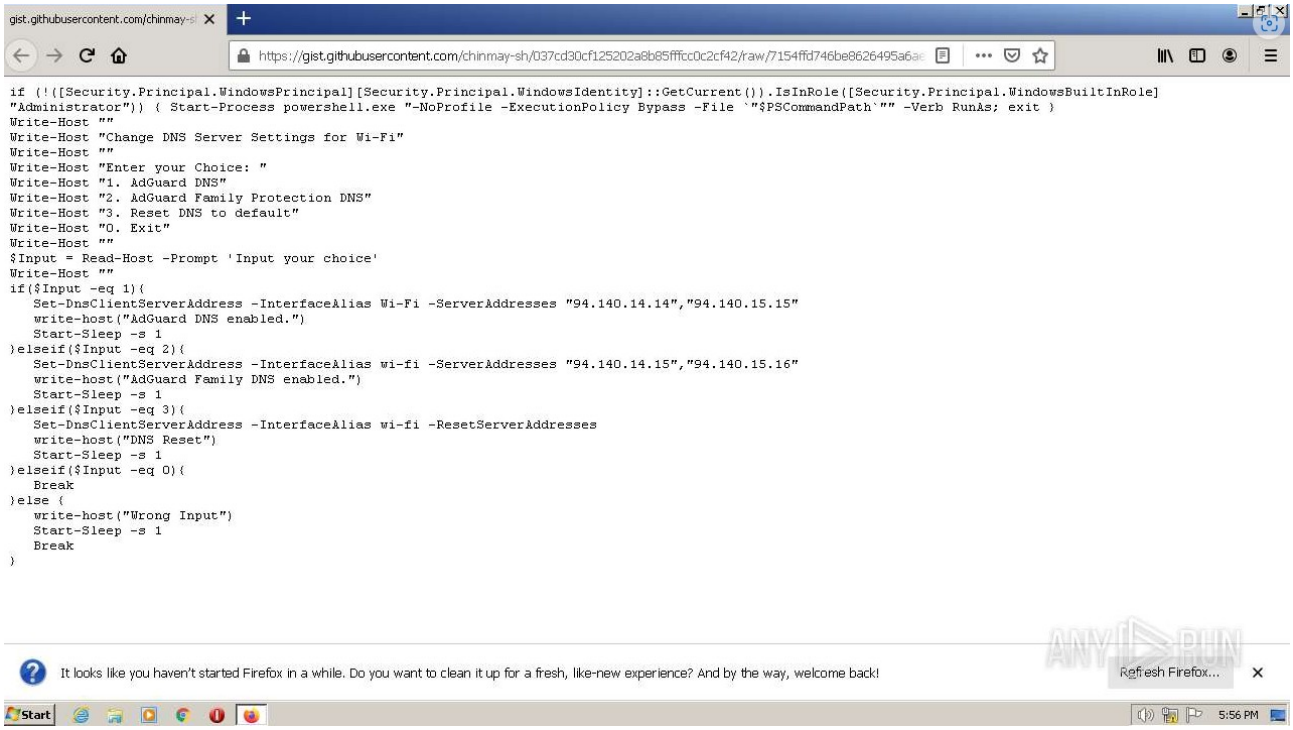
Azione preventive

Come detto nella traccia per prevenire attacchi di tipo SQLi o XSS potremmo aggiungere un web application firewall



Analisi attacco

Dopo aver eseguito il file sul browser tramite il link con l’aiuto di any.run ho potuto sintetizzare l’attacco malware attraverso un text report.
Da questo di deduce che il codice avesse come obbiettivo di bypassare Windows powerShell, alterando il server:visibile nel secondo screen.
Di seguito troviamo alcuni screen dove è possibile vedere l’analisi del file tramite virustotal dove ci restituisce un risultato suspicious.


gist.githubusercontent.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ac
if (!([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]
"Administrator")) { Start-Process powershell.exe "-NoProfile -ExecutionPolicy Bypass -File `"$PSCommandPath`"" -Verb RunAs; exit }
Write-Host ""
Write-Host "Change DNS Server Settings for Wi-Fi"
Write-Host ""
Write-Host "Enter your Choice: "
Write-Host "1. AdGuard DNS"
Write-Host "2. AdGuard Family Protection DNS"
Write-Host "3. Reset DNS to default"
Write-Host "0. Exit"
Write-Host ""
$Input = Read-Host -Prompt 'Input your choice'
Write-Host ""
if($Input -eq 1){
Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.14","94.140.15.15"
write-host("AdGuard DNS enabled.")
Start-Sleep -s 1
}elseif($Input -eq 2){
Set-DnsClientServerAddress -InterfaceAlias wi-fi -ServerAddresses "94.140.14.15","94.140.15.16"
write-host("AdGuard Family DNS enabled.")
Start-Sleep -s 1
}elseif($Input -eq 3){
Set-DnsClientServerAddress -InterfaceAlias wi-fi -ResetServerAddresses
write-host("DNS Reset")
Start-Sleep -s 1
}elseif($Input -eq 0){
Break
}else {
write-host("Wrong Input")
Start-Sleep -s 1
Break
}
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Start
5:56 PM

Intendevi invece eseguire una ricerca nel corpus dei file? **Clicca qui**

0 / 90

Punteggio della community

No security vendors flagged this URL as malicious

Reanalyze | Search | Graph | API

https://tinyurl.com/linklosco1
tinyurl.com

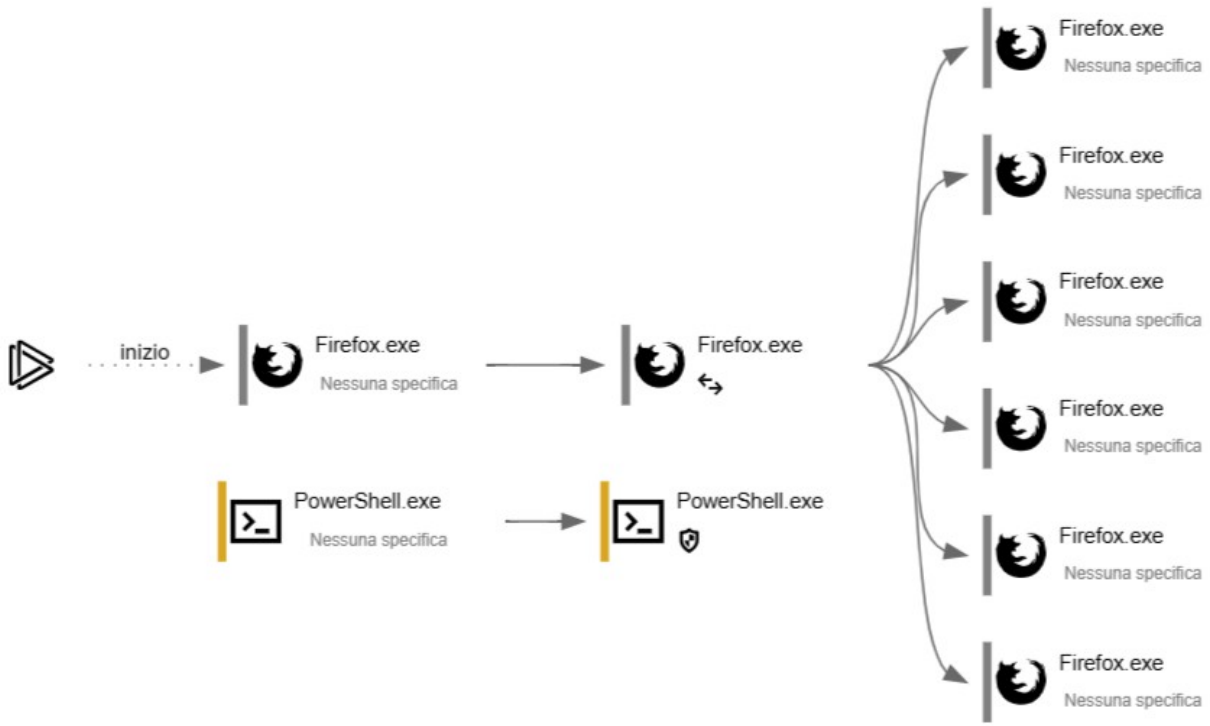
Status 200 | Last Analysis Date 1 minute ago

SCOPERTA | DETTAGLI | COMUNITÀ

Unisciti alla community VT e usufruisci di ulteriori approfondimenti della community e rilevamenti in crowdsourcing, oltre a una chiave API per automatizzare i controlli.

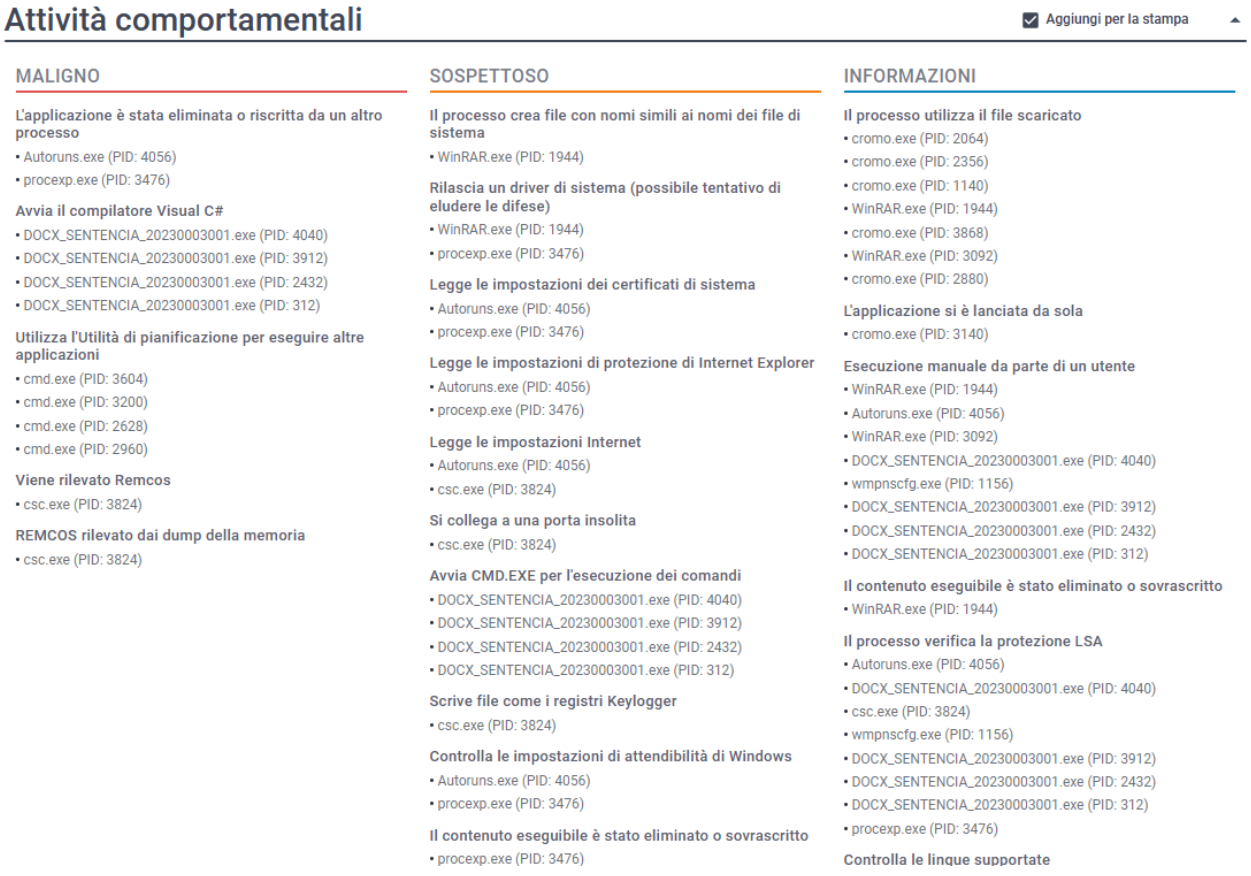
Security vendors' analysis | Do you want to automate checks?

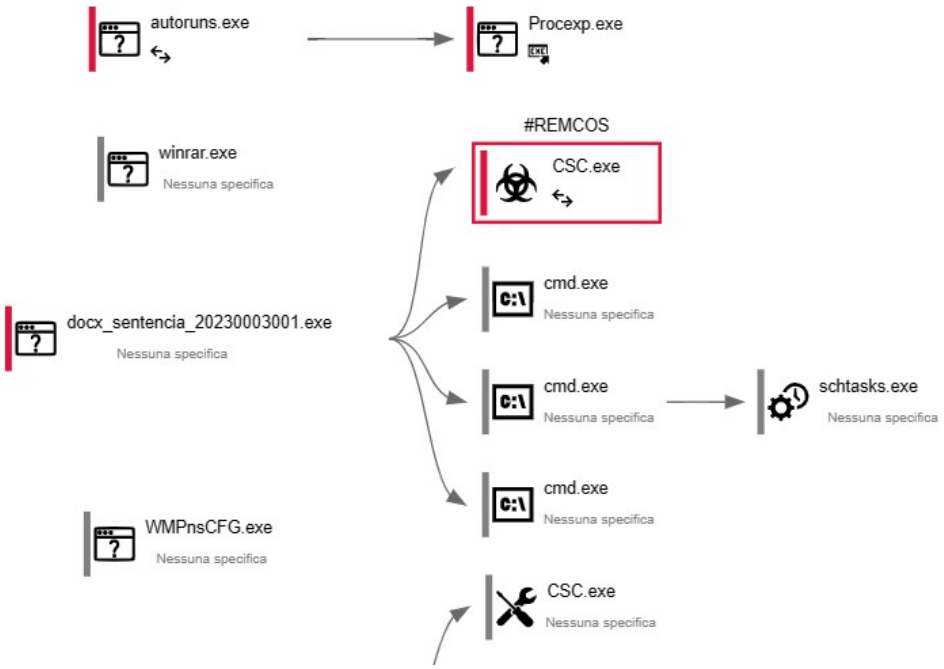
ArcSight Threat Intelligence	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean
Emsisoft	Clean	ESET	Clean
ESTsecurity	Clean	Feodo Tracker	Clean
Forcepoint ThreatSeeker	Clean	Fortinet	Clean
G-Data	Clean	Google Safebrowsing	Clean

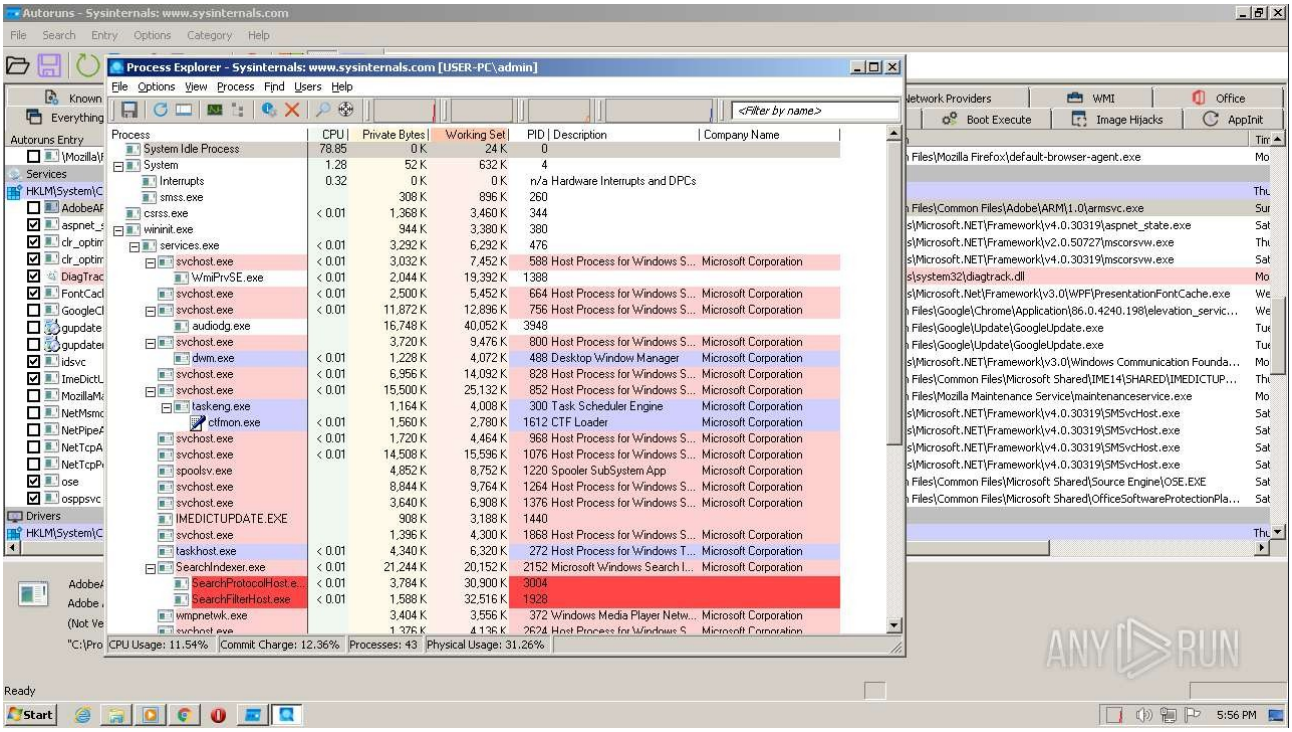

inizio
Firefox.exe
Nessuna specifica
Firefox.exe
PowerShell.exe
Nessuna specifica
PowerShell.exe
Firefox.exe
Nessuna specifica
Firefox.exe
Nessuna specifica
Firefox.exe
Nessuna specifica
Firefox.exe
Nessuna specifica
Firefox.exe
Nessuna specifica
Firefox.exe
Nessuna specifica

Secondo file

Anche in questo caso ho eseguito un analisi con any.run ed virustotal e tramite il text report, notiamo la presenza di un malware che permette il controllo della macchina bersaglio, permettendo il totale accesso tipica funzione della backdoor.
In basso possiamo vedere le attività maligne eseguite dal malware con il conseguente percorso che ha permesso il controllo della macchina



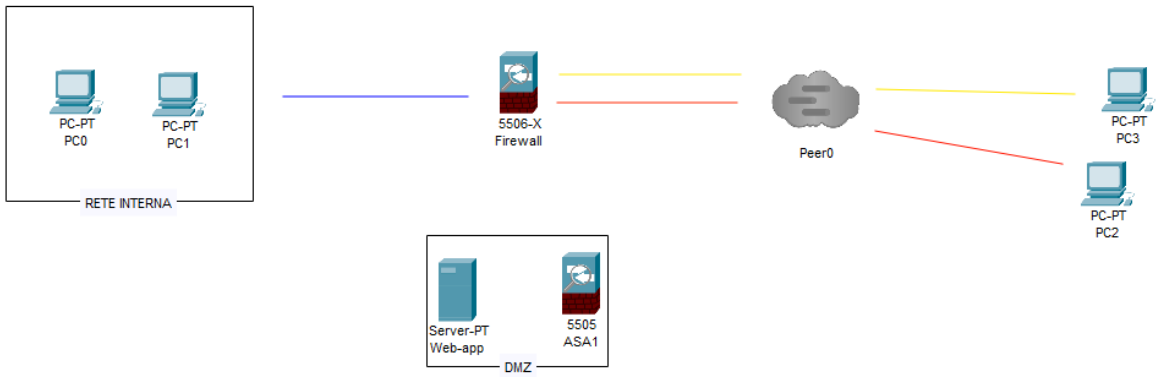

autoruns.exe
Procexp.exe
#REMCOS
winrar.exe
Nessuna specifica
CSC.exe
cmd.exe
Nessuna specifica
docx_sentencia_20230003001.exe
Nessuna specifica
cmd.exe
Nessuna specifica
schtasks.exe
Nessuna specifica
cmd.exe
Nessuna specifica
WMPnsCFG.exe
Nessuna specifica
CSC.exe
Nessuna specifica


Autoruns - Sysinternals: www.sysinternals.com
Process Explorer - Sysinternals: www.sysinternals.com [USER-PC\admin]
CPU Usage: 11.54%
Commit Charge: 12.36%
Processes: 43
Physical Usage: 31.26%
ANY RUN
Ready
Start
5:56 PM

Response

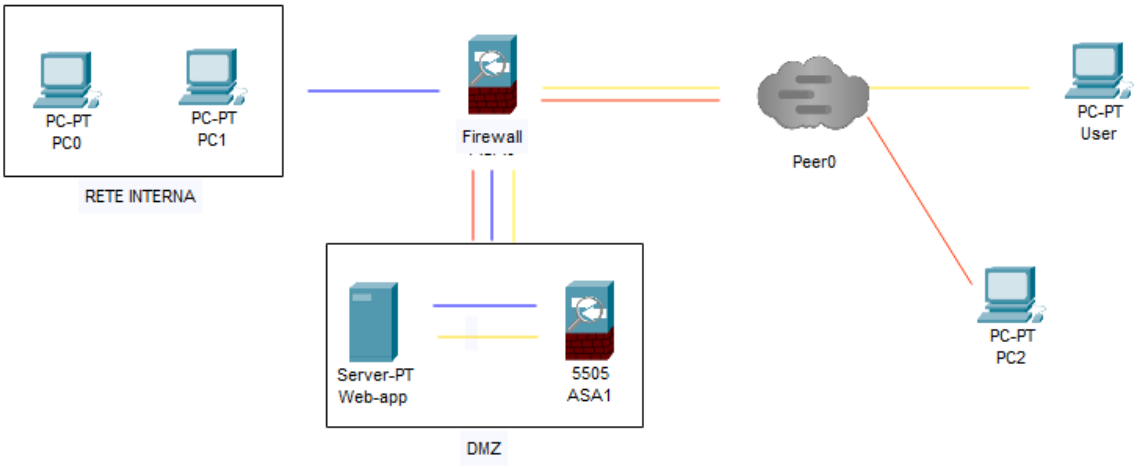
In questo caso il malware ha infettato il web app e di conseguenza dobbiamo evitare che si propaghi nell’intera rete provocando molti danni…

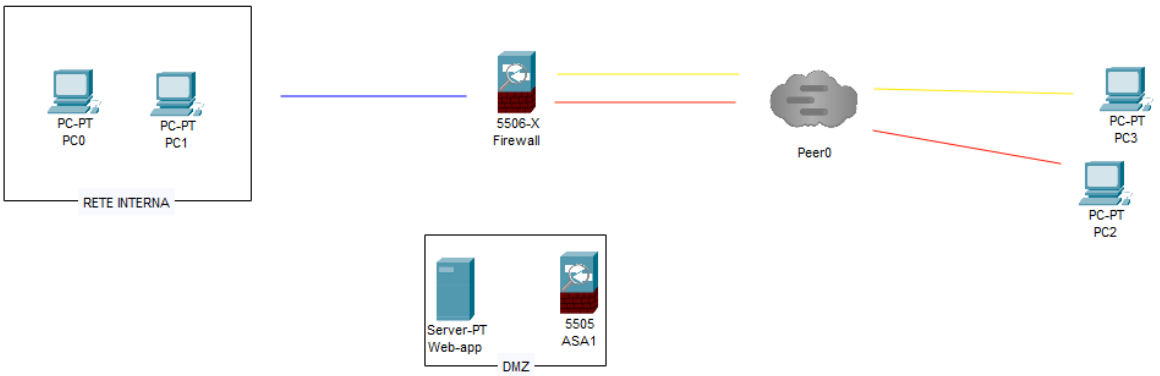
Come descritto nell’immagine ho isolato il web server evitando l’accesso a chiunque evitando qualsiasi tipo di intr

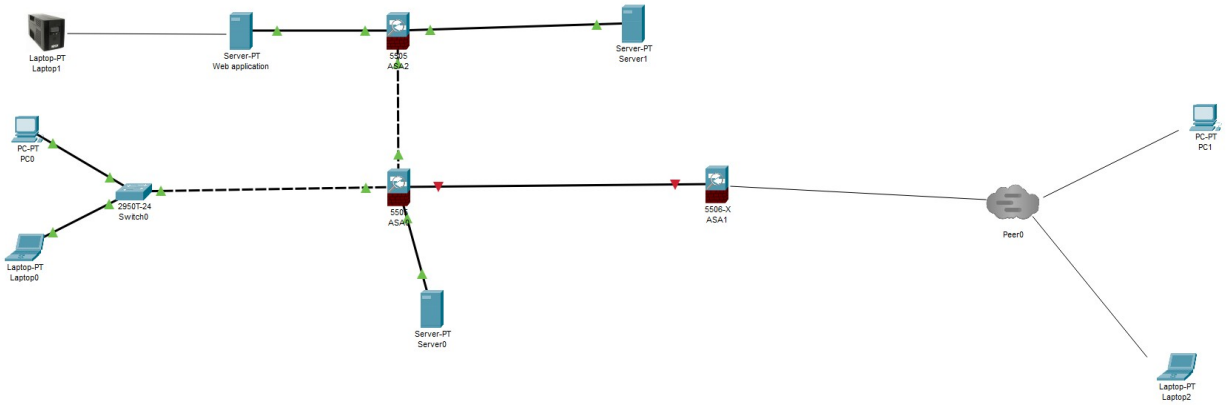


Soluzione completa

Unione delle precedenti schemi




PC-PT
PC0
PC-PT
PC1
RETE INTERNA
5506-X
Firewall
Peer0
PC-PT
PC3
PC-PT
PC2
Server-PT
Web-app
5505
ASA1
DMZ


Laptop-PT
Laptop1
Server-PT
Web application
5505
ASA2
Server-PT
Server1
PC-PT
PC0
2950T-24
Switch0
5505
ASA
5506-X
ASA1
Peer0
PC-PT
PC1
Laptop-PT
Laptop0
Server-PT
Server0
Laptop-PT
Laptop2

Modifica aggressiva

Per rendere la rete più sicura/aggressiva potremmo aggiungere un firewall, con tecnologia ngfw open source con diverse funzionalità, quali: la vpn, web filtering, DdoS protection, email security… con quest'ultimo è possibile controllare l'intera gestione della sicurezza molto più semplicemente attraverso un'unica soluzione. In aggiunta al firewall possiamo anche integrare il dmz come descritto anche nel grafico che consente il data storage tramite il raid.
 Cioè un insieme rindondante di dischi indipendenti, infatti qualora un disco dovesse avere dei problemi entra in gioco il secondo, e cosi via creando un ecosistema in grado di mantenere e garantire la continuita del backup server anche nei casi più spiacevoli.