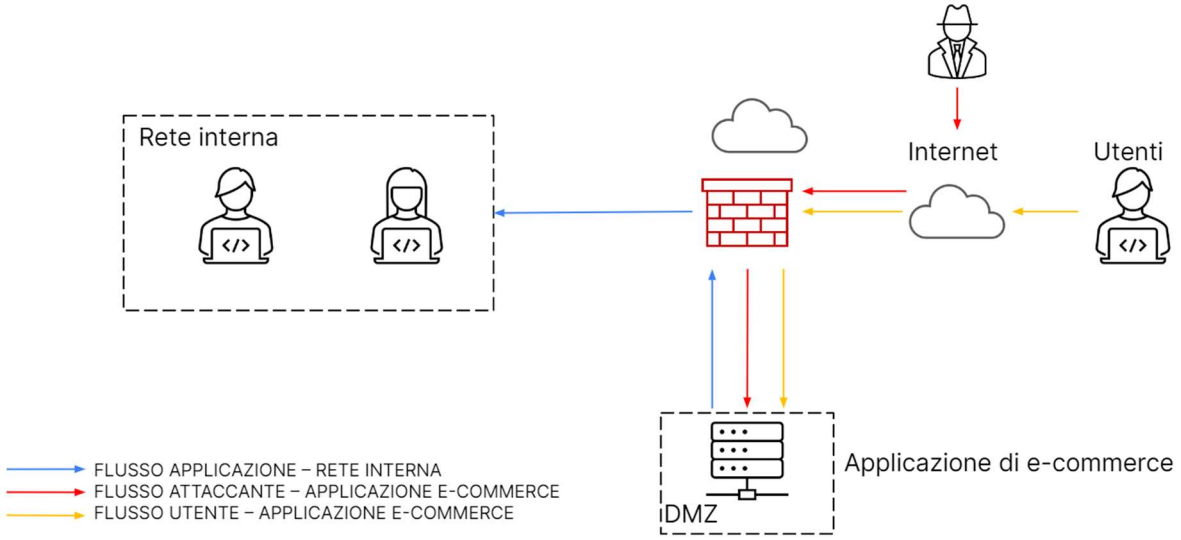
Pierluigi Amorese

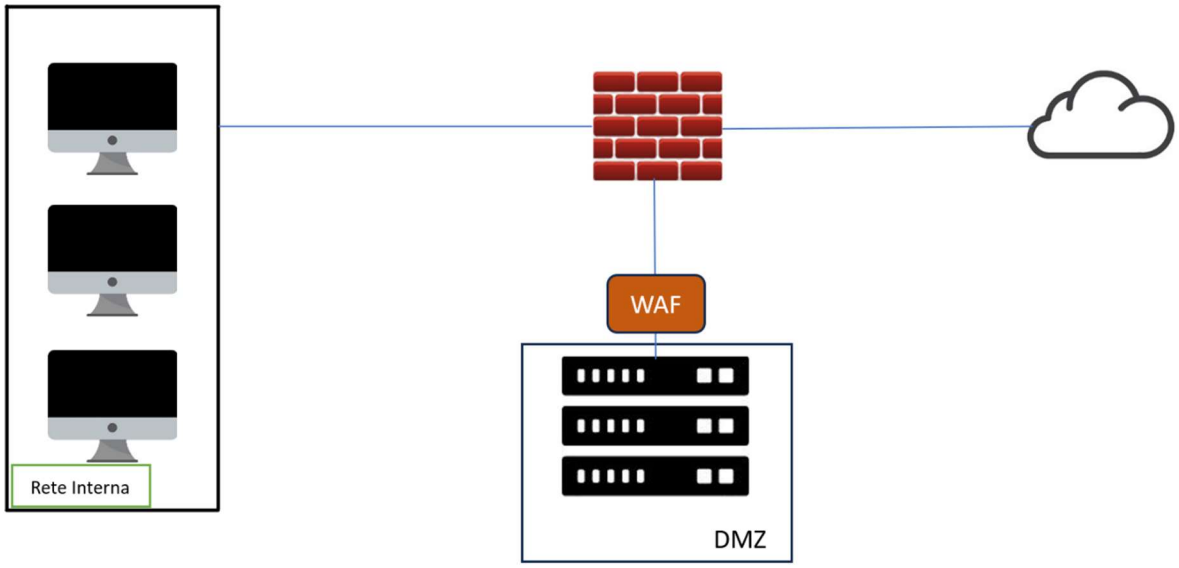
Progetto Giorno 5

La traccia di oggi ci propone di attuare delle azioni preventive, di analisi e di response di un caso reale.

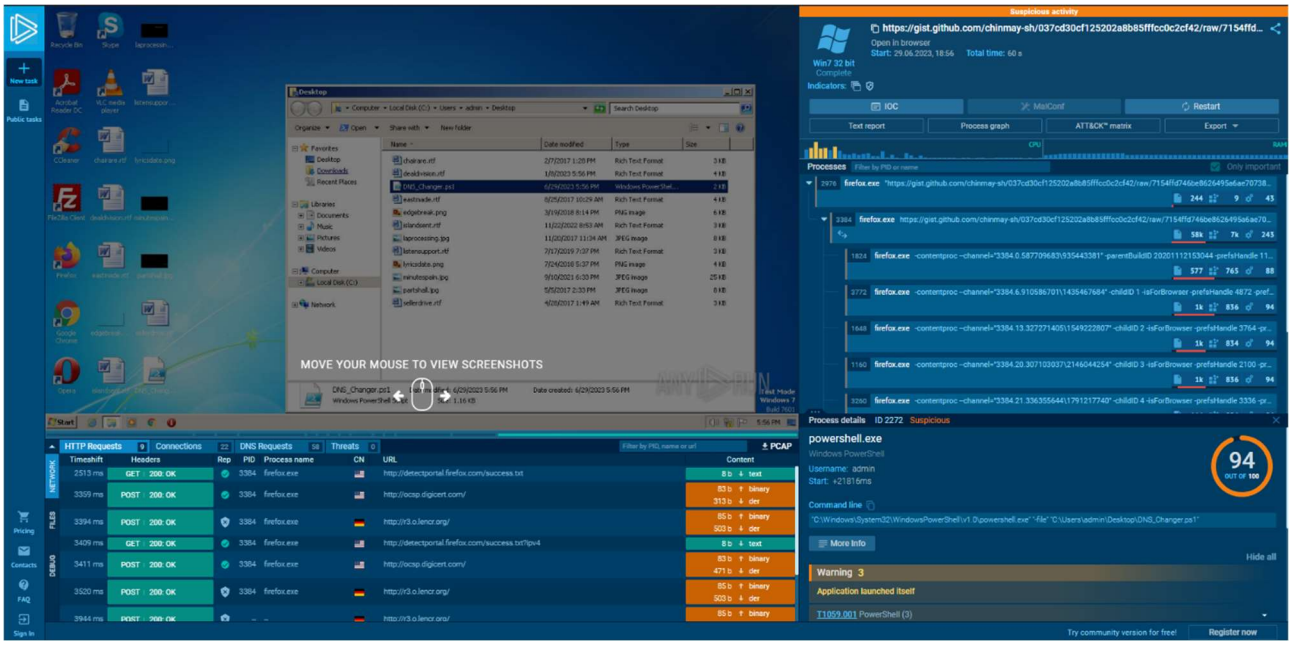
Data la figura sottostante il primo punto della traccia ci chiede quali azioni preventive si possono effettuare per difendere l'applicazione web da attacchi di tipo SQLi e XXS.



Come soluzione si propone di aggiungere come sistema di sicurezza un Web Application Firewall (WAF) ovvero un firewall che monitora, filtra e blocca i pacchetti di dati mentre viaggiano da e verso un sito Web o un'applicazione Web.



Come secondo task, la traccia ci chiede di analizzare i seguenti siti: https://tinyurl.com/linklosco1 https://tinyurl.com/linklosco2



Aprendo il primo link veniamo reindirizzati verso una pagina di Any.run e tramite il report possiamo capire di cosa si tratta:

Behavior activities

Add for printing

MALICIOUS

Bypass execution policy to execute commands
- powershell.exe (PID: 3300)

SUSPICIOUS

The process executes Powershell scripts
- powershell.exe (PID: 2272)

The process bypasses the loading of PowerShell profile settings
- powershell.exe (PID: 2272)

Reads the Internet Settings
- powershell.exe (PID: 2272)
- powershell.exe (PID: 3300)

Application launched itself
- powershell.exe (PID: 2272)

Using PowerShell to operate with local accounts
- powershell.exe (PID: 3300)

Starts POWERSHELL.EXE for commands execution
- powershell.exe (PID: 2272)

INFO

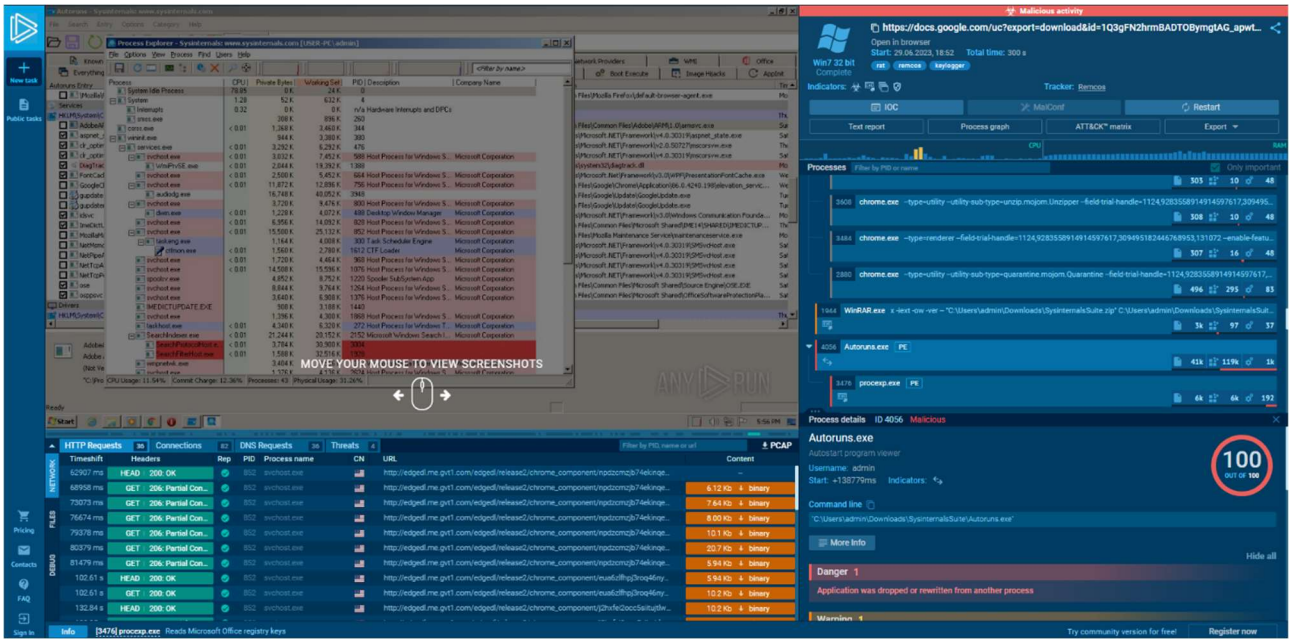
Application launched itself
- firefox.exe (PID: 2976)
- firefox.exe (PID: 3384)

The process uses the downloaded file
- powershell.exe (PID: 2272)
- firefox.exe (PID: 3384)

Manual execution by a user
- powershell.exe (PID: 2272)

L'analisi ci permette di capire che si tratta di uno script in grado di aprire (grazie a permessi da amministratore di default) in automatico una shell sulla macchina vittima.

Nel secondo link viene analizzato Remcos Rat o Remote Control and Surveillance, commercializzato come un software legittimo per gestire in remoto i sistemi Windows.



Remcos è un sofisticato Trojan di accesso remoto (RAT) che può essere utilizzato per controllare e monitorare completamente qualsiasi computer Windows da XP.

Behavior activities

Add for printing

MALICIOUS

Application was dropped or rewritten from another process
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Starts Visual C# compiler
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Uses Task Scheduler to run other applications
- cmd.exe (PID: 3604)
- cmd.exe (PID: 3200)
- cmd.exe (PID: 2628)
- cmd.exe (PID: 2960)

Remcos is detected
- csc.exe (PID: 3824)

REMCOS detected by memory dumps
- csc.exe (PID: 3824)

SUSPICIOUS

The process creates files with name similar to system file names
- WinRAR.exe (PID: 1944)

Drops a system driver (possible attempt to evade defenses)
- WinRAR.exe (PID: 1944)
- procexp.exe (PID: 3476)

Reads settings of System Certificates
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads security settings of Internet Explorer
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads the Internet Settings
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

Connects to unusual port
- csc.exe (PID: 3824)

Starts CMD.EXE for commands execution
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Writes files like Keylogger logs
- csc.exe (PID: 3824)

Checks Windows Trust Settings
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Executable content was dropped or overwritten
- procexp.exe (PID: 3476)

INFO

The process uses the downloaded file
- chrome.exe (PID: 2064)
- chrome.exe (PID: 2356)
- chrome.exe (PID: 1140)
- WinRAR.exe (PID: 1944)
- chrome.exe (PID: 3868)
- WinRAR.exe (PID: 3092)
- chrome.exe (PID: 2880)

Application launched itself
- chrome.exe (PID: 3140)

Manual execution by a user
- WinRAR.exe (PID: 1944)
- Autoruns.exe (PID: 4056)
- WinRAR.exe (PID: 3092)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

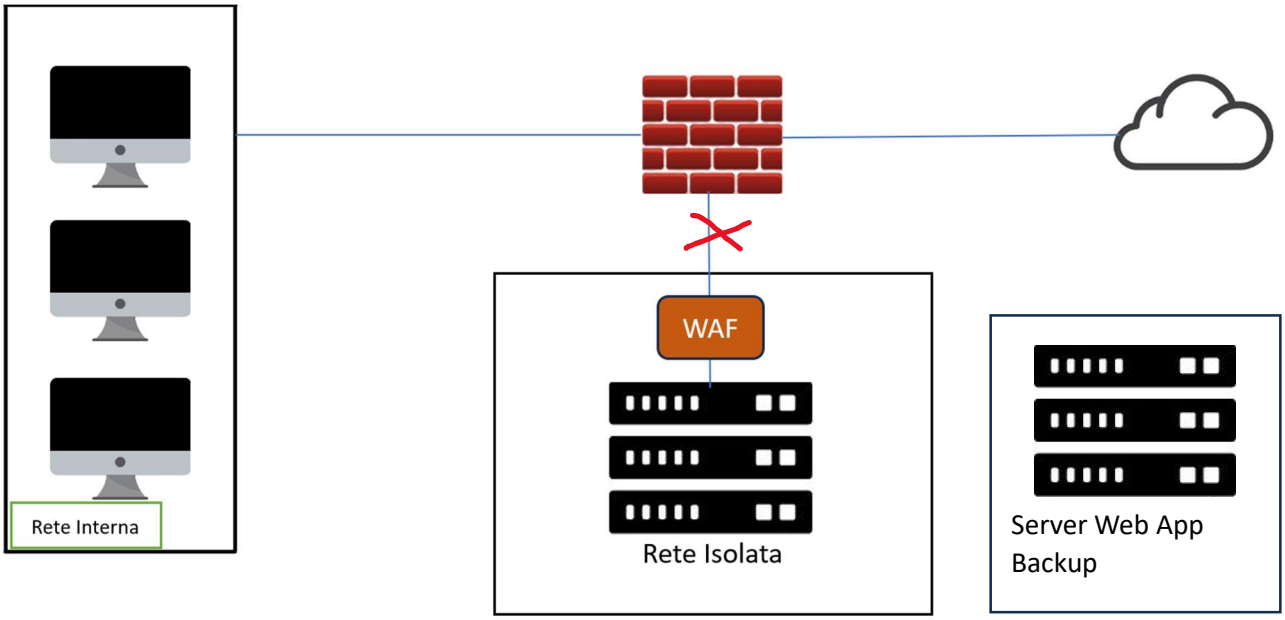
Executable content was dropped or overwritten
- WinRAR.exe (PID: 1944)

The process checks LSA protection
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)
- procexp.exe (PID: 3476)

Checks supported languages

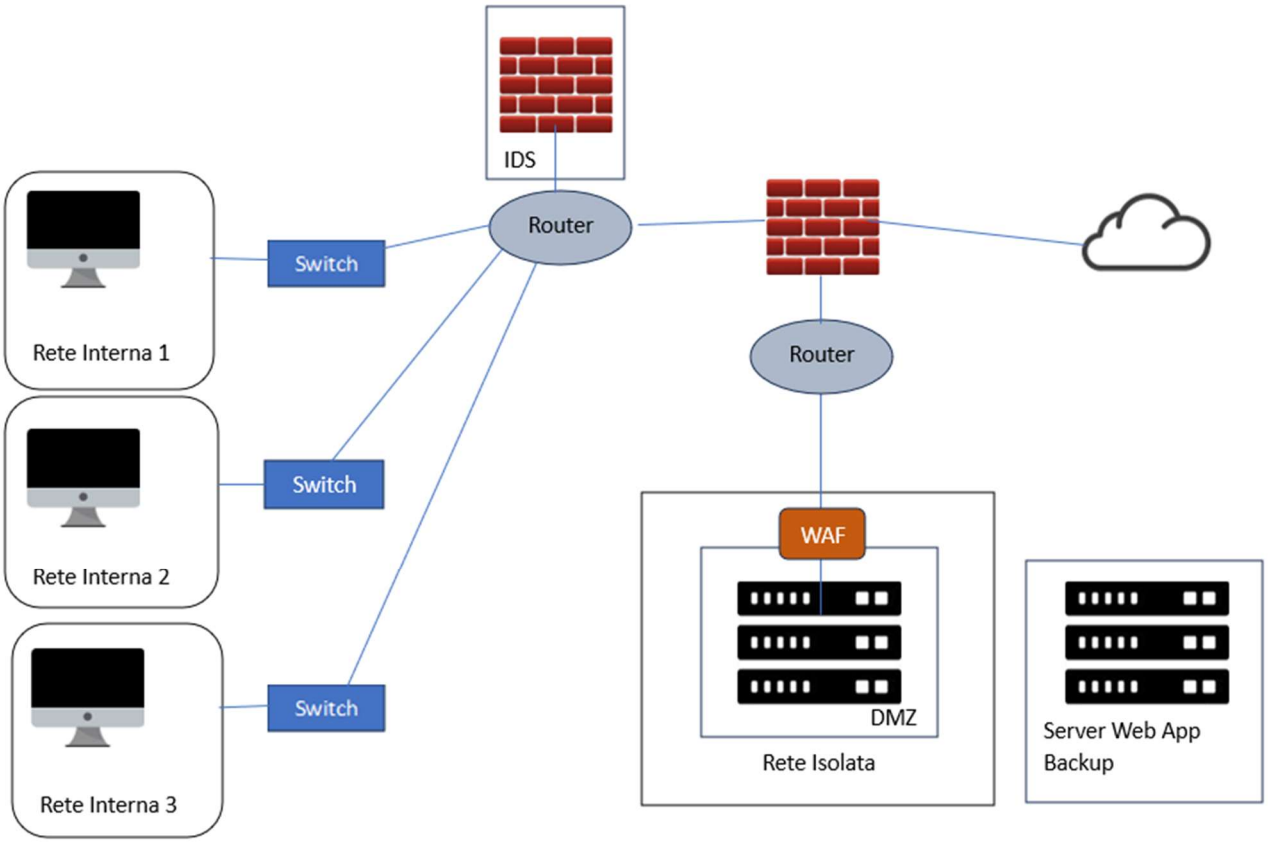
Nonostante il programma abbia intenzioni legittime, si capisce perché sia utilizzato in maniera malevola, infatti esso permette all'attaccante di controllare il computer infetto da remoto; si possono eseguire comandi, accedere ai file, monitorare le attività dell'utente, registrare la tastiera e la webcam, e persino rubare informazioni sensibili. Se ciò non dovesse bastare, RAT ha la capacità di mantenere la sua presenza nel sistema infetto, in modo da poter essere riattivato in futuro anche dopo un riavvio del computer.

Nella terza parte dell'esercitazione la traccia ci dice che l'app web è stata infettata da un malware. Il nostro compito sarà quello di evitare la propagazione di esso sulla rete interna e impedire la divulgazione delle informazioni sensibili verso internet.



In questa parte dell'esercizio troviamo l'app web in Isolamento ed il backup già pronto all'uso.

La quarta ed ultima parte dell'esercizio richiedeva di unire le configurazioni di rete del primo e del terzo punto.



Quindi nel complesso le azioni che sono state eseguite per migliorare il livello della rete sono:

- Inserito WAF per avere protezione contro attacchi mirati alle applicazioni web e da possibili vulnerabilità;
- aggiunti switch separati per reti diverse in modo di segmentare la rete limitando la propagazione di minacce;
- aggiunto backup nella rete isolata che permette di separare i dati di backup dalla rete principale;
- aggiunti un router tra il firewall e la rete DMZ e un router tra firewall e rete interna come ulteriore strato di protezione per limitare l'accesso non autorizzato ai sistemi;
- aggiunto IDS collegato al router della rete interna come ulteriore protezione.