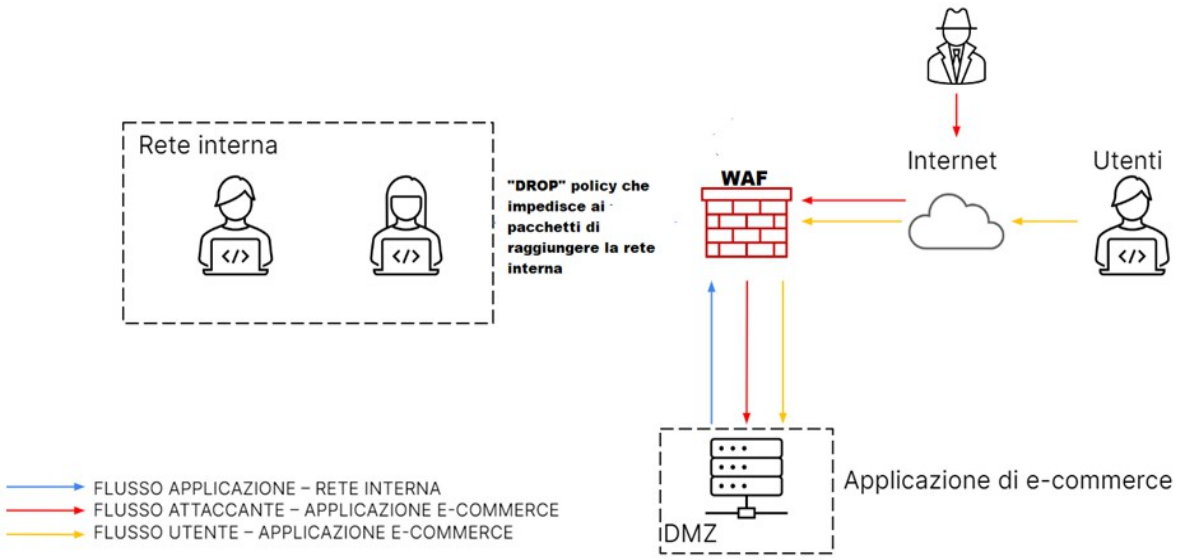
REPORT WEEK 1 UNIT 3

PUNTO 1:

Come da Traccia il primo punto dell'esercizio odierno consiste nel difendere la nostra web app da attacchi di tipo SQLI e XSS .In questo caso abbiamo provveduto all'installazione di un WAF(Web App Firewall) che filtra la rete con una policy drop per limitare i pacchetti in entrata della nostra web app.



PUNTO 2:

Nel secondo punto della traccia siamo andati ad anilizzare due link potenzialmente malevoli:

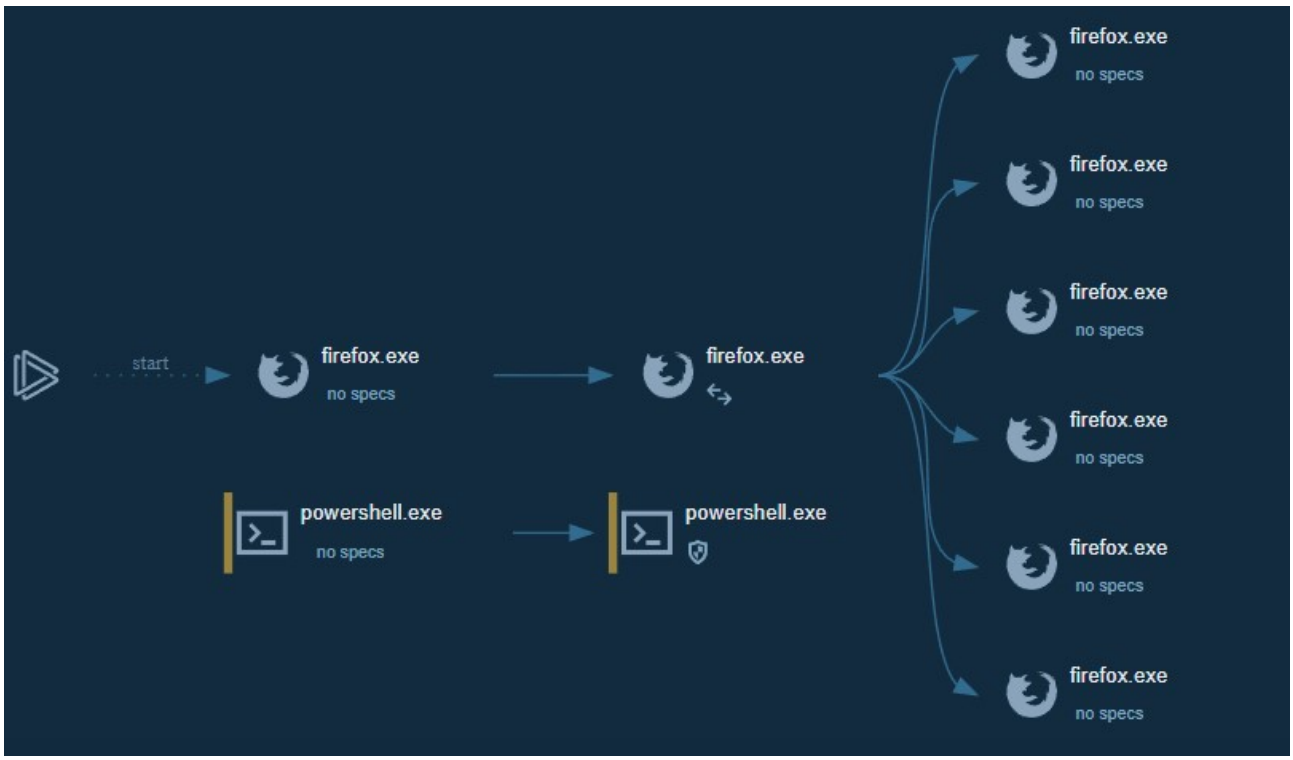
1 https://tinyurl.com/linklosco1

2 https://tinyurl.com/linklosco2

Per questa analisi abbiamo usato il tool ANY:RUN , uno strumento per il rilevamento,il monitoraggio e la ricerca di minacce informatiche in tempo reale.

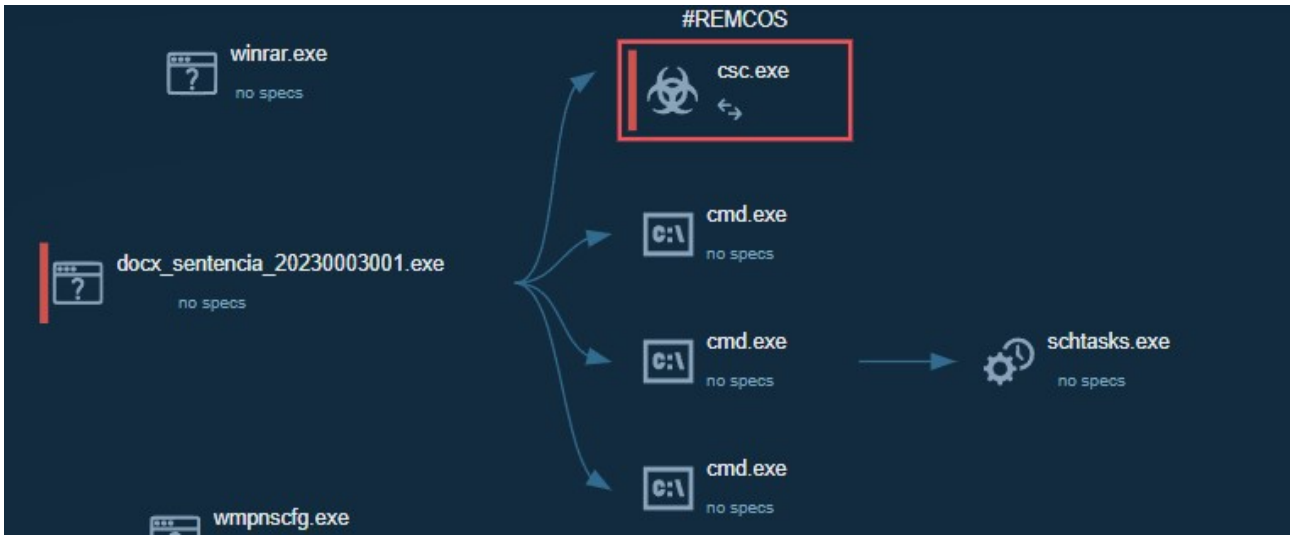
Per quanto riguarda il nostro linklosco abbiamo scoperto che si tratta di un codice malevolo in grado di una shell sulla macchina infetta.Il codice in questione va a bypassare le policy di Powershell andando ad operare sul server DNS ,ottenendo di fatto il controllo remoto sulla macchina.

Processo Link 1:



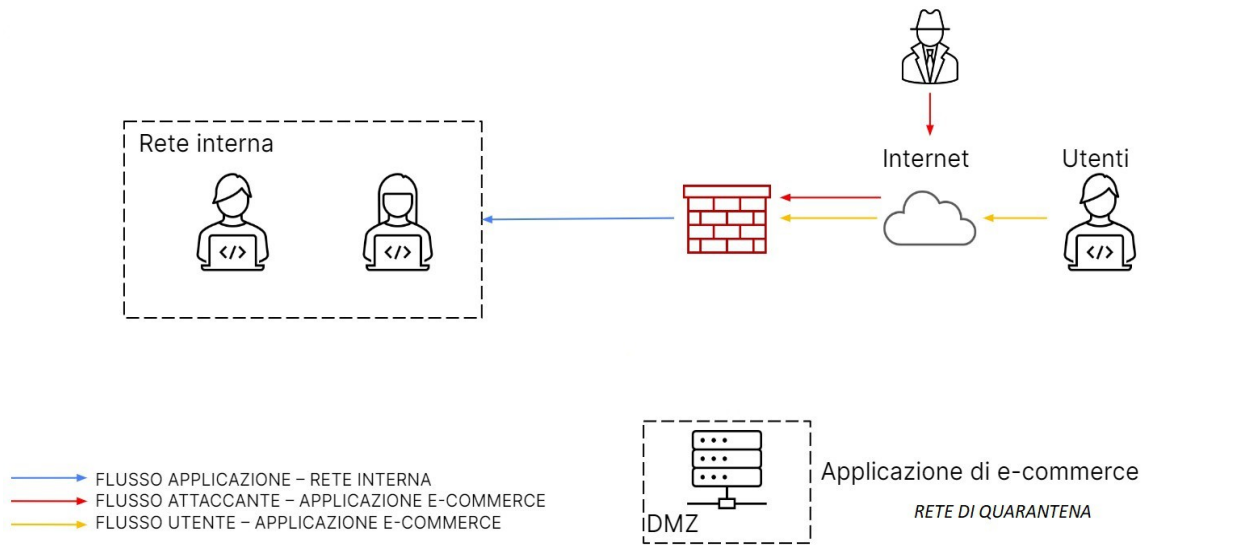
Per quanto riguarda il secondo link, si tratta di un malware iniettato sulla macchina bersaglio di nome REMCOS (acronimo di Remote Control & Surveillance Software) , uno strumento commerciale di accesso remoto per controllare i computer bersaglio.
REMCOS è pubblicizzato come software legittimo che può essere utilizzato per scopi di sorveglianza e Pentest, ma è stato utilizzato in numerose campagne di hacking.
Compiuta l'installazione, il malware apre una backdoor sul computer, garantendo ad un utente remoto la totale libertà di azione sulla macchina infetta.

Processo Link 2:



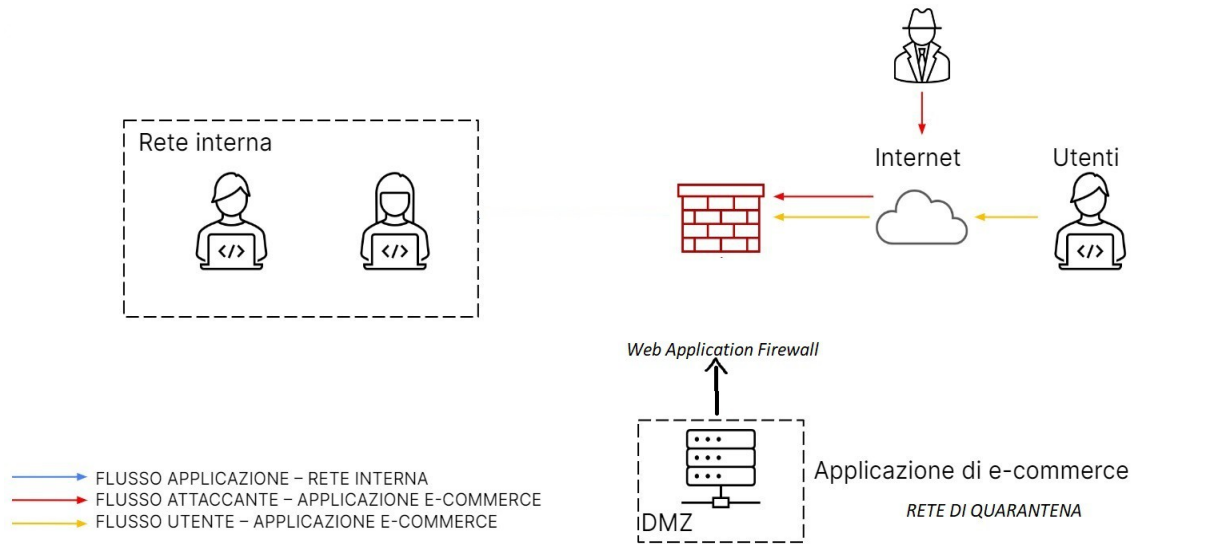
PUNTO 3:

Nel terzo punto la nostra Web App viene infettata da un malware.Dobbiamo a questo punto porre un azione di rimedio affinchè il malware non si propaghi nella rete e che non vengano divulgati dati sensibili,in questo caso effettuiamo una **Rimozione.**
Questo tipo di tecnica viene effettuata togliendo dalla rete la macchina infetta relegandola in un nuovo spazio chiamata “Rete di quarantena”,impedendo la connessione da parte dell'attaccante ,ma anche da parte degli utenti connessi.



Punto 4:

Nel quarto punto abbiamo unito le soluzioni del primo (WAF) e del terzo punto (Rimozione), lasciando la nostra web app in rete di quarantena in modo che non possa interagire con nessun utente sulla rete.



Punto 5:

Per l'ultima parte della traccia abbiamo modificato la nostra infrastruttura di rete in una maniera più aggressiva:

1) INSTALLAZIONE DI UN IDS
   abbiamo adotatto questa configurazione per migliorare e semplificare l'amministrazione della sicurezza.
2) INSTALLAZIONE SISTEMA DI BACKUP RAID 5
   nella nostra DMZ abbiamo installato un server di backup server,che insieme al web app server vanno a comporre un sistema FAILOVER CLUSTER ,dove in caso di problemi tecnici o di attacchi al web app server ,avvieremo come server principale quello di backup.
3) INSTALLAZIONE HONEY POT
   Un dispositivo che permette di monitorare e rilevare potenziali aggressori,per migliorare le misure di sicurezza
4) UPS
   un dispositivo che permette un alimentazione di emergenza nella zona DMZ in caso di problemi elettrici.