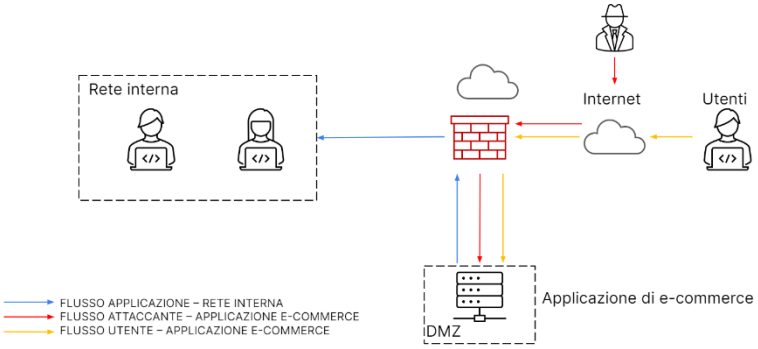
Progetto week 1 unit 3

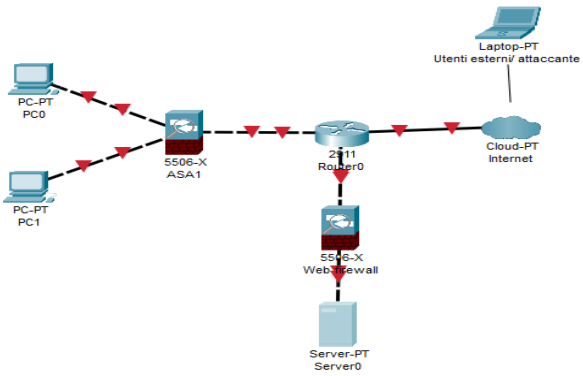
La consegna si divide in 4 punti che verranno affrontati nell'ordine posto:

1: Azioni preventive



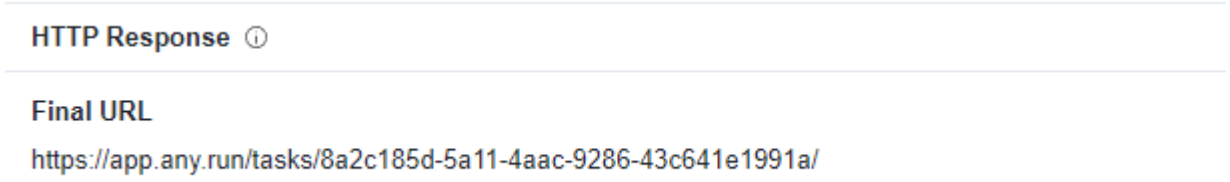
Data l'immagine affianco ci viene chiesto di modificare la struttura implementando azioni preventive per difendere l'applicazione web da possibili attacchi di SQLi o XSS da parte di un'utente malintenzionato. Ho scelto di usare Cisco Pachet Tracer per simulare la possibile soluzione.

Come si può vedere dall'immagine sottostante ho deciso di separare la rete interna aziendale dalla porzione del servizio DMZ. In più è presente un WAF (Web Application Firewall) ossia un dispositivo di sicurezza concepito per proteggere applicazioni da attacchi proprio come SQLi e il XSS.



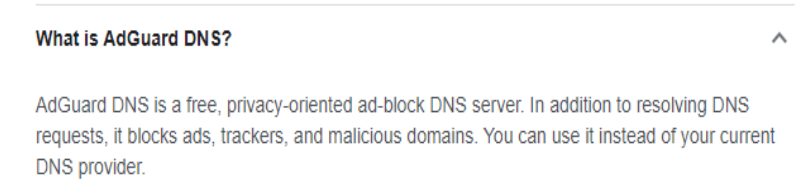
2: Analisi attacco

Ci sono stati forniti due link "loschi" da analizzare, essendo descritti come tali la prima cosa che ho fatto è stato analizzarli senza aprirli usando un sito chiamato "Virustotal", incollando i link mi viene confermato che sono sicuri e leggendo le informazioni date riconoscono che gli url originali riconducono a delle analisi fatte su "ANY.RUN" ,che è una piattaforma di analisi malware automatizzata in cui è possibile caricare ed eseguire qualsiasi file dannoso da analizzare senza ripercussioni (come si può vedere dall'immagine).

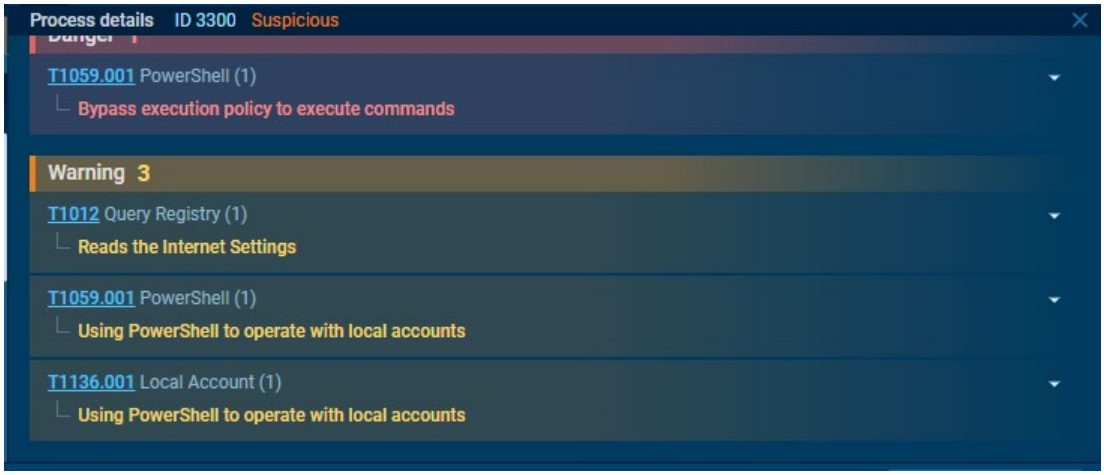


Una volta cliccati i link ci vengono aperte le analisi di ANY.RUN e procedo a commentarle:
Report link1

Dalla prima analisi possiamo dedurre che non è presente nessun tipo di minaccia ma solo operazioni sospette da parte del proprietario, sembra abbia copiato una shell che ti permette di cambiare velocemente il servizio DNS verso il server “AdGuard DNS” e viceversa, il server in questione con una rapida ricerca si scopre essere un server gratuito orientato alla privacy.

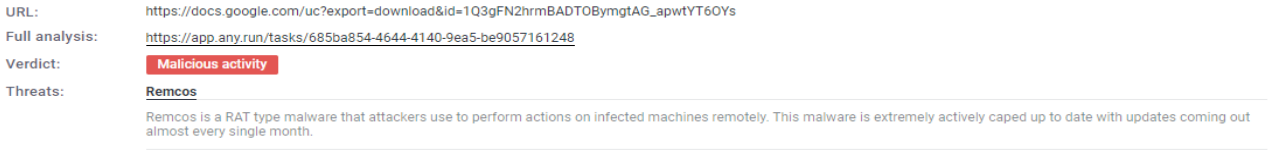


Il proprietario successivamente avvia la shell ignorando il prompt del firewall sul fatto che lo script non sia affidabile innescando un allarme come azione sospetta come possiamo vedere dall’immagine:



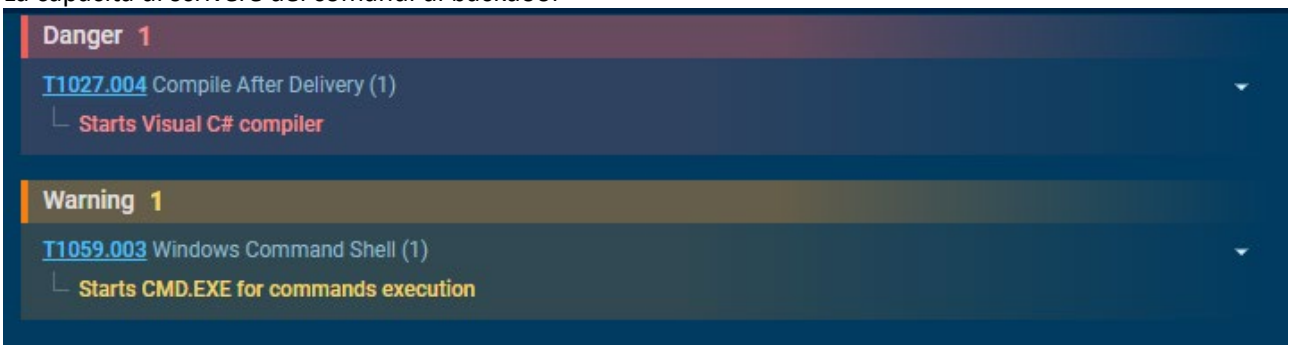
Report Link2

La seconda analisi sembra riscontrare un caso più complesso, cercando di filtrare la quantità di informazioni richiedo a ANY.RUN un report testuale che mi aiuta a constatare che siamo davanti alla minaccia di un malware, più precisamente un “Remcos” un malware di tipo RAT (Remote Access Trojan) che permette all’attaccante di eseguire comandi o altre azioni sulla macchina infetta da remoto.

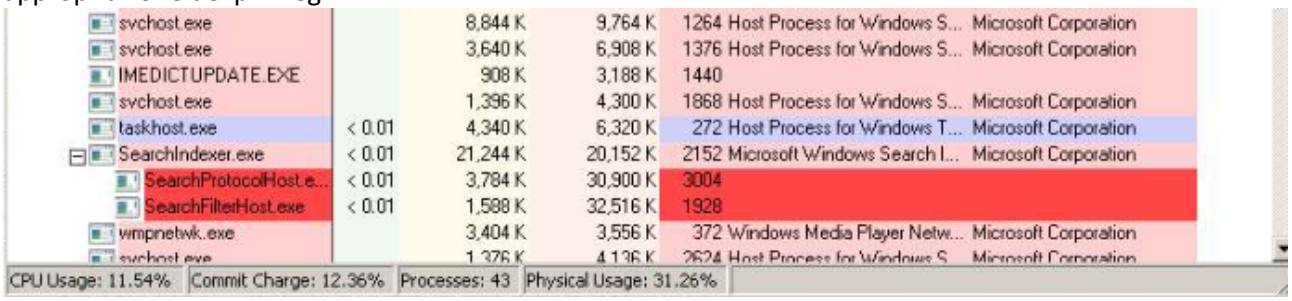


Dagli screen possiamo osservare che l’infezione è avvenuta a causa di un download da Chrome e studiando sia gli screen dell’evento sia i dettagli dei processi analizzati possiamo confermare i comportamenti per cui questo malware è conosciuto tra cui:

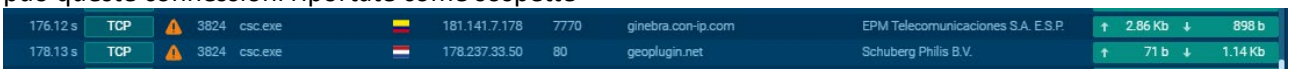
- La capacità di scrivere dei comandi di backdoor



- L’appropriazione di informazioni legate agli user/admin come credenziali e logs, con possibile appropriazione dei privilegi

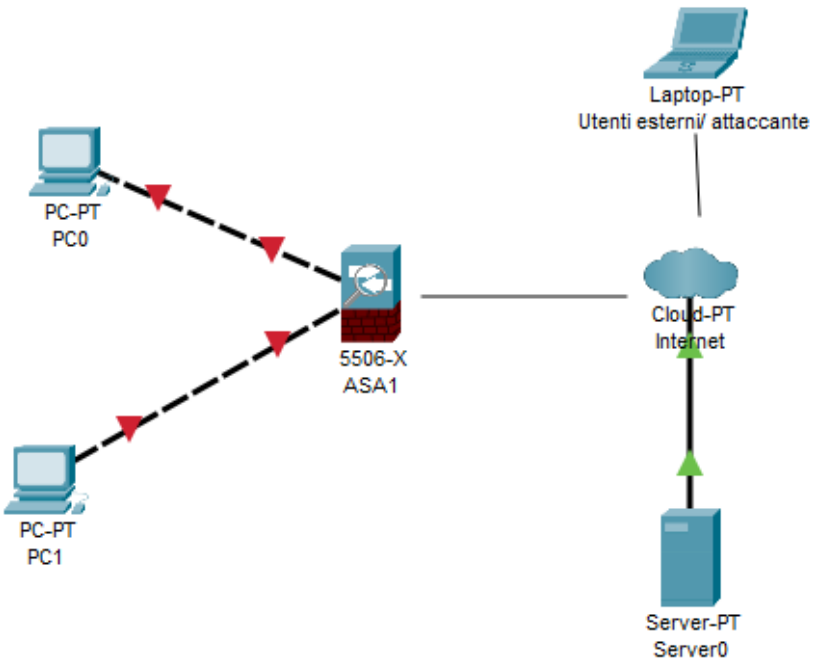


- Permettere ad attaccanti esterni di scrivere comandi e eseguire azioni nella macchina infetta, che può queste connessioni riportate come sospette



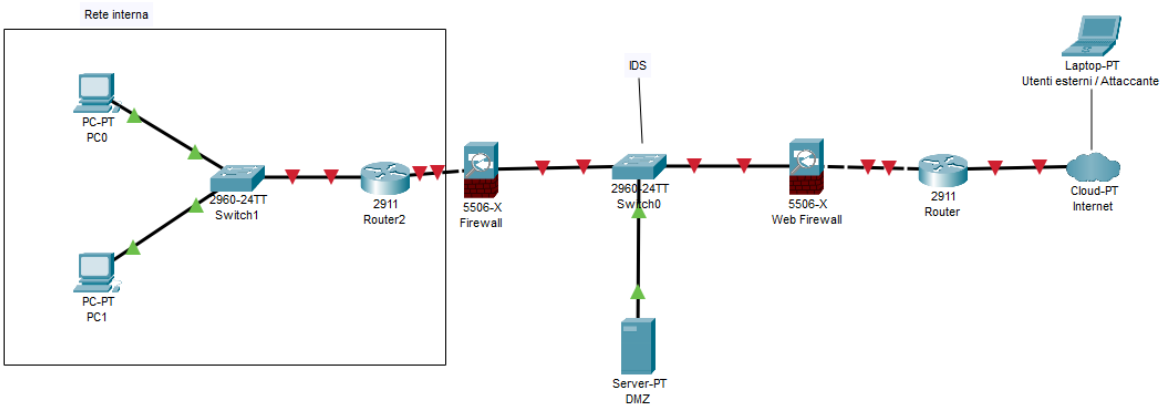
3: Response

Rifacendosi all’immagine proposta nella slide 2 ristrutturarla a causa di un malware che ha infettato l’applicazione web. La priorità è mantenere la sicurezza della rete interna aziendale ma anche che si eviti la divulgazione di informazioni sensibili nel verso internet. Premetto che il metodo più efficace se pur estremo di fare ciò sarebbe **rimuovere** temporaneamente la porzione DMZ della rete. Ma se volessimo studiare il tipo di attacco e da dove è passato evitando la propagazione del malware potremmo usare un approccio di **isolamento**:



4: Soluzione completa

Nella soluzione completa ho integrato le immagini proposte prima, le reti rimando separate in quanto ora è presente un router nella rete interna, ma ho aggiunto uno switch con in ascolto in IDS per rivelare possibili azioni sospette:



5: Modifica aggressiva dell'infrastruttura

In questo ultimo punto ripropongo una versione più complessa della precedente, i cambiamenti più importanti è l'aggiunta di un server DMZ ridondante in modo che in caso di attacchi futuri i possibile passare al secondario per mantenere il servizio attivo e un'aggiunta di un IPS per controllare in modo più aggressivo i dati che si dirigono verso la rete interna con un IDS aggiuntivo in esso per avere visione anche di ciò che avviene internamente all'azienda.