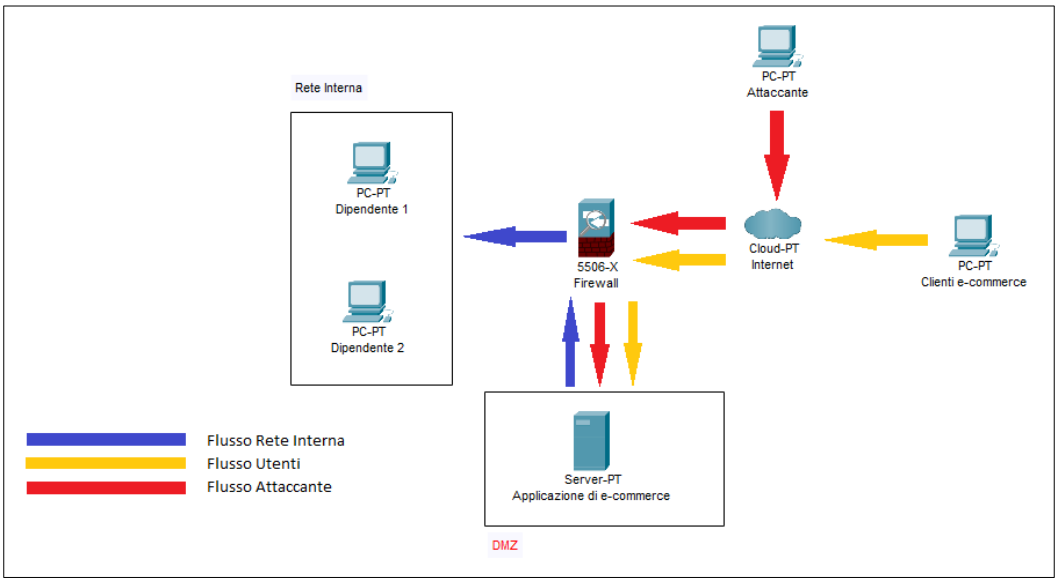
Rete di e-commerce

Obiettivo:
Applicare azioni preventive e di risposta all'attacco di un'applicazione di e-commerce.

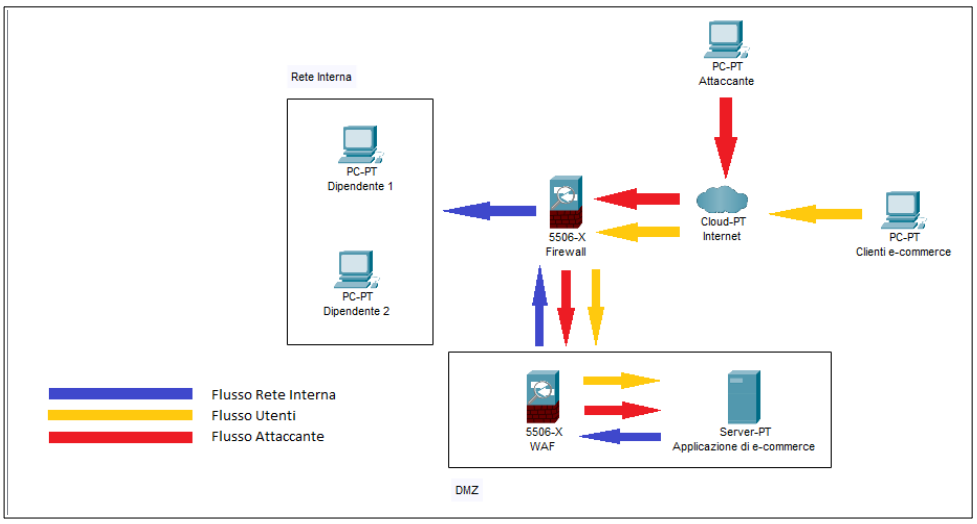
1) Architettura di Rete

La traccia ci pone l'architettura di rete dell'applicazione.



2) Azioni Preventive

Il primo punto della traccia chiede di applicare delle azioni preventive per difendere l'applicazione Web da attacchi di tipo **XSS** e **SQLI** modificando il disegno. Ho cominciato le modifiche aggiungendo un **Web Application Firewall**.
Installato tra il nostro **Server** e **Internet** questo dispositivo protegge dalle vulnerabilità Web, in questo caso è perfetto per gli attacchi sopracitati; inoltre può essere utile a controllare il traffico web in entrata e in uscita oltre a gestire l'autenticazione e l'autorizzazione degli utenti.



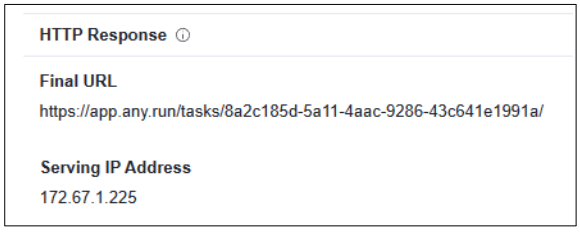
Il **WAF** è inoltre utile a mitigare attacchi di tipo **Ddos (Distributed Denial of Service)** oltre ad offrire un supporto di **Monitoraggio** e **Reportistica degli eventi**, molto utili in caso di attacco hacker.

3) Analisi Attacco

La seconda parte della traccia chiede invece di analizzare due Link sospetti. Ipotizzando e simulando un ambiente di lavoro non ho aperto direttamente i due file ma ho iniziato la loro analisi caricandoli su **VirusTotal**. La sezione ***Detection*** non ha dato messaggi critici tranne un "suspicious" da parte di *ArcSight Threat Intelligence*.

ArcSight Threat Intelligence	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean

Cercando invece nella sezione ***Details*** ho trovato informazioni riguardo all'*URL di destinazione* dei link e il *titolo della pagina HTML* dove essi portano.

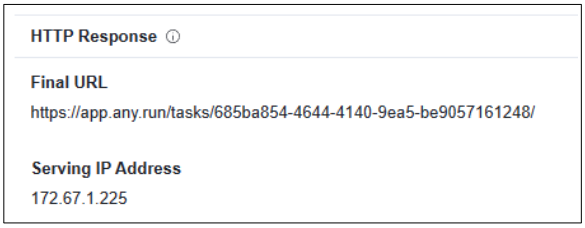


HTTP Response

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

Serving IP Address
172.67.1.225

Analisi Primo Link



HTTP Response

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

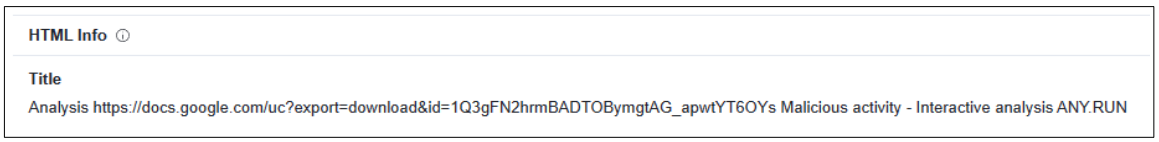
Serving IP Address
172.67.1.225

Analisi Secondo Link

L'indirizzo IP porta a *Coudflare*, un'azienda di Content Delivery Network, probabilmente a uno dei suoi server. I Final URL invece sembrano portare alla piattaforma **Web Sandbox ANY.RUN**.

HTML Info

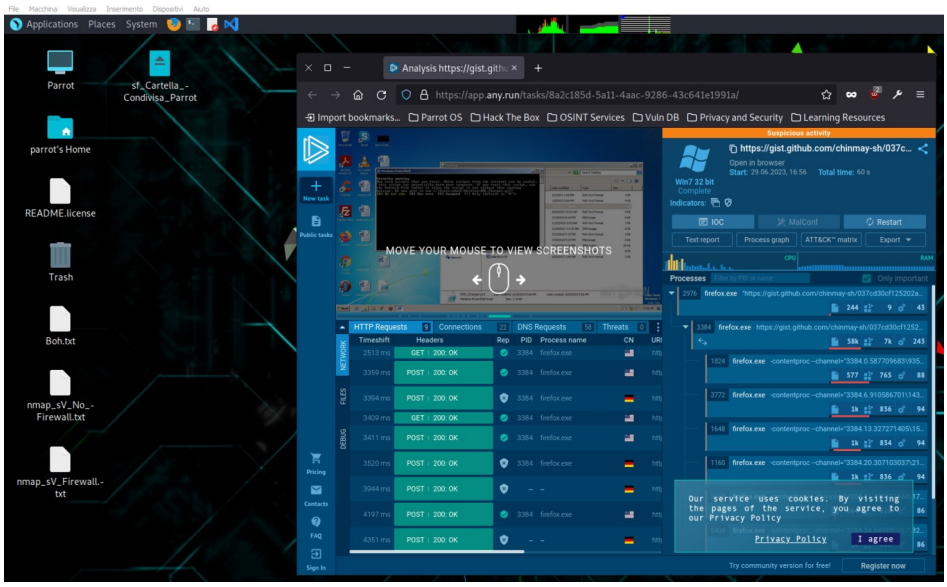
Title
Analysis https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1 Suspicious activity - Interactive analysis ANY.RUN



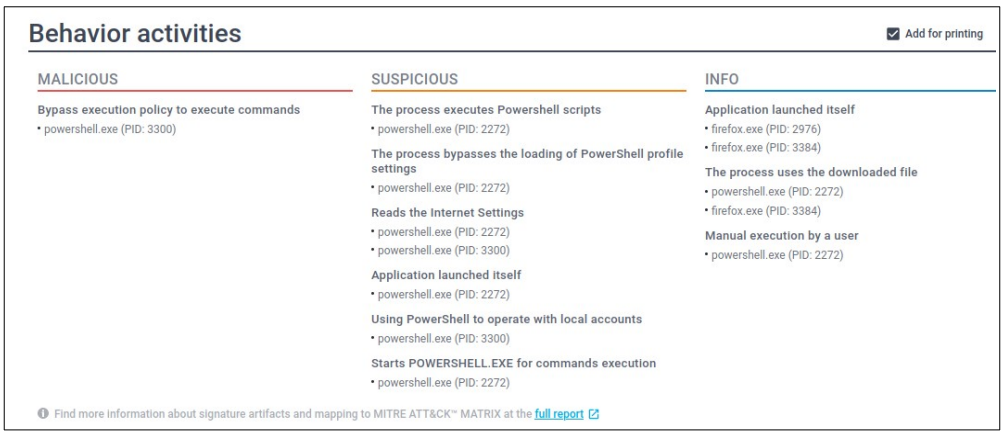
HTML Info

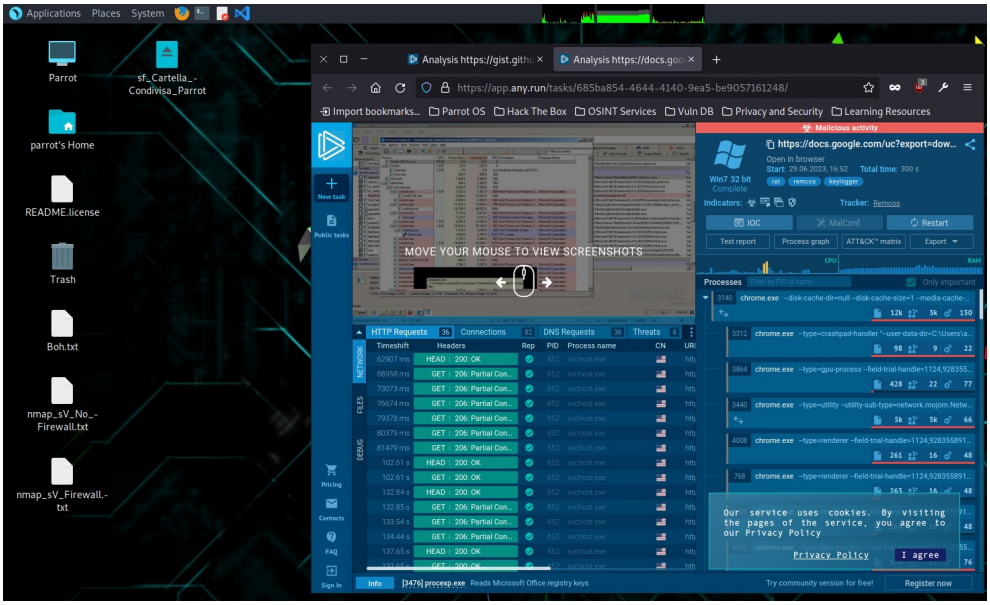
Title
Analysis https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgtAG_apwtYT6OYs Malicious activity - Interactive analysis ANY.RUN

Entrambi i link sono analisi eseguite su **ANY.RUN**. Questa piattaforma è utilizzata per caricare file, URL o eseguire eseguibili sulla *sandbox* per rilevare eventuali attività malevole o sospette.
Per comprovare l'analisi di **VirusTotal** ho aperto i due link su **Parrot** simulando un *Ambiente Sicuro*.



Il primo link ci riporta all'analisi di un ***DNSChanger***. Potrebbe riferirsi a un tipo di **Trojan** attivo molti anni fa che modificava i DNS dei PC infettati puntandoli verso siti malevoli.
Il sito ci fornisce anche un elenco dettagliato delle attività che vengono svolte, in questo caso c'è il bypass delle policy per eseguire *powershell* con l'apertura automatica di **Firefox**, probabilmente verso siti malevoli come già accennato.

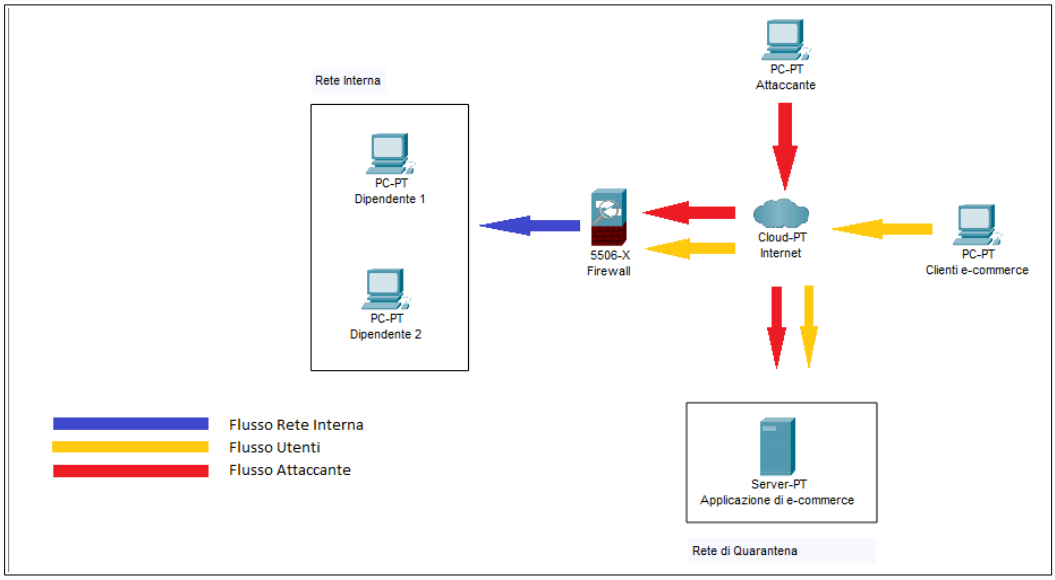




Il secondo link invece porta ad un'analisi di **Remcos**, un software di accesso remoto che permette a un attaccante di assumere il controllo di un computer a distanza.

4) Response

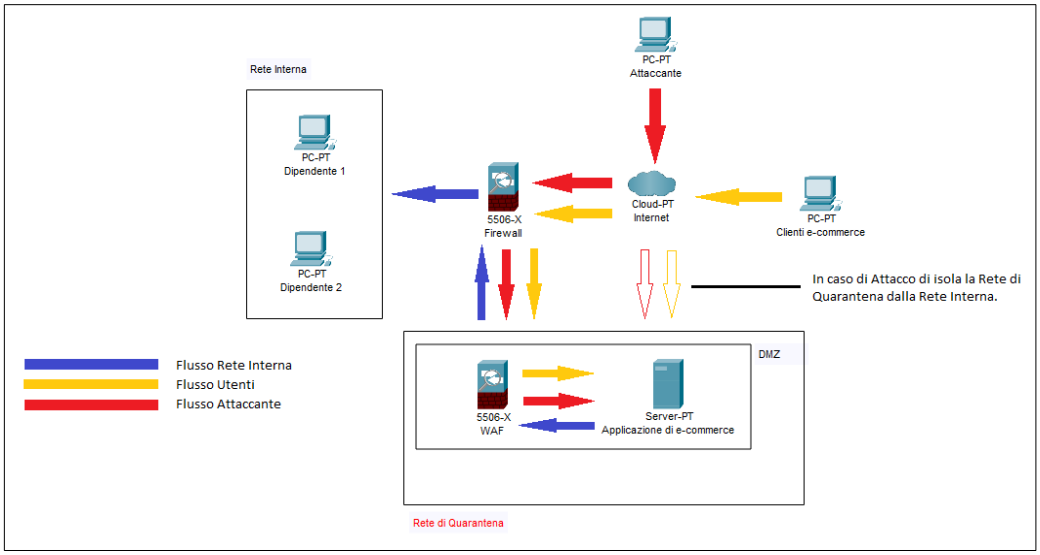
Il terzo punto della traccia chiede invece di modificare la rete se l'applicazione WEB venisse infettata da un **Malware**. In questo caso si potrebbe pensare ad una **Segmentazione** ma questa pratica mantiene il Server infettato collegato alla Rete Interna.
Per poter studiare l'attacco in corso ma senza permettere all'attaccante hacker di penetrare all'interno della Rete suggerisco di optare per l'opzione di **Isolamento**, in maniera tale che il Server resti collegato ad Internet e si possa procedere allo studio dell'attacco e dell'attaccante cercando magari di scoprire l'indirizzo IP dell'attaccante, leggere i **Log di Sistema** e **Monitorare il Traffico dei Dati** per vedere quali indirizzi IP sono collegati all'applicazione).



Una volta ottenuti dati a sufficienza di potrà passare alla **Rimozione** del Server per il Recupero dei Dati compromessi. Trattandosi di un sito di e-commerce queste pratiche andrebbero a creare ingenti perdite di denaro ove non sia presente un *Secondo Server* apposito che entri in azione automaticamente non appena il *Server Primario* venga manomesso o reso inaccessibile, perché basandosi su transazioni online se il Server è staccato da Internet i clienti non possono acquistare i prodotti della piattaforma. Suggerirei quindi di avere un buon **BCP (Business Recovery Plan)** che permetta al Secondo Server di "avviarsi" in caso il primo venga infettato; questa implementazione aiuta anche il piano di **DR (Disaster Recovery)** mitigando gli effetti dell'attacco subito.

5) Soluzione Completa

Quarto punto della traccia è di unire la **Protezione Preventiva** con la **Response**.



Unendo le due decisioni prese precedentemente possiamo notare che a proteggere il Server da Attacchi alle Web App è presente il **Web Application Firewall**; in caso il Server venga attaccato è già stabilita una **Rete di Quarantena** in maniera tale da Isolare il Server.
Il **WAF** come già detto è un dispositivo di sicurezza molto efficiente ma potrebbe essere bypassato da un attaccante per vari motivi, ad esempio:

- **Errata Configurazione** delle policy;
- **Vulnerabilità sconosciute**, ad esempio Attacchi Zero-Day;
- **Falsi Positivi e Negativi**, bloccando traffico “buono” e facendo passare traffico malevole”;
- **Mancanza di Aggiornamenti e Patch** che permettono ad attaccanti di bypassare le difese.

6) Modifica all’infrastuttura

L’ultimo punto ci chiede di modificare la struttura della Rete in modo tale che sia più sicura.
Aggiunte che suggerisco sono:

- **IDS (Intrusion Detection System)** posizionato tra **Internet** e il **Firewall Aziendale**, questo dispositivo identifica gli accessi non autorizzati all’interno della Rete e segnala probabili intrusioni con degli Alert. Non ho voluto utilizzare un **IPS** perché potrebbe bloccare traffico di dati non necessariamente malevolo.
Esistono vari **IDS Open-Source** (come *Snort*, *Suricata* e *Security Onion*) altrimenti a pagamento come ad esempio **IDS Cisco** che partono almeno dagli 8000 Euro circa.

- **UPS (Uninterruptible Power Supply)** per mantenere On la **Web App** in casi di Interruzione della Corrente Elettrica. Suggerisco l’acquisto di un **UPS** di 3000 VA ad un costo di circa 900-1000 Euro.

- **NAS (Network-Attached Storage)** per il **Backup** della Web App e non solo di essa, i prezzi variano a seconda di quanto spazio si vuole archiviare; un QNAP TS-h972AX da 0-100 TB ha un prezzo di 1150 euro circa.

- **Un secondo Server di Backup** nel caso il Primo venga rimosso come detto in precedenza a seguito di un attacco. Può essere situato in un'area geografica completamente diversa dal **Server Principale**. Il prezzo in questo caso varia a seconda della **Web App**.

- Avere più Reti in maniera tale da diminuire la *Vulnerability Surface* e avere un minore impatto da parte di attacchi esterni.

Ulteriori suggerimenti che posso dare sono il **Monitoraggio dei Log** con la quale si può tenere traccia di comportamenti anomali e infine di eseguire regolarmente dei **Pentest** per testare le vulnerabilità che possono essere presenti e quindi patcharle con gli ultimi aggiornamenti.

I prezzi che ho elencato sono indicativi, bisogna innanzitutto capire quanto è grande l'azienda che va ad attuare queste implementazioni di sicurezza. Un'azienda piccola non potrà sopportare una spesa troppo grande di componenti a differenza di un colosso (Amazon ad esempio) che può permettersi di avere moltitudini di Server, Software e Hardware anche a costi molto elevati.