Azioni preventive: Per difendere un'applicazione web da attacchi di tipo SQL (SQL injection) o XSS (Cross-Site Scripting) da parte di utenti malintenzionati, è possibile implementare le seguenti azioni preventive:

1. Validazione dei dati in ingresso: Implementare controlli di validazione per garantire che i dati inseriti dagli utenti siano conformi alle aspettative. Ciò include la verifica della correttezza dei formati (come indirizzi email o numeri di telefono) e la rimozione di caratteri speciali o pericolosi che potrebbero essere utilizzati per eseguire attacchi.

2. Utilizzo di query SQL parametriche o prepared statements: Evitare la concatenazione diretta di valori degli utenti nelle query SQL. Utilizzare invece query parametriche o prepared statements che separano i dati dalle istruzioni SQL, impedendo così l'iniezione di codice SQL dannoso.

3. Escape dei caratteri speciali nell'output: Quando si visualizzano dati forniti dagli utenti all'interno delle pagine web, assicurarsi di effettuare l'escape dei caratteri speciali. Questo previene l'interpretazione erronea dei caratteri come codice HTML o JavaScript, evitando così attacchi XSS.

4. Utilizzo di librerie di codifica sicura: Utilizzare librerie o framework che forniscono funzioni di codifica sicura per manipolare i dati dell'utente. Queste funzioni garantiscono che i caratteri speciali vengano correttamente codificati per evitare l'interpretazione errata come codice eseguibile.

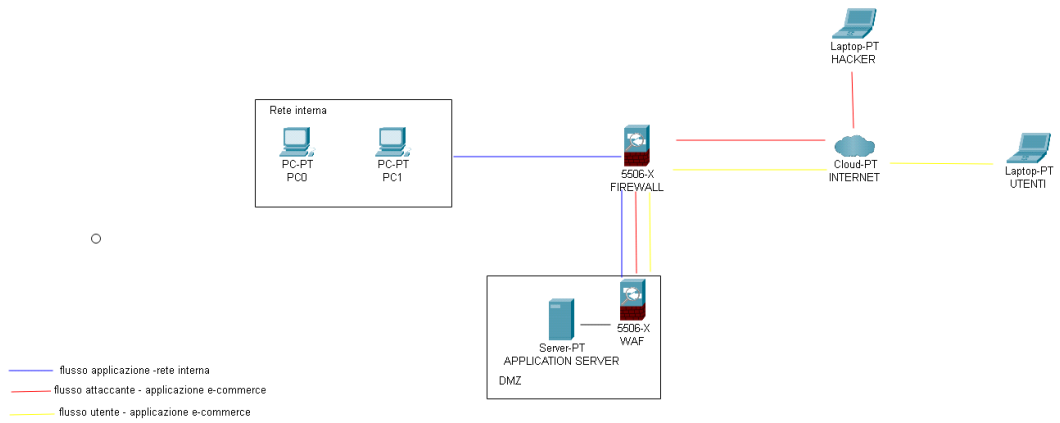
5. Implementazione di politiche di sicurezza del browser: Configurare le intestazioni HTTP come Content Security Policy (CSP) per limitare l'esecuzione di script non autorizzati o l'inclusione di risorse esterne nelle pagine web. Ciò riduce il rischio di attacchi XSS basati su script dannosi provenienti da fonti non attendibili.

6. Aggiornamento regolare e patching dell'applicazione: Mantenere l'applicazione web aggiornata con gli ultimi patch e aggiornamenti di sicurezza rilasciati dal produttore. Questo riduce il rischio di sfruttamento di vulnerabilità note.

7. Monitoraggio del traffico e dei log di sicurezza: Implementare sistemi di monitoraggio e rilevamento delle intrusioni per identificare attività sospette o tentativi di attacco. Analizzare regolarmente i log di sicurezza per individuare eventuali anomalie o attività potenzialmente dannose.

8. Consapevolezza e formazione degli utenti: Educare gli utenti sull'importanza delle pratiche di sicurezza, come l'utilizzo di password forti, l'evitare di aprire link sospetti o l'inserimento di dati sensibili su siti non affidabili. La formazione degli utenti contribuisce a ridurre il rischio di attacchi basati sull'ingegneria sociale.

Queste azioni preventive combinate aiutano a proteggere l'applicazione web da attacchi SQL injection e XSS, garantendo la sicurezza dei dati e la continuità delle operazioni.



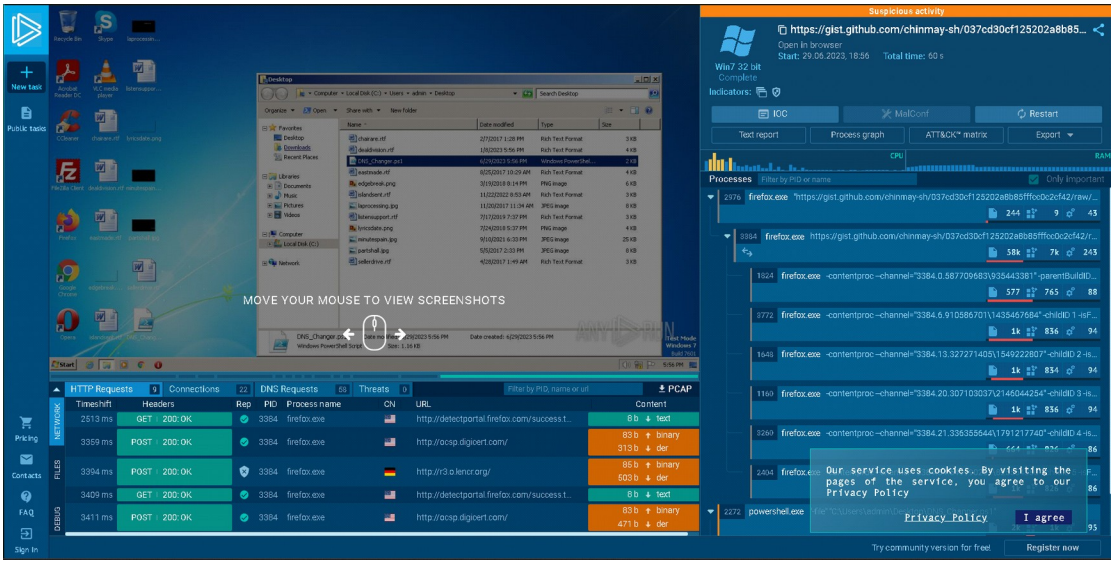
Andiamo ad ampliare il disegno di rete semplicemente andando a mettere un **WAF** per andare a contrastare le **SQL injection** e le **XSS** malevole:

Un **WAF (Web Application Firewall)** è un'applicazione o un dispositivo che protegge le applicazioni web da attacchi e minacce. Monitora e filtra il traffico HTTP/HTTPS in ingresso e in uscita, rilevando e bloccando richieste sospette o dannose. Il WAF valida i dati, protegge dalle vulnerabilità e offre reportistica per la sicurezza delle applicazioni web all'interno di una rete aziendale.

Analisi attacco: Abbiamo utilizzato un tool online chiamato "Toolset" per aprire il link e verificare il suo contenuto.

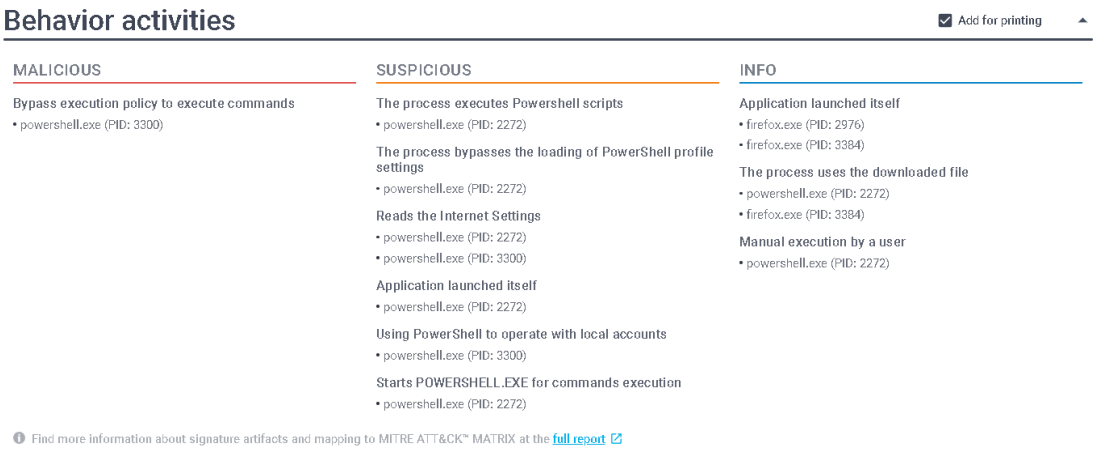
Toolset è una piattaforma o un insieme di strumenti online che fornisce diverse funzionalità e servizi per l'analisi e la gestione di link, file o risorse digitali. Questi strumenti possono includere verifiche di sicurezza, analisi di URL, controlli di reputazione dei siti web, analisi di file sospetti e altre funzionalità correlate alla sicurezza e all'analisi digitale. Toolset è progettato per assistere gli utenti nel valutare la sicurezza e l'affidabilità dei link o dei contenuti digitali, consentendo loro di prendere decisioni informate e mitigare potenziali rischi.

Successivamente, abbiamo notato che il link conteneva un ulteriore link che puntava a **any.run**. Abbiamo deciso di aprire questo secondo link per vedere quale risultato ci restituisse.



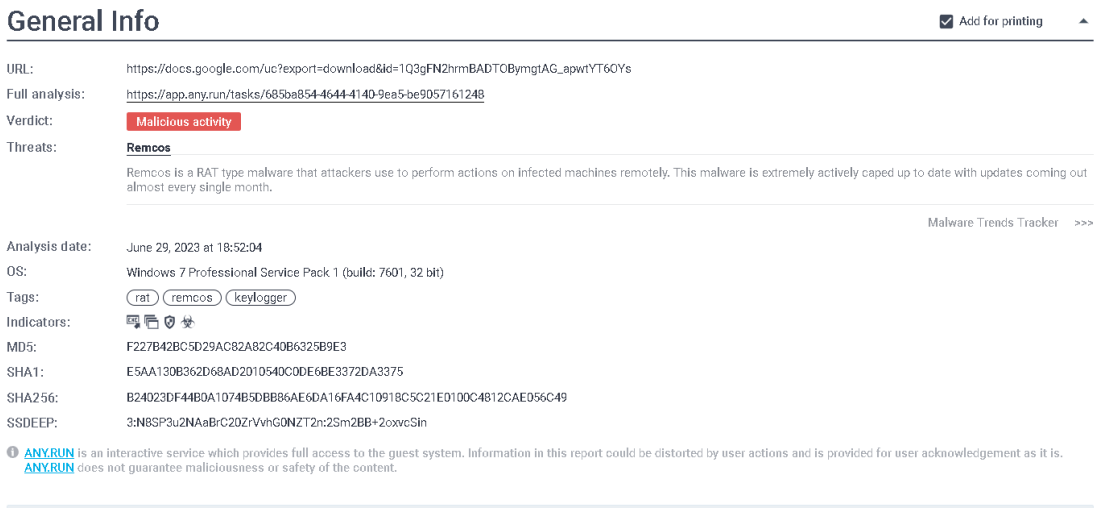
Any.run è una piattaforma online che offre un ambiente di esecuzione sicuro e controllato per analizzare il comportamento di file e link sospetti. Consente agli utenti di caricare file o eseguire link all'interno di un sandbox virtuale, dove vengono monitorate le attività del file o del link in un ambiente isolato. Any.run registra e analizza il comportamento dei malware, inclusi i cambiamenti del registro di sistema, le connessioni di rete, le modifiche dei file e altre azioni potenzialmente dannose. Questo tipo di analisi aiuta gli utenti a comprendere meglio le potenziali minacce e adottare misure appropriate per la sicurezza informatica. Any.run è spesso utilizzato dagli esperti di sicurezza, dagli analisti delle minacce e dagli utenti che desiderano eseguire una valutazione approfondita di file o link sospetti prima di prenderne ulteriori azioni.

il primo any.run ci restituiva questo piccolo report:



I dati mostrano attività sospette che coinvolgono i processi powershell.exe e firefox.exe. Powershell.exe esegue comandi, script e operazioni di lettura delle impostazioni di Internet. Firefox.exe utilizza un file scaricato. Alcune azioni sono state avviate autonomamente, mentre altre sono state eseguite manualmente da un utente. Queste attività richiedono un'analisi approfondita per valutare il loro impatto sulla sicurezza del sistema.

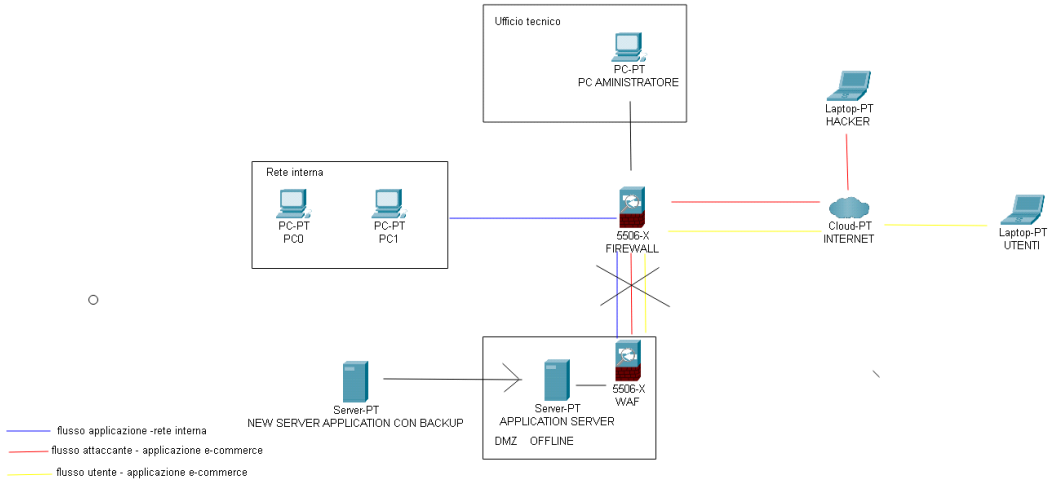
Il secondo invece conteneva questo check su quest'altro file malevolo:



L'analisi dei dati fornisce informazioni su un URL sospetto contenente un file eseguibile malevolo. Il file è stato identificato come il malware noto "**Remcos**", un RAT (Remote Access Trojan) che consente agli aggressori di eseguire azioni sulle macchine infette da remoto. L'analisi è stata condotta su un sistema operativo Windows 7 Professional Service Pack 1 a 32 bit. I risultati evidenziano attività sospette, tra cui la creazione di file, la lettura delle impostazioni di sistema, la connessione a porte non comuni e l'utilizzo di PowerShell per l'esecuzione di comandi. Questi comportamenti indicano la potenziale presenza di un file dannoso e richiedono ulteriori valutazioni sulla sicurezza del sistema.

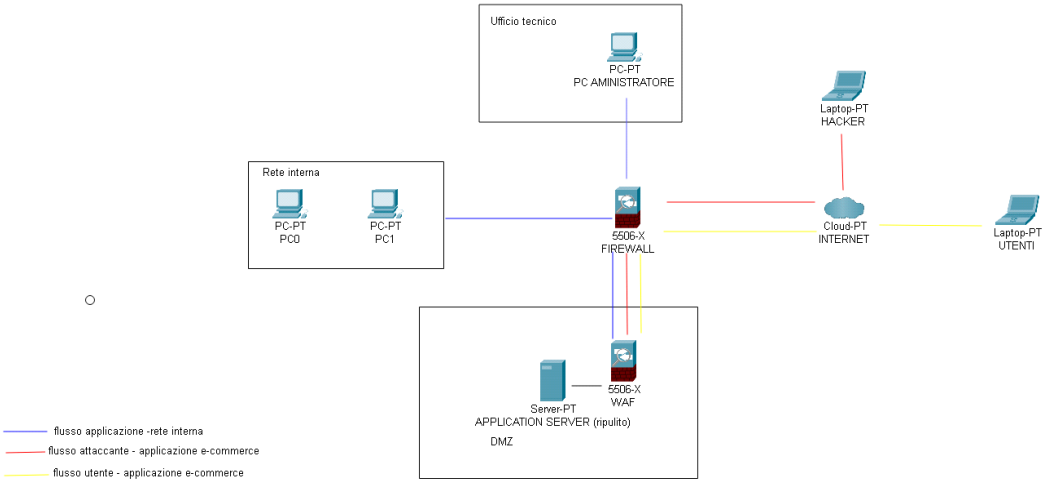
Response: La nostra rete aziendale è stata attaccata da un malware. Per proteggere le nostre informazioni e i dati sensibili, abbiamo scollegato i server aziendali dalla connessione Internet, rendendoli offline. Questa misura è finalizzata a prevenire ulteriori danni e ci consente di valutare l'attacco, identificare le vulnerabilità e prendere le contromisure necessarie. La sicurezza dei dati e la

riservatezza delle informazioni sono la nostra massima priorità.

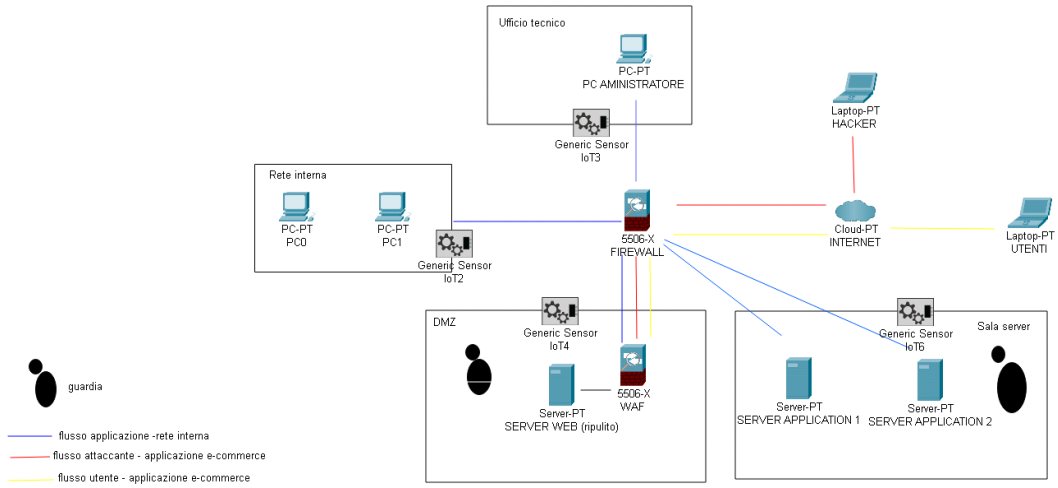


Quando un'applicazione web viene infettata da malware, è fondamentale proteggere la rete da una possibile diffusione del malware e garantire la sicurezza delle informazioni sensibili. Per farlo, è necessario isolare l'applicazione compromessa dalla rete principale, bloccare il traffico dannoso con un firewall, rimuovere il malware attraverso una scansione approfondita del sistema e mantenere l'applicazione e il sistema operativo aggiornati con le patch di sicurezza. Inoltre, è consigliabile effettuare un backup dei dati dell'applicazione prima di procedere con la rimozione del malware e considerare un'analisi forense per comprendere l'entità dell'attacco e prevenire futuri rischi.

Soluzione completa: Abbiamo completato l'integrazione delle reti tra il punto uno e il punto tre, dopo aver risolto l'incidente causato dal malware. Durante questo processo, abbiamo apportato alcune piccole modifiche per migliorare la sicurezza complessiva del sistema. Inoltre, abbiamo eliminato la minaccia eseguendo un rebuild completo del server interessato. Siamo lieti di confermare che il server è stato ripristinato con successo e ora è di nuovo online, garantendo la continuità delle operazioni aziendali. Continueremo a monitorare attentamente la situazione per prevenire futuri attacchi e garantire la massima protezione dei nostri dati e delle nostre risorse.



Modifica della rete:



Abbiamo implementato una serie di importanti misure di sicurezza per proteggere la nostra rete aziendale. Innanzitutto, abbiamo introdotto un ufficio tecnico dotato di un computer dedicato a un tecnico che monitorerà costantemente la rete e i log di attività. Inoltre, abbiamo implementato ulteriori controlli per garantire la sicurezza degli accessi, tra cui l'utilizzo di badge per l'identificazione, la presenza di guardie di sicurezza e l'imposizione di restrizioni sugli accessi ai computer aziendali. Sia i dipendenti che i clienti avranno accesso alla rete tramite un sistema multifattoriale per garantire un'autenticazione sicura.

Per garantire una maggiore resilienza del sistema, abbiamo introdotto due server applicativi. In questo modo, se uno dei server dovesse avere un guasto, l'altro server prenderà immediatamente il relativo carico di lavoro, garantendo la continuità delle operazioni aziendali. Inoltre, abbiamo implementato un server web che consentirà ai nostri clienti e agli addetti ai lavori di accedere alle risorse aziendali in modo sicuro. Saranno comunque applicati controlli rigorosi sugli accessi per prevenire intrusioni interne, compresi controlli multifattoriali per garantire che solo le persone autorizzate possano accedere alle

risorse sensibili.

Queste misure di sicurezza sono state implementate per proteggere la nostra rete aziendale da potenziali minacce esterne e interne. Continueremo a vigilare attentamente sulle attività di rete e ad aggiornare le nostre politiche di sicurezza per garantire la massima protezione dei dati e delle risorse aziendali.