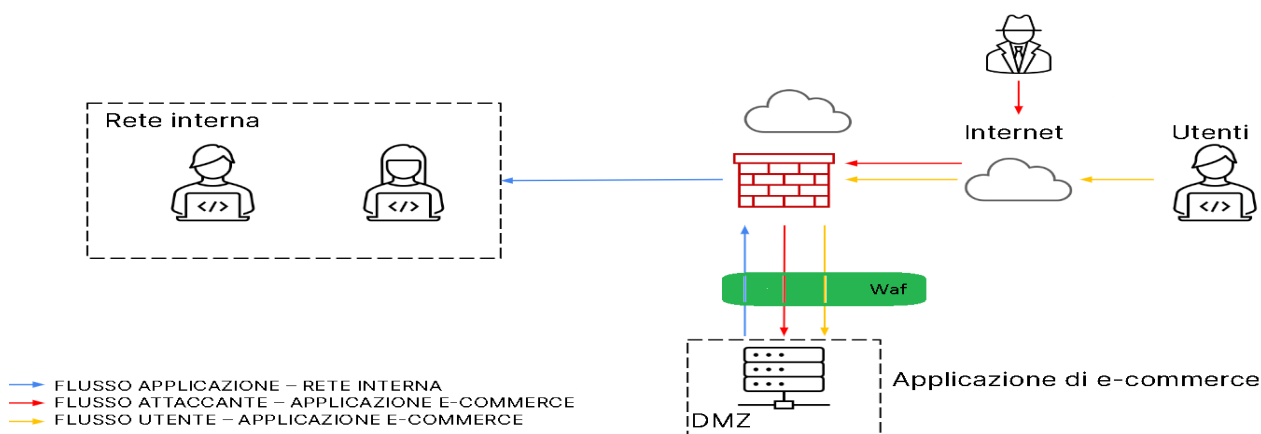


Progetto giorno 5

Azione preventiva

Ho introdotto un Web Application Firewall (WAF) che è una misura preventiva per proteggere un web server dagli attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS). Un WAF è un'applicazione o un dispositivo di sicurezza che filtra il traffico HTTP/HTTPS in ingresso e in uscita per rilevare e bloccare attacchi alle applicazioni web. Un WAF può analizzare il traffico HTTP in ingresso e identificare tentativi di SQLi. Utilizzando firme o modelli predefiniti, può rilevare caratteristiche sospette nelle query SQL e bloccare le richieste sospette. Inoltre può eseguire una validazione dei dati in input in tempo reale, identificando i caratteri e le sequenze pericolose che potrebbero essere utilizzate in un attacco XSS. Può bloccare o neutralizzare questi input dannosi prima che raggiungano l'applicazione web.



Analisi dell'attacco

Ho utilizzato il sito "ExpandURL" per ottenere i link completi da due short link che ho ricevuto. Questi short link sembravano reindirizzare alla pagina del sito Any.Run. Any.Run è una piattaforma online che consente di eseguire e analizzare in modo sicuro file e URL sospetti in un ambiente controllato.

Results for <https://tinyurl.com/linklosco1>



Title: Analysis https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1
Suspicious activity - Interactive analysis ANY.RUN

Short URL: <https://tinyurl.com/linklosco1>

Redirects: 1 (show details)

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



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

Short URL: <https://tinyurl.com/linklosco2>



Redirects: 1 (show details)

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

Dopo aver analizzato i due link ottenuti dalla pagina di Any.Run, ho notato che uno dei link era uno script di PowerShell che sembrava cambiare le impostazioni del server DNS per la connessione Wi-Fi. Questa attività è stata segnalata come sospetta dalla piattaforma Any.Run. Lo script di PowerShell sembra avere la capacità di modificare le impostazioni del server DNS, il che potrebbe comportare potenziali rischi per la sicurezza e la privacy delle connessioni Internet. Il secondo link, invece, è stato identificato come Remcos dalla piattaforma Any.Run. Remcos è un software remoto di accesso e controllo, che può essere utilizzato per scopi legittimi, ma può anche essere utilizzato in modo malevolo per acquisire il controllo remoto di un computer senza il consenso dell'utente. La piattaforma Any.Run ha classificato questo link come potenzialmente dannoso.

General Info

✓ Add for printing

URL: https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1
Full analysis: <https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a>
Verdict: **Suspicious activity**
Analysis date: June 29, 2023 at 18:56:12
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:  

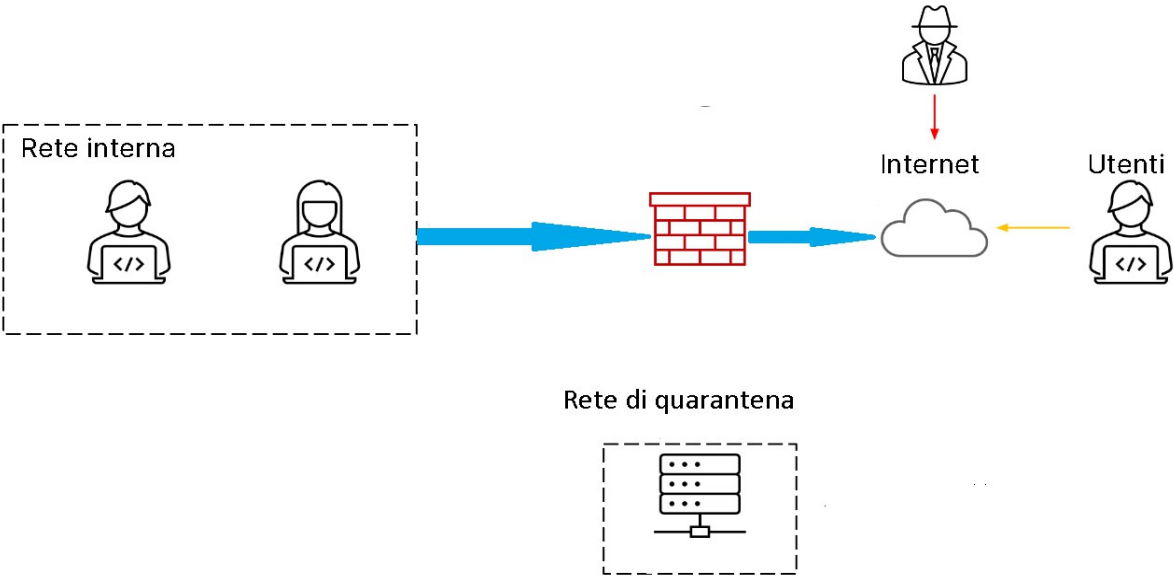
General Info

✓ Add for printing

URL: https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgTAG_apwtYT6OYs
Full analysis: <https://app.any.run/tasks/685ba854-4644-4140-9ea5-be9057161248>
Verdict: **Malicious activity**
Threats: **Remcos**
Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively capped up to date with updates coming out almost every single month.

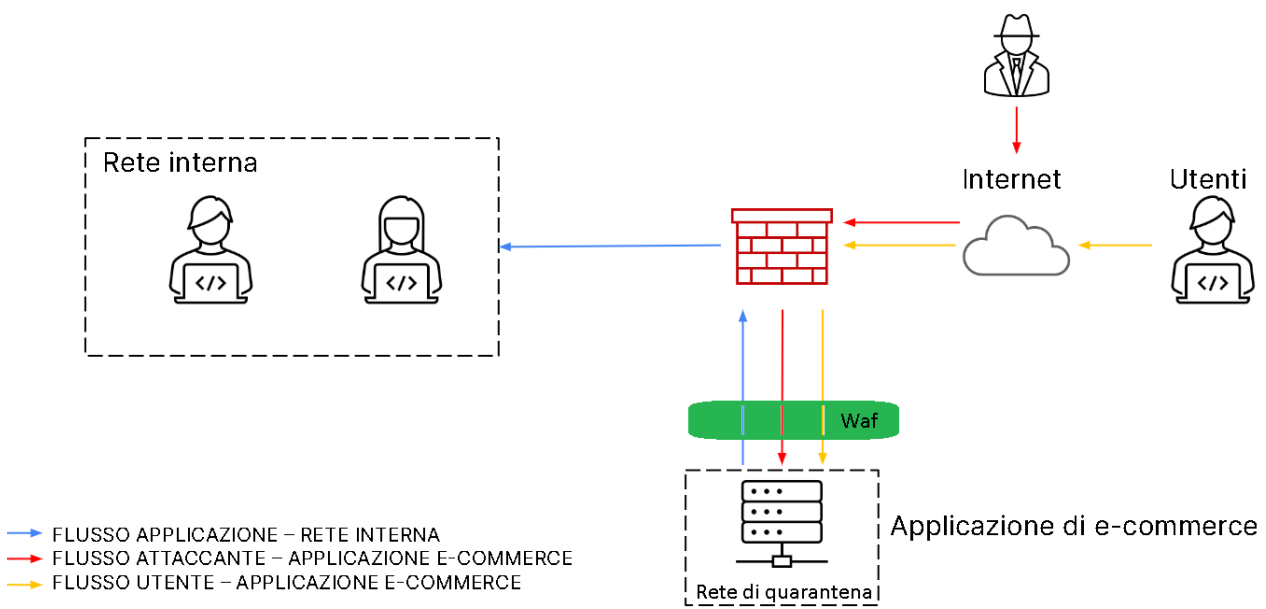
Response

Ho modificato la rete a causa di un malware che ha colpito il web server. Per proteggere la rete, ho eliminato completamente il web server sia dall'accesso esterno tramite Internet che dalla rete interna. Con questa azione, impedisco al malware di avere accesso alla rete interna attraverso il server compromesso. Eliminando completamente il web server dalla rete interna e bloccando l'accesso a Internet al malware, riduco al minimo il rischio di ulteriori infezioni o di divulgazione di informazioni. Infine, consiglio di ristabilire il web server solo dopo aver implementato adeguate misure di sicurezza e aver verificato che sia privo di malware.



Soluzione completa

Ho implementato un sistema di sicurezza per proteggere il Web Server e la rete interna, combinando l'uso di un WAF (Web Application Firewall) e una rete di quarantena. Collocando il WAF tra Internet e la nostra rete interna esso analizza il traffico in ingresso al Web Server e blocca eventuali attività sospette o tentativi di attacco noti. Questo strumento ci consente di applicare regole di sicurezza personalizzate, filtrando e bloccando le minacce comuni alle applicazioni Web. Successivamente, ho adottato una strategia di segmentazione di rete attraverso l'implementazione di una rete di quarantena. Ho creato una zona isolata in cui è posizionato il Web Server. Questa rete è progettata per limitare l'accesso diretto al Web Server dalla rete interna principale, creando una barriera aggiuntiva contro le minacce esterne. Ciò significa che il Web Server è isolato dal resto della rete, riducendo la probabilità di un potenziale attacco che si propaghi alla rete interna. Si possono configurare regole di routing e firewall per consentire solo il traffico autorizzato tra il WAF, la rete di quarantena e il Web Server. Ogni richiesta che proviene dall'esterno viene filtrata dal WAF e solo quelle considerate sicure vengono inoltrate al Web Server. Inoltre, possiamo implementare il monitoraggio continuo del traffico di rete e dei log del WAF per rilevare rapidamente eventuali attività anomale.



Misure di sicurezza ulteriori

Per migliorare ulteriormente la sicurezza possiamo implementare una serie di misure aggiuntive per proteggere il Web Server e l'infrastruttura di rete:

1. **Failover Cluster:** Adottando un'architettura di failover cluster per il Web Server. Un failover cluster è un gruppo di server che lavorano insieme per fornire ridondanza. In caso di guasto o inutilizzabilità di un server fisico, il carico di lavoro viene automaticamente spostato su un altro server funzionante nel cluster, garantendo la continuità del servizio e minimizzando il tempo di inattività.
2. **Utilizzo di Sistemi di Virtualizzazione:** Implementando sistemi di virtualizzazione si può ottenere un ambiente informatico virtualizzato. Questo consente di creare macchine virtuali che possono sostituire rapidamente un server fisico in caso di necessità.
3. **IDS e IPS:** Implementando sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS) si possono monitorare il traffico di rete e rilevare eventuali attività sospette. Gli IDS analizzano il traffico in tempo reale e generano avvisi in caso di anomalie, mentre gli IPS intervengono attivamente per bloccare il traffico malevolo o dannoso.

4. Hardening dei Sistemi e delle Configurazioni: Possiamo applicare pratiche di hardening per rafforzare la sicurezza dei nostri sistemi e delle configurazioni. Questo include l'eliminazione di servizi, protocolli o porte non necessari, l'applicazione di patch di sicurezza regolari, la configurazione di password robuste e l'implementazione di politiche di accesso e autorizzazione ben definite.

5. Penetration Test Periodici: Periodicamente, sottoponiamo sistema a penetration test, in cui esperti di sicurezza informatica simulano attacchi per identificare eventuali vulnerabilità o punti deboli nel sistema.

