Log Analysis

CS0124

S9-L5 - Progetto

Indice

Team Progetto

Verdiana Germani

Bruno Falconi

Francesco Ficetti

Francesco Mineo

Alessio Rossetti

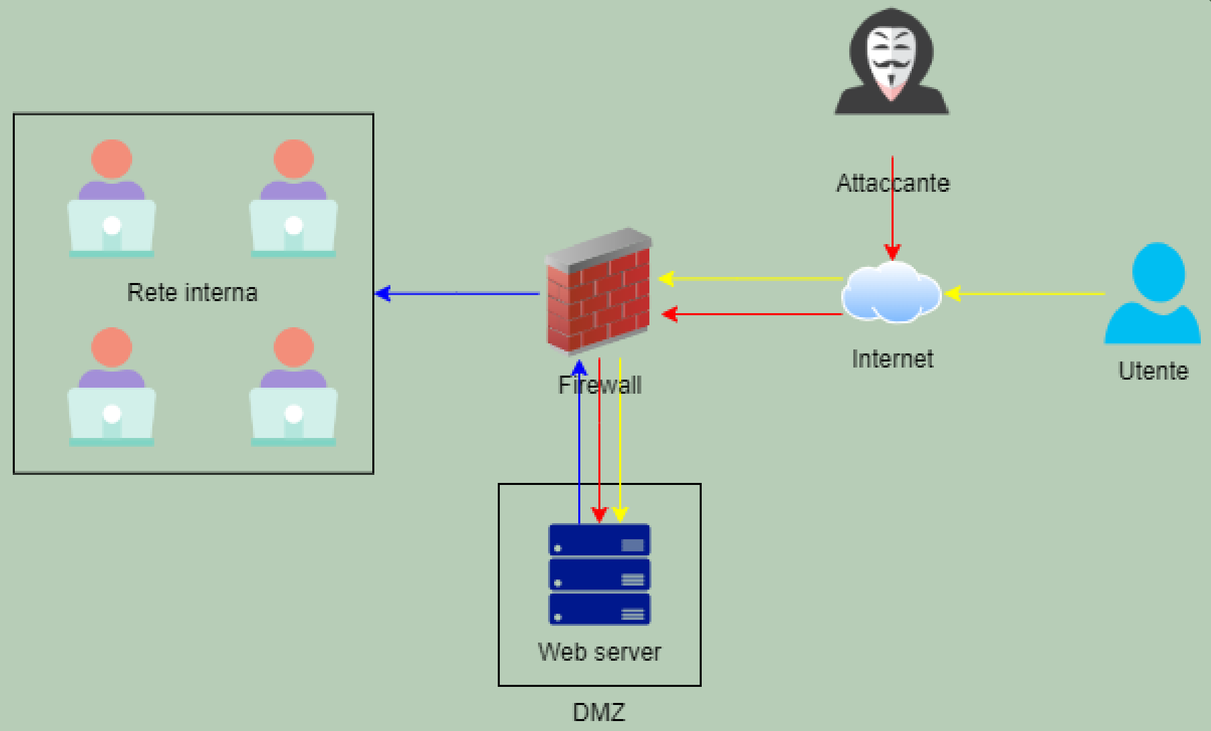
Flaviano Sedici

Traccia

Rispondere ai seguenti quesiti.

1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLioppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta .
4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

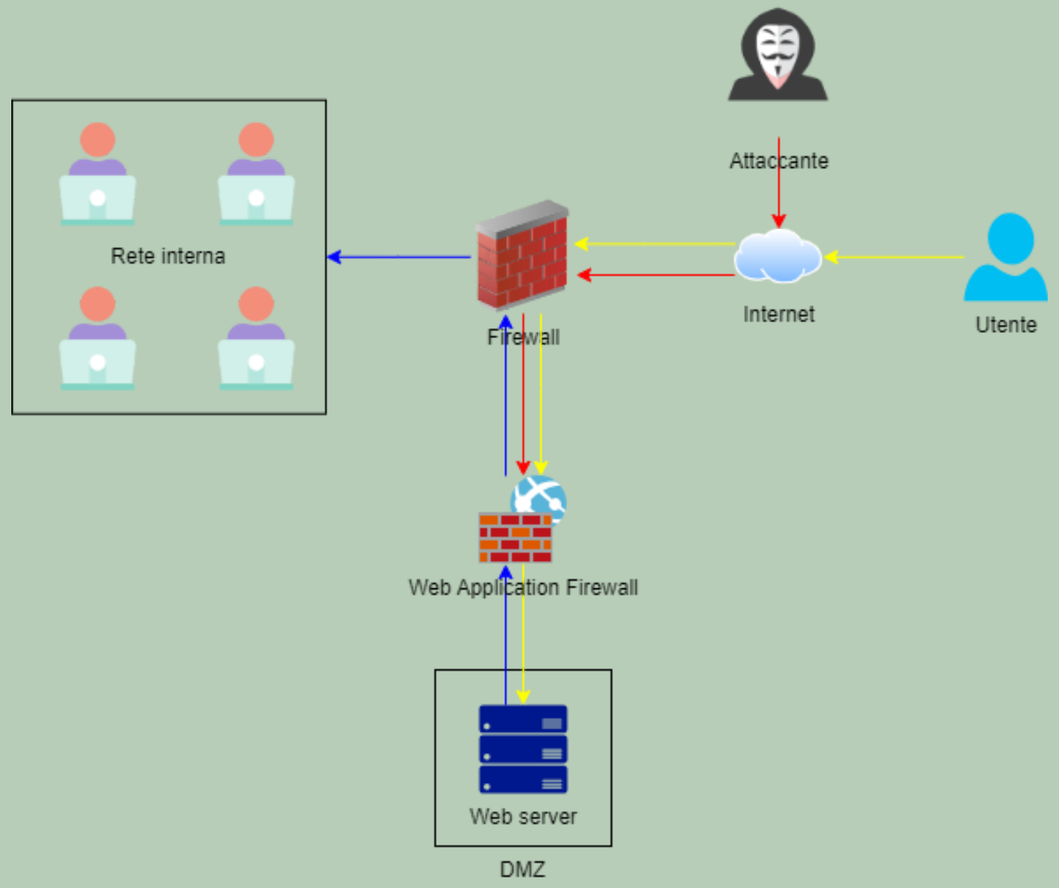
Architettura di rete



L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

Azioni preventive

Per proteggere le applicazioni Web – in questo caso il nostro sito di e-commerce ospitato all'interno di una **DMZ** – da eventuali attacchi di tipo SQLi o XSS, potremmo introdurre un WAF (Web Application Firewall).



Altre opzioni di implementazione della sicurezza potrebbero essere la sanitizzazione dell'input utente e il monitoraggio del traffico di rete.

Definizioni

WAF

Il WAF (Web Application Firewall) è un firewall progettato per proteggere le applicazioni web da minacce e vulnerabilità, monitorando e filtrando il traffico HTTP tra l'applicazione e il cliente.

DMZ

La DMZ (zona demilitarizzata) è una rete intermedia tra Internet e la rete interna di un'organizzazione, utilizzata per ospitare servizi pubblici accessibili dall'esterno, come server web, e-mail e FTP, mentre protegge la rete interna dai rischi esterni.

SQLi

SQLi (SQL Injection) è una vulnerabilità che consente agli attaccanti di inserire codice SQL dannoso attraverso i campi di input dell'applicazione web, consentendo l'esecuzione di comandi non autorizzati sul database.

XSS

XSS (Cross-Site Scripting) è una vulnerabilità che consente agli attaccanti di inserire script dannosi all'interno delle pagine web visualizzate dagli utenti, compromettendo la sicurezza dell'applicazione e potenzialmente rubando informazioni sensibili degli utenti.

Impatti sul business

Durante l'attacco **DDoS** (Distributed Denial of Service), il servizio diventa irraggiungibile ai clienti per circa 10 minuti. Dai dati storici rilevati dall'impresa, ogni minuto gli utenti spendono € 1.500 sulla piattaforma di e-commerce. A causa dei 10 minuti di interruzione del servizio, l'impresa ha presumibilmente perso circa € 15.000. Al fine di evitare la perdita potrebbe essere ridotta o evitata con un corretto BCP (Business Continuity Plan), che permetterebbe ad un servizio di continuare ad operare anche in situazioni critiche, come nel caso di un attacco DDoS, danni accidentali o addirittura calamità naturali.

Calcolo impatto sul business alla non raggiungibilità del servizio:
Spesa media x Servizio fuori uso = **1.500 x 10 = 15.000**

Impatti sul business

Per elaborare un **BCP** efficace dovremmo identificare i fattori di rischio, partendo da quelli più critici (Risk Assessment), valutare l'impatto che questi avrebbero sull'azienda (BIA, Business Impact Analysis), erogare regolarmente la formazione al personale dipendente, effettuare backup o hot site per ridurre al minimo il disservizio del sistema. Una continua implementazione e revisione del BCP consente di gestire al meglio le lessons learned facendo fronte alle nuove ed emergenti minacce alla cybersecurity.

Definizioni

DDoS

DDoS (Distributed Denial of Service) è un tipo di attacco informatico in cui un aggressore utilizza una rete di computer compromessi, chiamati botnet, per sovraccaricare un server o una rete con un flusso di traffico illegittimo, rendendo il servizio inaccessibile agli utenti legittimi.

BCP

BCP (Business Continuity Planning) è il processo di identificazione dei rischi aziendali, sviluppo di strategie di risposta agli incidenti e creazione di piani operativi per garantire la continuità delle operazioni in caso di interruzioni impreviste, come disastri naturali o attacchi informatici.

Hot Site

Un hot site è una struttura completamente attrezzata e pronta all'uso che viene attivata immediatamente in caso di interruzione delle operazioni presso il sito principale dell'azienda. Serve come sito alternativo in grado di ripristinare rapidamente le operazioni aziendali essenziali in caso di disastro.

BIA

BIA (Business Impact Analysis) è una analisi sistematica dei processi aziendali critici e dei loro impatti finanziari, operativi e di reputazione in caso di interruzioni. Aiuta a identificare priorità di ripristino e a pianificare strategie di continuità aziendale.

Response

Una strategia efficace per proteggere la rete interna e quindi prevenire danni, proteggere dati sensibili e i sistemi critici, potrebbe essere l'isolamento del sistema compromesso. Questo significa creare una quarantena così da limitare l'attaccante e impedirgli di accedere ai dati sensibili e ai dispositivi critici. Sebbene l'attaccante malevolo abbia ancora la possibilità di interagire con il sistema compromesso, andando ad isolare il dispositivo, interrompiamo il suo accesso alla rete interna limitando in questo modo l'attacco

Questa soluzione permette all'azienda di limitare i danni tecnici ed economici, in quanto consente di lasciare il servizio disponibile agli utenti mentre l'azienda identifica e risolve le vulnerabilità della web app ed interviene per ripristinare la sicurezza del sistema, o trasferire il servizio su un nuovo asset non compromesso.

Definizioni

Isolamento

L'isolamento di un asset dalla rete interna di un'azienda è il processo di separazione fisica o logica di un dispositivo o sistema dalla rete aziendale principale per proteggerlo da accessi non autorizzati o per prevenire la diffusione di malware o attacchi all'interno della rete. Ad esempio lasciando l'asset libero di accedere ad internet senza che il suo traffico transiti per il firewall aziendale.

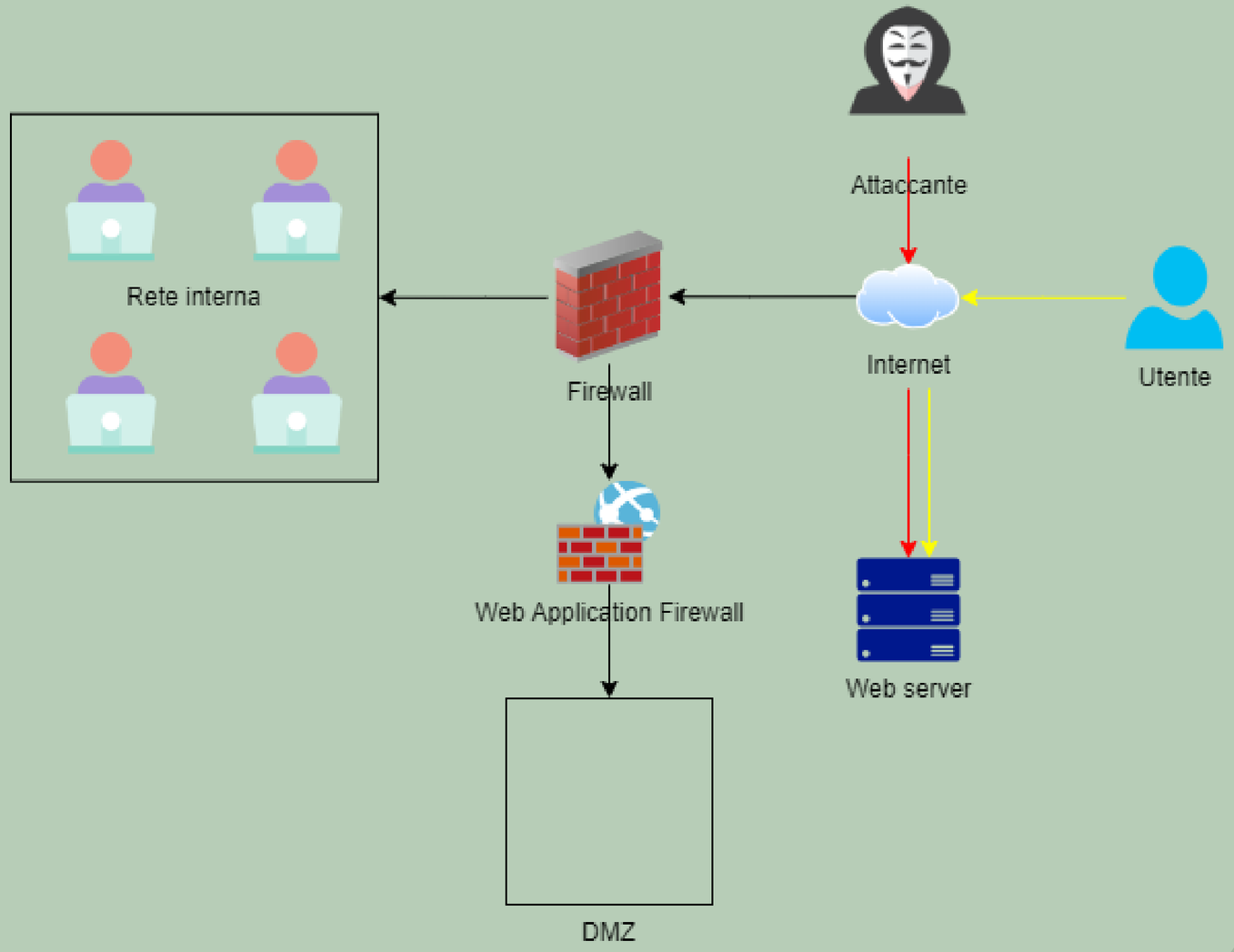
Malware

Il malware è un software progettato per danneggiare, controllare o rubare dati dai dispositivi informatici. Include virus, worm, trojan, ransomware e spyware, distribuiti attraverso e-mail, siti web compromessi o dispositivi infetti.

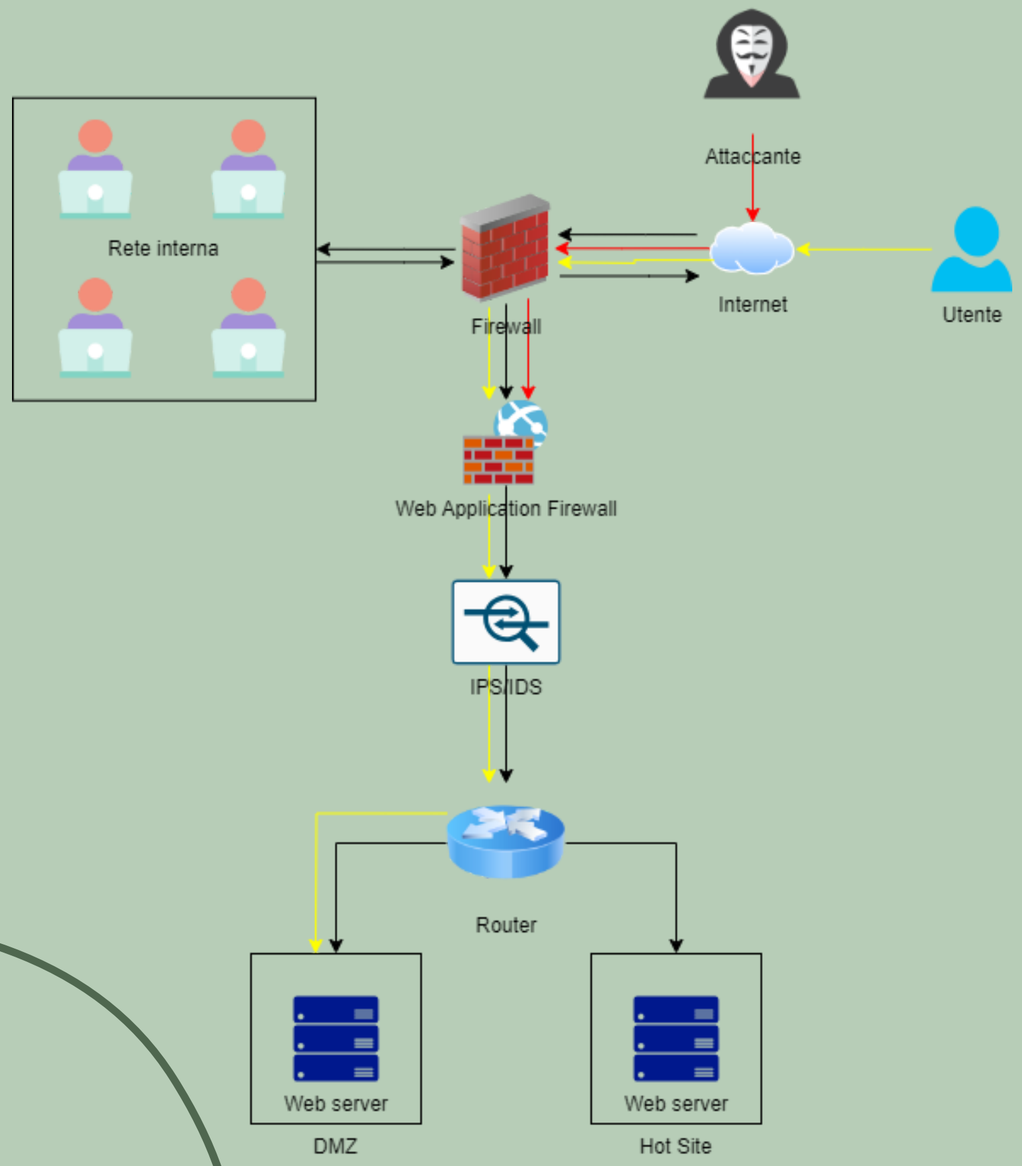
Quarantena

La quarantena di un asset da una rete interna di un'azienda è il processo di isolamento temporaneo di un dispositivo o sistema sospetto o compromesso dalla rete aziendale principale per prevenire la diffusione di minacce e consentire un'analisi approfondita e la risoluzione del problema. Il processo avviene ad esempio tramite la creazione di un VLAN separata.

Soluzione completa



Modifiche aggressive



Al fine di rafforzare la sicurezza dell'architettura di rete, si consiglia l'inserimento di un dispositivo IDS/IPS a valle del Web Application Firewall in modo da controllare ulteriormente il traffico in transito alla ricerca di possibili minacce.
L'IDS/IPS aggiunge quindi un nuovo layer a protezione di attacchi DDoS, SQLi e XSS.
Si consiglia inoltre l'inserimento di un router e un hot site in modo che la continuità del servizio sia assicurata in caso di attacco.
Il router consente un buon isolamento del hot site dalla rete internet fino al momento della sua attivazione proteggendolo anche nel caso in cui il firewall principale venga compromesso.
Infine si suggerisce di modificare le firewall policies in modo che gli utenti della rete interna non possano accedere direttamente alla DMZ, eliminando la possibilità che, in caso di compromissione degli endpoint, un eventuale attaccante possa facilmente accedere ai webservers.

Definizioni

IDS

Un IDS (Intrusion Detection System) è un sistema di sicurezza informatica che monitora attivamente il traffico di rete o le attività dei sistemi per identificare e segnalare potenziali intrusioni, attacchi informatici o comportamenti anomali, aiutando a proteggere gli asset digitali dell'organizzazione.

IPS

Un IPS (Intrusion Prevention System) è un sistema di sicurezza informatica che analizza il traffico di rete in tempo reale per individuare e prevenire attivamente gli attacchi informatici. Utilizza regole predefinite o algoritmi avanzati per bloccare immediatamente i tentativi di intrusione o di violazione della sicurezza.

Router

Un router è un dispositivo di rete che instrada il traffico dati tra reti o subnet diverse. Funge da gateway tra la rete locale e Internet, determinando il percorso ottimale per inviare i dati in base agli indirizzi IP di destinazione.

Firewall Policies

Le policy del firewall sono regole configurate su un firewall per regolare il flusso del traffico di rete. Definiscono cosa è consentito o bloccato in base a criteri come indirizzi IP, porte, protocolli e applicazioni, garantendo la sicurezza e il controllo dell'accesso alla rete.

Bonus 1

Questo malware
PERFORMANCE_BOOSTER_v3.6.exe
si finge un file che ha come obbiettivo quello di migliorare le prestazioni dell'end-point (in questo caso un windows 7).
Questo file, invece, esegue un comando sulla **CLI** che permette di avviare dei file eseguibili dannosi per il sistema e nascondendo la sua presenza.
Il file in quesione può essere di grave impatto per la rete nella quale il client infetto è connesso perchè - agendo in incognito - avrebbe accesso a dati sensibili e potrebbe mettersi in ascolto tra due o più dispositivi collegati fra loro creando ulteriori danni.
Il miglior modo per contrastrare il malware è quello di disinstallare immediatamente il file, successivamente avviare una scansione specifica antivirus e con l'autorizzazione del dipartimento di competenza controllare i log per risalire alla sorgente da dove è stato scaricato il file.

Definizioni

CLI – Command Line Interface

CLI (Command Line Interface), noto anche come prompt dei comandi, console, riga di comando, shell o terminale, è un'interfaccia testuale presente in molti sistemi operativi. Consente agli utenti di interagire direttamente con il sistema operativo attraverso comandi testuali, eseguendo operazioni come la gestione dei file, la navigazione tra le cartelle, l'automazione di compiti ripetitivi e la risoluzione dei problemi.

MITM – Man in the Middle

Un attacco "man in the middle" (MITM) è un tipo di attacco in cui un malintenzionato intercetta segretamente la comunicazione tra due parti che credono di comunicare direttamente tra loro. L'attaccante può ascoltare, alterare o inserire nuovi messaggi nella conversazione, compromettendo così la privacy e l'integrità dei dati scambiati.

LOG

I log sono file di testo che registrano eventi rilevanti nei sistemi informatici. Servono per monitorare attività, analizzare problemi, garantire sicurezza e ottimizzare prestazioni. Contengono dettagli come tipo di evento, data e ora, e sono spesso usati per diagnosticare errori o comportamenti anomali.

End-point

Un end-point è un dispositivo, come un computer, un laptop, uno smartphone o un tablet, che si connette a una rete per accedere a risorse o servizi. Gli endpoint possono includere anche dispositivi IoT, come stampanti di rete o dispositivi intelligenti.

Bonus 2

Questo malware:
https://1drv.ms/u/s!At7eQ7h8kx6-nQMIRTCuz3aQspOE
si camuffa come aggiornamento per il browser di windows.
Una volta avviata l'azione GET il computer inizia a scaricare file dannosi all'interno del sistema, fingendosi file di sistema. Il file in questione va a manipolare le impostazioni di rete ed i log di sistema tramite un server remoto, creando una serie di danni che gravano sulla produttività del dispositivo rendendo difficoltosa qualsiasi tipo di operazione online. Il miglior modo per contrastare questo tipo di vulnerabilità è quello di installare un WAF (Web Application Firewall) così da rilevare più facilmente file malevoli di questo tipo. Inoltre, sarebbe opportuno redigere un "playbook" contenente le regole e procedure da seguire nel momento in cui si devono eseguire degli aggiornamenti di sistema o di software interni. Nel caso in cui il malware sia già installato all'interno del sistema, andrebbe eseguita una scansione antivirus specifica, ed agire secondo Remediation Actions.

Definizioni

Remediation Actions

Le "remediation actions" in informatica si riferiscono alle azioni intraprese per risolvere o mitigare i problemi o le minacce identificate all'interno di un sistema. Queste azioni sono parte integrante dei processi di gestione delle minacce e dei rischi nelle organizzazioni e sono progettate per ripristinare l'integrità, la disponibilità e la sicurezza dei sistemi informatici.

Antivirus

Un antivirus è un software progettato per rilevare, prevenire e rimuovere malware dai dispositivi informatici. Utilizza metodi come la scansione dei file, l'analisi del comportamento e le firme digitali per identificare e neutralizzare virus, worm, trojan, ransomware e altre minacce alla sicurezza.

Playbook

Un playbook è un documento o una serie di istruzioni dettagliate che delineano le procedure e le azioni da seguire in risposta a determinate situazioni o scenari. Nei contesti della sicurezza informatica e della gestione degli incidenti, i playbook sono spesso utilizzati per standardizzare e automatizzare la risposta agli incidenti, fornendo istruzioni chiare e strutturate per il personale di sicurezza.

GET- http verbs

GET è un metodo di richiesta HTTP utilizzato dai client per ottenere risorse dai server web. Nella richiesta GET, i parametri sono trasmessi attraverso l'URL come stringa di query, consentendo ai server di recuperare i dati specificati e inviarli al client come risposta.

Grazie!