PROGETTO SETTIMANALE S9/L5

CS0224

Christopher Caruso

29/04/2024

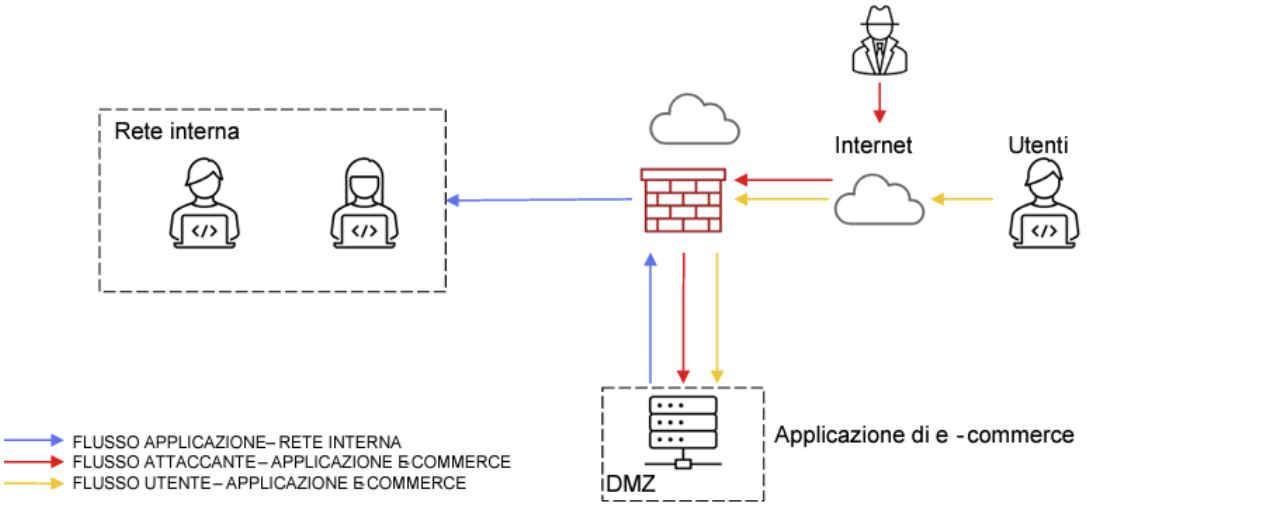
SOMMARIO

TRACCIA

I punti della traccia sono inseriti nelle relative sezioni di dettaglio.

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.

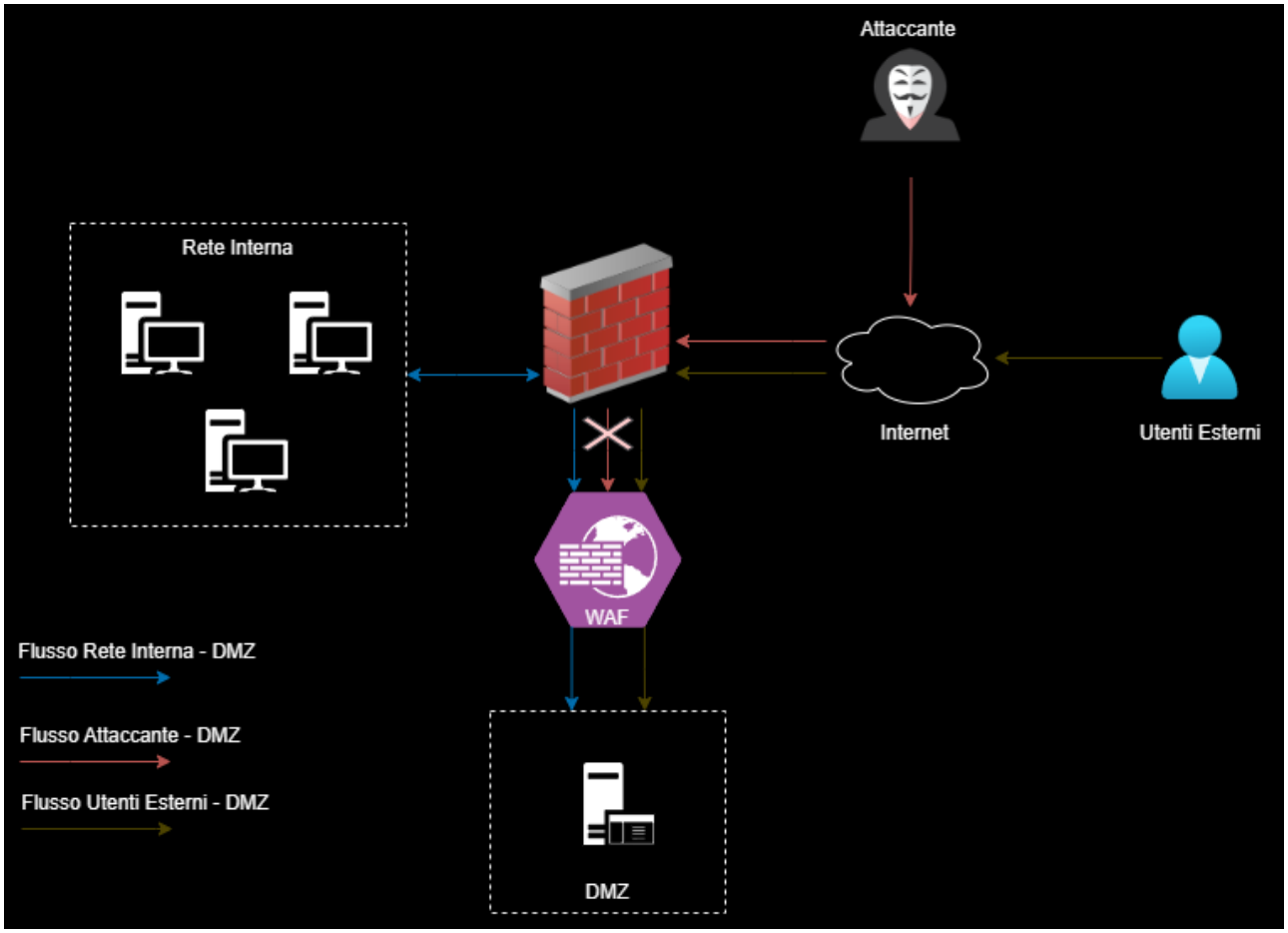


Con riferimento alla figura, rispondere ai seguenti quesiti.

1. Azioni Preventive

Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

Schema rivisitato



Nell'immagine dello schema di rete è stato introdotto l'utilizzo di un WAF (Web Application Firewall).

L'inserimento di un WAF potrebbe essere gestito in modi diversi, ad esempio tramite gestione dei record DNS facendo in modo che tutte le richieste alla web app vengano dirottate verso il WAF (configurazione tipica di cloudflare).

Lo schema proposto dunque non è vincolante rispetto alla posizione del WAF ma è da considerarsi a titolo di esempio in merito al flusso dati che entra in gioco.

Grazie alle regole sul traffico impostate nel WAF il traffico dell'attaccante relativo ad eventuali attacchi XSS o SQL Injection non viene inoltrato alla web app.

È stata introdotta un'ulteriore modifica relativa al traffico tra rete interna e DMZ.
Concettualmente l'apertura del traffico della rete interna è outbound verso la DMZ e non inbound dalla DMZ.
I client che hanno bisogno di effettuare richieste alla web app ricevono risposte sui socket aperti dalla connessione, non è quindi necessario aprire il traffico in ingresso dalla DMZ alla rete interna.
Per quanto riguarda il traffico a livello di server (tuttavia non introdotto nello schema della traccia), al più sarebbe necessario introdurre un proxy in grado di intercettare e filtrare le richieste della web app verso un server interno (e.g. query verso un database, richiesta auth LDAP etc.).
Nello schema proposto, anche il traffico della rete interna verso la web app deve passare dal WAF così che, se in rete interna fosse presente un client compromesso il traffico anomalo verrebbe bloccato.

2. Impatti sul Business

L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per dieci 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.

Se la web app non è raggiungibile per 10 minuti, a seguito di un attacco DDoS, e la media del guadagno a minuto è 1.500€, è sufficiente moltiplicare il guadagno medio a minuto per il totale dei minuti a cui ammonta il fermo del servizio.

Calcolo:
1.500 * 10 = 15.000

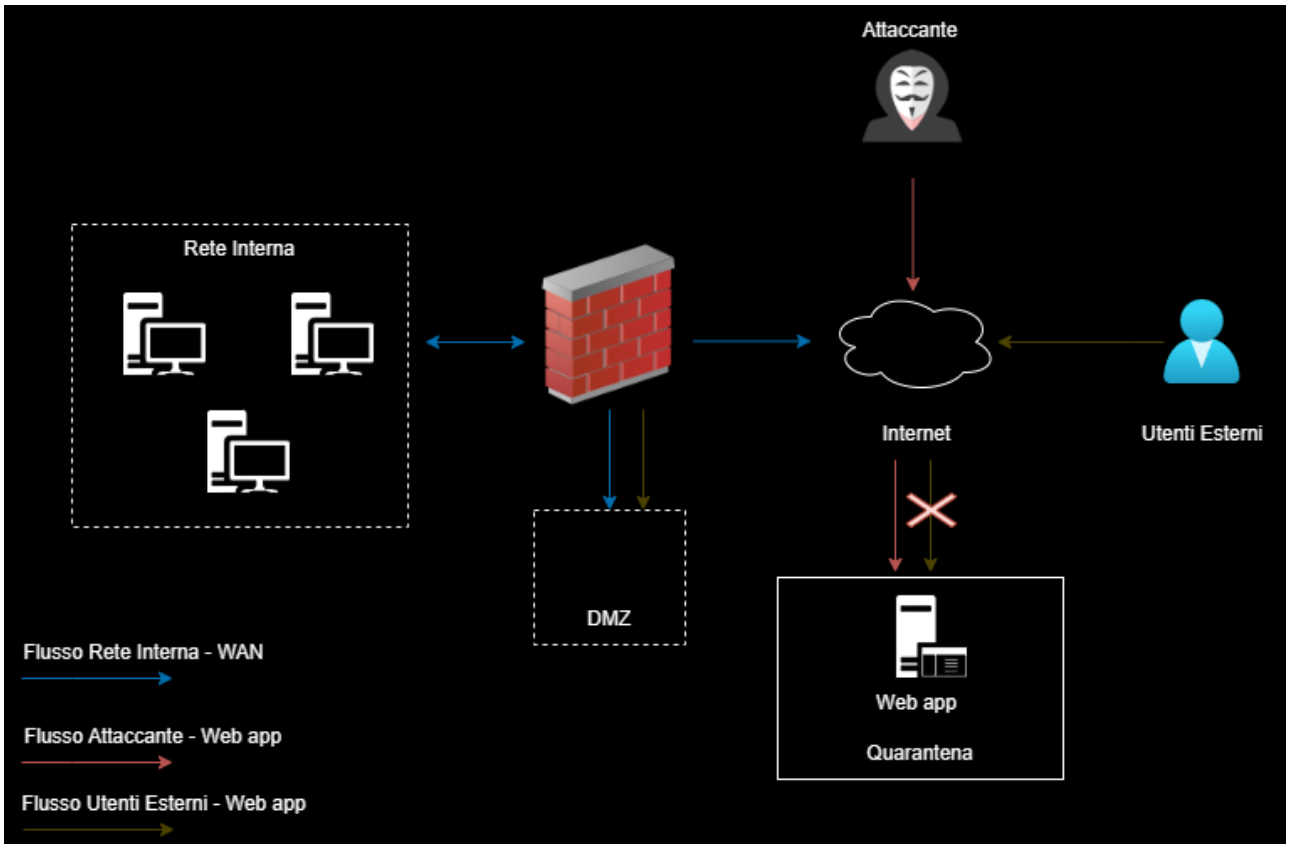
Considerazioni:

La perdita potenziale totale per l'azienda ammonta a 15.000 €.
Per la protezione da questo tipo di attacco ci sono diverse tecniche, è possibile introdurre servizi di protezione da attacchi DDoS a livello di Firewall; *cloudflare*, ad esempio, introduce la possibilità di prevenire attacchi DDoS ma ci sono alternative come *radware* che sono focalizzate sulla protezione da questo tipo di attacchi.
Nel caso in cui una web app sia esposta tramite cloud Azure si può introdurre la protezione tramite Azure DDoS Protection, nel caso in cui ci si appoggi ad un qualsiasi SP per hosting privato (e.g. Aruba) solitamente la protezione da attacchi DDoS è inclusa nel servizio.
Un' altro metodo è quello di ricorrere alle famose CDN - Content Delivery Network (Rete di distribuzione dei contenuti) che sono costituite da una rete di server geograficamente dispersi composte da un server host, dove è ospitato il contenuto originale dell'applicazione, e una serie di server "edge" che memorizzano in cache delle copie del contenuto originale e rispondono alle richieste degli utenti in base alla vicinanza geografica dal nodo in cui si trova il server edge stesso. Questo porta a numerosi vantaggi: riduzione del consumo di banda, distribuzione del carico di richieste, latenza ridotta e gestione ottimale dei picchi di traffico di richiesta e, inoltre, protezione nativa da attacchi DDoS. Un esempio di CDN è il servizio *CloudFront* di AWS.
In merito ai concetti affrontati durante il corso andrebbe previsto un meccanismo di ridondanza Hot Site o Warm Site, a seconda dei costi, per ridurre il down del servizio esposto (nel caso della CDN questo concetto è incluso).

3. Response

L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide due con la soluzione proposta.

Schema rivisitato



Nell'immagine dello schema di rete è stato proposto un isolamento della web app posizionata in una rete di quarantena isolata rispetto a DMZ e rete interna. Lo schema proposto prevede la creazione di una rete di quarantena, che nella realtà è sempre segmentata dal firewall che abilita solo il traffico inbound/outbound tra Rete Quarantena e WAN, ma per rafforzare il concetto visivo è stata posta esternamente. Questa tecnica di isolamento parziale durante la fase di contenimento esercitata dal *CSIRT (Computer Security Incident Response Team)* permette all'attaccante di accedere alla web app ma isola il sistema compromesso dal resto della DMZ e dalla rete interna. Non si dovrebbe mai usare questa tecnica, procedendo sempre con un isolamento completo

soprattutto nel caso in cui l'attaccante possa accedere a dati sensibili. Questo schema viene così proposto in attinenza alla traccia. Questa soluzione è utile solo nel caso in cui la priorità non sia solamente proteggere il sistema compromesso ma anche dare, per secondi fini, all'attaccante l'impressione di agire indisturbato.

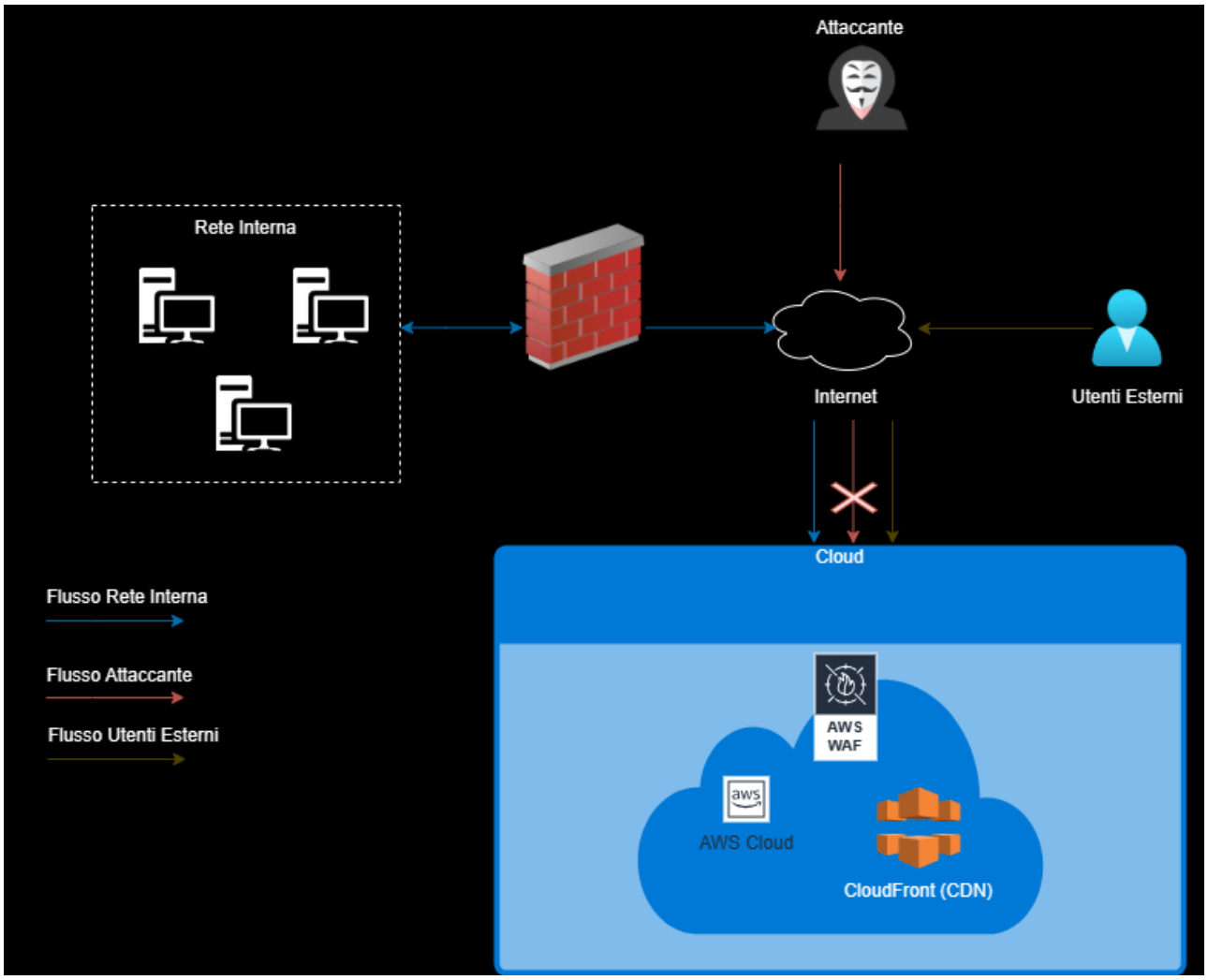
4. Soluzione Completa

Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

Questa richiesta non trova un senso poiché mettendo un WAF l'attaccante perde accesso e quindi le richieste del punto 3 non sarebbero soddisfatte. Ammesso che non si voglia configurare il WAF per lasciare libero l'accesso all'attaccante ma sarebbe far perdere tempo al reparto IT interno.

5. Modifica <<più aggressiva>> dell'infrastruttura

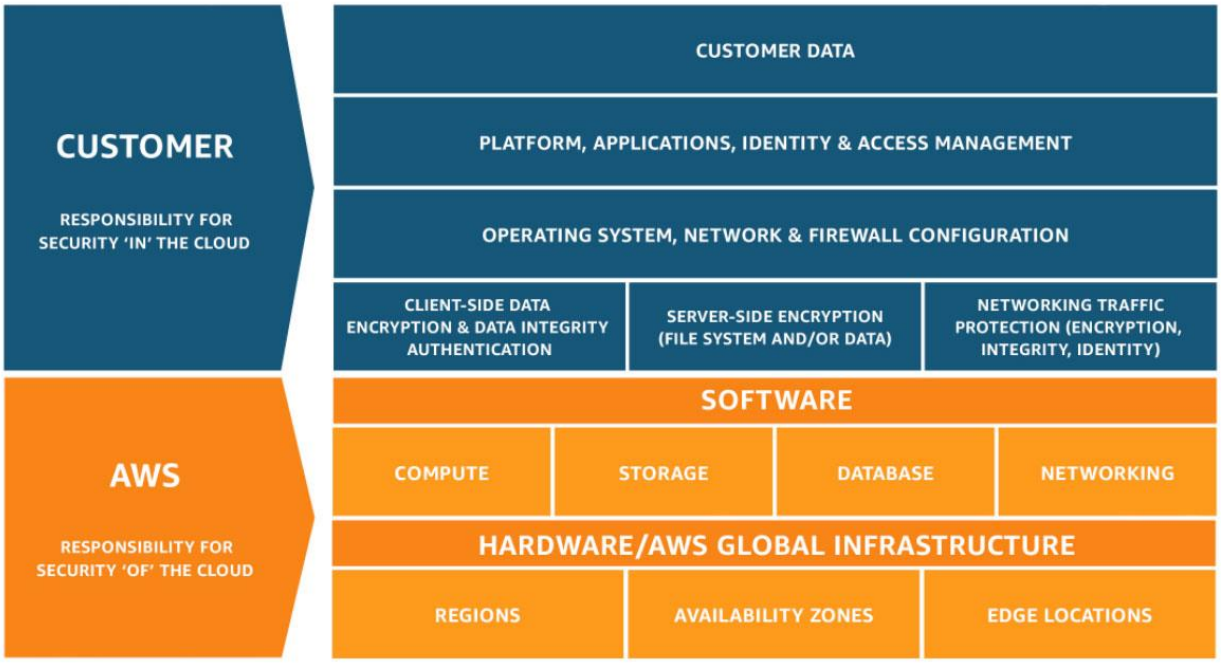
Integrare eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto due).



Questo schema riporta una delle infinite soluzioni alternative. Quella illustrata è una soluzione più drastica che prevede l'introduzione di un sistema cloud (nello specifico AWS) che implementa servizi di protezione avanzati (e.g. WAF, CDN precedentemente citati), servizi di scalabilità e ulteriori numerosi vantaggi che permettono di ottimizzare i costi e ridurre gli impatti.

Un ulteriore vantaggio del cloud, soluzione sempre più adottata dalle aziende per l'implementazione di servizi verso l'esterno, è lo schema di responsabilità condivisa che permette alle aziende di concentrare la forza lavoro e il proprio effort su un insieme più ristretto di attività inerenti alla sicurezza e protezione del sistema e dei dati in esso contenuti.

Di seguito lo schema di AWS:



Implementando questo tipo di soluzione l'azienda avrà in carico le attività di sicurezza indicate come "Responsability for Security IN the Cloud".
Per irrobustire la messa in sicurezza sono da citare ulteriori sistemi, tecnologie e metodi non inseriti nello schema di rete per semplicità:

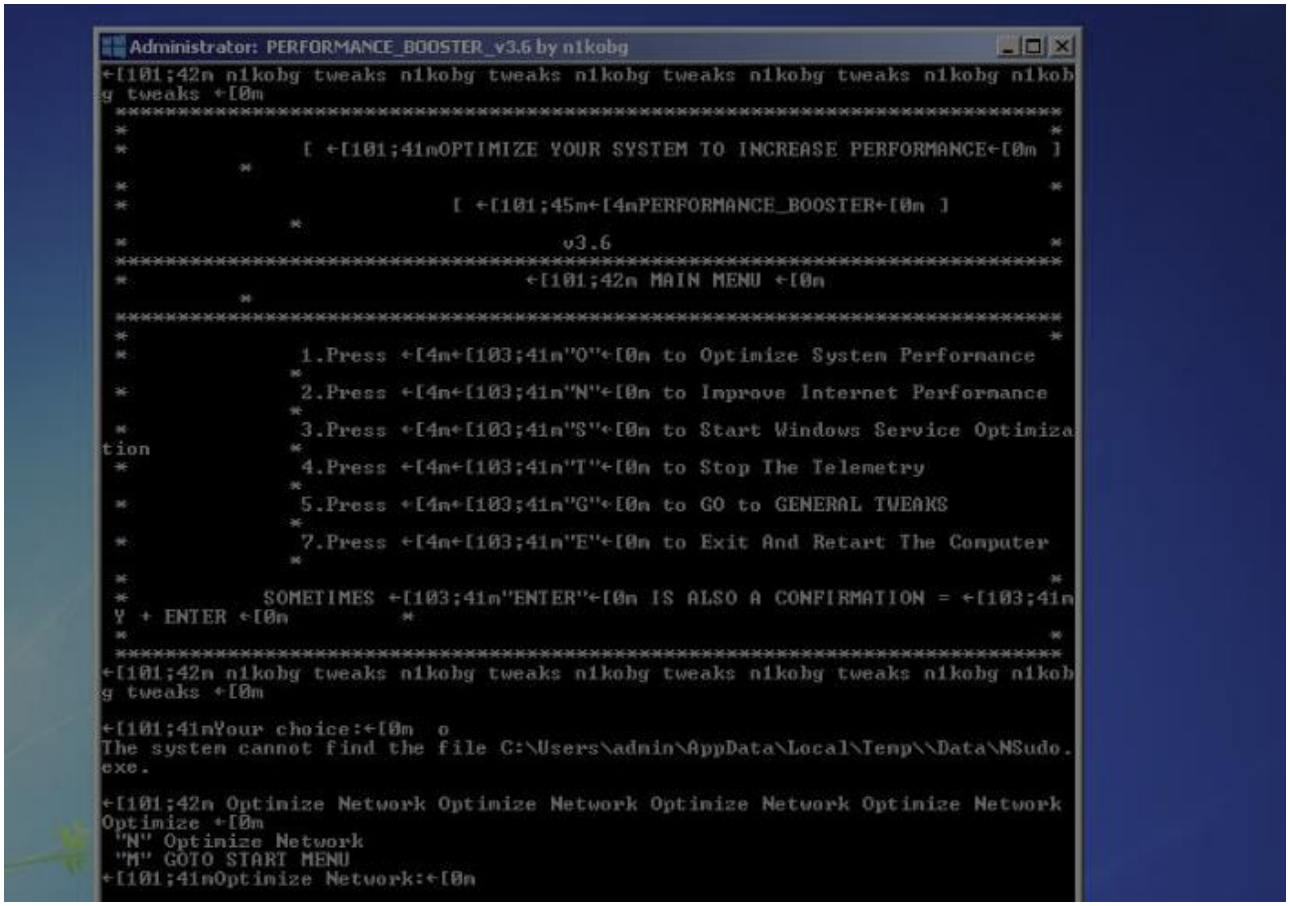
- Introduzione di un sistema *DR – Disaster Recovery* (magari sfruttando il cloud per un ambiente Hybrid) per i servizi critici;
- Introduzione di sistemi *SIEM (Secuirity Information Event Management)* e *SOAR (Security Orchestration, Automation and Response)* per un monitoraggio real-time degli eventi e l'implementazione di azioni di rimedio automatiche definite tramite playbooks;
- Segmentazione della rete più strutturata dividendo in VLAN a seconda del livello di criticità;
- Introduzione di sistemi di ridondanza su tutti gli asset critici (e.g. cluster HA, active-active e/o active-passive);
- Attivare meccanismi di encryption sui dati;
- Attivare policy di backup ottimali con l'esecuzione di almeno un Full settimanale ed un incrementale giornaliero, mantenendo una retention adeguata di almeno due Full per mese con relativa catena di incrementali.

BONUS

Analizzare le seguenti segnalazioni caricate su anyrune, fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/
https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

Analisi prima segnalazione



La segnalazione rilevata nel primo link riguarda un file eseguibile PERFORMANCE_BOOSTER_v3.6.exe costituito dal seguente hash MD5: 166903c9a390527ccd7728ae799a9d87.

Questo eseguibile svolge le seguenti operazioni critiche:

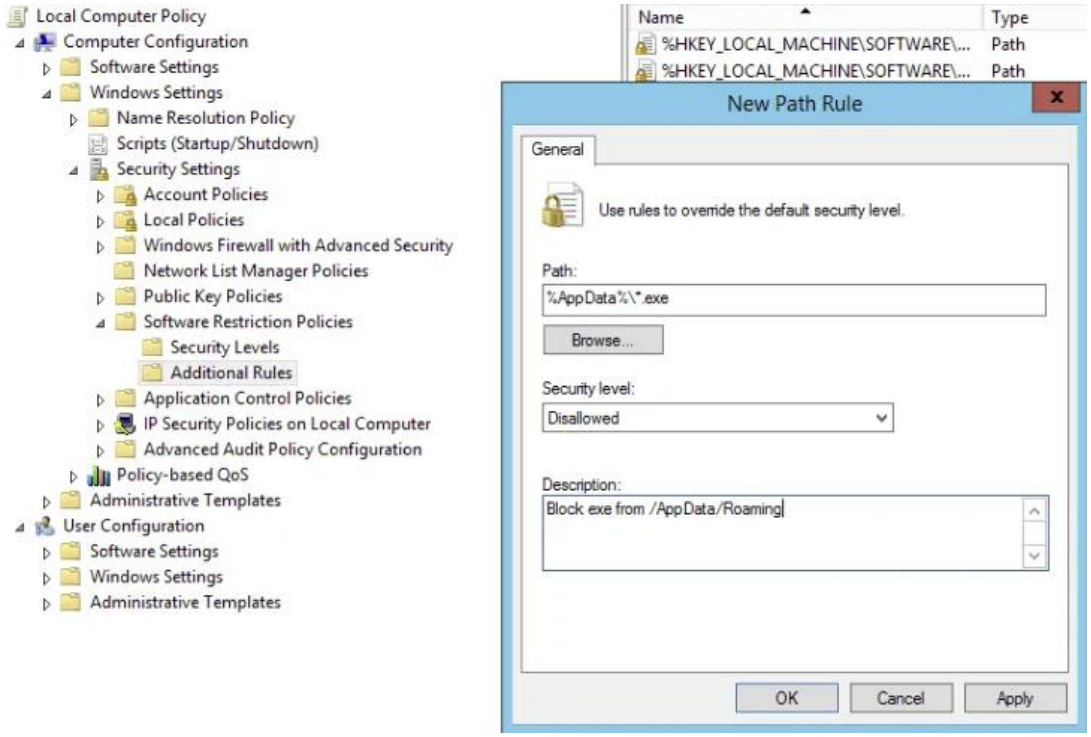
1) Modifica policy esecuzione powershell *Unrestricted* per poter eseguire script PowerShell con utenza locale ed esecuzione di script da cartella temporanea;
2) Recupero informazioni registro di sistema, creando una copia di backup, tra le quali sono stati recuperati l'elenco dei software installati, le connessioni RDP stabilite di recente, path di installazione di Outlook etc. ;
3) Modifica file host tramite ATTRIB e modifica permission di file e directory etc.

Si tratta, con molta probabilità, viste le operazioni di recupero delle informazioni da registro di sistema, di uno Spyware che ha lo scopo di recuperare informazioni dal client per poterle sfruttare in un secondo momento tramite altri vettori di attacco.

Azioni preventive e/o mitigative suggerite:

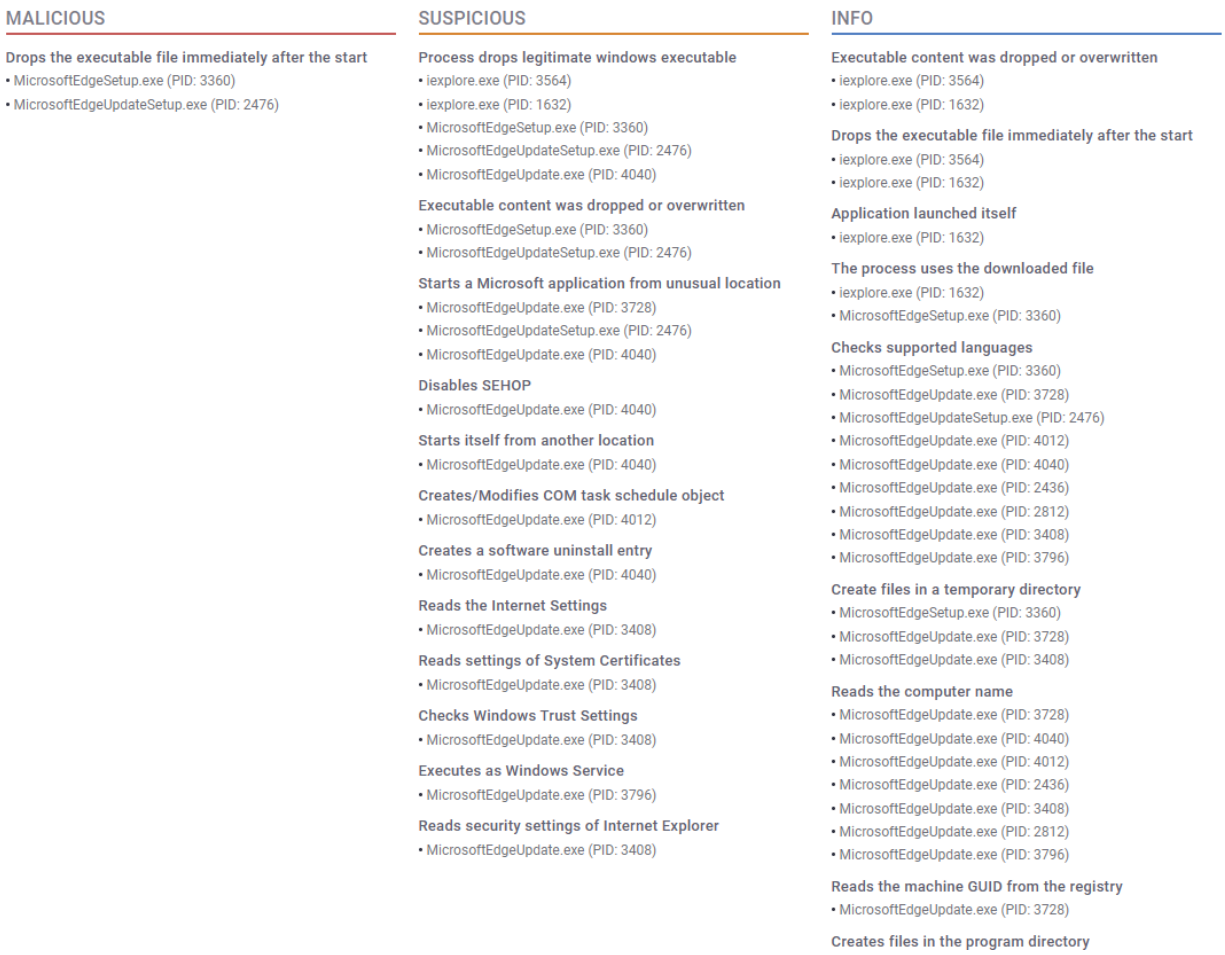
1) Dotare tutti gli asset di sistema antivirus next-gen, capace di riconoscere software malevoli non solo dal loro hash (come quello indicato precedentemente) tramite meccanismo di firma, ma anche analizzando il loro comportamento in fase di esecuzione effettuando blocchi preventivi (un esempio di software anti-malware next-gen è *Cortex*, prodotto da Palo Alto Networks);
2) Verificare sempre la fonte di file eseguibili ed evitare il download da fonti non sicure;
3) Abilitare la visualizzazione delle estensioni dei file (altrimenti un .exe potrebbe essere mascherato come falso .pdf);
4) Introdurre tramite group policy il blocco sul download di eseguibili;

5) Introdurre tramite antispam il filtro su allegati che contengono macro o file eseguibili;
6) Creare GPO per il blocco dell'esecuzione di file eseguibili da percorsi notoriamente graditi ai malware (e.g. %AppData%).



Analisi seconda segnalazione

La segnalazione rilevata nel secondo link riguarda un file eseguibile scaricato da una fonte non attendibile, mascherato sottoforma di aggiornamento del browser Microsoft Edge.



MALICIOUS

Drops the executable file immediately after the start
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

SUSPICIOUS

Process drops legitimate windows executable
- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Executable content was dropped or overwritten
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

Starts a Microsoft application from unusual location
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Disables SEHOP
- MicrosoftEdgeUpdate.exe (PID: 4040)

Starts itself from another location
- MicrosoftEdgeUpdate.exe (PID: 4040)

Creates/Modifies COM task schedule object
- MicrosoftEdgeUpdate.exe (PID: 4012)

Creates a software uninstall entry
- MicrosoftEdgeUpdate.exe (PID: 4040)

Reads the Internet Settings
- MicrosoftEdgeUpdate.exe (PID: 3408)

Reads settings of System Certificates
- MicrosoftEdgeUpdate.exe (PID: 3408)

Checks Windows Trust Settings
- MicrosoftEdgeUpdate.exe (PID: 3408)

Executes as Windows Service
- MicrosoftEdgeUpdate.exe (PID: 3796)

Reads security settings of Internet Explorer
- MicrosoftEdgeUpdate.exe (PID: 3408)

INFO

Executable content was dropped or overwritten
- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)

Drops the executable file immediately after the start
- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)

Application launched itself
- iexplore.exe (PID: 1632)

The process uses the downloaded file
- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)

Checks supported languages
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4012)
- MicrosoftEdgeUpdate.exe (PID: 4040)
- MicrosoftEdgeUpdate.exe (PID: 2436)
- MicrosoftEdgeUpdate.exe (PID: 2812)
- MicrosoftEdgeUpdate.exe (PID: 3408)
- MicrosoftEdgeUpdate.exe (PID: 3796)

Create files in a temporary directory
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdate.exe (PID: 3408)

Reads the computer name
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdate.exe (PID: 4040)
- MicrosoftEdgeUpdate.exe (PID: 4012)
- MicrosoftEdgeUpdate.exe (PID: 2436)
- MicrosoftEdgeUpdate.exe (PID: 3408)
- MicrosoftEdgeUpdate.exe (PID: 2812)
- MicrosoftEdgeUpdate.exe (PID: 3796)

Reads the machine GUID from the registry
- MicrosoftEdgeUpdate.exe (PID: 3728)

Creates files in the program directory

Questo eseguibile svolge le seguenti operazioni critiche:

1) Rimozione di file eseguibili legittimi di Windows (nello specifico gestore aggiornamenti di Edge);
2) Disabilita il supporto per la protezione da sovrascrittura per la gestione delle eccezioni strutturata (SEHOP). Questa funzionalità è progettata per bloccare gli exploit che utilizzano la tecnica di sovrascrittura SEH (Structured Exception Handler);
3) Crea dei task nello scheduler;
4) Recupera informazioni sensibili come impostazioni di sicurezza di Internet Explorer e del sistema operativo etc.

Azioni preventive e/o mitigative suggerite:

1) Dotare tutti gli asset di sistema antivirus next-gen, capace di riconoscere software malevoli non solo dal loro hash (come quello indicato precedentemente) tramite meccanismo di firma, ma anche analizzando il loro comportamento in fase di esecuzione effettuando blocchi preventivi

(un esempio di software anti-malware next-gen è *Cortex*, prodotto da Palo Alto Networks);

2) Verificare sempre la fonte di file eseguibili ed evitare il download da fonti non sicure;
3) Abilitare la visualizzazione delle estensioni dei file (altrimenti un .exe potrebbe essere mascherato come falso .pdf);
4) Introdurre tramite group policy il blocco sul download di eseguibili.