Settimana 9 - Esercizio 5

Alessio Golfetto, 09/02/2024

Traccia:

Con riferimento alla figura in slide nella pagina successiva, 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 DDoSdall'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 malwarenon 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.

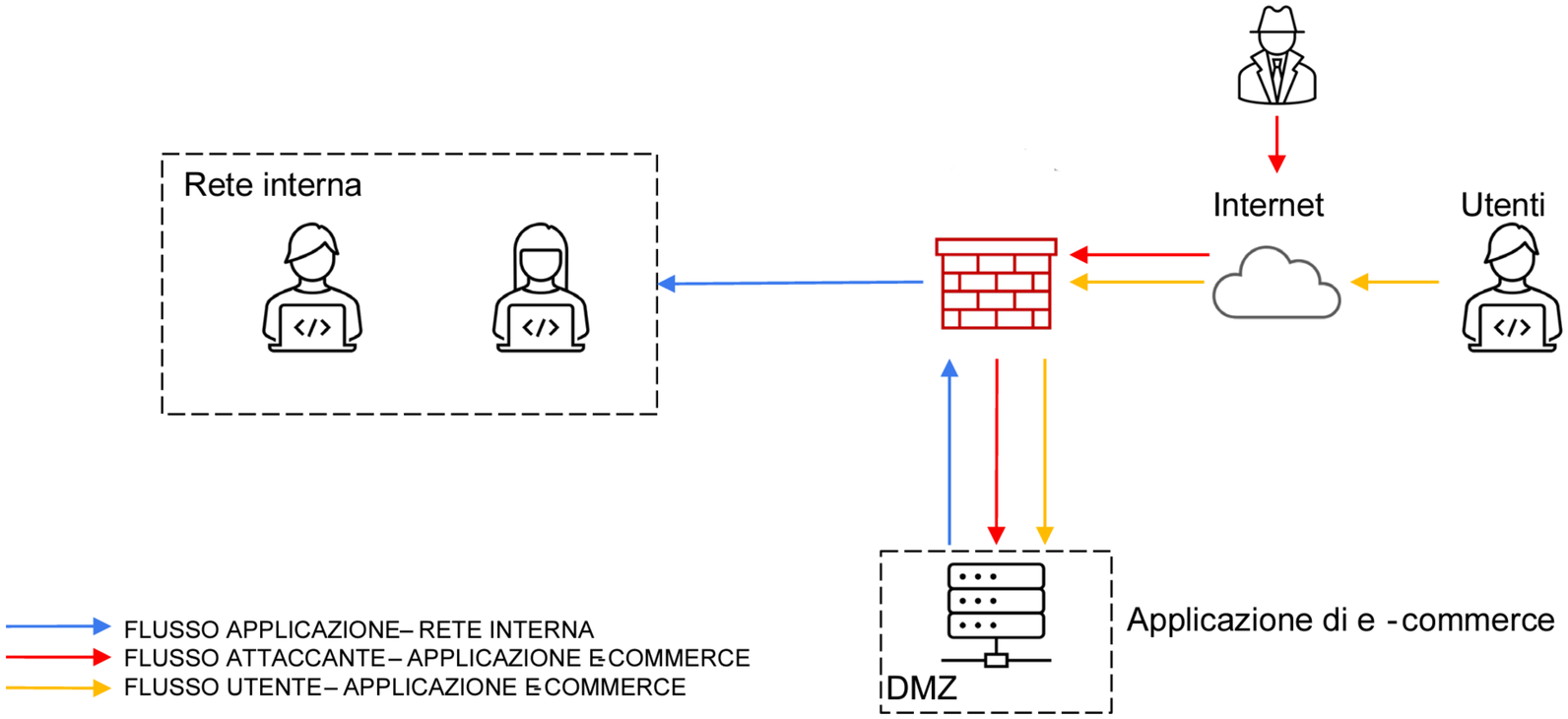
4.Soluzione completa : unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3)

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:

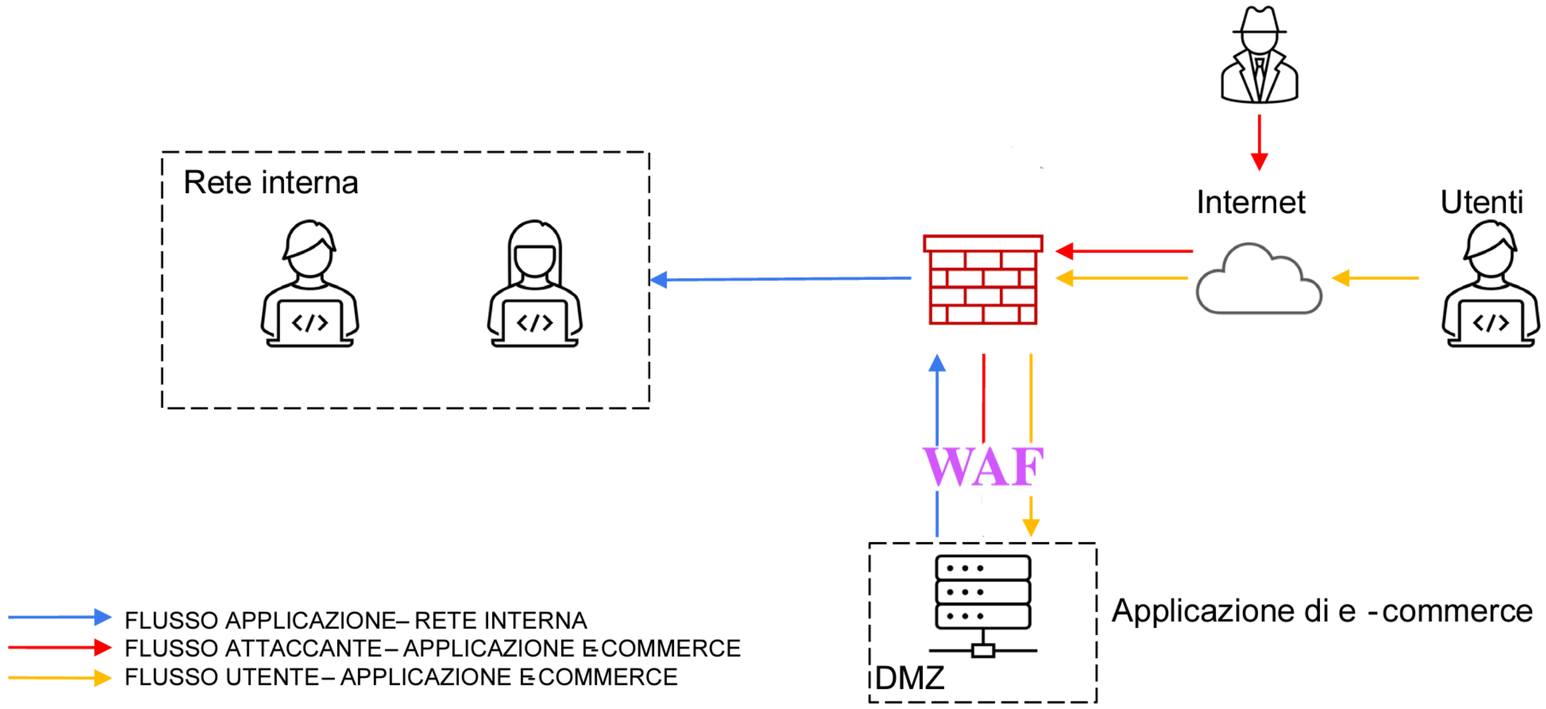
L’applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

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.



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

Per andare a prevenire un tipo potremmo andare ad implementare l'utilizzo di un WAF (web application firewall). Il waf è un sistema di sicurezza progettato per proteggere le applicazioni web da diverse forme di minacce, inclusi attacchi informatici, exploit e altre vulnerabilità che potrebbero compromettere la sicurezza di un'applicazione web.



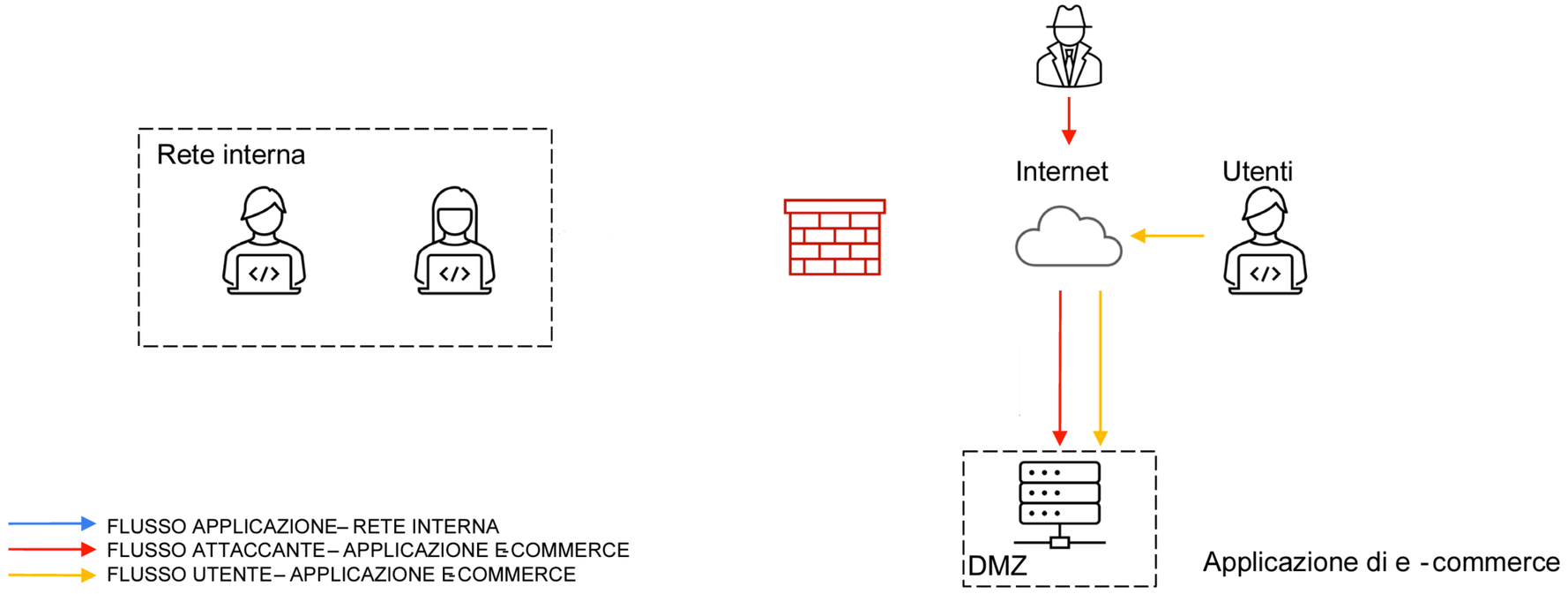
2. Impatti sul business : l'applicazione Web subisce un attacco di tipo DDoSdall'esterno che rende l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

Come prima cosa calcoliamo l'impatto che questo attacco ha avuto sul business. Moltiplichiamo la spesa media per il tempo in cui l'applicazione non è stata raggiungibile, quindi ci risulta 15000€.

Come eventuali eventuali azioni preventive potremmo consigliare di non vere solo un unico server per la web application, ma di averne magari due. In questo modo nel caso di un eventuale attacco ad uno dei server potremmo ricorrere al *"failover cluster"*, cioè quando il server attivo smette di funzionare, il secondo server prende il suo posto come server attivo.

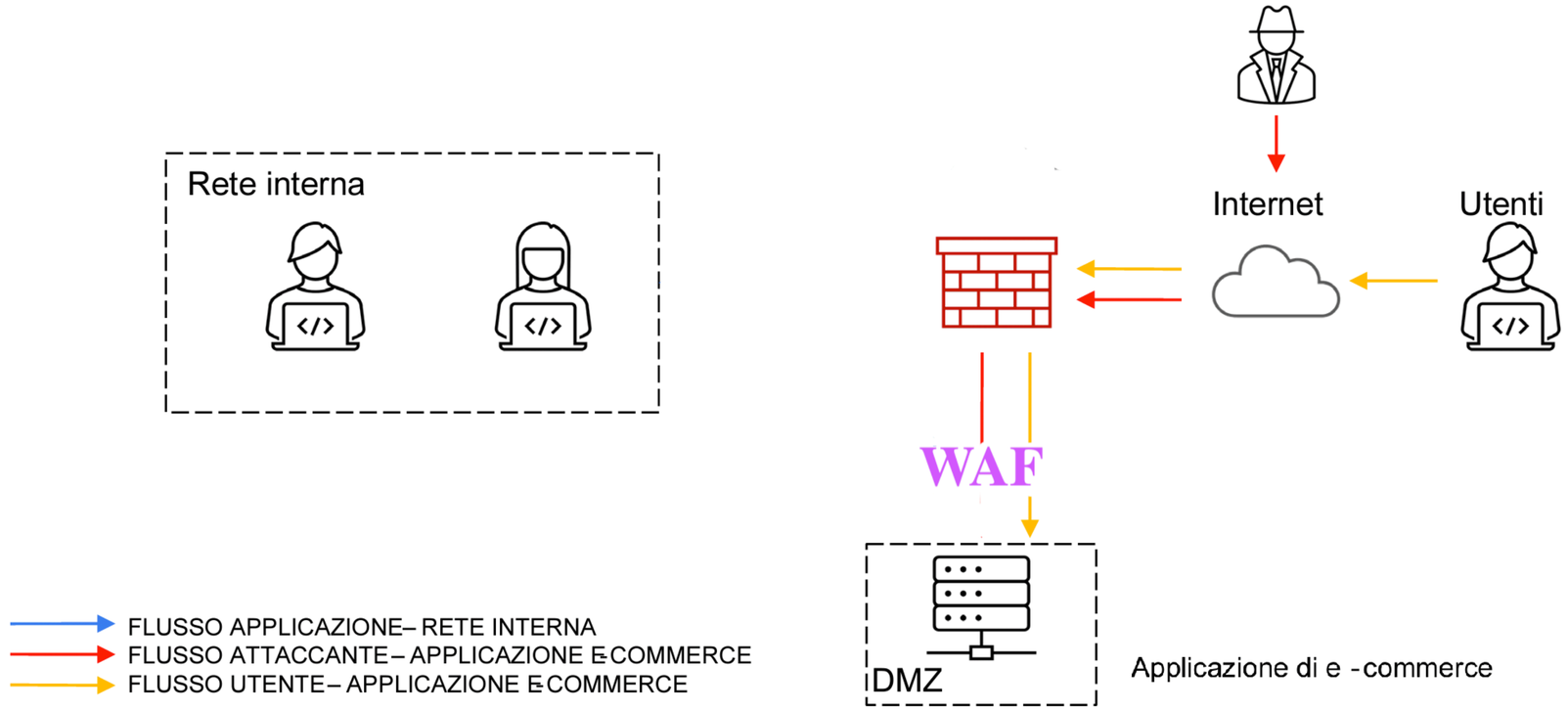
3.Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

Per risolvere quanto ci viene richiesto, ricorriamo alla tecnica dell'*isolamento* che consiste nella completa disconnessione della web application dalla rete interna, per impedirne l'accesso da parte dell'attaccante, ma senza impedirgli l'ingresso al server della web application. Cosi facendo non ci sarà più flusso applicazione-rete interna.



4.Soluzione completa : unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3)

Dall'unione delle soluzioni 1 e 3 possiamo evincere che il server della web application verrà completamente estruso dalla rete interna e a sua protezione verrà aggiunto un waf. Anche in questo caso non ci sarà flusso tra applicazione e rete interna.



5.Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

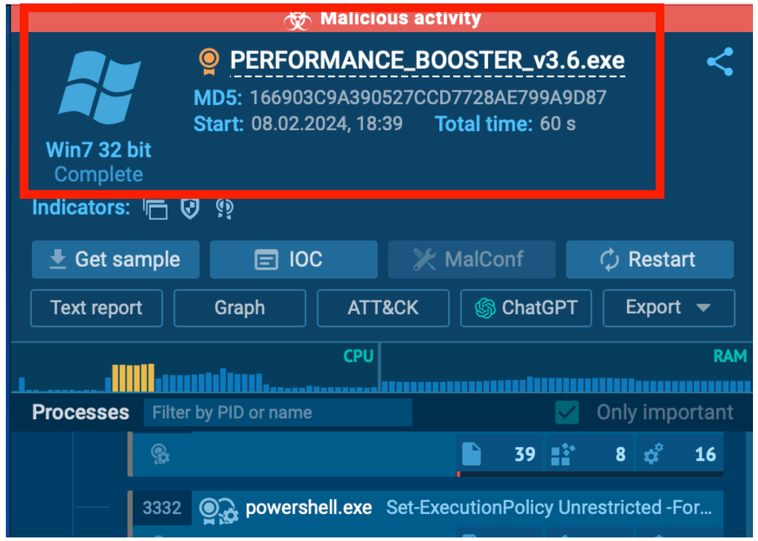
Eventuali elementi di sicurezza che potremmo andare a suggerire di implementare, singolarmente o combinati tra loro, all'interno dell'infrastruttura potrebbero essere:

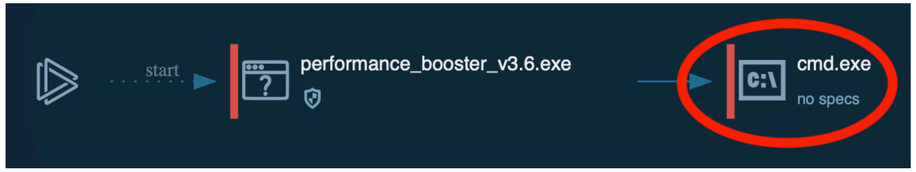
- Implementazione di un WAF a difesa della web application
- Subnetting per dividere la rete tra la dmz e la rete interna
- Implementazione di un secondo server per la web application, così che ci sia un bilanciamento del carico e in caso di attacco l'altro server possa funzionare per non mandare in down completamente il nostro e-commerce (come suggerito nella soluzione 2)
- Filtraggio DNS per bloccare l'accesso a siti o domini considerati o segnalati come dannosi
- Utilizzo sistemi IDS (che ci segnala se rileva una possibile attività dannosa) o IPS (che invece blocca direttamente l'eventuale attività malevola rilevata)

Bonus

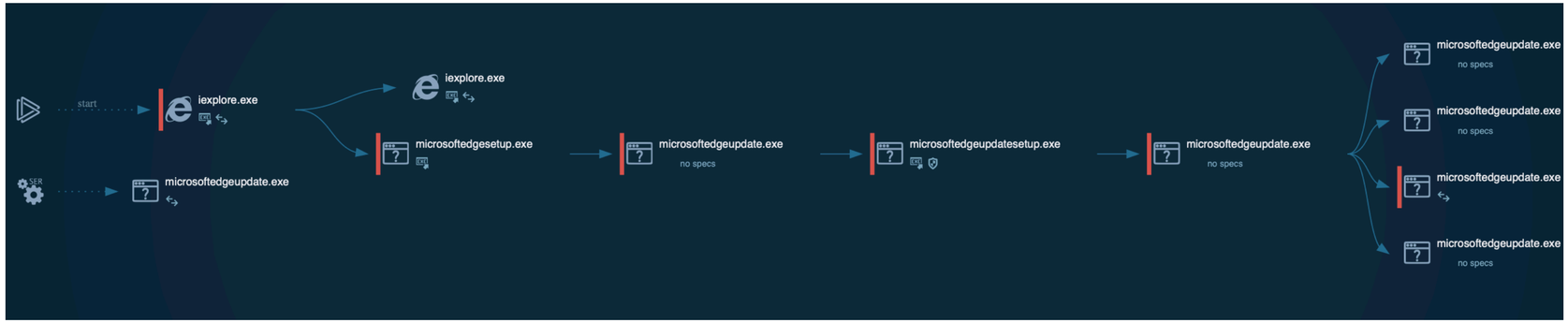
Analizzare le seguenti segnalazioni caricate su anyrune fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:
https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/
https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

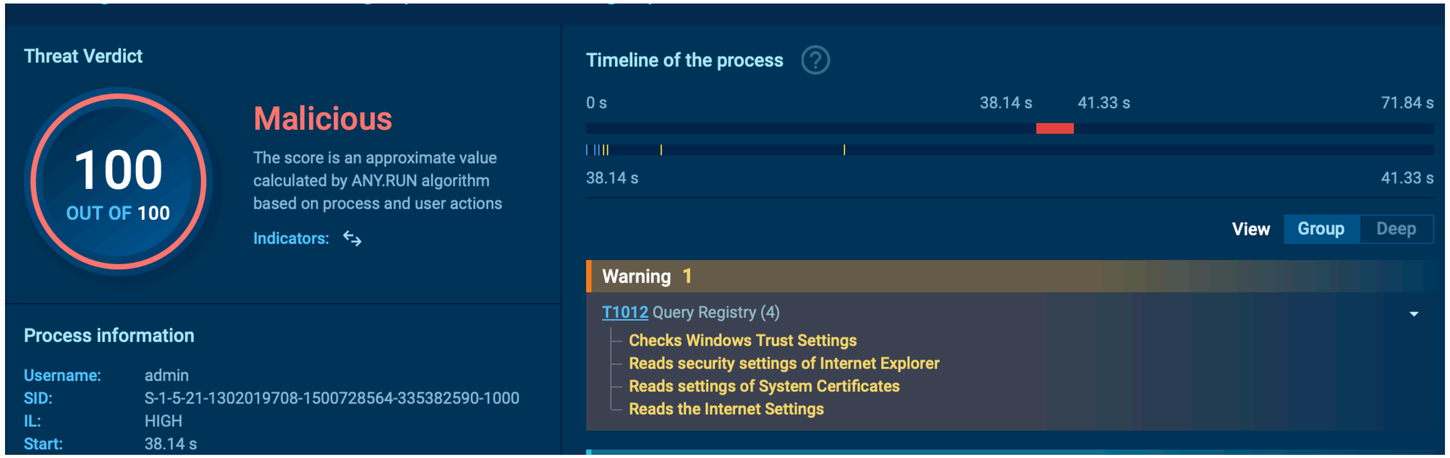
- La prima segnalazione ci riporta al report di un malware che si spaccia per un software eseguibile che incrementa le performance del sistema, ma nella realtà va a modificare le impostazioni della powershell execution policy per poter eseguire linee di comando dannose. Apre un prompt con il quale può inserire comandi e avere anche accesso remoto al nostro sistema. Per proteggersi da questo tipo di file si deve evitare di scaricare file con origine sconosciuta da internet, cancellare l'eventuale file già scaricato ed effettuare una scansione con un antivirus. Suggerirei anche di avviare una campagna informativa sul phishing ai dipendenti.





- Nel secondo caso abbiamo sempre un malware che si trova all'interno di un eseguibile che dovrebbe servire per installare microsoft edge. Nella realtà una volta dato inizio all'installazione viene eseguito un malware che va ad agire sul kernel di windows e potrebbe scalare i privilegi. Anche in questo caso per prevenire situazioni analoghe consiglieremmo di effettuare una campagna informativa sul phishing ai propri dipendenti, di cancellare il file.exe ed effettuare una scansione con un antivirus.





Fine