Traccia:

Con riferimento alla figura in slide 2, 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

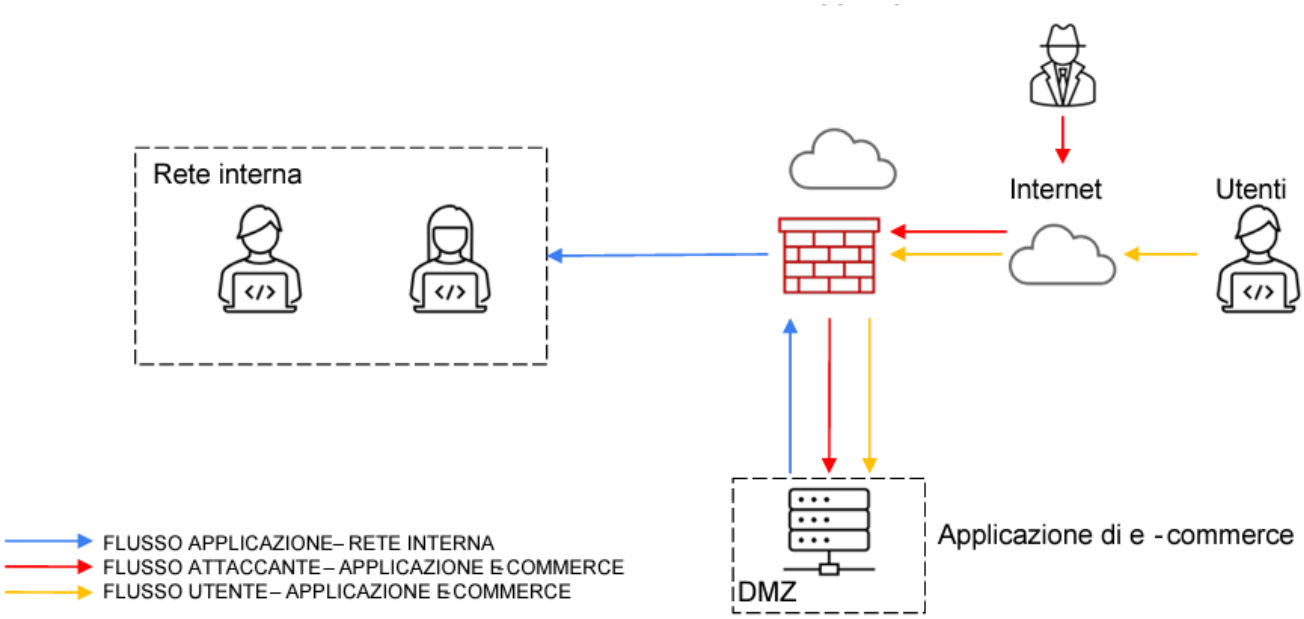
2. **Impatti sul business** : l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla 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 vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura con la soluzione proposta.

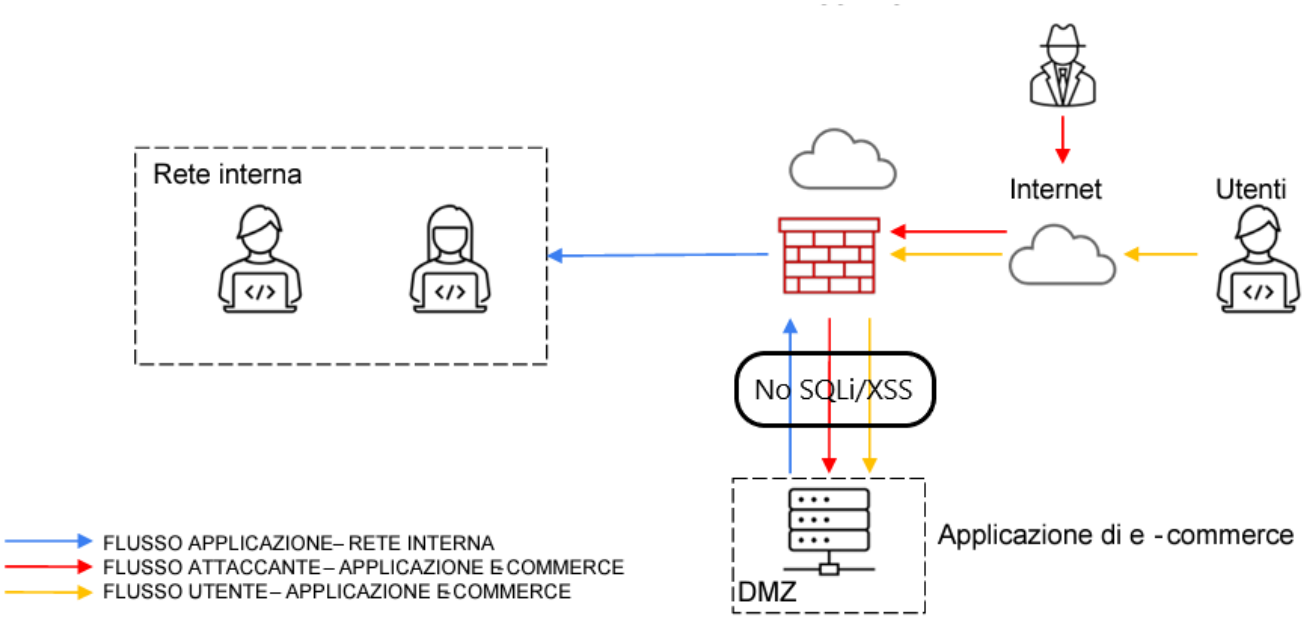
4.**Soluzione completa** : unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3)

5.**Modifica «più aggressiva» dell'infrastruttura**: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2) **Budget € 7.000**

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:



SQLi (SQL Injection) è un attacco che sfrutta la vulnerabilità del linguaggio SQL e mira alle applicazioni che gestiscono dati attraverso Database relazionali, permettendo la creazione di nuovi utenti o il download completo del database.
XSS (Cross-Site Scripting) è un attacco da remoto che inietta script dannosi nelle singole paginecon lo scopo di rubare informazioni riservate o installare malware sui browser degli utenti.

Le difese a queste tipologie di attacco potrebbero essere:

- Aggiornamenti periodici delle applicazioni con nuove patch di sicurezza;
- Scansione regolare delle applicazioni tramite l'utilizzo dei tool di Vulnerability Scanner;
- Evitare di aprire link sospetti;
- Disabilitare lo script;
- Eliminare gli applicativi utilizzati raramente.

2. Impatti sul business

Attacco DDoS ogni 10 minuti
Costo Utenti = € 1.500/minuto

SLE € 15.000/10 minuti

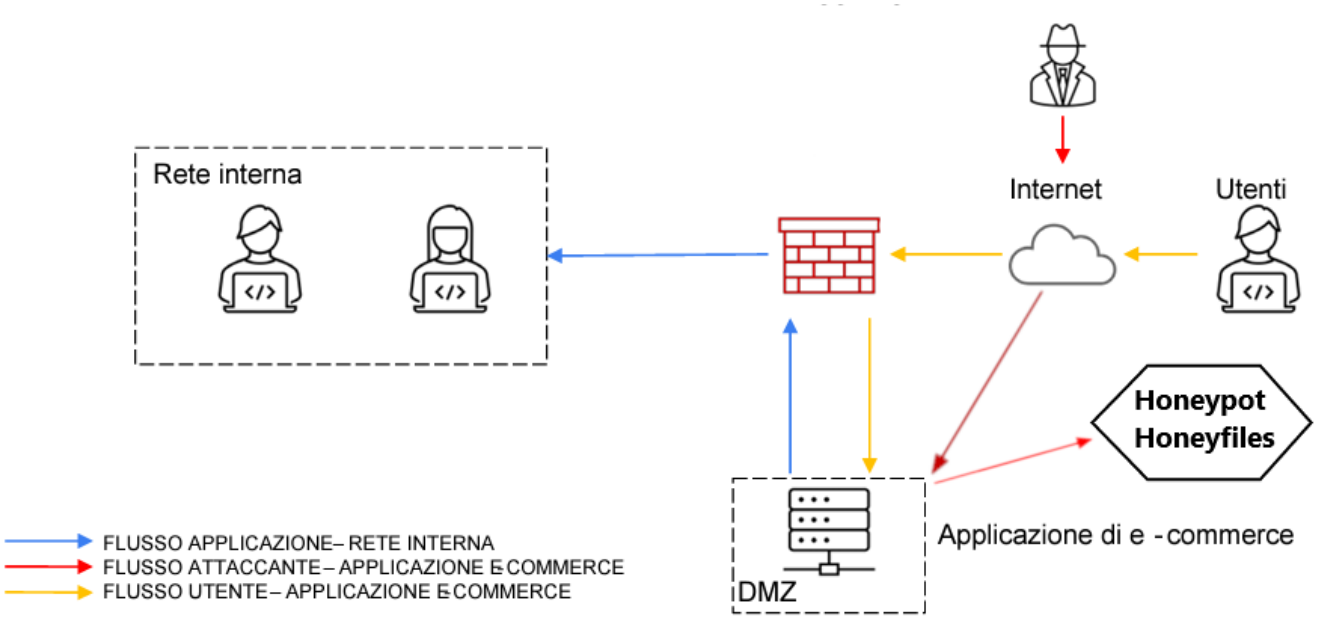
EF = 100%

SLE (Single Loss Expectancy): Misura monetaria della perdita
EF (Exposure Factor): Percentuale impatto dell'evento

DDoS (Distributed Denial of Service) è un attacco che ha lo scopo di saturare il sistema informatico inviando simultaneamente molte richieste di accesso alla stessa risorsa, permettendo di rendere inaccessibile un sito web, un server o in Data Center.
Alcune difese possono essere:

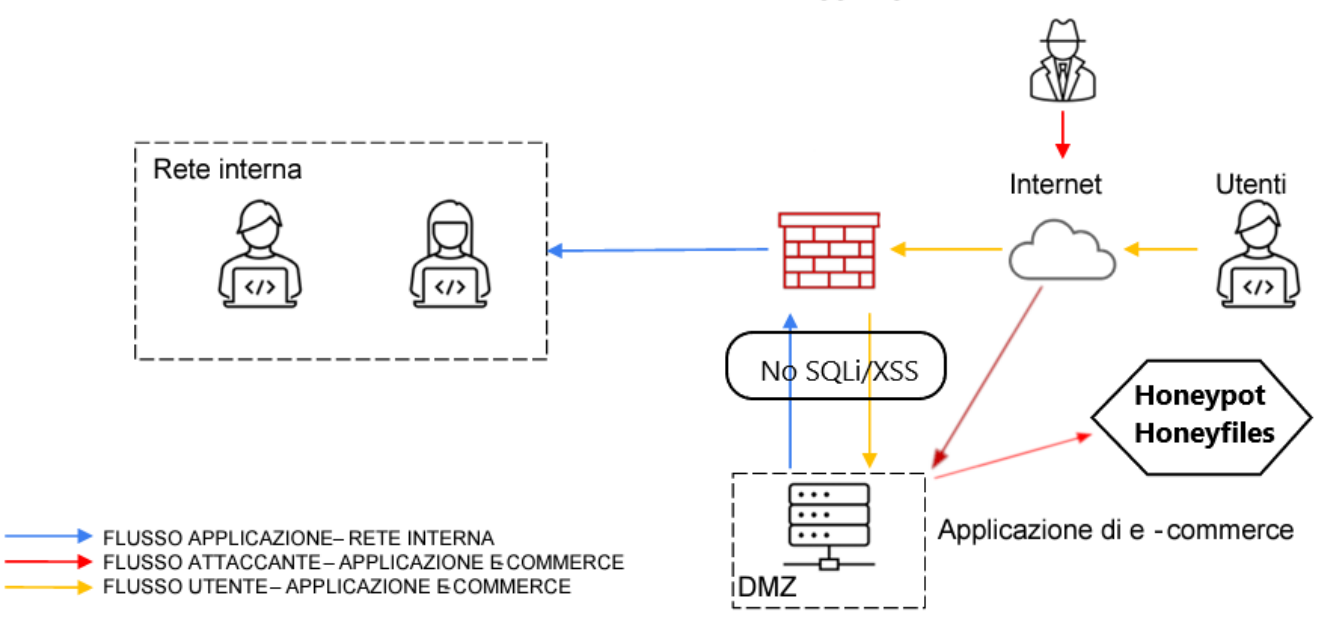
- Deviare il traffico verso un vicolo cieco;
- Applicare filtri a livello Router/Firewall;
- Creare una Blacklist di IP sospetti, bloccandoli in automatico;
- Deviare il traffico in eccesso verso altri server gemelli distanti e non sottoposti all'attacco.

3.**Response**

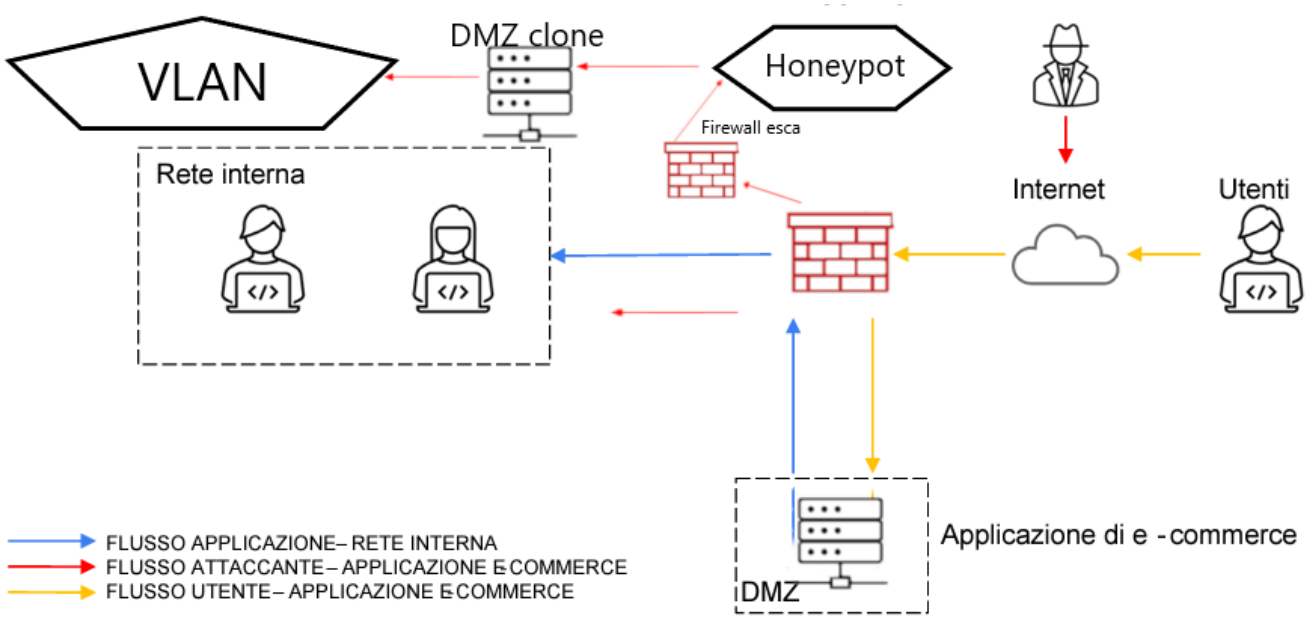


Utilizzo di un **Honeypot/Honeyfiles** per far credere all'attaccante di essere riuscito an entrare nel sistema.

Soluzione completa



5.**Modifica «più aggressiva» dell'infrastruttura**



Per evitare che un attaccante possa intrufolarsi all'interno della rete, si potrebbe:

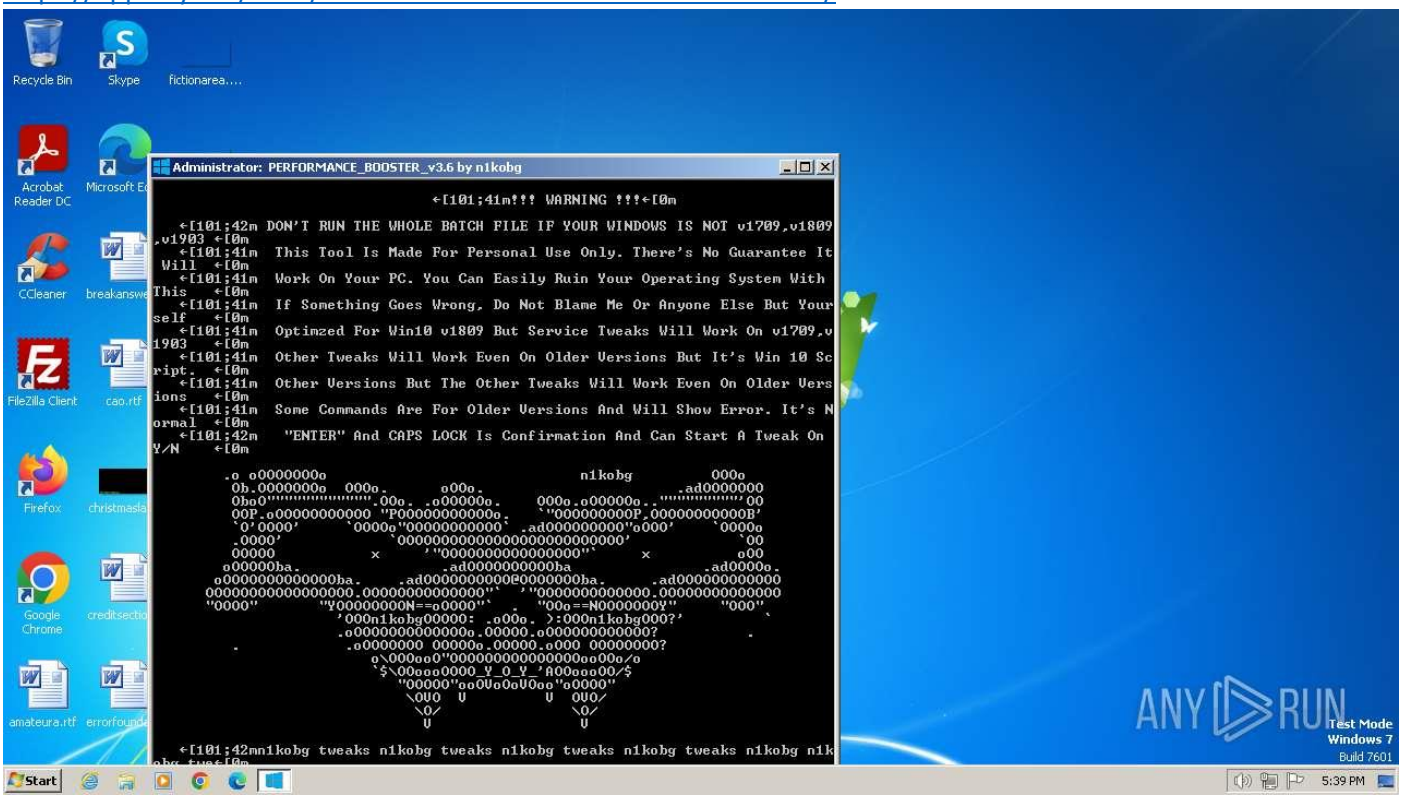
- Aggiunta di un secondo firewall esce, per fargli credere che vi sia una seconda rete;
- Creare un DMZ;
- Creare un VLAN.

Così facendo l'attaccante potrebbe indirizzarsi verso la rete virtuale, pensando che possano esserci file importanti.

BONUS:

Analizzare le seguenti segnalazioni caricate su anyrun e 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:

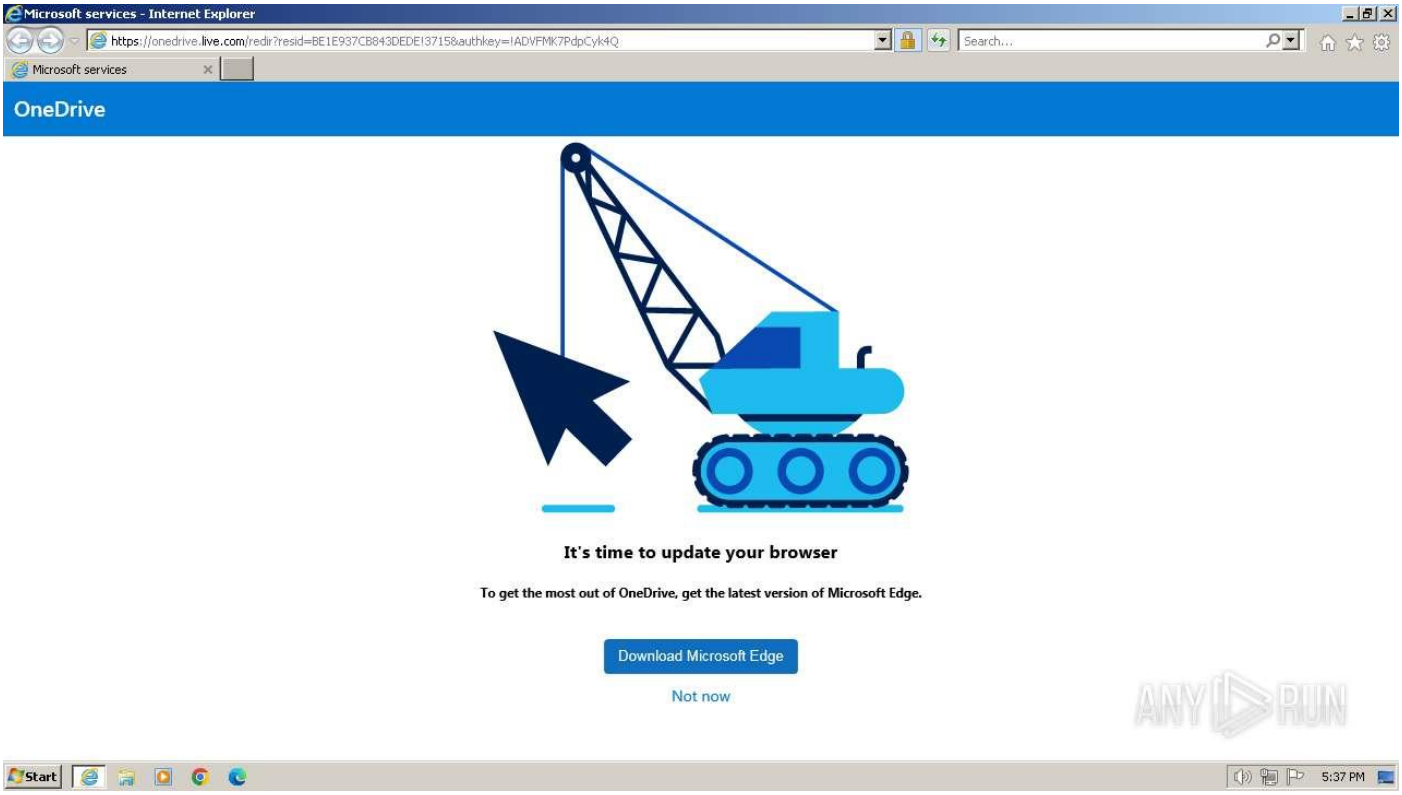
https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/



Il software PERFORMANCE_BOOSTER_v.3.6.exe è molto pericoloso.
Mandandolo in esecuzione, esegue un comando di tipo BATCH (.bat) avviando il «cmd.exe» (prompt dei comandi), cambiando le regole di esecuzione della Powershell, permettendo di:

- cambiare gli attributi del sistema;
- leggere la configurazione di rete;
- essere utilizzata come operatore locale;
- Modificare il registro di sistema per l'installazione di software non leciti;
- Controllare la path di Outlook.

https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/



Questa tipologia di accatto prevede l'aggiornamento del Browser Microsoft Edge.
Aggiornando il Browser, l'attaccante potrebbe:

- Creare/Modificare la pianificazione delle attività;
- Leggere le impostazioni di sicurezza di Interne Explorer;
- Leggere le impostazioni dei certificati di sistema;
- Avviare in qualsiasi momento l'update del Browser come se fosse un servizio lecito.

Questi sono attacchi molto comuni.
Per aggirarli, è consigliato di scaricare/aggiornare Software/App da fonti conosciute e certificate, e non da messaggi arrivati via email o banner di allerta.