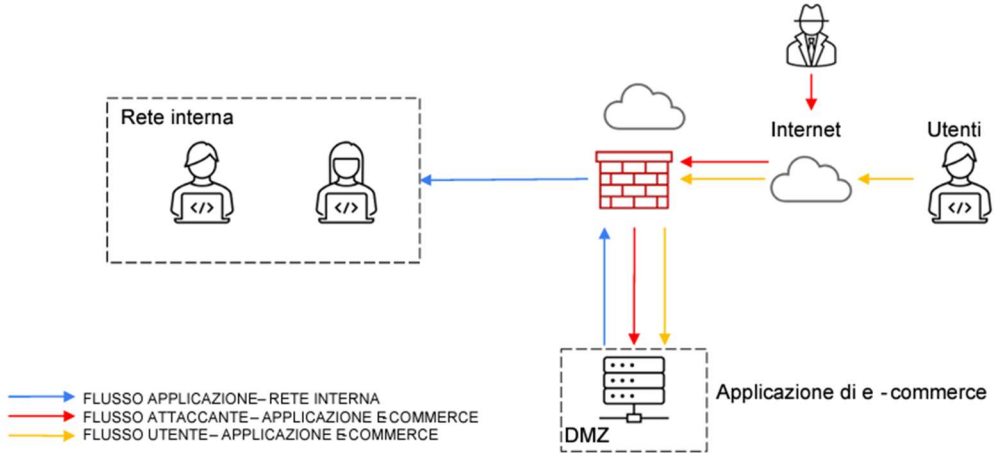
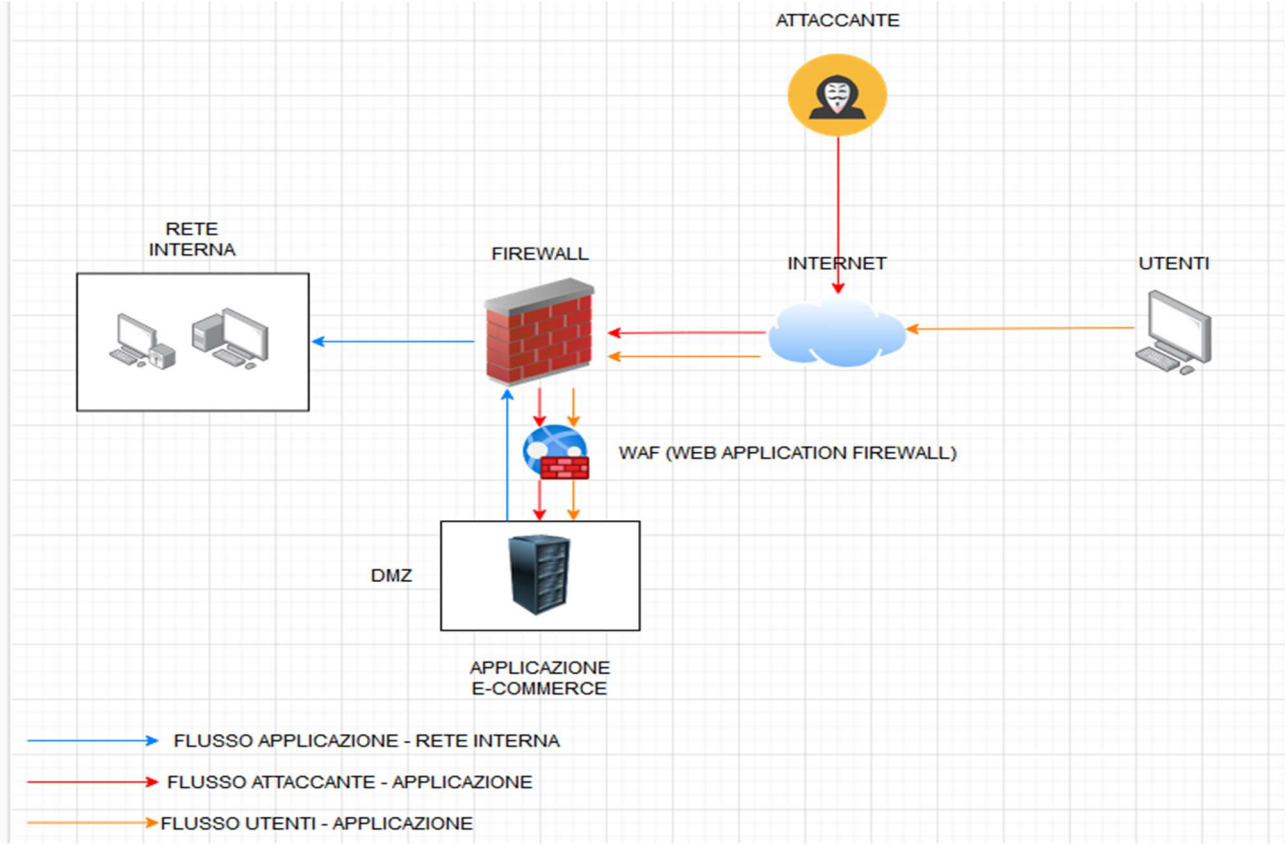
Architettura di rete:
L'applicazione di e -commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

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.



Quesito 1: Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLinjection oppure XSS da parte di un utente malintenzionato? Modificare la figura in modo da evidenziare le implementazioni.

Per proteggere la Web App da minacce quali **XSS** e **SQLinjection** si può utilizzare un **Web Application Firewall** (**WAF**, il cui scopo specifico è proteggere le Web App); esso viene posizionato a protezione del traffico in entrata sulla Web App da Internet (quindi da utenti e attaccante). Oltre all'utilizzo di un WAF si rammenta che comunque è sempre opportuno **validare e sanitizzare l'input utente** nella Web App per assicurarsi che contenga solo caratteri ammessi e non includa script malevoli che possono essere interpretati come codice eseguibile.



Quesito 2: Impatti sul business; l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione Web 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.

L'attacco di tipo **DDos** causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale ipotizzata degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10).
Di conseguenza: **Impatto sul business** = 1.500 € x 10 minuti = 15.000 €
Per 10 minuti di indisponibilità la compagnia ha perso 15.000 € di acquisti potenziali (è solo un'ipotesi, è comunque probabile che l'utente intenzionato ad effettuare l'acquisto lo faccia comunque al termine del disservizio sulla piattaforma).

Tra le **azioni preventive** che si possono attuare per la problematica in questione si indicano:

Implementazione di un Web Application Firewall (WAF):

Un WAF può rilevare e bloccare il traffico sospetto, filtrando le richieste malevole prima che raggiungano l'applicazione; se ben configurato può prevenire con successo gli attacchi DDoS, minimizzando l'interruzione del servizio e le potenziali perdite finanziarie. Tuttavia la sua implementazione potrebbe comportare costi iniziali e costi di manutenzione.

Utilizzo di un servizio anti-DDoS di un provider esterno:

Utilizzare un servizio di mitigazione DDoS offerto da un provider esterno per filtrare il traffico malevolo prima che raggiunga l'infrastruttura dell'azienda; questo servizio può rapidamente mitigare gli attacchi DDoS, mantenendo l'applicazione web accessibile agli utenti e riducendo le perdite finanziarie. Tuttavia potrebbe comportare costi ricorrenti.

Architettura scalabile e ridondante:

Implementare un'architettura di sistema scalabile e ridondante per distribuire il traffico e prevenire l'interruzione del servizio in caso di picchi di traffico anomalo; una infrastruttura ridondante può assicurare la continuità del servizio anche durante gli attacchi DDoS, ma potrebbe comportare costi elevati per l'implementazione e la manutenzione.

Monitoraggio e analisi del traffico di rete:

Monitorare costantemente il traffico di rete per identificare e mitigare rapidamente gli attacchi DDoS in corso; il monitoraggio proattivo del traffico di rete può consentire una risposta rapida agli attacchi DDoS, minimizzando l'interruzione del servizio e le perdite finanziarie.

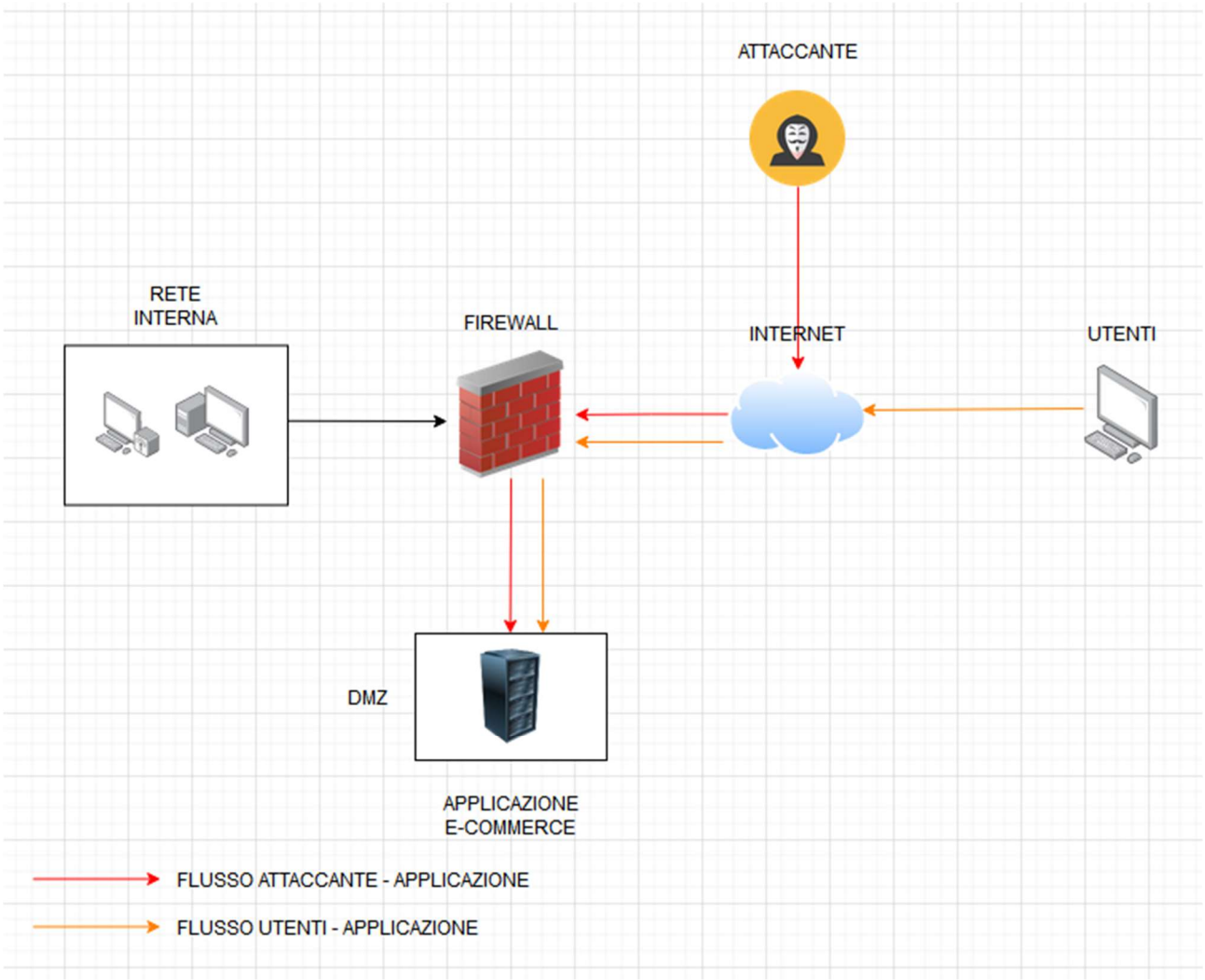
Piano di risposta agli incidenti DDoS:

Elaborare un piano di risposta agli incidenti DDoS dettagliato per definire le azioni da intraprendere in caso di attacchi; un piano di risposta agli incidenti ben strutturato può garantire una risposta rapida ed efficace agli attacchi DDoS, riducendo l'impatto sul business e la perdita di reddito.

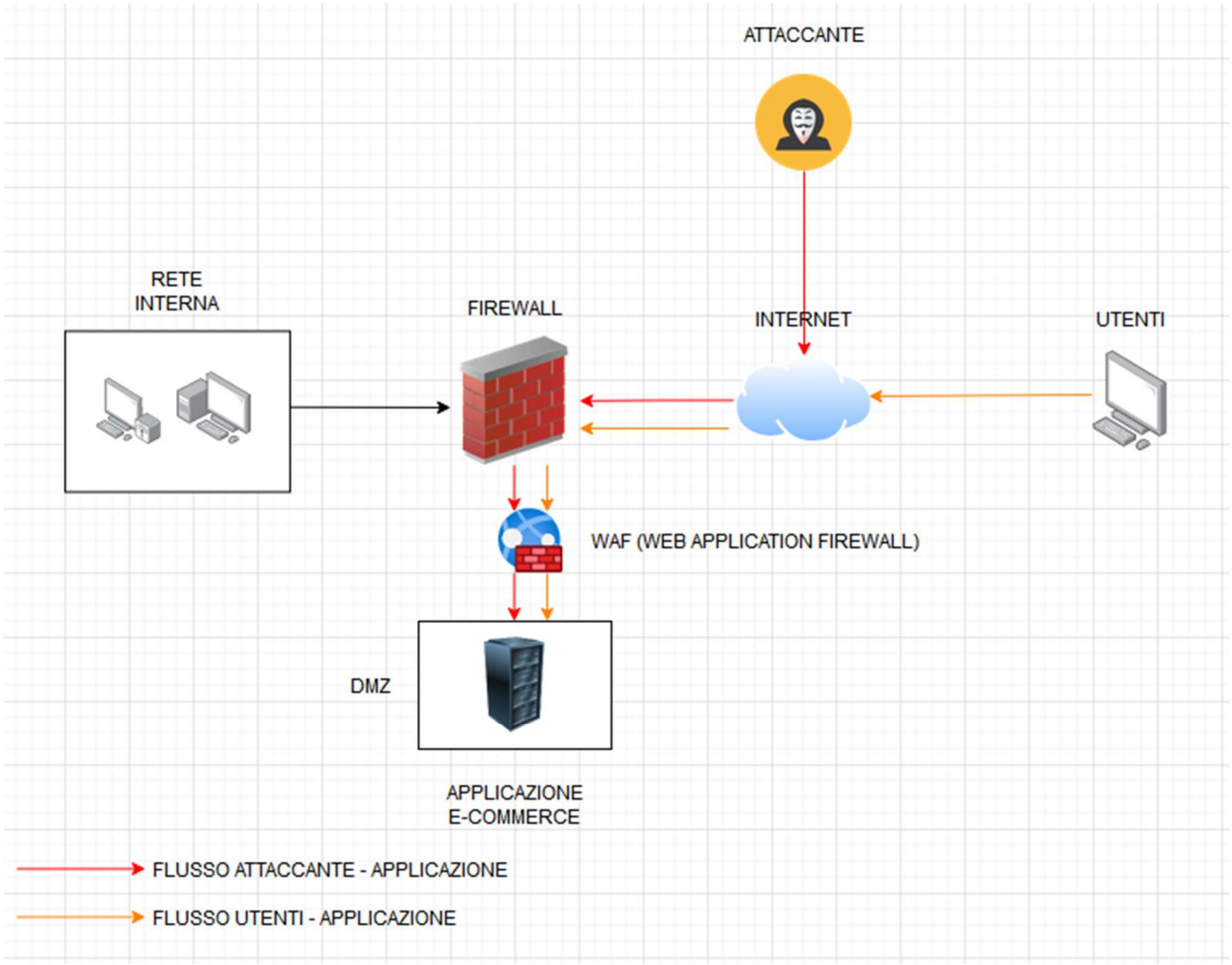
Quesito 3: Response; l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura con la soluzione proposta.

Considerata la richiesta della traccia, si può adottare una strategia basata sull'**isolamento** della macchina infettata. L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete interna , per impedire l'accesso a essa da parte dell' attaccante. Tuttavia la macchina infetta (l'applicazione Web nel nostro caso) sarà ancora direttamente collegata ad internet, raggiungibile quindi dall'attaccante ma non più connessa alla rete interna. **La rete interna può comunque continuare ad accedere ed utilizzare internet.**

Si noti comunque che se l'applicazione Web viene infettata da un malware non si può semplicemente isolarla dalla rete interna, poiché ad essa continuano ad accedere gli utenti utilizzatori dal servizio e questo può **compromettere la loro sicurezza e la loro privacy**. Nella realtà quindi l'approccio da adottare sarà diverso; si deve rimuovere il malware e ripristinare il servizio per tutelare gli utenti.



Quesito 4: Soluzione completa; unire i disegni dell'azione preventiva e della response.



Quesito 5: Modifica più aggressiva dell'infrastruttura integrando eventuali altri elementi di sicurezza.

Una modifica più aggressiva all'infrastruttura potrebbe riguardare la **rimozione** del collegamento a internet dall'applicazione Web in maniera tale che essa non sia più accessibile da parte dell'attaccante, al fine di rimuovere il malware e ripristinare i sistemi, per poi far tornare online il servizio una volta implementate delle soluzioni per impedire o mitigare la probabilità che il problema possa ripresentarsi.

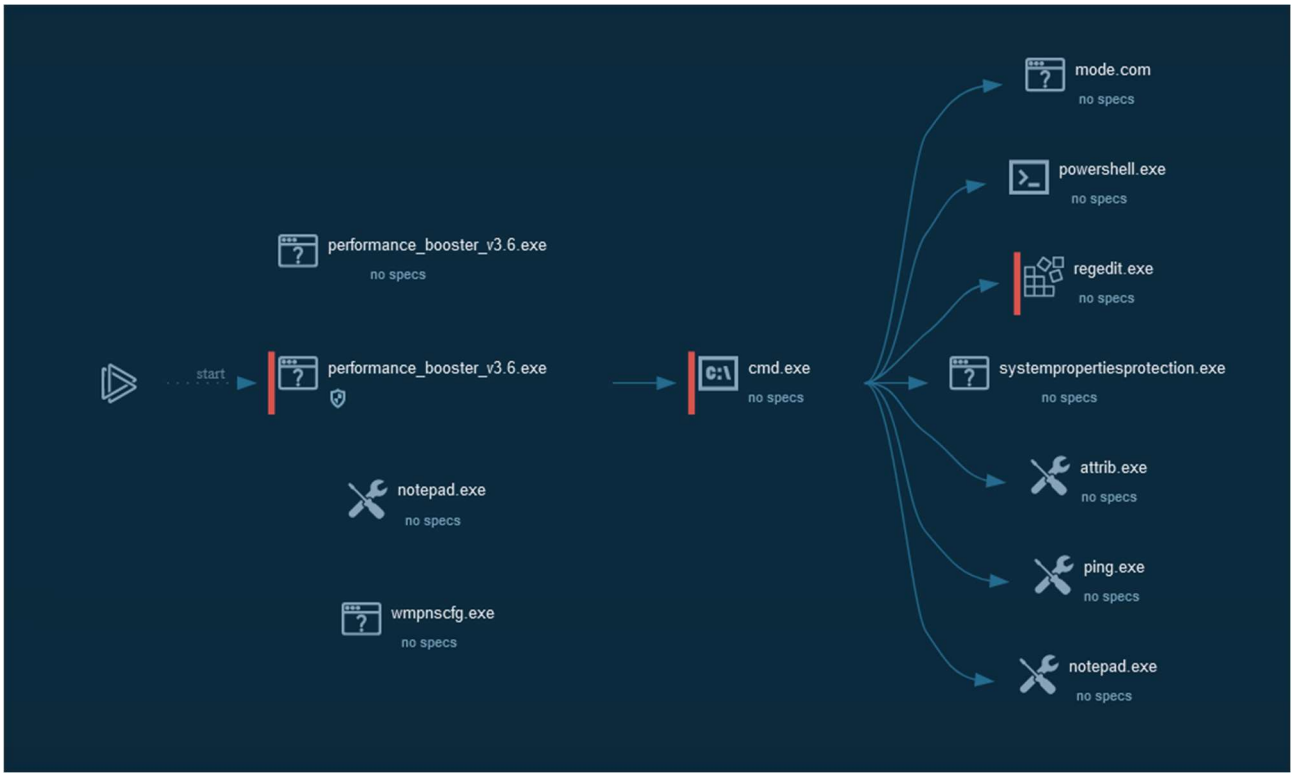
Riguardo altri elementi di sicurezza da integrare potrebbe essere aggiunto un ulteriore **firewall**, insieme a meccanismi **IPS e IDS**, per garantire una maggiore protezione della rete interna (posizionati tra la rete interna e il firewall perimetrale andando a costituire un ulteriore livello di sicurezza).
Possono inoltre essere implementate ulteriori azioni preventive come dettagliatamente descritto nella risposta al Quesito 2, insieme ad aggiuntive contromisure contro gli attaccanti (es. **honeypot**).

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/

Riguardo questa segnalazione, un utente ingenuo ha scaricato ed eseguito un file eseguibile di nome **perfomance_booster.exe**.

Una volta eseguito ha effettuato un **discovery** di file e impostazioni del dispositivo, modificato i **permessi** di file e directory, creato un account locale per garantire la **persistenza** dell'attacco ed eseguito una sessione di **powershell** (command and scripting interpreter -shell- di Windows) con **privilegi elevati**; da qui in poi il software malevolo ha il completo controllo del computer infettato.



Behavior activities

Add for printing

MALICIOUS

Changes powershell execution policy (Unrestricted)
• cmd.exe (PID: 668)

Drops the executable file immediately after the start
• PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

SUSPICIOUS

Starts CMD.EXE for commands execution
• PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Using PowerShell to operate with local accounts
• powershell.exe (PID: 3332)

Starts POWERSHELL.EXE for commands execution
• cmd.exe (PID: 668)

Executing commands from a ".bat" file
• PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Checks for the .NET to be installed
• regedit.exe (PID: 2824)

Reads the Internet Settings
• powershell.exe (PID: 3332)

Reads Microsoft Outlook installation path
• regedit.exe (PID: 2824)

Searches for installed software
• regedit.exe (PID: 2824)

Runs PING.EXE to delay simulation
• cmd.exe (PID: 668)

Reads the history of recent RDP connections
• regedit.exe (PID: 2824)

Uses ATTRIB.EXE to modify file attributes
• cmd.exe (PID: 668)

INFO

Reads the machine GUID from the registry
• regedit.exe (PID: 2824)

Reads Microsoft Office registry keys
• regedit.exe (PID: 2824)

Checks transactions between databases Windows and Oracle
• regedit.exe (PID: 2824)

Create files in a temporary directory
• PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Checks supported languages
• PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)
• mode.com (PID: 2380)

Manual execution by a user
• notepad.exe (PID: 3372)
• wmpnscfg.exe (PID: 3828)

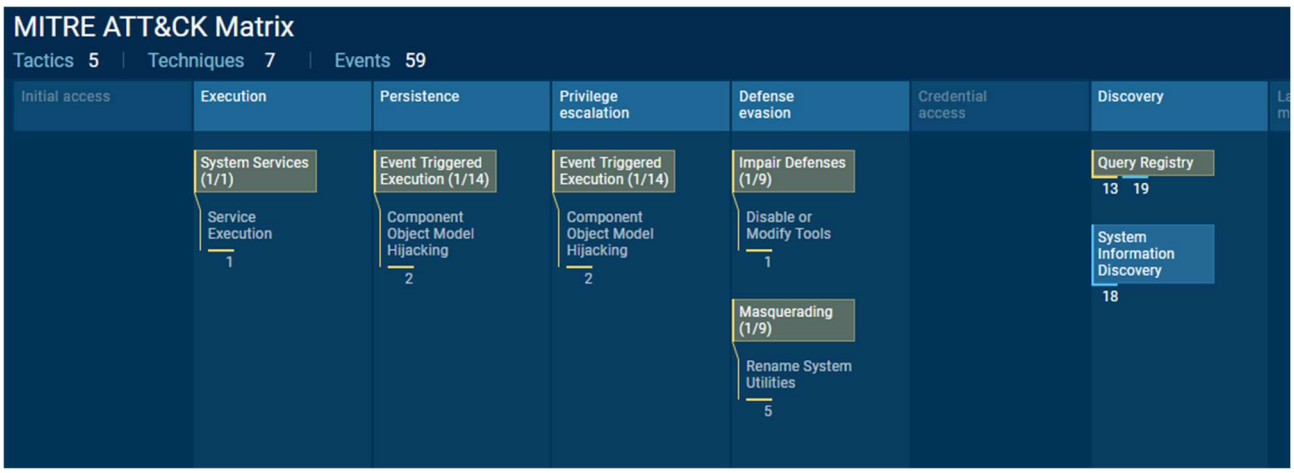
Reads Windows Product ID
• regedit.exe (PID: 2824)

Per evitare queste tipologie di attacchi in futuro non vanno assolutamente scaricati ed eseguiti file (soprattutto eseguibili con estensione .exe) da internet per i quali non si ha la **ASSOLUTA** certezza che provengano da fonti sicure ed affidabili; è importante quindi **formare** adeguatamente gli utilizzatori dei dispositivi riguardo tali tipologie di attacchi e sui comportamenti da adottare per impedirli.

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

Riguardo questa segnalazione, il software malevolo si **maschera** come legittimo (Microsoft Edge per Windows) per ingannare sia gli utenti che il sistema stesso, **disabilita** le difese del dispositivo infettato, effettua un **discovery** di file e impostazioni, viene installato in modo **persistente** e si avvia come **servizio di Windows con privilegi di amministratore**, in modo tale da avere completo controllo sul sistema infettato.

Per proteggersi da questo tipo di attacchi è fondamentale avere un buon **software di protezione** installato sul dispositivo ed **aggiornare** il sistema operativo ed i programmi alle versioni più recenti; evitare di installare ed eseguire software di dubbia sicurezza ed attendibilità dal web.



Behavior activities

Add for printing

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)