PROGETTO
S9-L5

Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

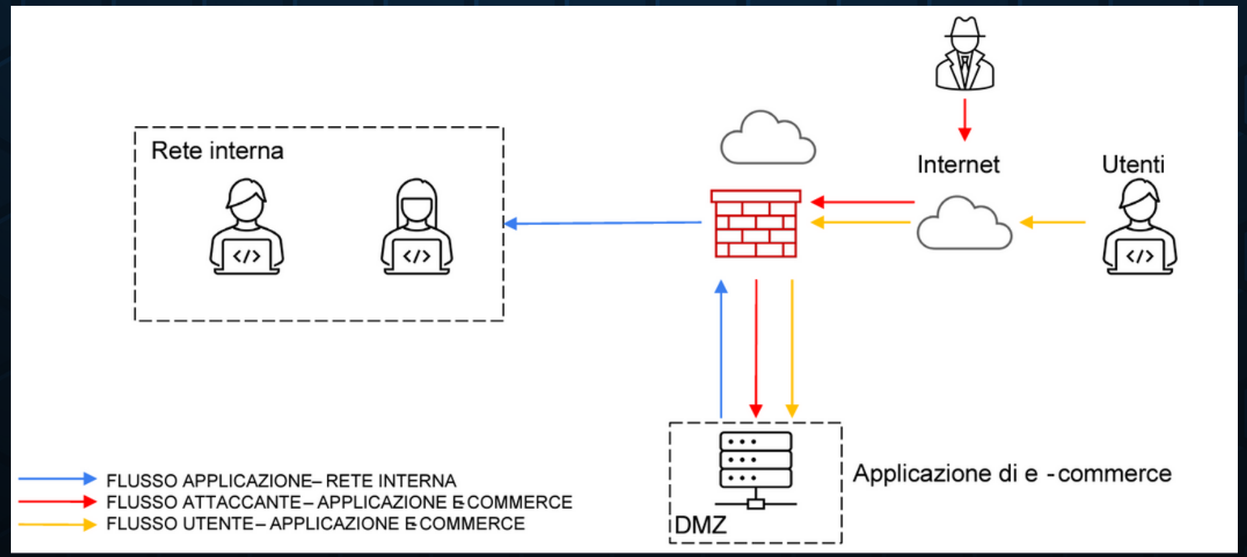
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLioppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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 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.

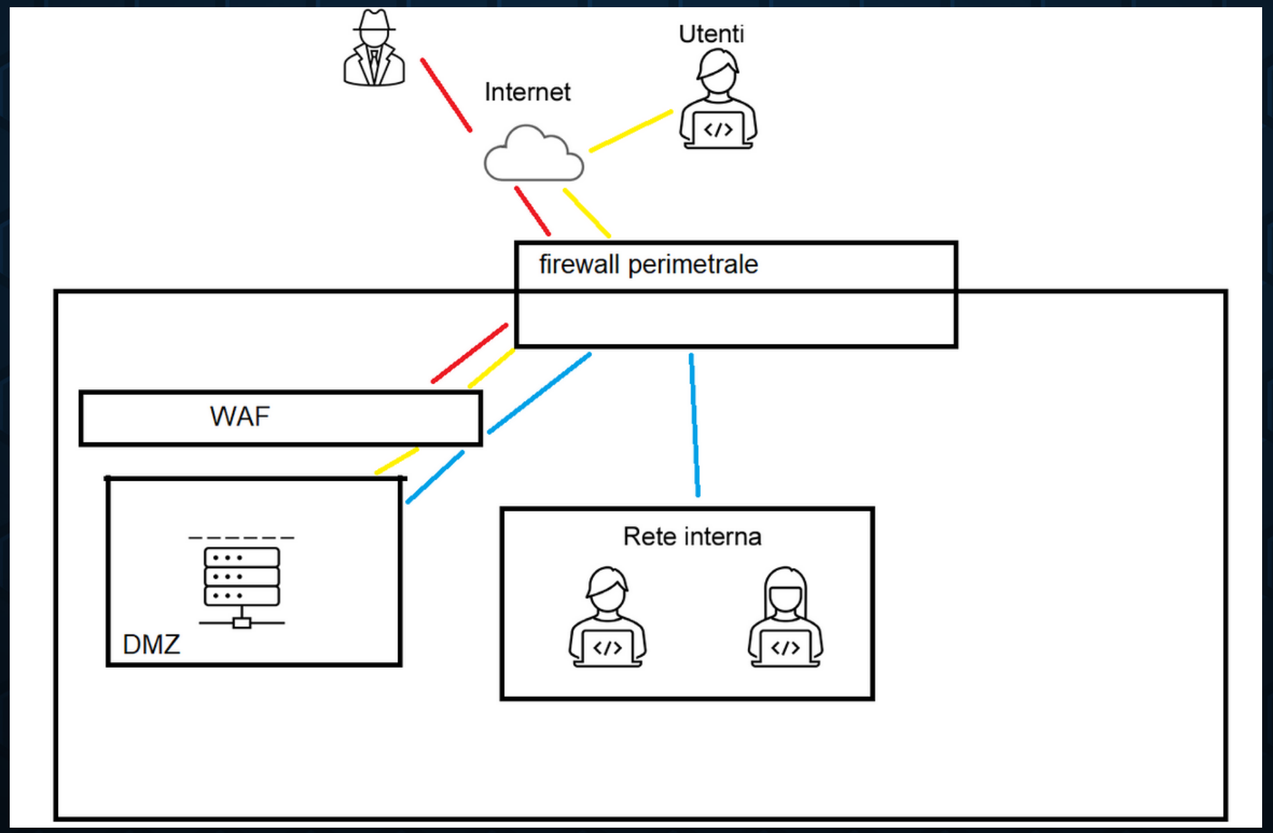
4.Soluzione completa: unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3)

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



TRACCIA 1:

Per evitare degli attacchi come “XSS” o “SQLi” la cosa migliore che possiamo andare a fare è implementare un “WAF”, Web Application Firewall. Ovvero un firewall progettato proprio per proteggere le applicazioni web, in quanto dotato di un database che gli permette di confrontare i dati nei pacchetti e riconoscere così pacchetti malevoli, così facendo il waf andrà a filtrare gli input utenti non permettendo ai vari script di essere eseguiti.



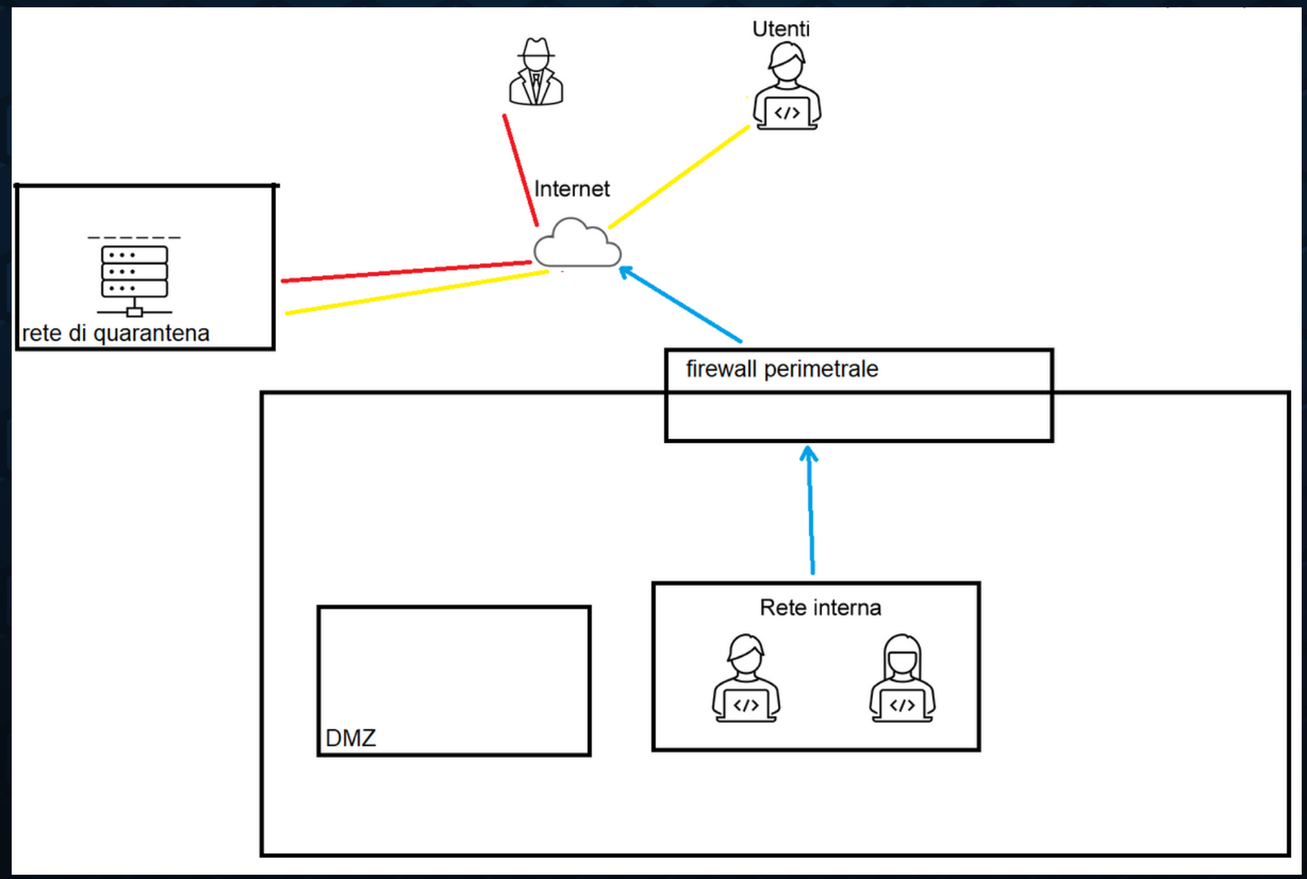
TRACCIA 2:

Nel contesto aziendale, è consigliabile anticipare e identificare le potenziali minacce che potrebbero compromettere le continuità operative dell'azienda.
Un modo per farlo è mediante la creazione di un piano specifico denominato "Business Continuity Plan".
Per elaborare un BCP efficace, è fondamentale condurre un'analisi dettagliata sugli impatti economici e finanziari associati a eventi dannosi, conosciuta come "Business Impact Analysis".
Attraverso l'impiego di strumenti di calcolo e previsione, è possibile stimare in modo approssimativo i possibili danni economici e finanziari che potrebbero derivare da tali incidenti.

BCP

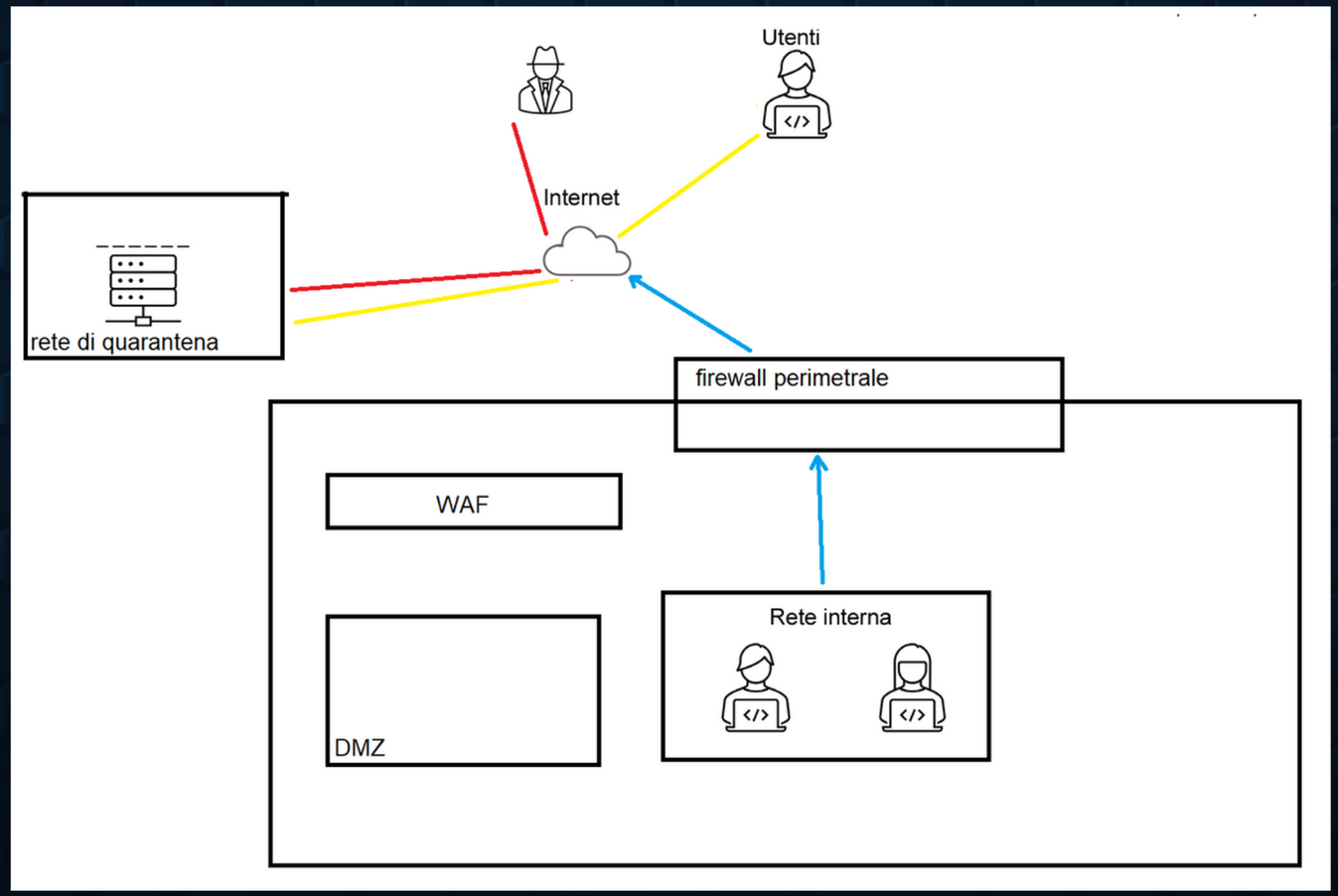
TRACCIA 3:

Nella situazione in cui ci troviamo la nostra priorità è evitare che il malware infetti altri dispositivi, la cosa migliore da fare per evitare di rimuovere direttamente il dispositivo infetto è quella di andare ad applicare la tecnica dell' "isolamento", mettendolo in una rete esterna a quella aziendale, mantenendo così la connessione a internet.



TRACCIA 4:

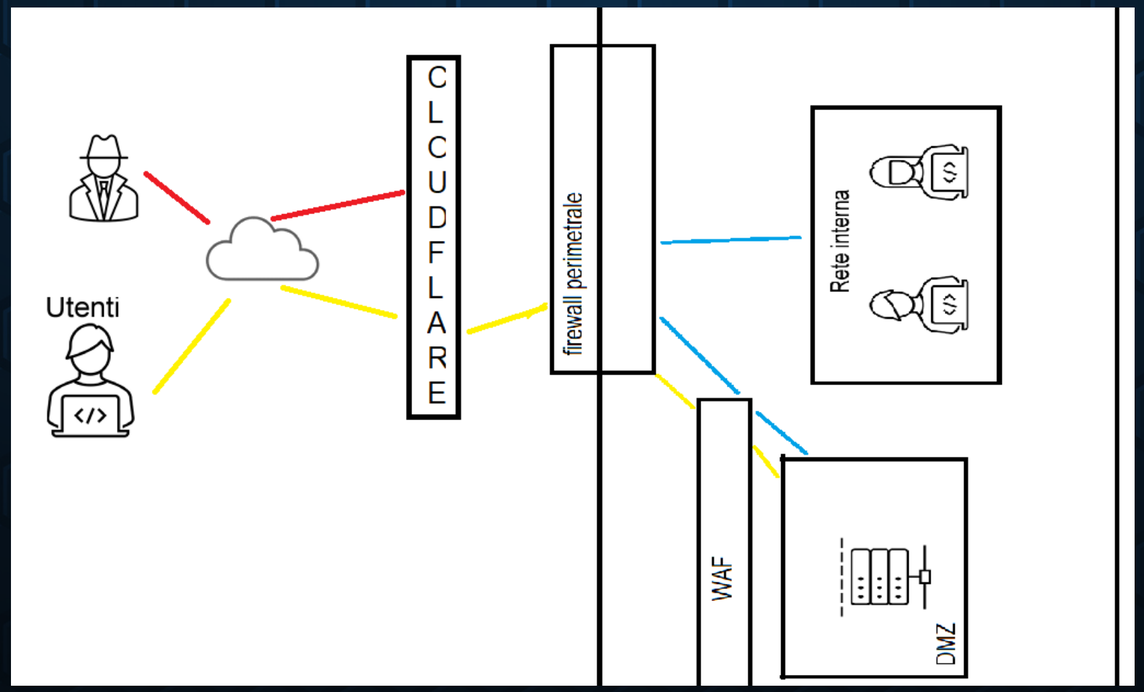
Nella situazione in cui ci troviamo siamo andati a isolare un server web infetto per evitare che si diffondesse anche agli altri dispositivi della rete, andando a preparare un WAF per limitare le possibilità che si riverifichi questa situazione, andando a proteggere correttamente il web server saranno molto inferiori le necessità di ricorrere a tecniche come l'isolamento o rimozione.



TRACCIA 5:

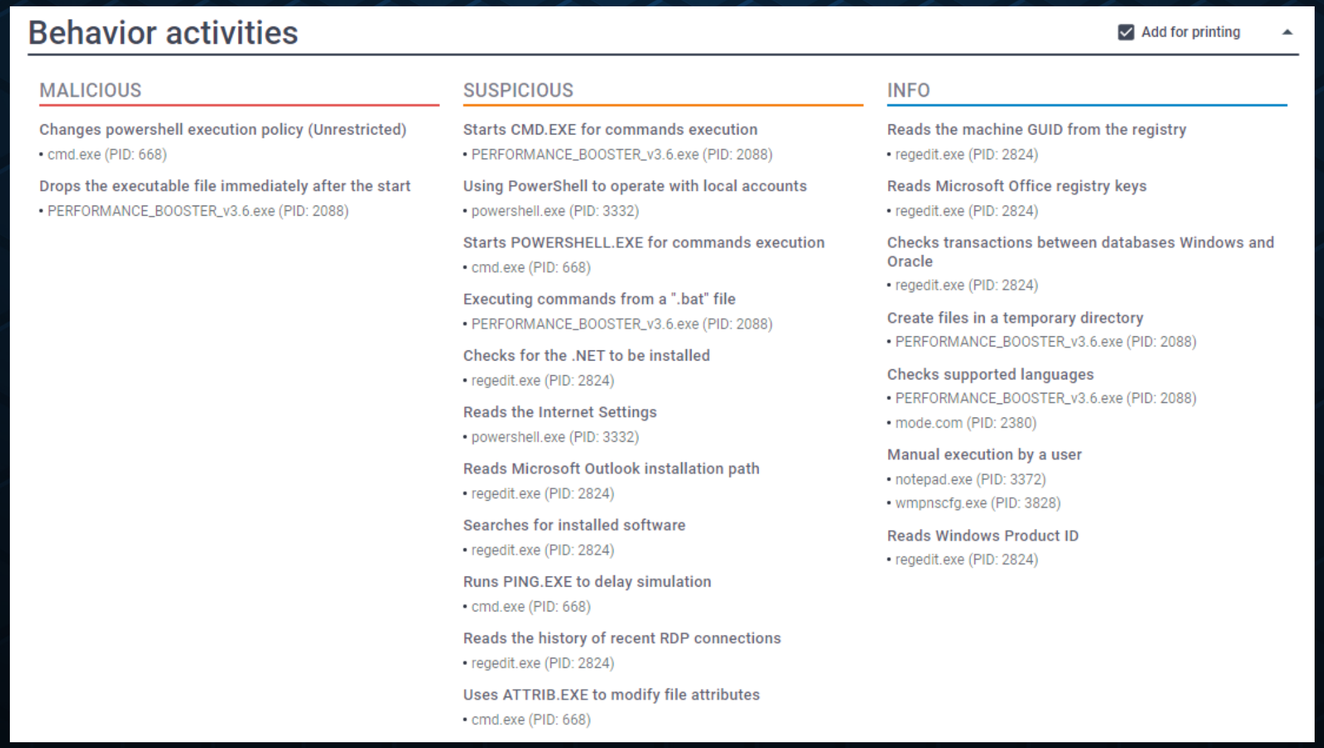
Per andare a migliorare l’infrastruttura data possiamo andare a integrare vari dispositivi di sicurezza:

- per risolvere il problema presentato alla traccia 2, ovvero attacco di dos/ddos, potremmo appoggiarci a servizi di terze parti, come CloudFlare, che offrono servizi di proxy.
- aggiungere un IPS e/o un IDS, dispositivi di sicurezza (sia software che hardware) che agiscono a livello 3/4 del modello OSI, per monitorare il traffico di rete e rilevare eventualmente comportamenti sospetti, l’IPS si occuperà di bloccare direttamente la minaccia mentre l’IDS ci notificherà solo le anomalie.
- per una maggiore sicurezza della rete interna potrei andare a subnettare la rete o impostare delle vlan tramite i switch, la segmentazione della rete non permette ai worm di riprodursi e rallenterebbe un attaccante in quanto dovrà passare da una rete all’altra.



TRACCIA (BONUS 1):

Nella traccia ci viene richiesto di analizzare una segnalazione e fare un report. Per prima cosa una volta ritrovati davanti la segnalazione possiamo andare a controllare il text report per vedere alcune informazioni utili. Tra le prime cose che si possono notare, in questo report sono stati segnati alcuni comportamenti che questo programma ha nel momento in cui viene eseguito, tra i quali i più gravi risultano la modifica delle impostazioni PowerShell, il che gli permette di eseguire comandi dannosi, la possibilità di nascondere la sua presenza e la possibilità di accedere a informazioni sensibili dal registro di sistema. Per questo motivo il consiglio migliore è quello di scaricare software solo da siti web attendibili, senza passare per canali non certificati.



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)

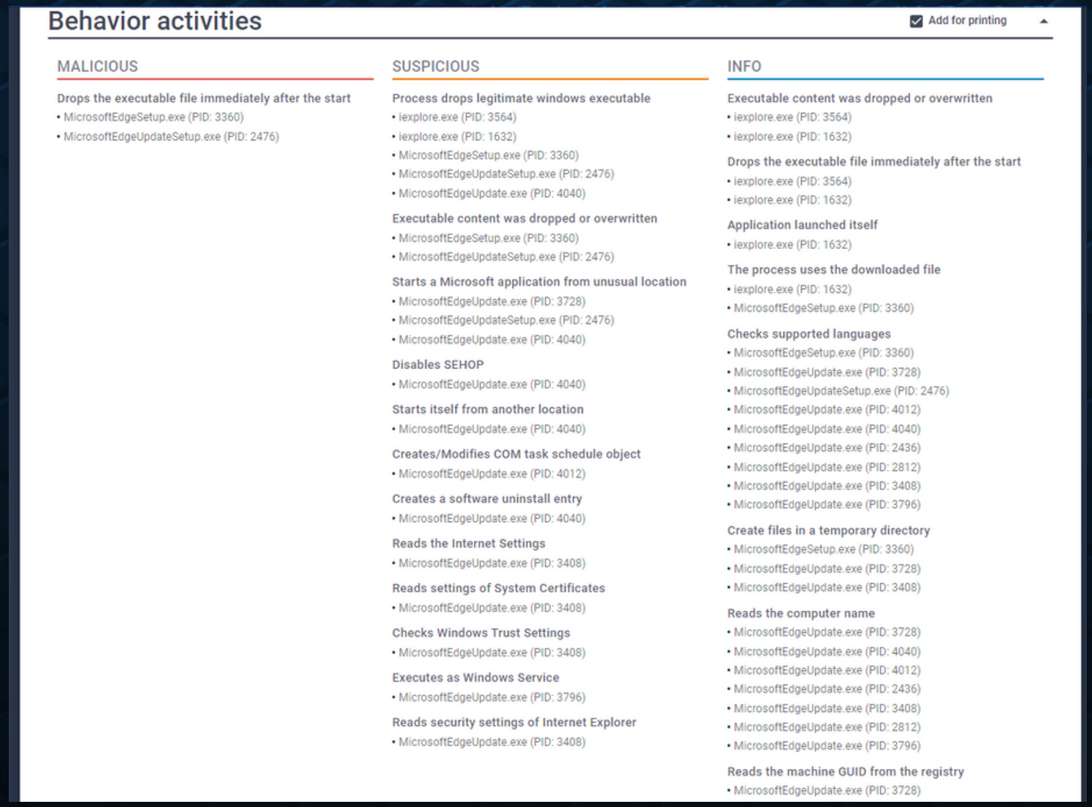
Manual execution by a user
- notepad.exe (PID: 3372)
- wmpnscfg.exe (PID: 3828)

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

TRACCIA (BONUS 2):

Andando ad analizzare anche questo report possiamo scoprire vari comportamenti che questo malware ha quando in esecuzione, tra cui i più pericolosi sicuramente risultano essere:

- il fatto che si camuffi come aggiornamento di microsoft edge.
- il fatto che non necessiti input utente
- il malware ha accesso diretto alle impostazioni di sicurezza di microsoft edge
- il software ha la capacità di avviarsi da solo all'accensione del pc vittima, andando a nascondersi e risultando più difficile la sua individuazione



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)

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