EPICODE

S9_L5

Progetto settimana 9

22 marzo 2024

Gruppo 3

Team leader - Manuel Di Gangi
Team:

- Davide Di Turo
- Francesco Perticaroli
- Jacopo Trovato
- Marco Fasani

We're back

INDICE

Riferimenti e versioni.....**3**
Traccia.....**4**
Fondamenti concettuali.....**5**
1. Azioni Preventive contro SQLi & XSS.....**7**
1.1 Fondamenti concettuali.....7
1.2 Illustrazione delle azioni preventive.....7
1.3 Implementazione WAF di rete.....9
2. Impatti sul business.....**10**
2.1 Azioni preventive.....10
3. Incident response.....**12**
3.1 Segmentazione.....12
3.2 Isolamento.....12
3.3 Azioni preventive.....13
4. Soluzione completa.....**16**
5. Modifica dell'infrastruttura.....**17**
5.1 Principali componenti della rete.....17
5.2 Funzionamento della rete.....18
6. Analisi delle segnalazioni di Anyrun.....**20**
6.1 Fondamenti concettuali.....20
6.2 L'.exe PERFORMANCE_BOOSTER.....26

Progetto settimana 9

Riferimenti e versioni

GdL **Team:**

Responsabile/referente del documento (di seguito Responsabili): Team

TL: Manuel Di Gangi

Risorse a supporto revisione (di seguito Risorse): Team

Versionamento

Versione	**Descrizione**	**Ruolo**	**Data**
1.0	Redazione - Capitolo 1	Di Turo	22/03/2024
1.0	Redazione - Capitolo 2	Trovato	
1.0	Redazione - Capitolo 3	Perticaroli	
1.0	Redazione - Capitolo 4	Di Gangi	
1.0	Redazione - Capitolo 5	Dituro - Di Gangi	
1.0	Redazione - Capitolo 6 a	Fasani	
1.0	Redazione - Capitolo 6 b	Fasani	
1.1	Formattazione documento	Di Gangi	
1.2	Revisione	Team 1	

Traccia

Con riferimento alla figura seguente, rispondere ai seguenti quesiti.

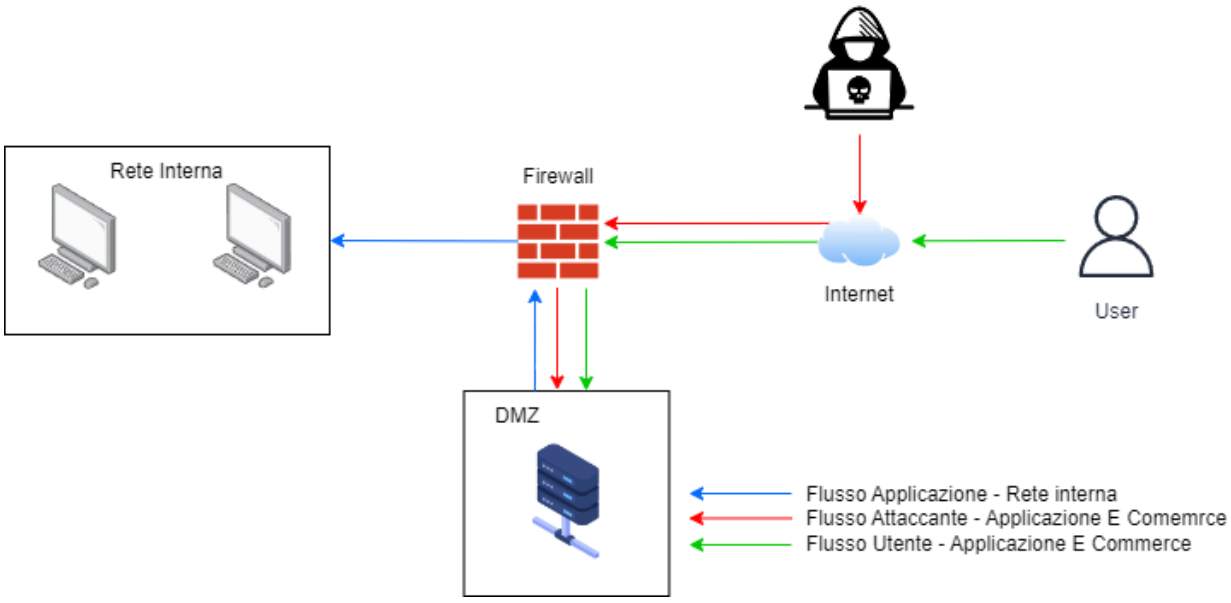
1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
2. Impatti sul business : l'applicazione Web subisce un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

5

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/



Fondamenti concettuali

La compromissione di un sistema informatico si verifica quando un'entità esterna o interna riesce ad accedere, manipolare o danneggiare il sistema senza autorizzazione. Questo può avvenire attraverso varie forme di attacchi informatici come hacking, malware, phishing, o exploit di vulnerabilità software. Una compromissione può portare alla perdita di dati, alla violazione della privacy, al furto di informazioni sensibili o al danneggiamento del sistema stesso.

La business continuity, o continuità operativa, è la capacità di un'organizzazione di mantenere o ripristinare rapidamente le sue operazioni critiche in seguito a eventi imprevisti o disastri, garantendo la sua resilienza e continuità nel lungo termine.

1. Azioni Preventive contro SQLi & XSS

1.1 Fondamenti concettuali

I servizi di operazioni di sicurezza sono attivati al manifestarsi di un evento noto come "incidente di sicurezza", il quale comporta un impatto negativo sulla sicurezza, mettendo a rischio la disponibilità e l'integrità delle risorse. Questi incidenti possono essere innescati da una violazione effettiva o potenziale, come una minaccia imminente o un attacco diretto ai sistemi informativi.

Ad esempio, possono verificarsi perdite di dati sensibili, intrusioni nei sistemi interni perpetrati da malintenzionati e l'introduzione di malware. È fondamentale che i servizi di sicurezza operativa siano prontamente attivati per mitigare gli effetti nocivi di tali situazioni e proteggere l'ambiente digitale dall'ulteriore compromissione.

Azioni preventive: sono messe in atto prima che si verifichi un incidente al fine di limitare i rischi di eventi indesiderati.

Le azioni correttive, invece, intervengono dopo l'incidente, con l'obiettivo di rispondere e risolvere i danni causati, garantendo il funzionamento stabile dei sistemi informativi.

1.2 Illustrazione delle azioni preventive

- **Implementazione WAF**: Una strategia comune per prevenire gli attacchi di tipo XSS, SQLi e altri attacchi alle applicazioni web consiste nell'implementare un WAF (Web Application Firewall) configurato adeguatamente. Questo dispositivo monitora il traffico di rete e limita le richieste inviate alle applicazioni, consentendo l'accesso solo agli utenti privilegiati. Nel caso di un attacco di tipo cross-site scripting, per esempio, il WAF è in

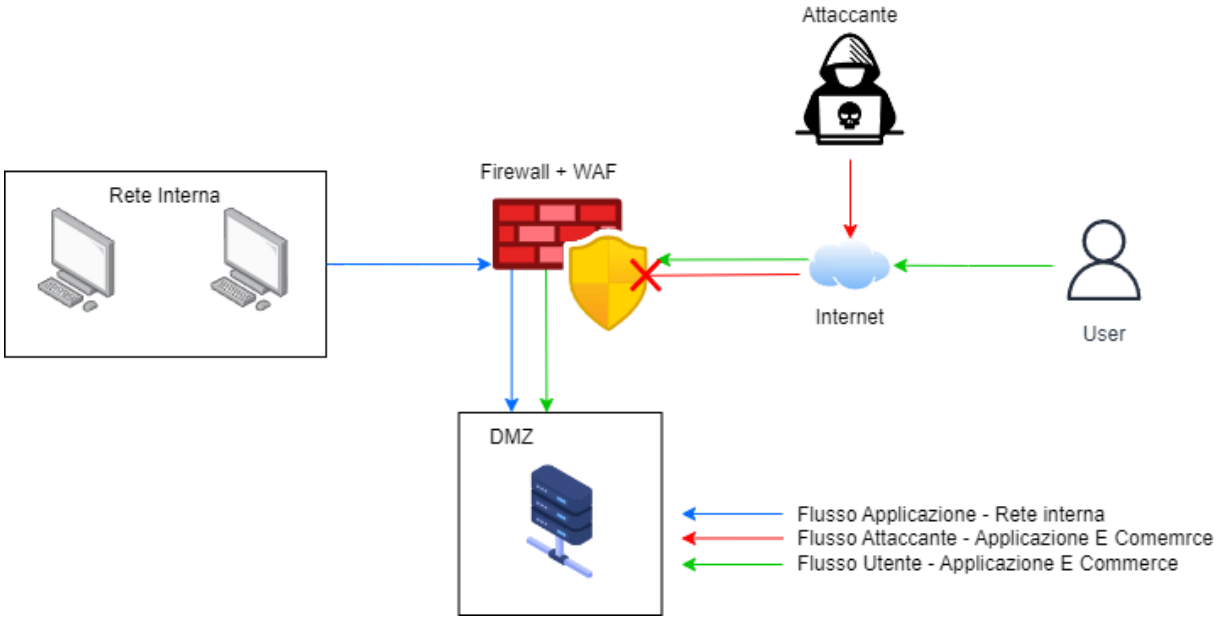
grado di rilevare tempestivamente la presenza di payload dannosi in una richiesta di tipo GET inviata al server web.

Tipologie di waf::

- WAF basati su rete: vengono installati come appliance hardware o software all'interno della rete e si occupano dell'analisi del traffico di rete a livello di pacchetto.
- WAF basati su cloud: sono forniti come servizio in abbonamento da un provider di sicurezza cloud e si occupano dell'analisi del traffico di rete a livello di applicazione.

- **Validazione e sanitizzazione dei dati in ingresso**: Assicurarsi che tutti i dati inseriti dagli utenti, inclusi quelli provenienti da form online, URL e cookie, siano correttamente validati e sanificati prima di essere utilizzati nel codice dell'applicazione. Ciò impedisce l'inclusione di script dannosi o comandi SQL nelle richieste.
- **Parametrizzazione delle query SQL**: Utilizzare query SQL parametrizzate per interagire con il database anziché costruire manualmente le query SQL concatenando i dati utente. Le query parametrizzate impediscono agli attaccanti di iniettare comandi SQL dannosi.
- **Utilizzo di meccanismi di escape per i dati dinamici**: Quando è necessario includere dati dinamici nelle pagine web, utilizzare meccanismi di escape appropriati come HTML encoding per evitare l'esecuzione di script indesiderati.

1.3 Implementazione WAF di rete



2. Impatti sul business

Per calcolare la perdita economica a seguito dei 10 minuti dove il servizio era sotto attacco andiamo a moltiplicare il numero di minuti in cui il sito è stato inaccessibile e il guadagno medio a minuto, quindi:

10 x 1.500 = 15.000 € è la perdita economica.

2.1 Azioni preventive

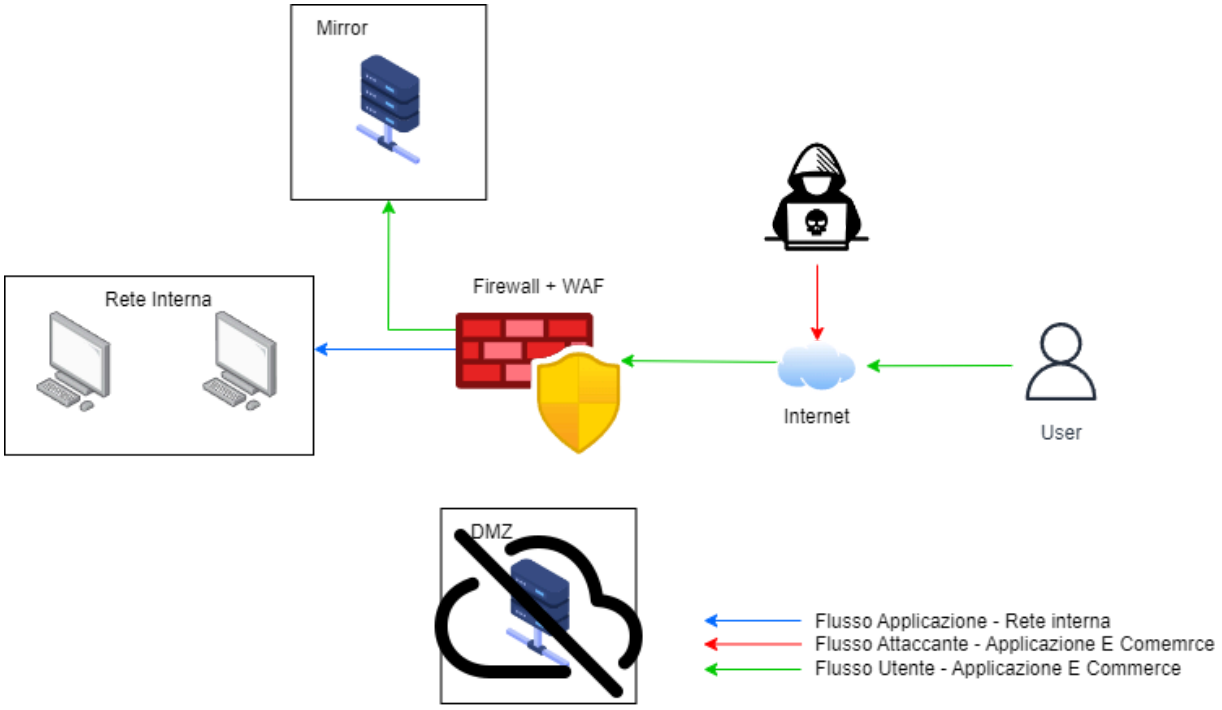
In questi casi, la mancata erogazione del servizio rappresenterebbe un danno non indifferente per l'azienda.

Per garantire la business continuity è bene effettuare delle azioni preventive:

- **Corretta configurazione del firewall:** Impostare regole nel firewall per limitare il traffico indesiderato e bloccare le richieste sospette provenienti da indirizzi IP noti per essere associati ad attacchi DoS.
    - **Configurare ACL** per filtrare il traffico in ingresso e uscita in base a criteri specifici, come indirizzi IP o tipi di protocollo, al fine di ridurre la superficie di attacco.
- **Rate Limiting**: "limitazione numero di tentativi infruttuosi di autenticazione", ovvero limita la frequenza con cui qualcuno può ripetere un'azione, come effettuare un login entro un determinato intervallo di tempo. Si basa sul monitoraggio degli indirizzi IP da cui provengono le richieste e sul monitoraggio di quanto tempo trascorre tra ogni richiesta. Il controllo si basa sul monitoraggio degli indirizzi IP da cui provengono le richieste e sull'analisi del tempo trascorso tra ciascuna richiesta. Questa tecnica è utile a contrastare l'impatto negativo di bot dannosi su un sito web o un'applicazione.

- **Limitazione delle connessioni**: Impostare limiti sul numero massimo di connessioni che possono essere stabilite da un singolo indirizzo IP, in modo da prevenire l'abuso di risorse.

Per garantire la business continuity una delle soluzioni possibili, dopo aver incrementato le firewall policy ed aver escluso la possibilità di ulteriori attacchi, è quella di utilizzare un **server mirror** che sostituisca il server principale, proseguendo l'erogazione del servizio.



3. Incident response

Il primo step della fase di “Contenimento, eliminazione e recupero" in un piano di risposta agli incidenti è il contenimento del danno causato dall’incidente di sicurezza, che deve iniziare quanto prima possibile una volta terminata la fase di analisi. Le attività di contenimento hanno lo scopo primario di isolare l’incidente in modo tale che non possa creare ulteriori danni alla rete/sistemi.

3.1 Segmentazione

Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete, è la "segmentazione", che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso. La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN.

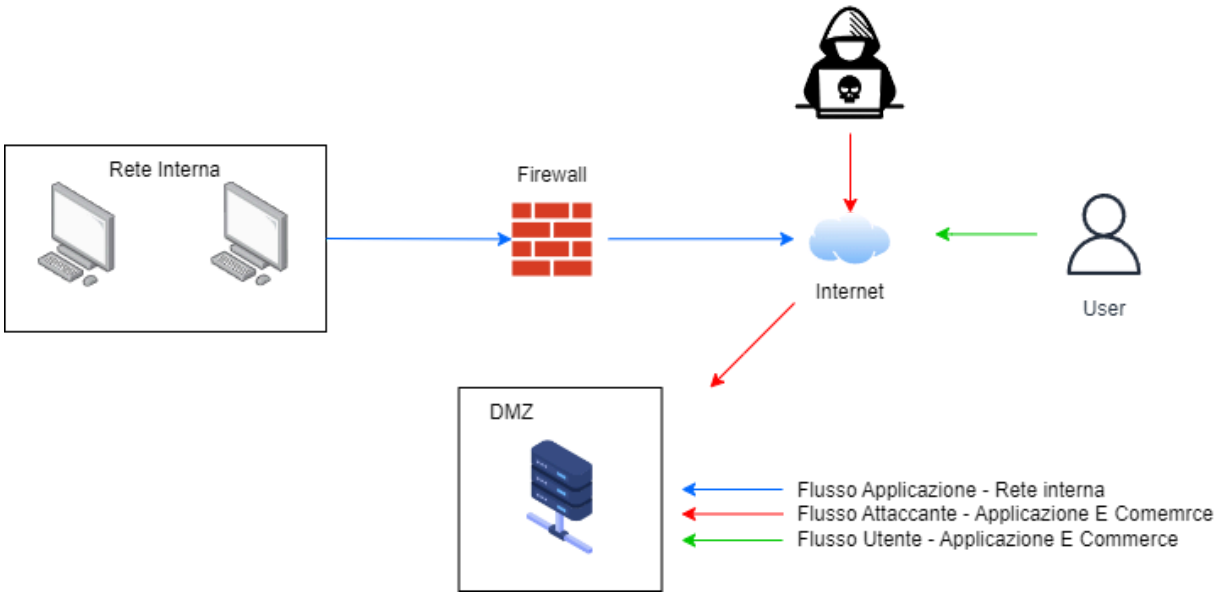
La segmentazione di rete divide una rete locale in parti più piccole allo scopo di migliorare prestazioni e sicurezza . E’ un’operazione che consiste nel delimitare il traffico dati entro specifici segmenti, noti in gergo come sottoreti. La segmentazione di rete rappresenta uno strumento essenziale per la protezione dei network aziendali. Consente, infatti, di rafforzare i controlli di sicurezza concentrandoli sulle singole sottoreti e limitare il movimento laterale di eventuali hacker e intrusi.

3.2 Isolamento

L’isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancor maggiormente l’accesso alla rete interna da parte dell’attaccante.

La soluzione proposta ,prevede di isolare la web application dalla rete in modo tale da evitare che l'attaccante possa trovare il modo di entrare nella nostra rete interna, inoltre andranno modificate le firewall policy inserendo l'IP dell'attaccante nella black list così da impedire eventuali tentativi di connessione.

Una volta isolata la rete, l'attaccante avrà ancora accesso alla rete DMZ tramite internet, tuttavia l'accesso e le operazioni di acquisto degli utenti leciti devono essere bloccati per evitare furto di informazioni, cookie, diffusione di virus o altre minacce, il che oltre a procurare un grave danno agli utenti della piattaforma sarebbe sarebbe un grave danno per l'immagine dell'azienda.



3.3 Azioni preventive

Le azioni preventive per evitare un attacco malware sono:

- **Corretta configurazione del firewall** (Trattata in precedenza);

- **Hardening dei sistemi e delle configurazioni:** si tratta di una serie di interventi di configurazione sia del sistema che dei suoi componenti, mirati a potenziare la sicurezza globale diminuendo la superficie di attacco. Queste azioni includono operazioni come la chiusura di porte non utilizzate, l'eliminazione di account non necessari sui sistemi operativi, la limitazione dei privilegi degli utenti quando non indispensabili e altre simili.

- **Patching dei sistemi:** Il termine "patch" si riferisce a una porzione di codice sviluppata per aggiornare o potenziare la sicurezza di un programma. Per esempio, quando viene scoperta una falla su un sistema operativo o un software, il produttore rilascia una correzione (patch) da applicare immediatamente per prevenire eventuali sfruttamenti della vulnerabilità. “Patch management” è il termine utilizzato per indicare il processo di implementazione e monitoraggio delle correzioni successive, una volta applicata.

- **Group policy**: offrono agli amministratori di rete la possibilità di gestire in modo centralizzato la sicurezza degli end point. Attraverso le GPO (Group Policy Object), è possibile distribuire in modo uniforme configurazioni predefinite per tutti i computer appartenenti a uno stesso workgroup o dominio, oppure personalizzare le impostazioni di sicurezza in base alla funzione specifica della macchina.

- **Penetration testing:** test di sicurezza che lancia un falso attacco informatico per identificare eventuali vulnerabilità in un sistema informatico. Si consiglia di effettuare almeno un penetration test ogni anno.

- **Logging**: la registrazione dei log, file che registrano gli eventi e le attività che avvengono su un sistema specifico. Contengono ulteriori informazioni come la data e l'orario dell'evento, l'utente responsabile dell'azione e il sistema coinvolto nell'evento. Si identificano vari tipi di log:

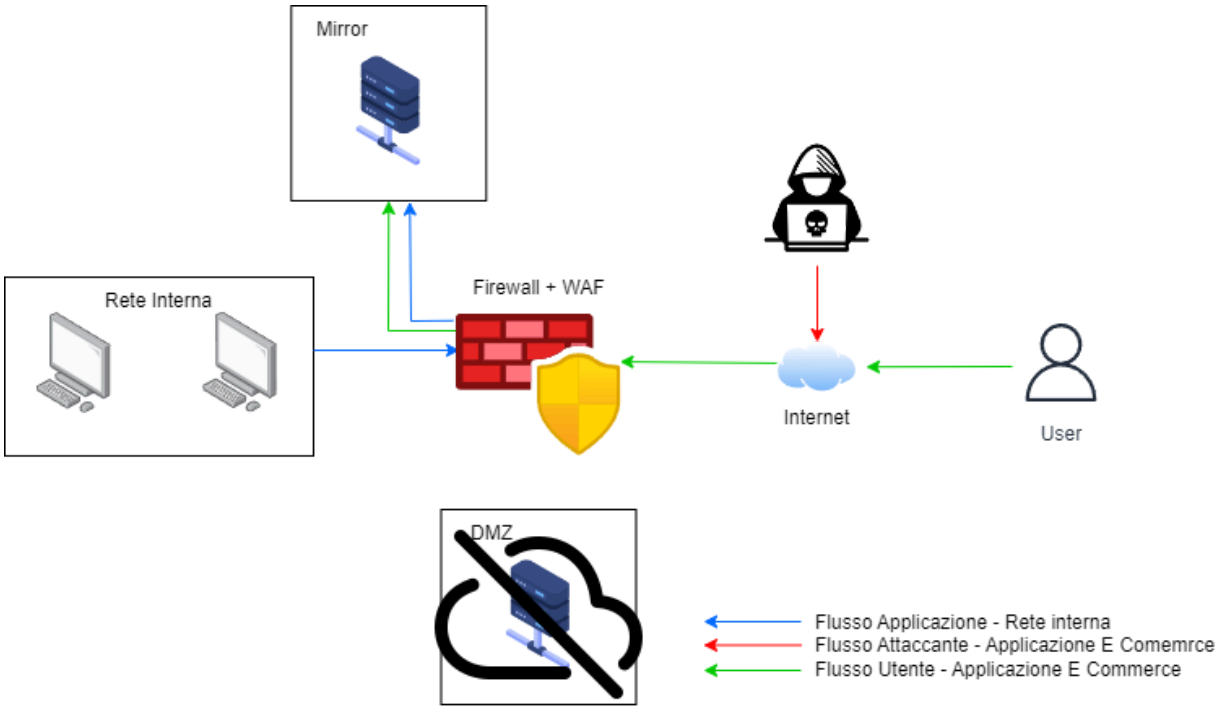
    - **Log di sicurezza**: un amministratore può monitorare tutti gli accessi ai propri sistemi, individuare chi ha apportato modifiche o cancellato specifici file. In

genere, i registri di sicurezza sono attivati per impostazione predefinita al fine di registrare gli eventi più rilevanti che si verificano su un sistema.

- **Log applicativi:** Registrano le informazioni per specifiche applicazioni web, come definite durante la fase di sviluppo dagli sviluppatori, ad esempio l'accesso ai database e le modifiche a determinate 'table'.
- **Log dei Firewall:** I log dei firewall contengono tutti gli eventi relativi al traffico che attraversa il firewall, sia per i flussi consentiti sia per quelli non consentiti. Di solito, tra le altre informazioni, vengono registrati: l'indirizzo IP di origine, l'indirizzo IP di destinazione, la porta di origine, la porta di destinazione, l'azione intrapresa sul flusso (accettato/rifiutato).

4. Soluzione completa

Come parzialmente anticipato nel paragrafo 2.1, la figura di seguito riporta un BCP che permette la difesa della rete da attacchi esterni. Nel caso si verifichi comunque una violazione la macchina compromessa viene immediatamente isolata per mantenere l'integrità e la sicurezza della rete interna ed il traffico lecito viene instradato verso un server di backup così da non avere alcuna interruzione del servizio.



5. Modifica dell’infrastruttura

5.1 Principali componenti della rete

Firewall perimetrale: è un dispositivo di sicurezza informatica posizionato all'ingresso della rete di un'organizzazione che filtra e controlla il traffico di rete in entrata e in uscita. Il suo obiettivo principale è proteggere la rete interna da minacce esterne, come intrusioni, attacchi informatici e malware, limitando l'accesso non autorizzato e bloccando il traffico dannoso.

Honeypot: Una rete honeypot è un sistema informatico progettato per sembrare una risorsa appetibile agli attaccanti, ma che in realtà è isolato dalla rete principale e monitorato attentamente. Scopo principale è raccogliere informazioni sugli attaccanti, le loro tecniche e gli strumenti utilizzati, al fine di migliorare le strategie di difesa e risposta agli attacchi.

Rete interna: Utilizzata esclusivamente dai dipendenti, è in grado di comunicare con l’esterno tramite internet e con la DMZ.

DMZ: All’interno della DMZ troviamo due web server che costituiscono i nodi del failover cluster, una struttura che include uno o più server che condividono un sistema di data storage. Questo permette l'esecuzione del sistema anche a fronte di un errore in uno dei due server. Se un web server dovesse smettere di funzionare, l’altro prenderà il suo posto come server principale con un processo chiamato failover.

Il disaster recovery backup è un processo di creazione e conservazione di copie di sicurezza dei dati critici e delle risorse informatiche di un'organizzazione, con l'obiettivo di ripristinarli in caso di perdita o danneggiamento dovuto a disastri o incidenti, come guasti hardware, errori umani, attacchi informatici, o catastrofi naturali. Queste copie di sicurezza, o backup, vengono utilizzate per ripristinare i dati e le operazioni aziendali al più presto possibile dopo un'emergenza, riducendo al minimo il tempo di inattività e i potenziali danni finanziari o operativi.

IPS (Intrusion Prevention System) è un sistema di sicurezza informatica progettato per monitorare e analizzare il traffico di rete in tempo reale al fine di individuare e prevenire attività

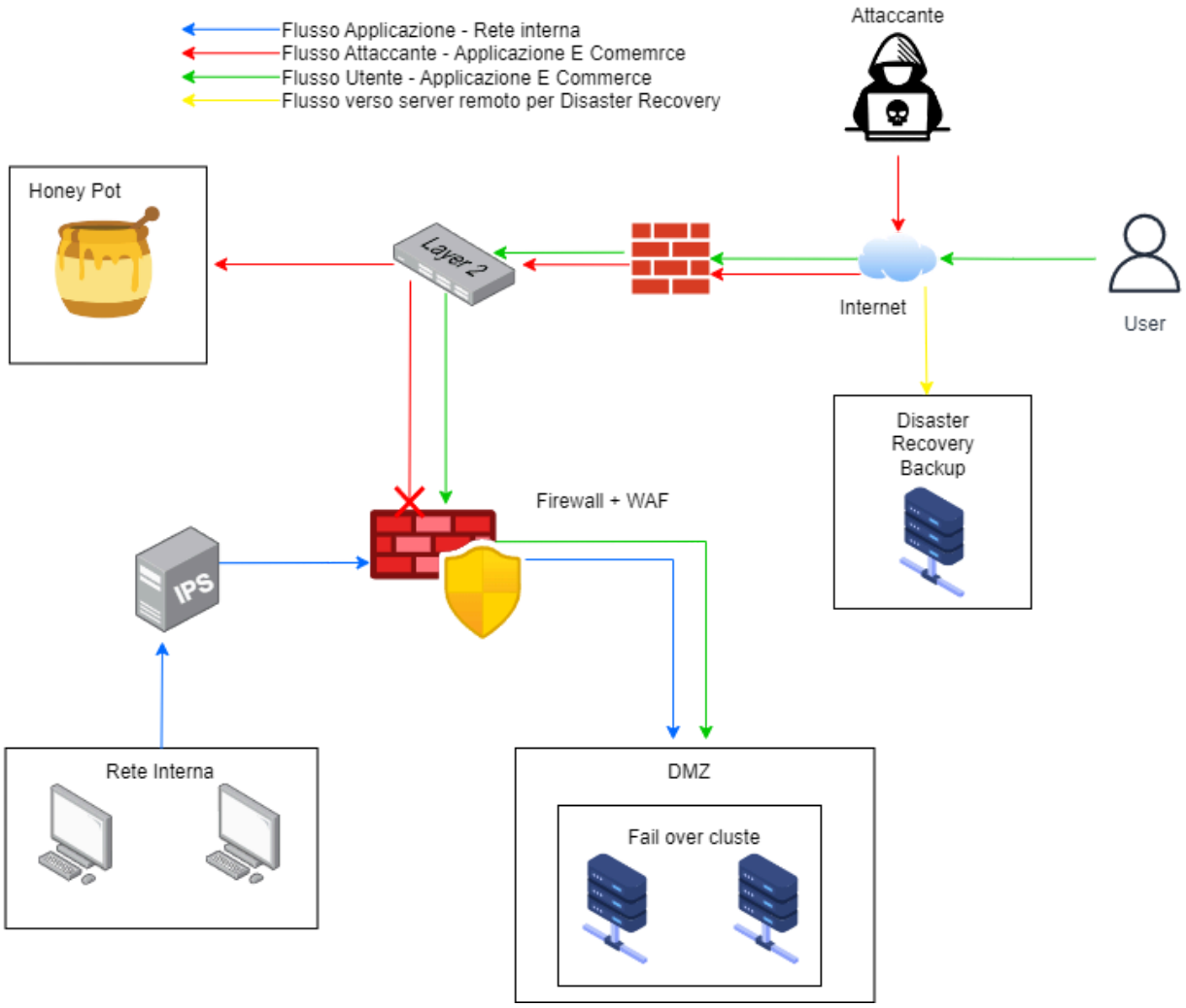
sospette o potenzialmente dannose. Utilizzando regole predefinite o modelli di comportamento, l'IPS identifica e blocca attivamente le intrusioni e gli attacchi informatici, proteggendo così la rete e i dispositivi connessi da minacce esterne e interne.

5.2 Funzionamento della rete

Tutto il traffico proveniente dell'esterno della rete (internet) viene filtrato da un firewall perimetrale sul quale vengono aggiornate regolarmente le policy, così da mantenere un elevato grado di sicurezza. La rete aziendale è stata suddivisa in tre sottoreti, una delle quali è particolarmente esposta: la rete Honeypot. Tale rete offre un target vulnerabile agli attaccanti, essendo costantemente monitorata, il team di sicurezza informatica è in grado di studiare il modus operandi degli attaccanti e prendere le giuste precauzioni per non permettere loro l'accesso alle infrastrutture aziendali.

All'interno della rete vi è un'altro firewall che combinato con un WAF offre un'ulteriore precauzione alle intrusioni. Sulla linea di ingresso della rete interna troviamo anche un IPS, tale ridondanza offre un buon controllo del traffico e assicura il rallentamento degli attacchi così da facilitare il lavoro del SOC.

Nella DMZ sono stati predisposti due server in cluster così da assicurare l'erogazione dei servizi anche in casi di malfunzionamento o compromissione. In aggiunta a questi è stato predisposto un altro server, posizionato al di fuori della rete aziendale in una rete remota, sul quale vengono effettuati giornalmente i backup così da poter aver un punto di ripristino in caso di disaster recovery.


Flusso Applicazione - Rete interna
Flusso Attaccante - Applicazione E Comemrce
Flusso Utente - Applicazione E Commerce
Flusso verso server remoto per Disaster Recovery
Attaccante
Honey Pot
Layer 2
Internet
User
Disaster Recovery Backup
Firewall + WAF
IPS
Rete Interna
DMZ
Fail over cluste

6. Analisi delle segnalazioni di Anyrun

6.1 Fondamenti concettuali

Any.Run è un servizio online che fornisce un ambiente sicuro e controllato per l'esecuzione e l'analisi dei file eseguibili, dei documenti e delle URL sospette o dannosi. Si tratta di una piattaforma che consente agli utenti di caricare e analizzare file o collegamenti web per identificare potenziali minacce informatiche come malware, virus o altre forme di software dannoso.

Ecco alcuni dei principali punti salienti e funzionalità di Any.Run:

- **Esecuzione sicura**: Any.Run fornisce un ambiente virtualizzato sicuro per eseguire i file e le URL caricati dagli utenti. Questo ambiente controllato consente di esaminare il comportamento del file o del collegamento senza rischiare di infettare il proprio computer o rete con malware.
- **Analisi comportamentale:** Durante l'esecuzione dei file o delle URL, Any.Run monitora e registra attentamente il comportamento del software in esecuzione. Questo include attività come la creazione o la modifica di file, la comunicazione di rete, l'interazione con il registro di sistema e altro ancora.
- **Report dettagliati:** Una volta completata l'analisi, Any.Run fornisce report dettagliati sul comportamento del file o del collegamento. Questi report possono includere informazioni utili come gli URL contattati, i file creati, le modifiche al registro di sistema e altro ancora. Questi dati possono aiutare gli utenti a identificare e comprendere meglio la natura delle minacce.

- **Condivisione e collaborazione**: Gli utenti possono condividere i loro risultati di analisi con altri utenti o esperti di sicurezza informatica. Questo favorisce la collaborazione e lo scambio di informazioni sulla minaccia tra la comunità.

- **Strumenti aggiuntivi**: Any.Run offre anche strumenti aggiuntivi come l'analisi statica dei file, la ricerca di indicatori di compromissione (IOC) e altre funzionalità utili per la ricerca e l'analisi delle minacce informatiche.

In generale, Any.Run è uno strumento prezioso per gli utenti e gli esperti di sicurezza informatica che cercano di analizzare e comprendere il comportamento dei file e delle URL sospette al fine di proteggere i propri sistemi e reti da potenziali minacce informatiche.

PowerShell è una shell della riga di comando e un linguaggio di scripting sviluppato da Microsoft per i sistemi operativi Windows. È stato progettato per essere più potente e flessibile del prompt dei comandi tradizionale (cmd.exe) e offre una vasta gamma di funzionalità avanzate per l'automazione delle attività di gestione e amministrazione dei sistemi Windows.

Ecco alcuni concetti chiave relativi a PowerShell:

- **Object-Based**: PowerShell tratta l'output dei comandi come oggetti anziché semplici stringhe di testo. Questo significa che è possibile manipolare i dati in modo più flessibile e potente, utilizzando le proprietà e i metodi degli oggetti.
- **Cmdlets**: PowerShell utilizza i cmdlet (pronunciato "command-lets") come i mattoni fondamentali per eseguire le operazioni. I cmdlet sono piccoli comandi che eseguono operazioni specifiche, come il recupero di informazioni di sistema, la gestione dei file o l'esecuzione di azioni di amministrazione. Ad esempio, Get-Process è un cmdlet che restituisce informazioni sui processi in esecuzione.
- **Pipeline**: PowerShell supporta la pipeline, che consente di concatenare i cmdlet in una sequenza, in modo che l'output di un cmdlet venga passato direttamente come input al successivo. Ciò consente di comporre operazioni complesse combinando cmdlet semplici. Ad esempio, Get-Process | Stop-Process elenca tutti i processi in esecuzione e quindi interrompe ognuno di essi.
- **Scripting Language**: PowerShell è un linguaggio di scripting completo con supporto per le variabili, le strutture di controllo del flusso (come cicli e condizioni), le funzioni e altro

ancora. Questo consente di scrivere script PowerShell per automatizzare compiti complessi e ripetitivi.

- **Integrazione con .NET**: PowerShell è strettamente integrato con il framework .NET, consentendo l'utilizzo delle librerie e delle funzionalità .NET all'interno degli script PowerShell. Ciò amplia notevolmente le capacità di PowerShell e ne facilita l'integrazione con altre tecnologie Microsoft.
- **Interfaccia utente grafica (GUI)**: PowerShell può essere utilizzato per creare semplici interfacce utente grafiche (GUI) attraverso Windows Presentation Foundation (WPF) o Windows Forms. Ciò consente agli amministratori di creare strumenti personalizzati per semplificare la gestione dei sistemi Windows.

In sintesi, PowerShell è uno strumento potente per automatizzare e semplificare la gestione dei sistemi Windows, offrendo una vasta gamma di funzionalità avanzate e una sintassi flessibile. È ampiamente utilizzato dagli amministratori di sistema e dagli sviluppatori per automatizzare le attività quotidiane e semplificare le operazioni di gestione dei sistemi Windows.

Un file .bat, abbreviazione di "batch file", è un tipo di file utilizzato principalmente nei sistemi operativi Windows per automatizzare una serie di comandi. Questi file contengono una sequenza di comandi DOS (Disk Operating System) che vengono eseguiti dall'interprete dei comandi del sistema operativo quando il file viene eseguito.

- **Automatizzazione delle attività:** I file batch sono comunemente utilizzati per automatizzare compiti ripetitivi o complessi. Ad esempio, possono essere utilizzati per eseguire una serie di comandi di sistema, copiare file da una posizione all'altra, modificare file di configurazione e così via.
- **Sintassi dei comandi**: I comandi all'interno di un file batch possono essere qualsiasi comando DOS o comando nativo del prompt dei comandi di Windows. Possono includere comandi per spostarsi tra le directory (cd), copiare file (copy), eliminare file (del), creare directory (mkdir), stampare testo (echo) e molti altri.

- **Estensione dei comandi:** I file batch possono includere variabili, cicli, condizioni e altri costrutti di programmazione per rendere le operazioni più dinamiche e flessibili. Ad esempio, è possibile utilizzare la struttura IF-ELSE per eseguire azioni diverse in base a condizioni specifiche.
- **Esecuzione dei file batch:** I file batch vengono eseguiti facendo doppio clic su di essi o digitando il loro nome nel prompt dei comandi di Windows. Quando viene eseguito, il sistema operativo esegue sequenzialmente tutti i comandi elencati nel file batch.
- **Modifica dei file batch:** I file batch possono essere modificati con qualsiasi editor di testo, come Notepad o Notepad++. È importante notare che i comandi all'interno di un file batch possono avere effetti significativi sul sistema, quindi è consigliabile fare attenzione durante la modifica e l'esecuzione dei file batch.

In sintesi, i file batch sono uno strumento potente per automatizzare compiti su sistemi Windows e sono utilizzati ampiamente dagli amministratori di sistema, dagli sviluppatori e dagli utenti avanzati per semplificare il lavoro quotidiano e migliorare l'efficienza.

exe

Un file con estensione .exe è un'eseguibile di Windows, ovvero un file che contiene codice eseguibile destinato a essere avviato direttamente dal sistema operativo Microsoft Windows. Ecco una spiegazione più dettagliata:

- **Codice eseguibile:** Un file .exe contiene istruzioni in linguaggio macchina, ovvero il linguaggio di basso livello comprensibile direttamente dalla CPU del computer. Queste istruzioni possono includere operazioni come l'esecuzione di programmi, l'interazione con l'hardware del computer, la gestione dei file e la comunicazione in rete.
- **Applicazioni software:** La maggior parte dei file .exe sono programmi software, come applicazioni desktop, utility di sistema, giochi e altro ancora. Quando si avvia un file .exe, il sistema operativo avvia il codice contenuto nel file e esegue il programma corrispondente.

- **Sicurezza**: I file .exe possono essere sicuri o dannosi. Mentre la maggior parte dei file .exe proviene da fonti attendibili e contiene software legittimo, alcuni file .exe possono essere malware o virus progettati per danneggiare il computer o rubare informazioni personali. È importante scaricare e eseguire solo file .exe da fonti attendibili e utilizzare software antivirus per proteggere il sistema da minacce informatiche.
- **Compatibilità:** I file .exe sono specifici per il sistema operativo Windows e non possono essere eseguiti direttamente su altri sistemi operativi come macOS o Linux. Tuttavia, è possibile eseguire alcuni file .exe su altri sistemi operativi utilizzando emulatori o strumenti di compatibilità.
- **Creazione di file .exe**: I file .exe vengono creati utilizzando software di sviluppo come Microsoft Visual Studio, Borland Delphi, o altri ambienti di sviluppo. Questi strumenti consentono agli sviluppatori di scrivere il codice sorgente del programma e compilare il codice in un file .exe eseguibile.

In sintesi, i file .exe sono eseguibili di Windows che contengono codice destinato a essere avviato direttamente dal sistema operativo. Possono includere una vasta gamma di software e applicazioni e sono un elemento fondamentale per il funzionamento del sistema operativo Windows.

cmd.exe

cmd.exe è il prompt dei comandi di Windows, noto anche come Command Prompt. È un'applicazione della riga di comando che fornisce un'interfaccia testuale per l'interazione con il sistema operativo Windows. Ecco una spiegazione più dettagliata:

- **Interfaccia testuale:** Il Command Prompt fornisce un'interfaccia testuale in cui gli utenti possono inserire comandi specifici per eseguire varie operazioni sul sistema. Gli input e gli output avvengono tramite testo, senza l'uso di grafica.
- **Esecuzione di comandi:** Gli utenti possono inserire comandi, ad esempio per eseguire programmi, navigare tra le directory del sistema, gestire file e cartelle, eseguire operazioni di rete, visualizzare informazioni di sistema e molto altro ancora.
- Sintassi dei comandi: I comandi nel prompt dei comandi di Windows seguono una sintassi specifica. Ad esempio, il comando dir viene utilizzato per elencare i file e le cartelle in una determinata directory, mentre cd viene utilizzato per cambiare la directory corrente.
- **Variabili di ambiente:** Il prompt dei comandi può anche essere utilizzato per visualizzare e modificare le variabili di ambiente del sistema, come ad esempio le variabili PATH che definiscono i percorsi di ricerca per i file eseguibili.
- **Scripting**: È possibile creare script batch utilizzando il Command Prompt, che consistono in una serie di comandi salvati in un file di testo con estensione .bat o .cmd. Questi script possono automatizzare una serie di compiti.
- **Privilegi amministrativi:** In Windows, il prompt dei comandi può essere eseguito con privilegi di amministratore, consentendo agli utenti di eseguire comandi che richiedono autorizzazioni elevate per modificare le impostazioni di sistema.

In sintesi, il Command Prompt (cmd.exe) è uno strumento versatile e potente per interagire con il sistema operativo Windows tramite una interfaccia testuale, fornendo agli utenti la possibilità di eseguire una vasta gamma di operazioni e comandi.

6.2 L'.exe PERFORMANCE_BOOSTER

Questo script batch sembra essere uno strumento di ottimizzazione del sistema destinato a migliorare le prestazioni dei sistemi Windows, in particolare delle versioni 1709, 1809 e 1903.

Ecco una panoramica di ciò che fa ciascuna sezione dello script:

Configurazione dell'ambiente:

@shift /0: Questo comando sembra essere invalido. Forse è destinato a fare qualcosa con gli argomenti della riga di comando, ma /0 non è un argomento valido per shift.

@ECHO OFF: Questo comando disattiva l'eco delle righe di comando. Fa sì che il file batch venga eseguito senza mostrare ogni comando eseguito.

pushd "%~dp0": Cambia la directory corrente nella directory del file batch. %~dp0 è una variabile speciale che rappresenta la directory del file batch.

Impostazione della modalità di visualizzazione:

MODE CON: COLS=78 LINES=54: Imposta la larghezza su 78 caratteri e l'altezza su 54 righe per la finestra della console.

Impostazione del titolo della finestra:

Imposta il titolo della finestra della console su "PERFORMANCE_BOOSTER_v3.6 by n1kobg".

Navigazione alla directory di sistema:

cd %systemroot%\system32: Cambia la directory corrente nella directory di sistema.

Impostazione della policy di esecuzione di PowerShell:

Powershell Set-ExecutionPolicy Unrestricted -Force: Imposta la policy di esecuzione di PowerShell su Unrestricted, consentendo l'esecuzione di tutti gli script senza restrizioni.

Cancellazione dello schermo:

CLS: Cancella lo schermo della console.

Visualizzazione di messaggi di avviso:

Visualizza diversi messaggi di avviso riguardanti l'uso e i rischi potenziali dell'esecuzione dello strumento.

Creazione di un punto di ripristino e backup del registro di sistema:

Chiede all'utente se desidera eseguire il backup del registro di sistema.

Se l'utente sceglie di eseguire il backup del registro, esporta il registro in un file sul desktop.

Crea un punto di ripristino di sistema.

Patching del file hosts:

Disabilita l'attributo di sola lettura del file hosts.

Copia un file chiamato "hosts" nella directory di sistema.

Apre il file hosts in Notepad per modificarlo.

Avviso aggiuntivo e informazioni:

Visualizza un messaggio di avviso finale.

Menu di avvio:

Visualizza un menu per avviare varie attività di ottimizzazione.

Visualizza il menu principale:

Stampa un'intestazione e un elenco di opzioni nel menu principale, come ottimizzazione delle prestazioni, miglioramento delle prestazioni Internet, ottimizzazione dei servizi Windows, stop del telemetria, tweak generali, e uscita.

L'opzione è associata a una lettera (ad esempio, "O" per ottimizzazione delle prestazioni).

Attende l'input dell'utente:

Richiede all'utente di inserire la lettera corrispondente all'opzione desiderata.

Se l'utente inserisce un'opzione valida, il programma passa al punto corrispondente nel codice.

Se l'input non corrisponde a nessuna opzione valida, il programma torna al menu principale.

Esegue l'azione corrispondente all'opzione selezionata:

Ogni opzione nel menu principale è associata a una sezione del codice che esegue un'azione specifica, come avviare un'ottimizzazione delle prestazioni, migliorare le prestazioni di Internet, ottimizzare i servizi Windows, stoppare il telemetria, applicare tweak generali o uscire dal programma.

Torna al menu principale:

Dopo aver eseguito un'azione, il programma torna al menu principale per consentire all'utente di selezionare un'altra opzione o di uscire dal programma.

Uscita dal programma:

Complessivamente, anche se lo script sembra fornire funzionalità utili per ottimizzare i sistemi Windows, potrebbe essere in realtà malevolo in quanto alla chiusura dello stesso lo script termina con una chiamata a un'esecuzione esterna chiamata "**Skull.exe**"

Lo script in sintesi

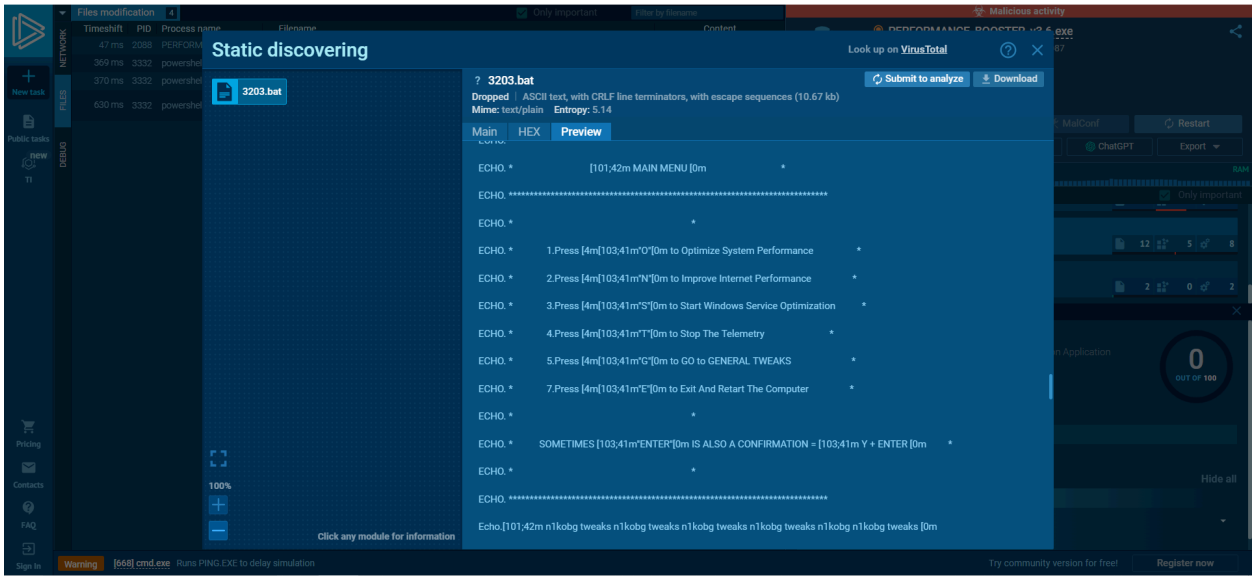
- Lo script inizia impostando i parametri per la finestra della console, impostando il titolo e cambiando la directory alla cartella system32.
- Imposta la policy di esecuzione di PowerShell su "Unrestricted" (Non limitata).
- Viene visualizzata una sezione di avviso che indica che lo strumento è progettato per versioni specifiche di Windows (v1709, v1809, v1903), e consiglia cautela in quanto un uso improprio potrebbe danneggiare il sistema.
- Viene chiesto all'utente di confermare di aver compreso gli avvisi.
- Vengono offerte opzioni per eseguire il backup del registro di sistema e creare un punto di ripristino del sistema.
- Viene modificato il file hosts e viene aperto in Notepad per la modifica.
- Viene visualizzato il menu principale che offre varie opzioni per l'ottimizzazione del sistema, come ottimizzare le prestazioni del sistema, migliorare le prestazioni di Internet, ottimizzare i servizi, interrompere la telemetria, applicare modifiche generali e uscire dal programma.
- Ogni opzione nel menu principale attiva un'azione specifica, spesso eseguendo uno strumento o uno script esterno per il compito di ottimizzazione.
- Alla chiusura apre il file Skull.exe

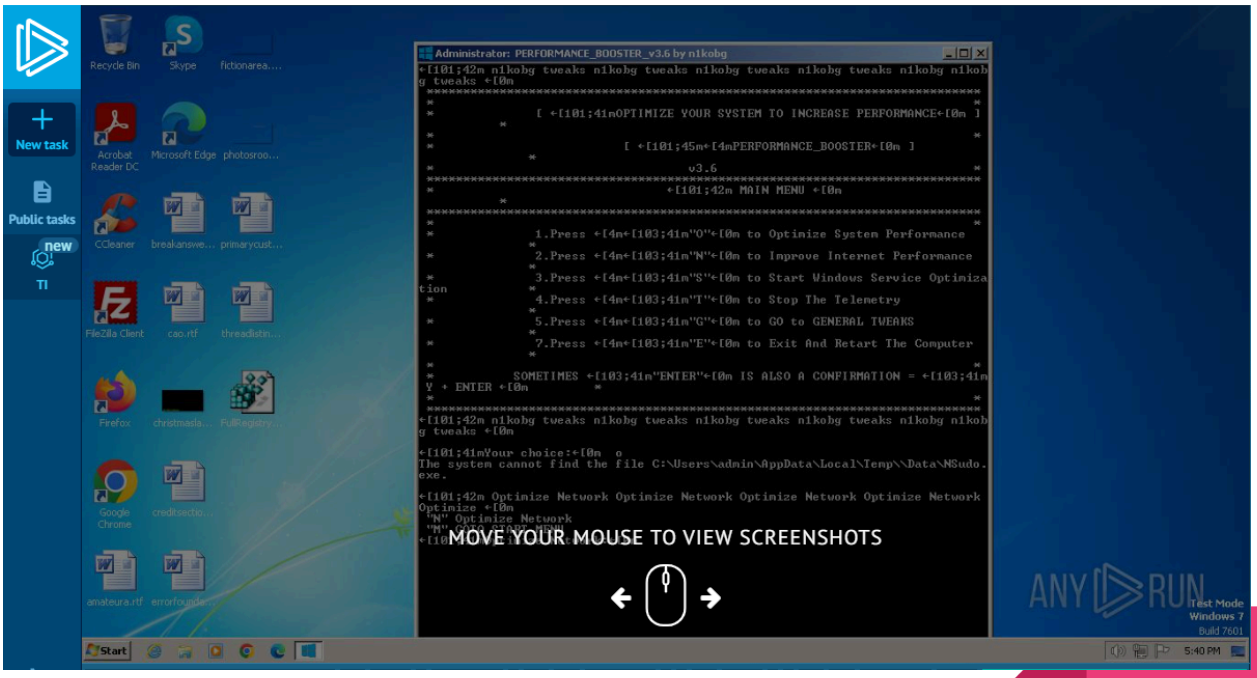
Le criticita

Andando ad analizzare le criticità tramite la pagina di riferimento fornita dalla traccia dell esercizio utilizzando **http//:any.run**

troviamo la sorgente del file dentro il tool di analisi,

Notiamo che il programma è ottimizzato per un PC Windows 10 a 64bit





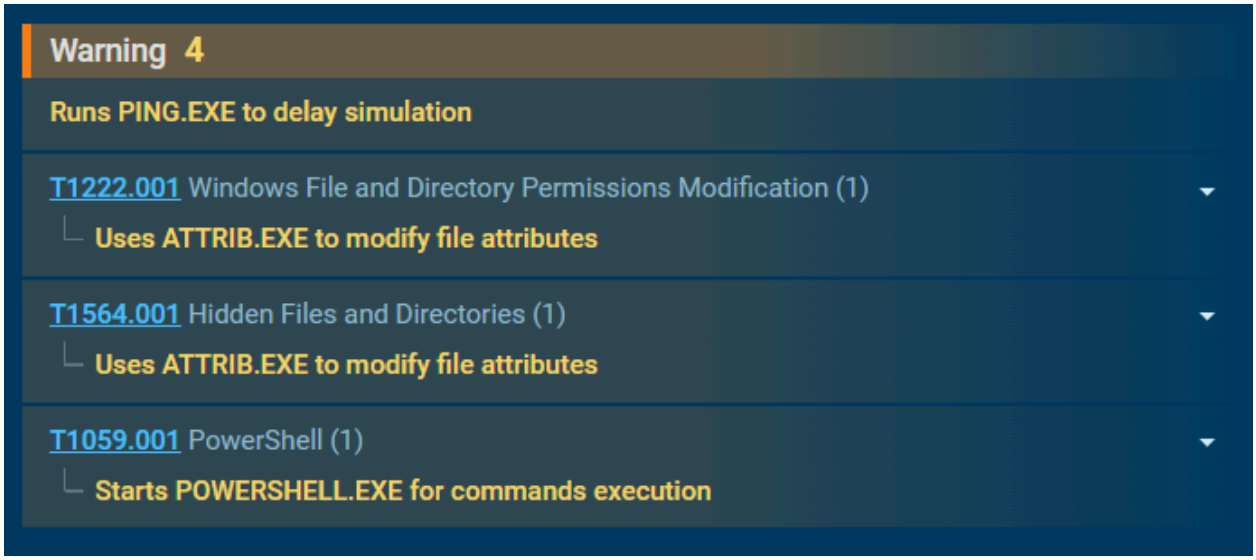
Dove quest'ultimo viene analizzato ed emergono delle criticità:

Il primo warning T1059 ha due sotto-punti molto preoccupanti:

- vi è l'esecuzione automatica del file .bat senza la richiesta/autorizzazine da parte dell'utente
- risulta esserci l'apertura da parte del programma dell cmd.exe in modalità amministratore

Il primo pericolo: ossia la modifica la politica di esecuzione di PowerShell (senza restrizioni):

È importante notare che impostare la Execution Policy su Unrestricted può essere rischioso, poiché consente l'esecuzione di qualsiasi script, incluso quello scaricato da Internet, senza restrizioni. Ciò potrebbe potenzialmente esporre il sistema a rischi di sicurezza. Tuttavia, in alcune situazioni, ad esempio durante l'esecuzione di script di automazione su un sistema di sviluppo o di test, questa impostazione può essere utile.



Gli ultimi 4 warning sono tali in quanto il programma va a modificare il file ATTRIB.EXE che serve per:

Visualizzazione degli attributi di un file o una directory: Il comando attrib.exe può essere utilizzato per visualizzare gli attributi di un file o una directory. Ad esempio, eseguendo attrib.exe nomefile.txt, il comando mostrerà gli attributi del file nomefile.txt.

Modifica degli attributi di un file o una directory: Il comando attrib.exe può anche essere utilizzato per modificare gli attributi di un file o una directory. Ad esempio, attrib.exe +r nomefile.txt imposterà il file nomefile.txt come "solo lettura", mentre attrib.exe -r nomefile.txt rimuoverà l'attributo "solo lettura" dal file.

Gestione degli attributi nascosti e di sistema: È possibile utilizzare attrib.exe per impostare o rimuovere gli attributi "nascosto" e "di sistema" dai file e dalle directory. Questo può essere utile per nascondere o mostrare determinati file e directory nel sistema operativo.

Operazioni su più file e directory: attrib.exe supporta l'esecuzione di operazioni su più file e directory contemporaneamente. Ad esempio, è possibile eseguire attrib.exe +r *.txt per impostare tutti i file con estensione .txt come "solo lettura".

In generale, il comando attrib.exe fornisce un modo semplice per gestire gli attributi dei file e delle directory tramite la riga di comando di Windows. È particolarmente utile quando si desidera automatizzare la modifica degli attributi di più file o directory.

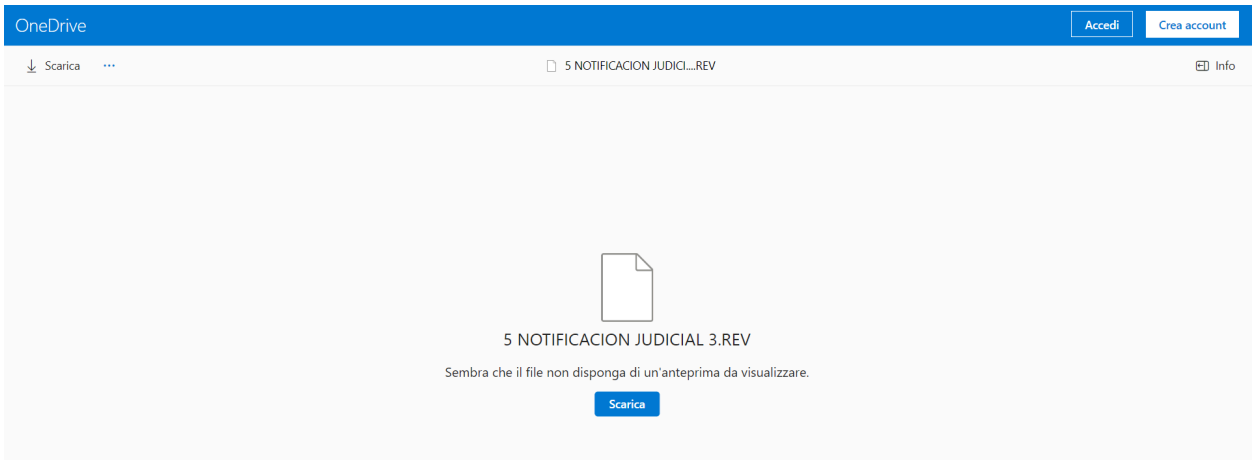
ma questo se attivato da una sorgente ed un codice malevolo potrebbe essere molto problematico e causare seri danni.

6.3 Installer Microsoft EDGE

Viene ricercato e aperto tramite any.run il seguente link

https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE

che ci rimanda ad una pagina di onedrive



Automaticamente a windows viene richiesto di scaricare microsoft edge in quanto come si può vedere in figura il link è stato aperto con Explorer anziché Edge;

Si può impostare Microsoft Edge come browser predefinito al posto di Windows Explorer per aprire determinati tipi di file o per la navigazione web, puoi seguire questi passaggi su un sistema operativo Windows:

Apri Impostazioni di Windows:

- Puoi farlo facendo clic sull'icona dell'ingranaggio nel menu Start o premendo il tasto Windows + I sulla tastiera.

Seleziona "App":

All'interno delle impostazioni di Windows, cerca e fai clic sull'opzione "App".

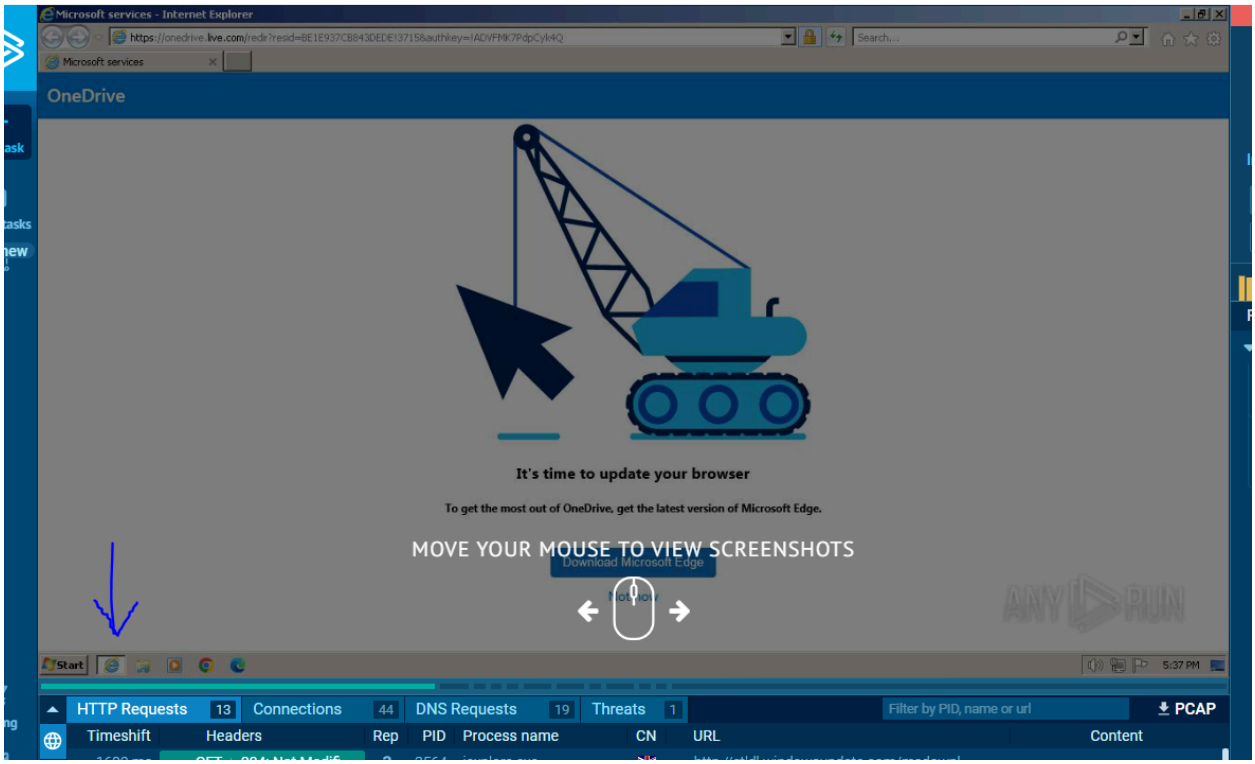
Impostazioni predefinite:

Nell'elenco di opzioni, trova e fai clic su "App predefinite" nella barra laterale sinistra.

Scegli il Browser Web:

Scorri verso il basso fino a trovare "Browser Web" nell'elenco delle app predefinite. Fai clic su di esso.

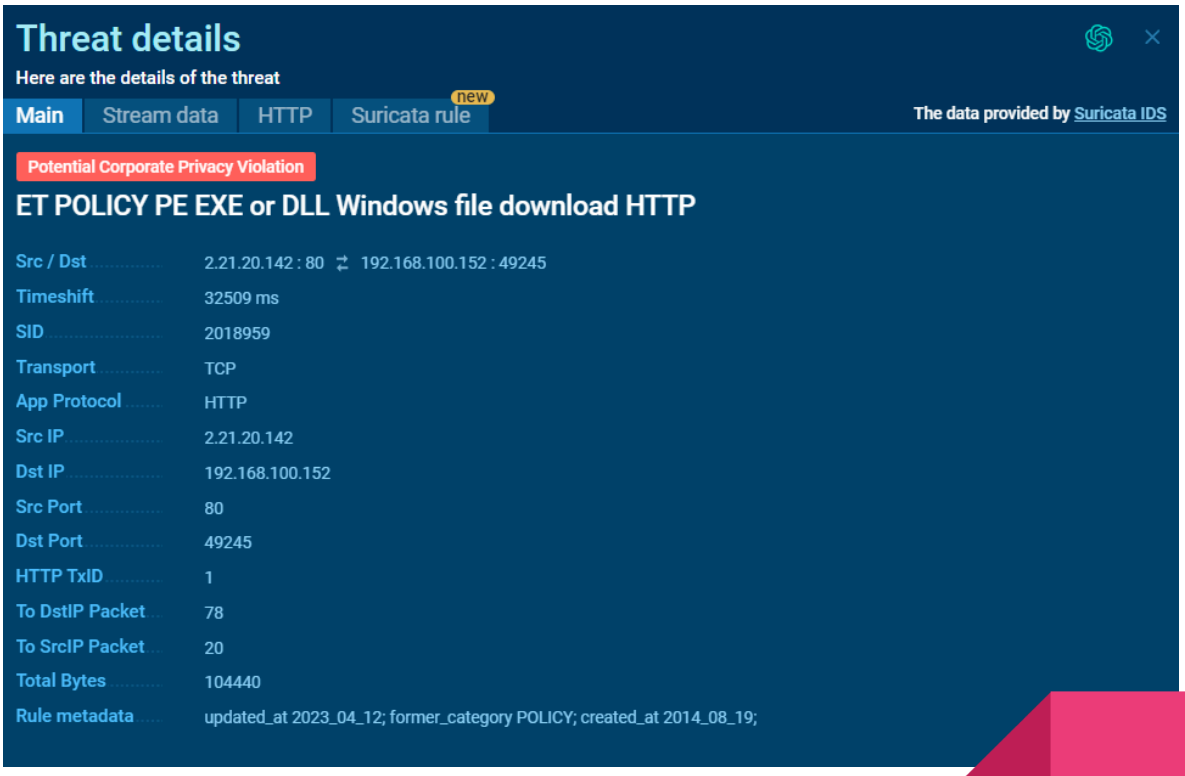
Seleziona Microsoft Edge dall'elenco di browser web disponibili, trova Microsoft Edge e fai clic su di esso per impostarlo come browser predefinito.



In automatico seguendo l'installazione guidata possiamo tenere traccia di tutti gli indirizzi che sono intercorsi per tale installazione

Al termine dell'installazione si aprirà microsoft edge che sarà correttamente installato sul dispositivo.

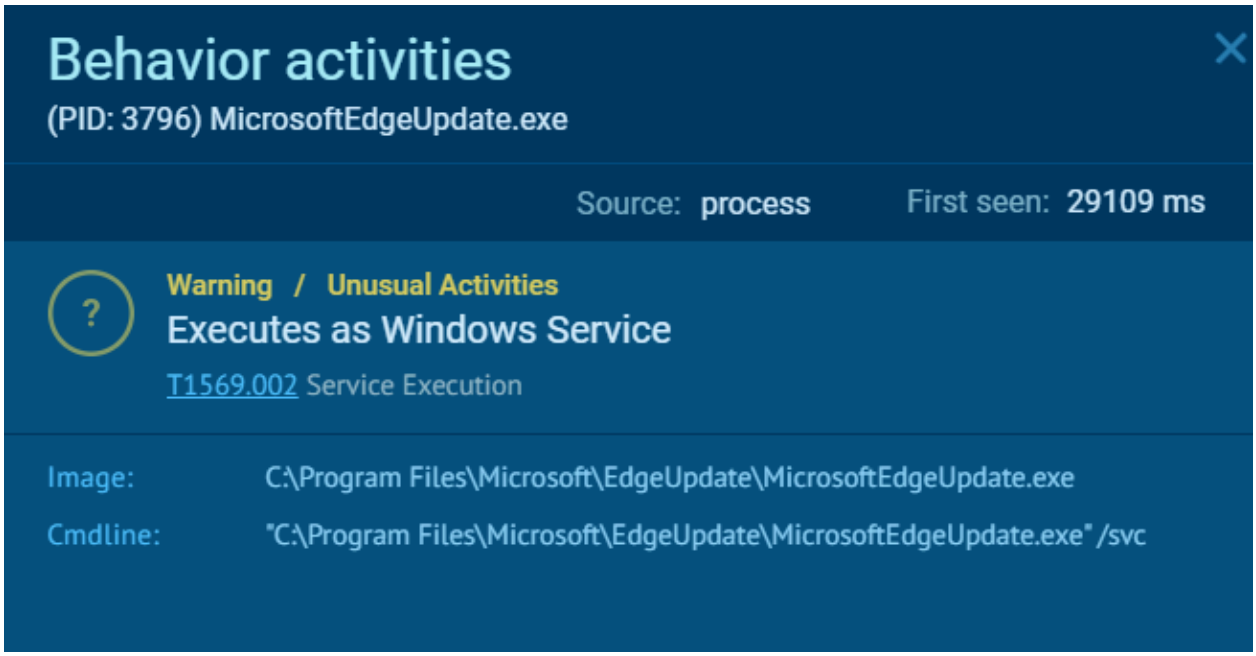
Una problematica riscontrata dall'analisi è la possibile violazione della privacy



Una potenziale violazione della privacy aziendale può avvenire quando un'azienda tratta in modo improprio o illegale le informazioni personali dei propri dipendenti, clienti o altre parti interessate. Questo può includere la raccolta non autorizzata di dati personali, l'accesso non autorizzato ai dati sensibili, la mancanza di sicurezza delle informazioni, la divulgazione non autorizzata dei dati personali e altri comportamenti che mettono a rischio la privacy delle persone coinvolte. Queste violazioni possono avere gravi conseguenze legali, finanziarie e reputazionali per l'azienda coinvolta. Pertanto, è essenziale che le aziende adottino politiche e pratiche rigorose per proteggere la privacy dei loro dipendenti e clienti.

È importante notare che è sempre bene prestare attenzione ai comandi che vengono eseguiti sul proprio computer, specialmente se si tratta di file eseguibili o comandi di sistema, per garantire che non ci siano potenziali rischi per la sicurezza o la privacy.

Invece come unico “Warning” riscontriamo:



"Unusual activities" significa letteralmente "attività insolite" o "attività non comuni". Nel contesto aziendale o della sicurezza informatica, il termine si riferisce a comportamenti o azioni che si discostano dal normale o dal consueto, e che potrebbero indicare una potenziale minaccia o un problema.

Andando a controllare l'indirizzo verifichiamo l'affidabilità della fonte.