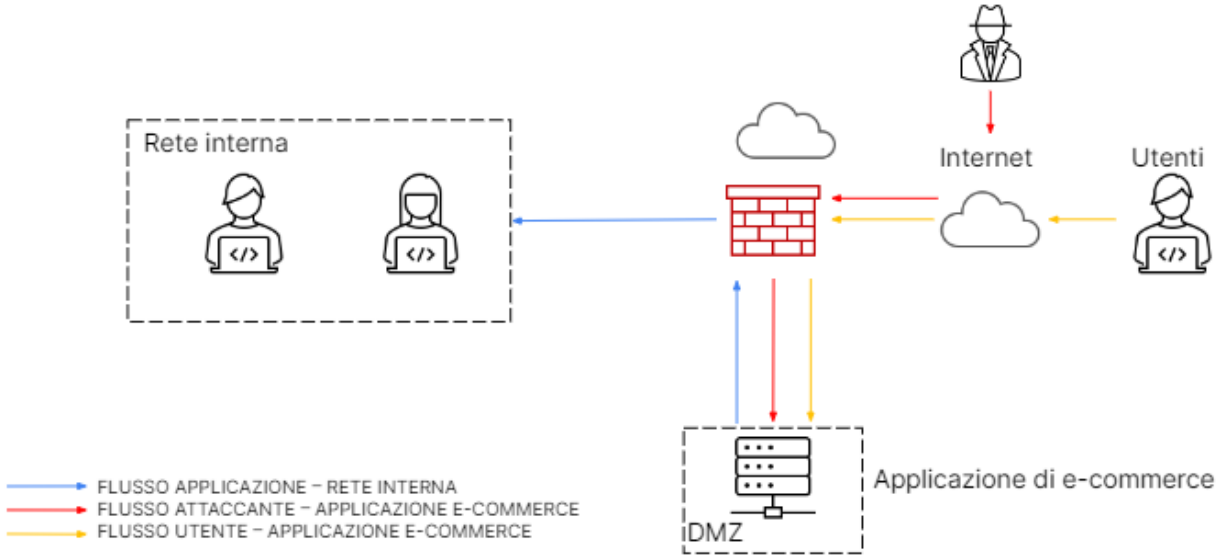
ANALISI DEI LOG – CASO REALE

Data l'interfaccia di rete sottostante, eseguire le seguenti task:

1. **Azioni preventive** da implementare **per difendere l'applicazione Web da attacchi SQLi e XSS** da parte di un potenziale attaccante;
2. **Analisi di link loschi con conseguente report**
3. Mettere in pratica un **Incident Response,** dopo che un malware ha infettato l'applicazione Web, **tenendo presente che il malware non deve propagarsi sulla rete interna, e non deve divulgare informazioni sensibili verso Internet**
4. **Soluzione completa;**
5. **Modificare in maniera più aggressiva l'infrastruttura di rete proposta.**



TASK 1 = **Azioni preventive** da implementare **per difendere l'applicazione Web da attacchi SQLi e XSS** da parte di un potenziale attaccante.

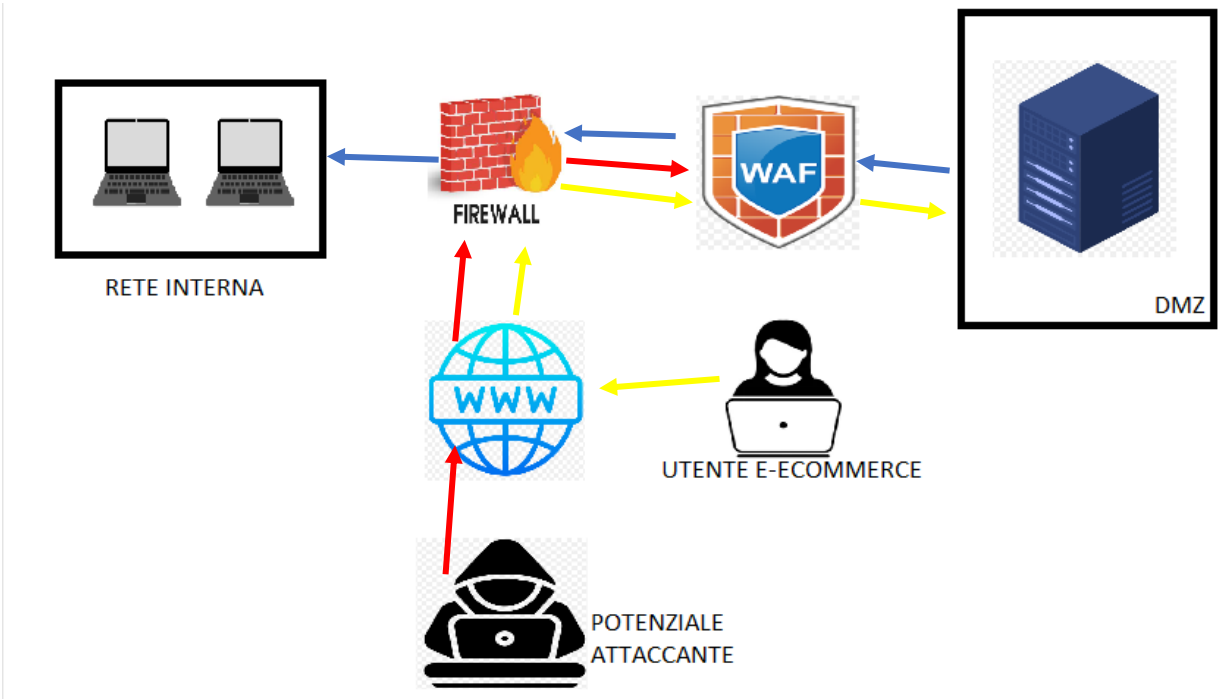
I servizi di Security Operations sono basati sulla gestione degli incidenti di sicurezza, ai quali si va incontro quando si verificano violazioni o minacce imminenti ai sistemi informativi. **Gli incidenti di sicurezza possono includere la perdita o la divulgazione di dati sensibili, intrusioni nei sistemi interni da parte di utenti malintenzionati o attacchi malware.**

Attenendoci ai task, focalizziamo il nostro interesse sulle azioni preventive, le quali vengono intraprese prima che si verifichi un incidente di sicurezza al fine di ridurre i rischi di eventi negativi. Ciò può comportare l'implementazione di misure di sicurezza, come firewall, sistemi di rilevamento delle intrusioni, politiche di accesso controllato e formazione del personale sulla sicurezza informatica.

Dunque, implementiamo delle misure preventiva **per difendere l'applicazione Web da attacchi SQLi e XSS** da parte di un potenziale attaccante. Per far ciò, è possibile aggiungere un **WAF** (Web Application Firewall), **il quale agisce come una barriera di protezione tra le applicazioni web e gli utenti esterni, rilevando e bloccando attacchi noti come Cross-Site Scripting (XSS) e SQL injection**.

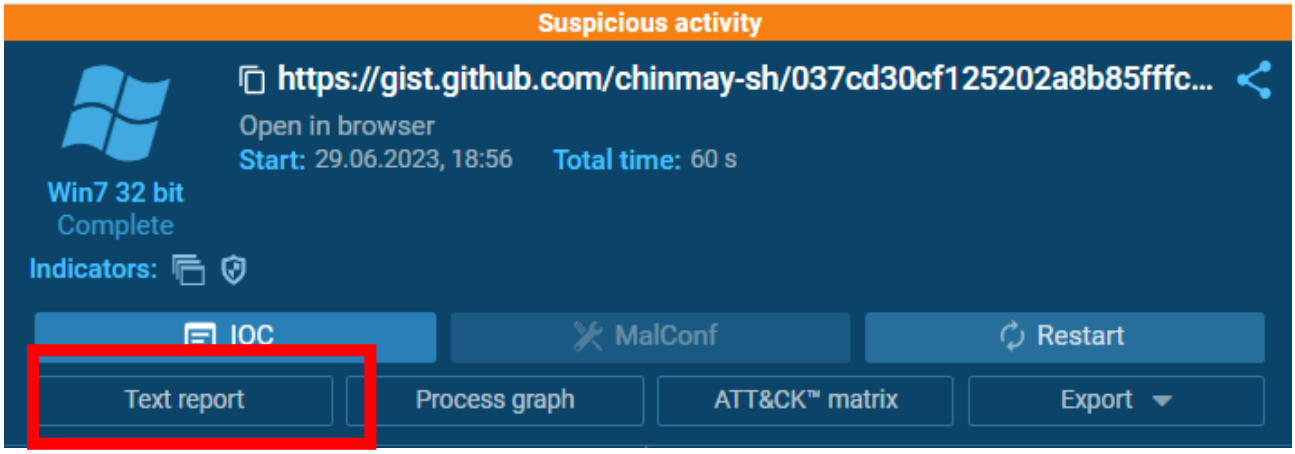
Di seguito un disegno dell'interfaccia di rete proposta in precedenza con l'aggiunta di un **WAF**, posizionato **all'esterno della DMZ, poiché in questo modo agirà come un punto di ingresso aggiuntivo per il traffico in arrivo dall'esterno e filtrerà le potenziali minacce prima che raggiungano la DMZ.**

Questa configurazione può semplificare la gestione del traffico e consentire al WAF di fornire una protezione globale per l'intera infrastruttura, compresa la DMZ e la rete interna



TASK 2 = Analisi di link loschi con conseguente report

LINK LOSCO 1



Dopo aver analizzato il link con il tool Any.run, e dopo aver cliccato su TEXT REPORT, ho iniziato un'analisi di ciò che il primo link losco sta effettuando sulla macchina target.

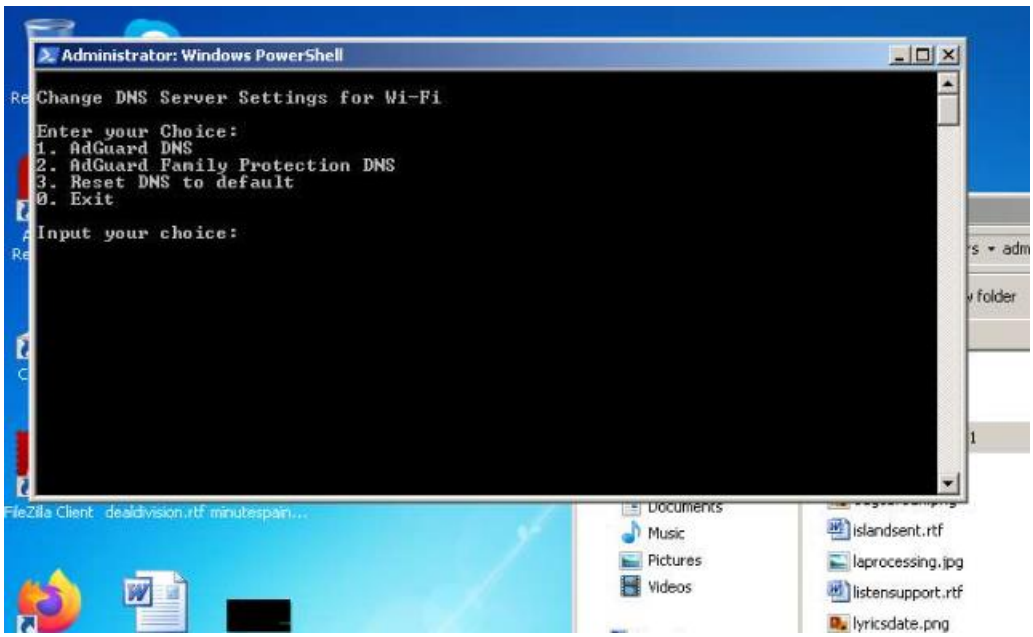
Da una prima analisi, sembrerebbe che il codice incorporato nella macchina abbia come "obiettivo" bypassare le politiche di esecuzione di PowerShell di Windows, influendo altresì sulle impostazioni dei server DNS.

La prima riga del codice verifica se lo script viene eseguito o meno con privilegi di amministratore, e nel caso in cui non lo fosse, **si avvia in automatico un processo di PowerShell con privilegi da amministratore, procedura questa potenzialmente dannosa, poiché vengono totalmente ignorate le policy di Powershell, consentendo all'attaccante di ottenere un accesso non autorizzato con privilegi da amministratore al prompt di Powershell.**


```
Write-Host ""
Write-Host "Change DNS Server Settings for Wi-Fi"
Write-Host ""
Write-Host "Enter your Choice: "
Write-Host "1. AdGuard DNS"
Write-Host "2. AdGuard Family Protection DNS"
Write-Host "3. Reset DNS to default"
Write-Host "0. Exit"
Write-Host ""
$Input = Read-Host -Prompt 'Input your choice'
Write-Host ""
if($Input -eq 1){
   Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.14","94.140.15.15"
   write-host("AdGuard DNS enabled.")
   Start-Sleep -s 1
}elseif($Input -eq 2){
   Set-DnsClientServerAddress -InterfaceAlias wi-fi -ServerAddresses "94.140.14.15","94.140.15.16"
   write-host("AdGuard Family DNS enabled.")
   Start-Sleep -s 1
}elseif($Input -eq 3){
   Set-DnsClientServerAddress -InterfaceAlias wi-fi -ResetServerAddresses
   write-host("DNS Reset")
   Start-Sleep -s 1
}elseif($Input -eq 0){
   Break
}else {
   write-host("Wrong Input")
   Start-Sleep -s 1
   Break
}
```

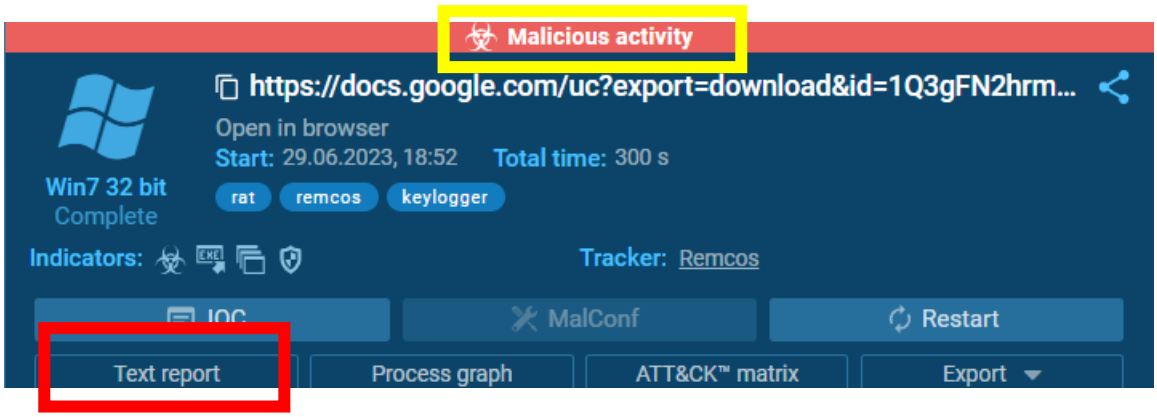
Analizzando lo script, vediamo che esso mostra un menu con diverse opzioni per le impostazioni del server DNS. In input l'utente può selezionare un'opzione inserendo il numero corrispondente (1, 2 o 3)

Se si selezionano in input 1 o 2, lo script cambierà automaticamente gli indirizzi IP di **AdGuard DNS** (con input 1) e **AdGuard Family Protecion** (con input 2). In caso l'input utente sia 3, verranno settati automaticamente i DNS prefefiniti, **il che ci fa presagire che lo script riesce a leggere le impostazioni di connessione a Internet della macchina target.**



LINK LOSCO 2

Any.run presenta fin da subito la potenzialità che il file in esame sia un malware, come indicato dal tool stesso.



Anche in questo caso, per vedere le evidenze ci spostiamo nella pagina **TEXT REPORT**, dove notiamo che è indicata la presenza **del malware REMCOS, un software commerciale di accesso remoto noto come strumento di controllo e sorveglianza dei computer bersaglio**.
Nonostante Remcos sia pubblicizzato come software legittimo per scopi di sorveglianza e pentesting**, è stato utilizzato in diverse campagne di hacking.** Una volta installato, **il malware apre una backdoor sul computer, permettendo a un utente remoto di avere un controllo completo sulla macchina infetta**.

Behavior activities

Add for printi

MALICIOUS

Application was dropped or rewritten from another process
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Starts Visual C# compiler
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Uses Task Scheduler to run other applications
- cmd.exe (PID: 3604)
- cmd.exe (PID: 3200)
- cmd.exe (PID: 2628)
- cmd.exe (PID: 2960)

Remcos is detected
- csc.exe (PID: 3824)

REMCOS detected by memory dumps
- csc.exe (PID: 3824)

SUSPICIOUS

The process creates files with name similar to system file names
- WinRAR.exe (PID: 1944)

Drops a system driver (possible attempt to evade defenses)
- WinRAR.exe (PID: 1944)
- procexp.exe (PID: 3476)

Reads settings of System Certificates
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads security settings of Internet Explorer
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads the Internet Settings
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

Connects to unusual port
- csc.exe (PID: 3824)

Starts CMD.EXE for commands execution
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

INFO

The process uses the downloaded file
- chrome.exe (PID: 2064)
- chrome.exe (PID: 2356)
- chrome.exe (PID: 1140)
- WinRAR.exe (PID: 1944)
- chrome.exe (PID: 3868)
- WinRAR.exe (PID: 3092)
- chrome.exe (PID: 2880)

Application launched itself
- chrome.exe (PID: 3140)

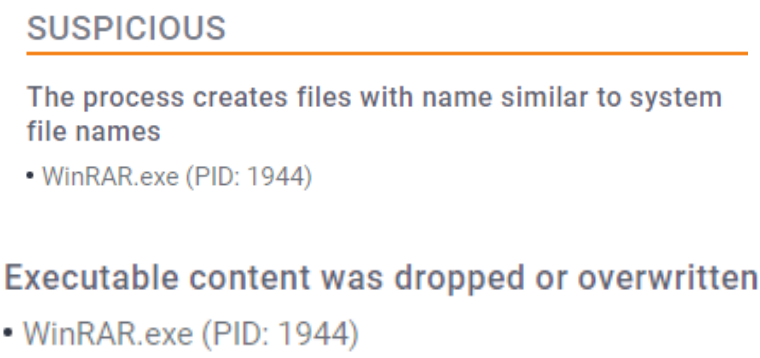
Manual execution by a user
- WinRAR.exe (PID: 1944)
- Autoruns.exe (PID: 4056)
- WinRAR.exe (PID: 3092)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Executable content was dropped or overwritten
- WinRAR.exe (PID: 1944)

The process checks LSA protection
- Autoruns.exe (PID: 4056)

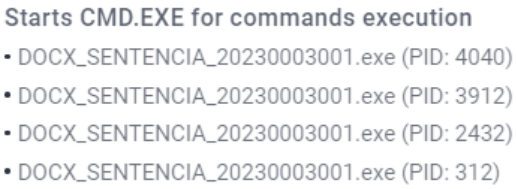
Da un’analisi più approfondita del report si nota che:

- Vengono creati file con nomi che assomigliano a quelli dei file di sistema, **potenzialmente utilizzati per nascondere attività sospette.**

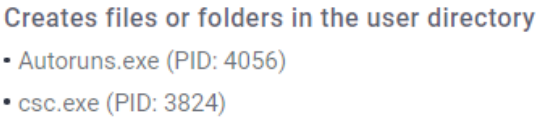


- Viene installato un driver di sistema, **probabilmente** per evitare le misure di sicurezza.

- Vengono **avviati processi CMD.EXE per eseguire comandi**.



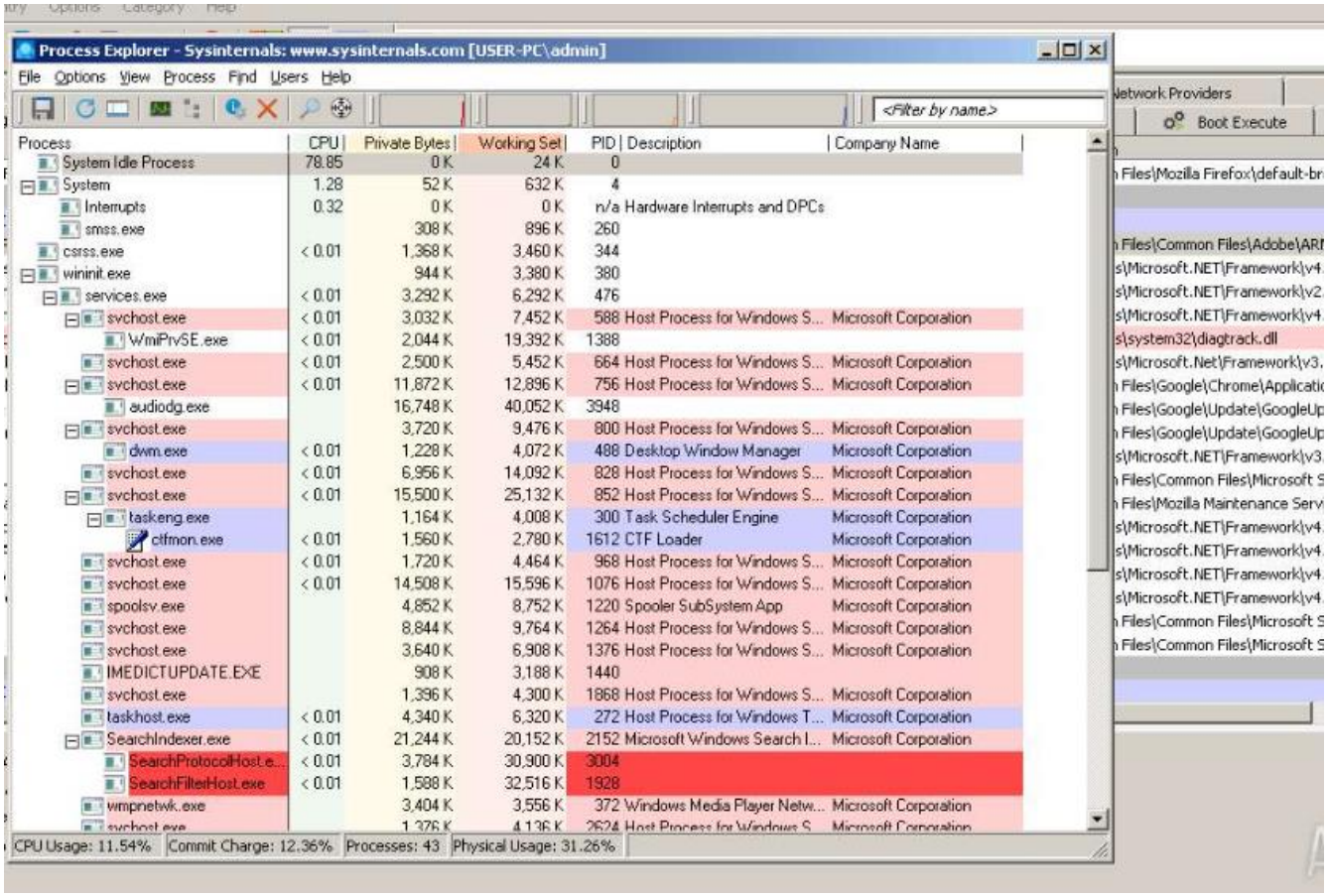
- Vengono **creati file o cartelle nella directory del programma.**



- Vengono scritti file che assomigliano a registri di **keylogger.**

- Vengono eseguiti file scaricati tramite **Chrome e WinRAR.**

- Si può anche osservare dallo screenshot sottostante che **il malware esaminato è molto avanzato**, come **indicato dal numero di processi autonomi che riesce ad eseguire dopo essere stato compilato e avviato.**



In conclusione, possiamo affermare che tra tutte le azioni menzionate, **una delle più pericolose ed invasive risulta essere la creazione di file che assomigliano a registri di un keylogger**. **Ciò fa presagire che il malware stia registrando, ad insaputa dell'utente, le attività di quest'ultimo**. A tal proposito, si segnala che registri di un keylogger possono contenere informazioni sensibili come password, dati finanziari o altre informazioni private e personali.

TASK 3 = Mettere in pratica un **Incident Response,** dopo che un malware ha infettato l'applicazione Web, tenendo presente che il malware non deve propagarsi sulla rete interna, e non deve divulgare informazioni sensibili verso Internet

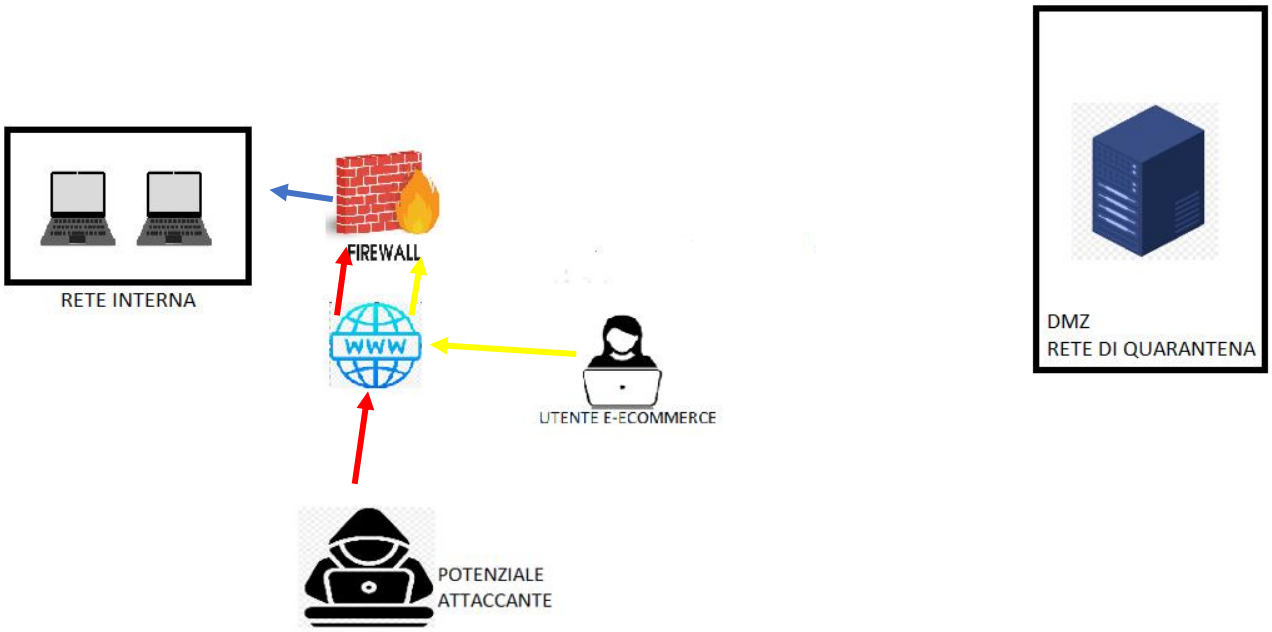
La risposta agli incidenti di sicurezza, nota come **INCIDENT RESPONSE**, segue un processo articolato in diverse fasi:

- Preparazione
- Rilevamento ed analisi
- **Contenimento, eliminazione e recupero**
- Attività post-incidente

Come da traccia, ci concentriamo sulla terza fase del processo di **incident response**, affrontando una situazione in cui un attaccante ha infettato una web application tramite malware. **Il primo passo di questa fase è il contenimento del danno causato dall'incidente, che deve essere effettuato il più rapidamente possibile per evitare la diffusione della minaccia ad altri sistemi e risorse aziendali.**

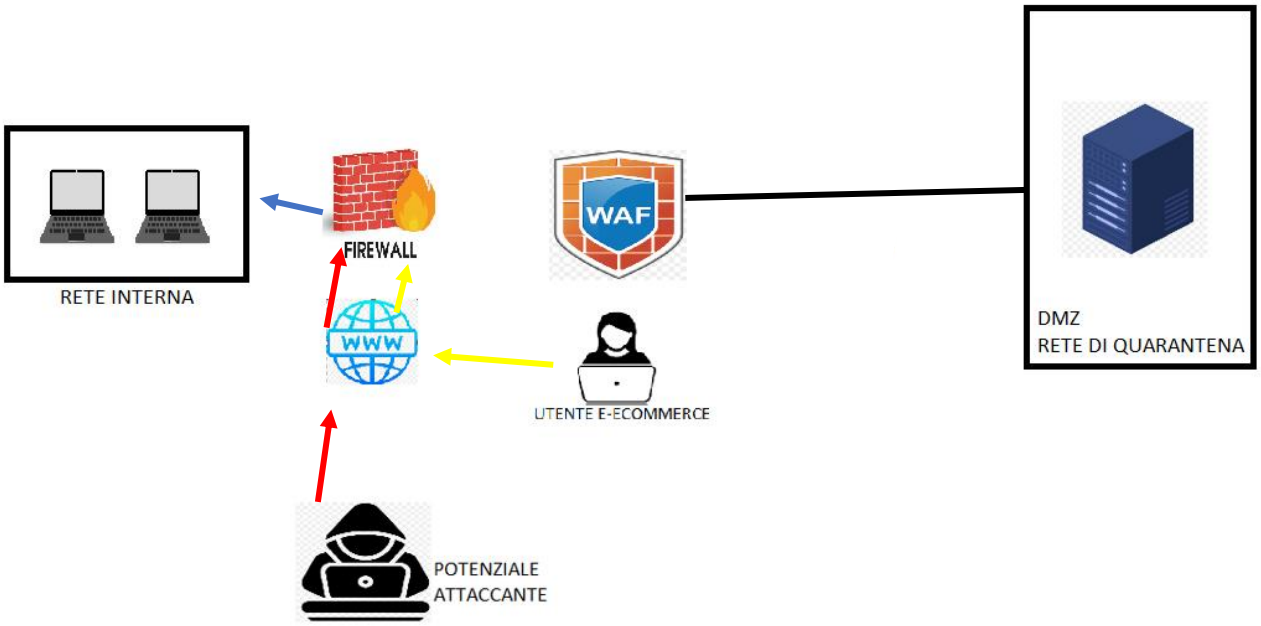
L'obiettivo principale del processo di contenimento è isolare l'incidente, evitando ulteriori danni alle reti e ai sistemi colpiti, **riducendo l'impatto generale dell'incidente**. Le tecniche utilizzate per raggiungere questo obiettivo includono la **segmentazione, l'isolamento e la rimozione.**

Ci sono situazioni in cui l'isolamento non è sufficiente e si richiede una misura di contenimento più rigorosa, che è la completa **RIMOZIONE del sistema dalla rete interna e da Internet**. **In questo scenario, l'attaccante non avrà accesso né alla rete interna né alla macchina infetta**. **Questa strategia estrema viene adottata quando l'attaccante rappresenta una minaccia critica e non si possono rischiare ulteriori compromissioni dei sistemi aziendali. A tal proposito, la rimozione completa del sistema dalla rete garantisce un isolamento totale e protegge l'azienda da ulteriori danni, fornendo una protezione più robusta.**



TASK 4 = **Soluzione completa**

Nell'implementazione proposta, **è stato incluso un WAF** (Web Application Firewall**) per proteggere l'applicazione web da attacchi XSS** (Cross-Site Scripting) e **SQLi** (SQL Injection), ed è stata mantenuta la misura di contenimento della rimozione completa del sistema dalla rete, il che garantisce un isolamento totale e protegge l'azienda da ulteriori danni, fornendo una protezione più robusta

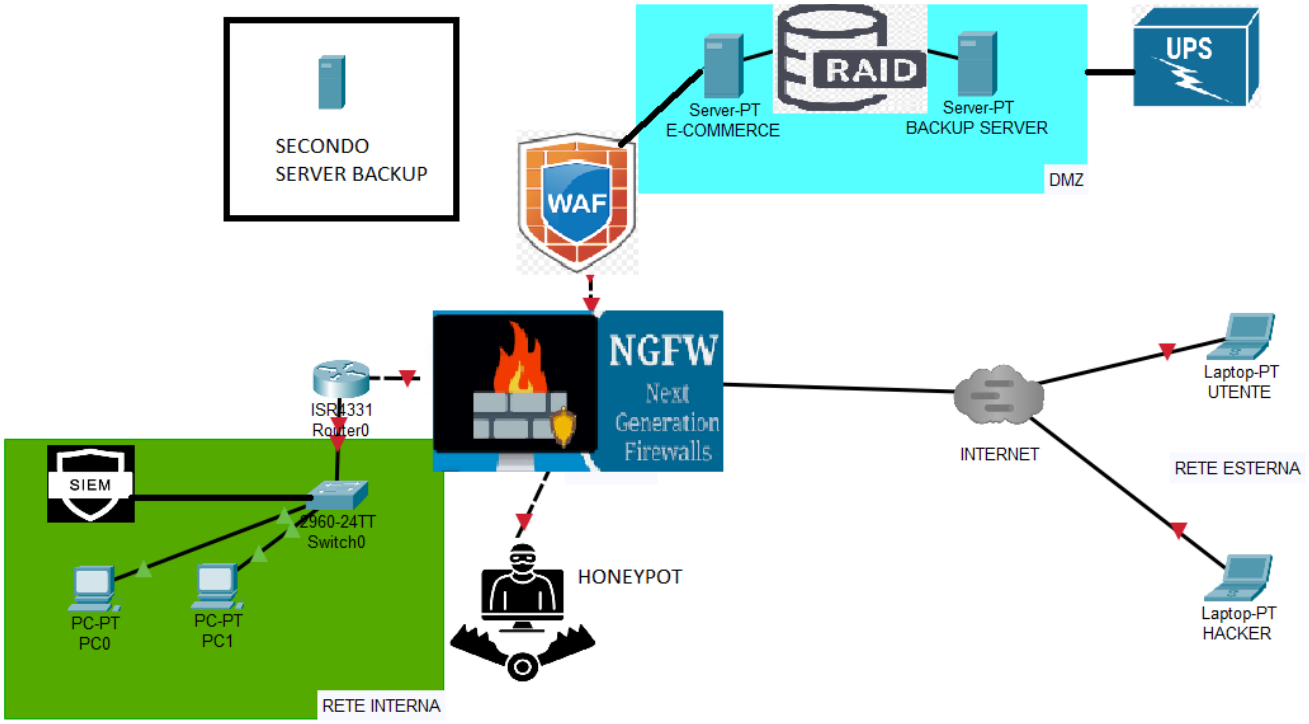


TASK 5 = **Modificare in maniera più aggressiva l'infrastruttura di rete proposta.**

Per modificare in maniera più aggressiva l'infrastruttura di rete, ho aggiunto:

- **NEXT GENERATION FIREWALL (NGFW), che include ancora più funzionalità di analisi rispetto ad un normale firewall, e permette l'analisi dei flussi basati sull'utente che effettua la connessione, sull'applicativo utilizzato ecc... In più, un NGFW, al proprio interno ha integrato un IDS, e tale configurazione semplifica drasticamente la gestione e l'amministrazione della sicurezza, in quanto tutte le funzionalità di protezione sono centralizzate in un'unica soluzione.**
- Nella **DMZ** (Demilitarized Zone) si trovano il **Web Server principale e un Backup Server**, entrambi parte di un meccanismo di **failover cluster**. **Questo significa che i due server condividono un sistema di archiviazione dati, RAID 5, una configurazione comune per il data storage, la quale, in caso di malfunzionamento del Web Server principale, avvia automaticamente il Backup Server come server principale**. In questo modo**, l'infrastruttura è resiliente e in grado di garantire la continuità del servizio anche in caso di attacchi DDoS o problemi tecnici.**
- Un **HONEYPOT** è un dispositivo o un sistema **progettato per simulare una vulnerabilità al fine di attirare e rilevare gli attacchi da parte di potenziali aggressori**. La sua funzione principale è quella di raccogliere informazioni sugli attaccanti, analizzarne i metodi e le tecniche utilizzate. **In pratica, un Honeypot è un'esca che aiuta a studiare il comportamento degli aggressori e a migliorare le misure di sicurezza.**

- **Un UPS, dispositivo che fornisce alimentazione elettrica di emergenza a un sistema o a un'apparecchiatura quando si verifica un'interruzione di corrente**
- **Un SIEM, accentratore di log, un'infrastruttura dedicata alle attività di logging & monitoring.**
- **Infine, un secondo server di backup, nel caso in cui il primo venga rimosso a seguito di un attacco. Ovviamente, il secondo server di backup verrà locato in un'area differente da quella in cui si trovamo server principale e server di backup.**



Con circa 30.000 € si possono limitare i problemi che l'infrastruttura di una rete aziendale potrebbe subire in caso di attacco. Di seguito ogni componente aggiuntivo con relativo costo:

NEXT GEN: 7000 €

WAF: 3000 €

SIEM da 500 € a 2000 €

RAID 5: da 800 € a salire

UPS: il costo varia a seconda del voltaggio (da 800 € a 14.000€)

SERVER DI BACKUP PRIMARIO E SECONDARIO: 10.000 €

HONEYPOT: può variare a seconda di diversi fattori, tra cui la complessità del sistema, funzionalità, ecc…