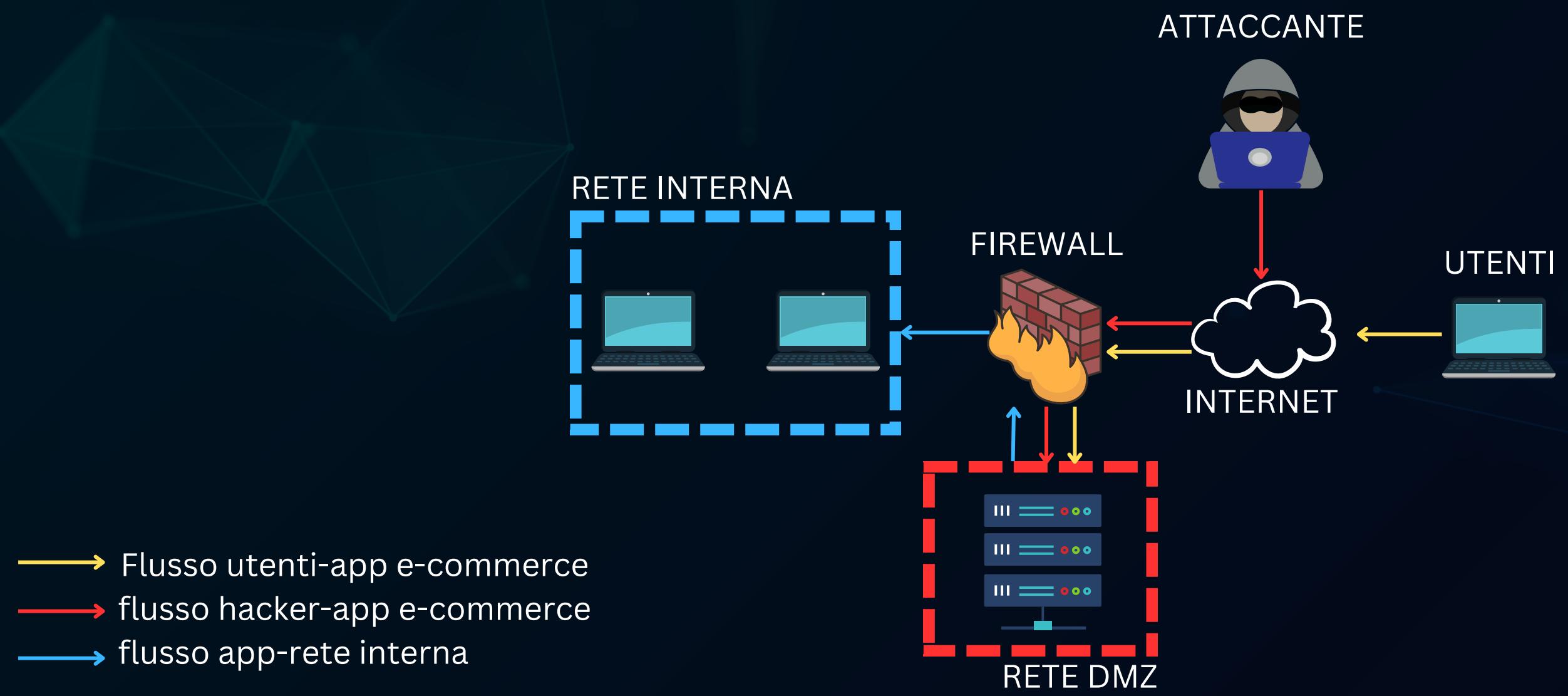


# REPORT

## S9-L5

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.

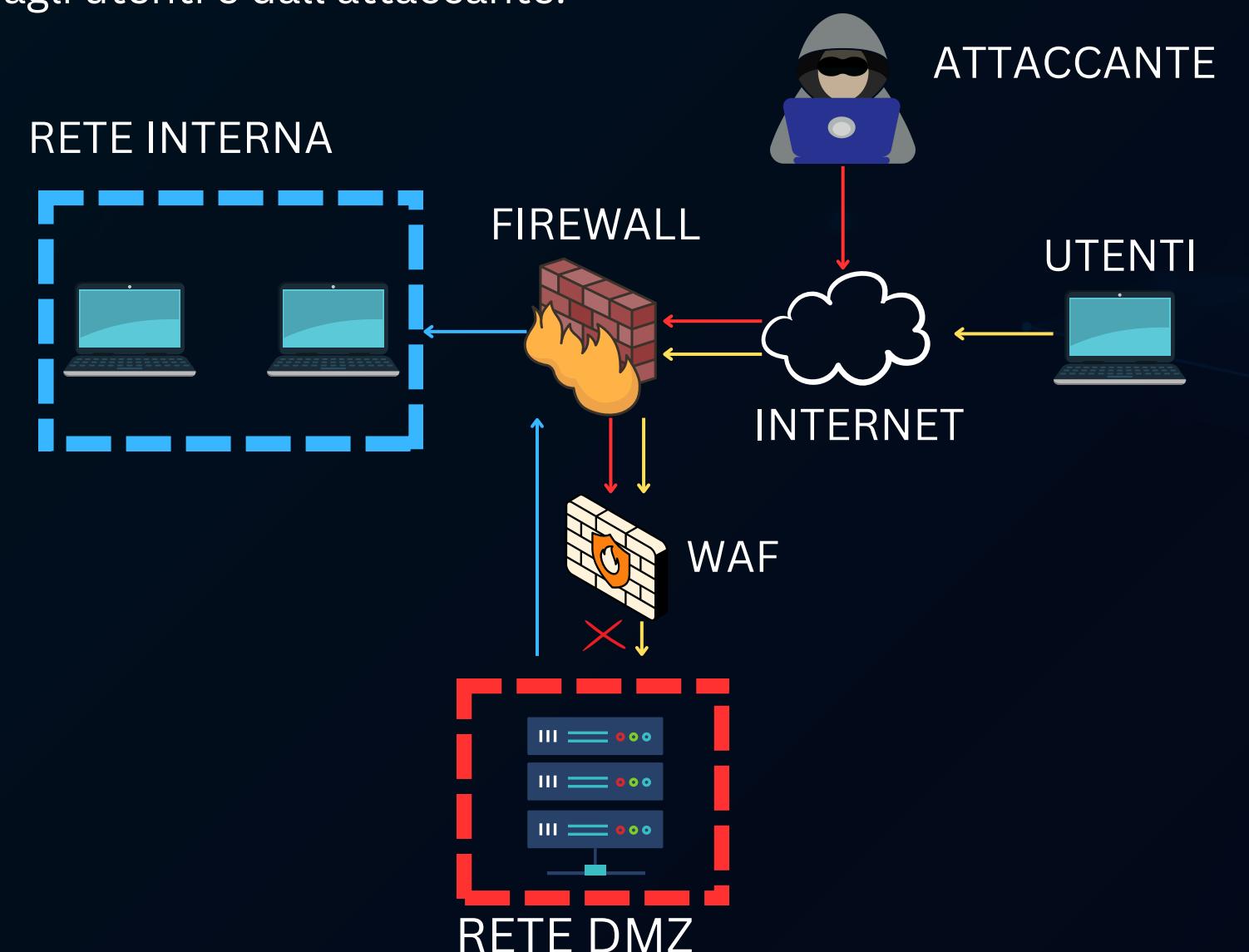


## 1-Azioni preventive

Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

Per prevenire attacchi di tipo SQLi o XSS esistono diverse misure di sicurezza tra cui:

- Effettuare regolarmente dei test di penetrazione per individuare eventuali vulnerabilità nel codice e nell'infrastruttura.
- Utilizzare strumenti di analisi statica del codice per identificare potenziali vulnerabilità nel codice sorgente.
- Implementare un WAF (Web Application Server) per filtrare e bloccare le richieste HTTP dannose, come quelle contenenti payload SQLi o XSS. In questo caso si è optato per questa soluzione dal momento che era richiesta una sola modifica, il WAF protegge la Web App dal traffico in entrata da internet, cioè dagli utenti e dall'attaccante.



## 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 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

DDoS sta per Distributed Denial of Service. In pratica, è come se un sito web venisse bombardato da un'enorme quantità di traffico proveniente da molte fonti diverse, tutte contemporaneamente, provocando agli utenti legittimi l'impossibilità di accedere a un sito web o a un servizio online e causando perdite finanziarie all'azienda a causa dell'inattività del servizio.

In questo esempio dal momento che gli utenti spendono 1.200€ ogni minuto, si può stimare il mancato guadagno del business moltiplicando la spesa potenziale degli utenti al minuto per i minuti di indisponibilità del servizio, quindi:

$$\text{Impatto sul business} = 1.200\text{€} \times 10 \text{ minuti} = 12.000\text{€}$$

L'azienda per soli 10 minuti di inattività perderebbe 12.000€.

### AZIONI PREVENTIVE:

- Molti provider cloud offrono servizi specifici per mitigare gli attacchi DDoS, che monitorano costantemente il traffico e deviano il traffico malevolo.
- Configurare correttamente il Firewall e creare regole personalizzate per identificare e bloccare i pattern di attacco DDoS comuni.
- Monitorare costantemente il traffico di rete per individuare picchi improvvisi o modelli insoliti che potrebbero indicare un attacco.
- Configurare sistemi di allarme per essere avvisati immediatamente in caso di sospette attività (IPS/IDS/SIEM).

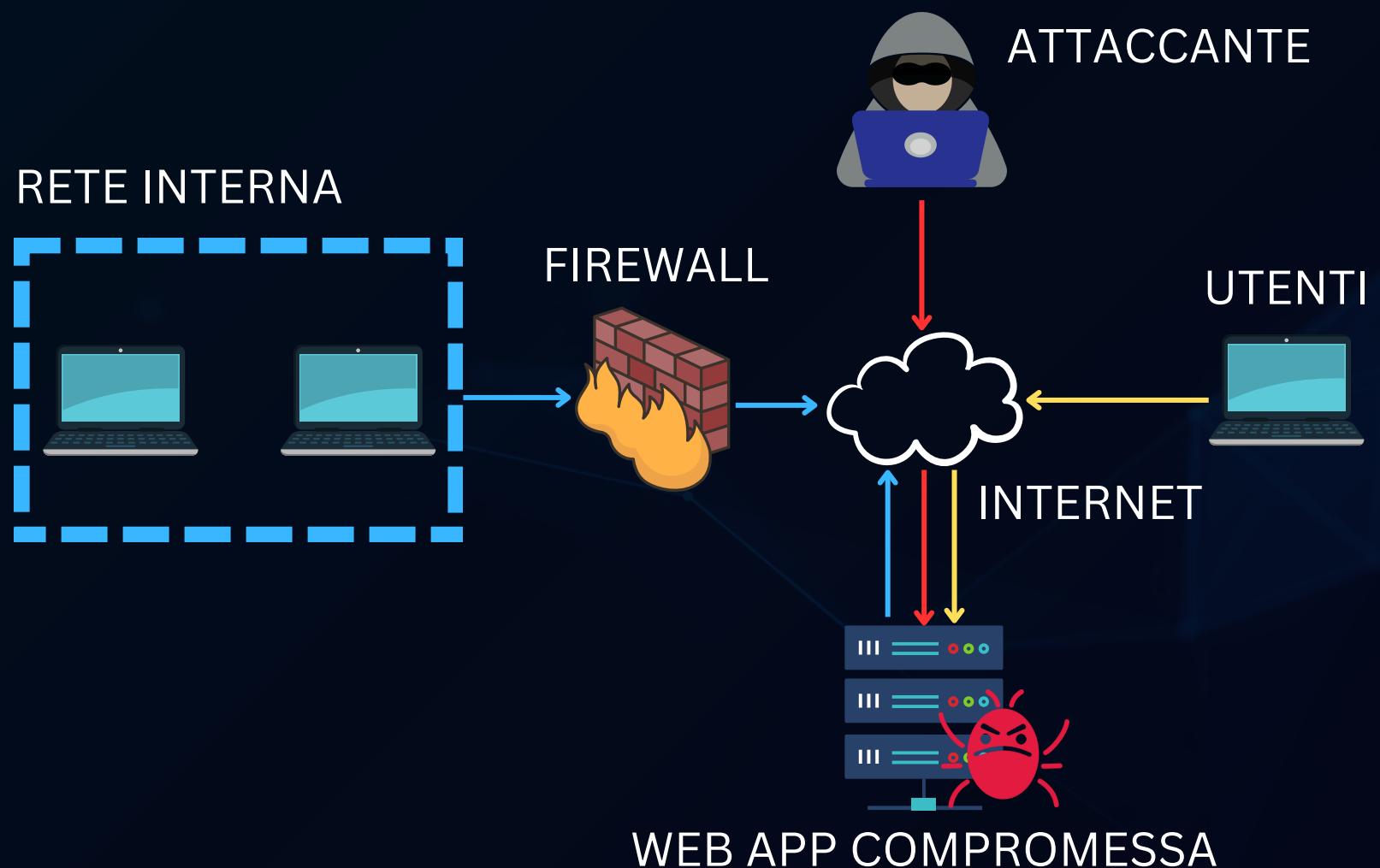
### 3-Response

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.

La prima azione da intraprendere è quella di isolare immediatamente la macchina infetta dalla rete. Questo impedirà al malware di diffondersi ad altri dispositivi o server. La web app è comunque connessa ad internet e l'attaccante ne ha accesso ma ora per l'attaccante sarà molto più difficile penetrare nella rete interna visto che si trova su una rete completamente differente, in questo caso le policy del firewall verranno cambiate rispetto all'esempio precedente, quindi anche se l'attaccante infetterà la Web App sarà molto difficile penetrare fino alla rete interna(figura sotto).

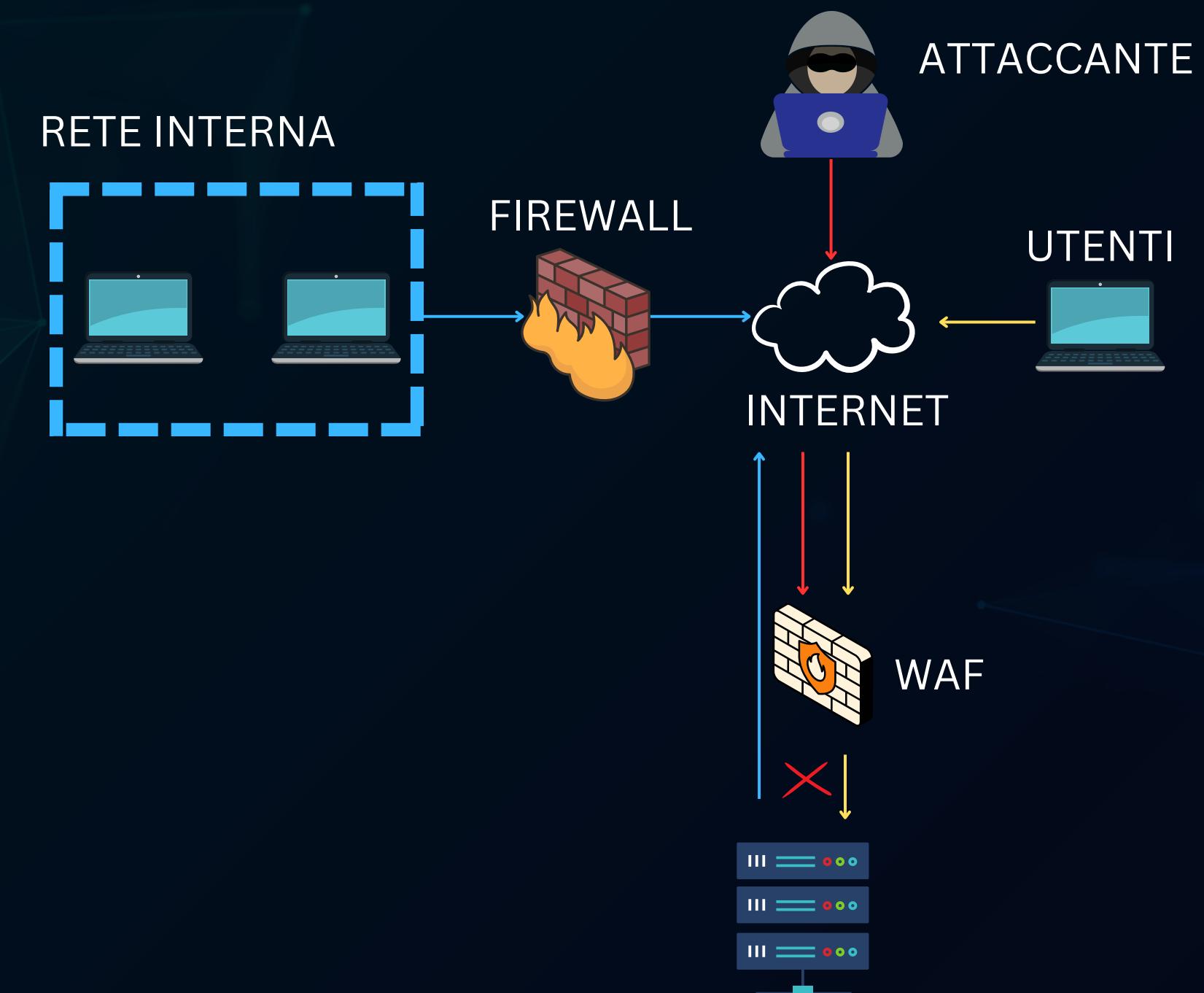
Possibili soluzioni aggiuntive in caso di compromissione della rete:

- Utilizzare strumenti di analisi malware per identificare il tipo di minaccia, il suo punto di ingresso e le sue modalità di diffusione.
- Disabilitare le funzionalità dell'applicazione web che potrebbero essere state compromesse dal malware.
- Limitare l'accesso all'applicazione web solo agli utenti autorizzati e necessari per le indagini.
- Implementare un sistema IDS per monitorare costantemente la rete e rilevare eventuali attività sospette.
- Analizzare i log di sistema e di applicazione per identificare eventuali anomalie o tentativi di accesso non autorizzato.
- Pianificare la rimozione del malware dalla macchina infetta e ripristinare da un backup pulito.
- Applicare tutte le patch di sicurezza disponibili per il sistema operativo, le applicazioni e i servizi utilizzati.
- Rivedere e rafforzare le misure di sicurezza per prevenire future intrusioni.



### 3-Soluzione completa

La web app dell'e-commerce è stata isolata su una rete separata così se dovesse essere attaccata sarà molto più difficile risalire alla rete interna e a protezione di essa è stato inserito un WAF per bloccare attacchi di SQLi o XSS



## 5-Esempio di modifica dell'infrastruttura

### WAF ALTE PRESTAZIONI (AD ESEMPIO AWS)

Costo di ACL Web = 5,00 USD \* 3 = 15,00 USD

Costi della regola = 1,00 USD \* (3 gruppi di regole gestite + 21 regole) = 24,00 USD

Costi delle richieste = 0,60 USD/milione \* 35 milioni = 21,00 USD

Costi totali di WAF = 60,00 USD/mese

Costi del Bot Control = 10,00 USD \* 3 = 30,00 USD

Costi delle richieste di Bot Control = 10,00 USD/milione \* (35 milioni di richieste - 1 milione di richieste gratuite) = 340,00 USD

Costi totali del Bot Control = 370,00 USD/mese

Costi totali combinati = 430,00 USD/mese

### WAF MEDIE PRESTAZIONI (AD ESEMPIO CLOUDFLARE)

Costi piano business Cloudflare con CDN, DNS, protezione DDoS, WAF, supporto = 200,00 USD/mese

### IPS

Costo IPS = ~ 5000 USD

### GRUPPO DI CONTINUITÀ'

Costo gruppo di continuità = ~ 1500 USD

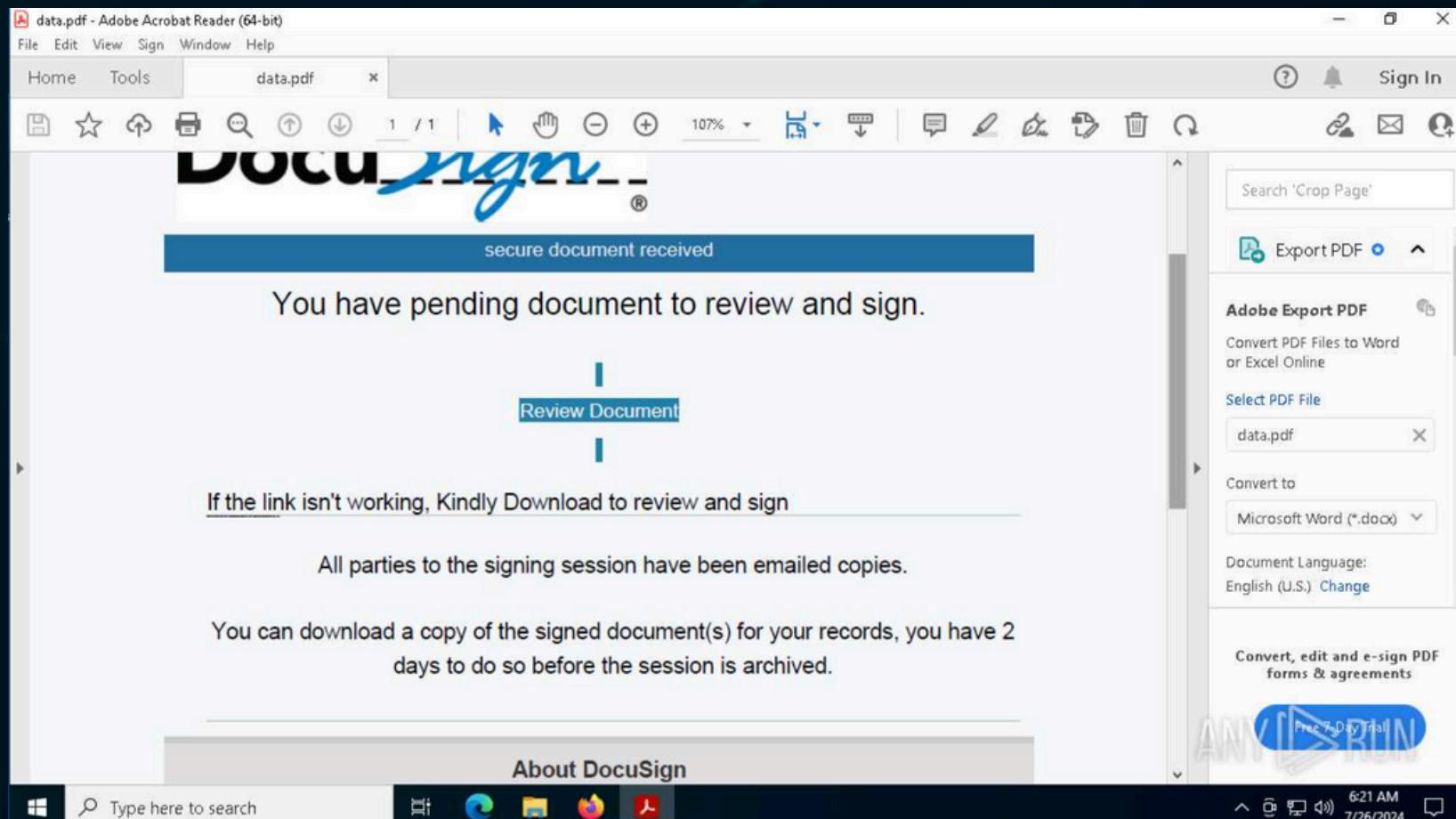
Soluzione migliore = IPS + WAF AWS + BOT CONTROL + GRUPPO CONTINUITÀ' = ~11.000 USD

Soluzione media = IPS + WAF Cloudflare + GRUPPO CONTINUITÀ' = ~7.000 USD



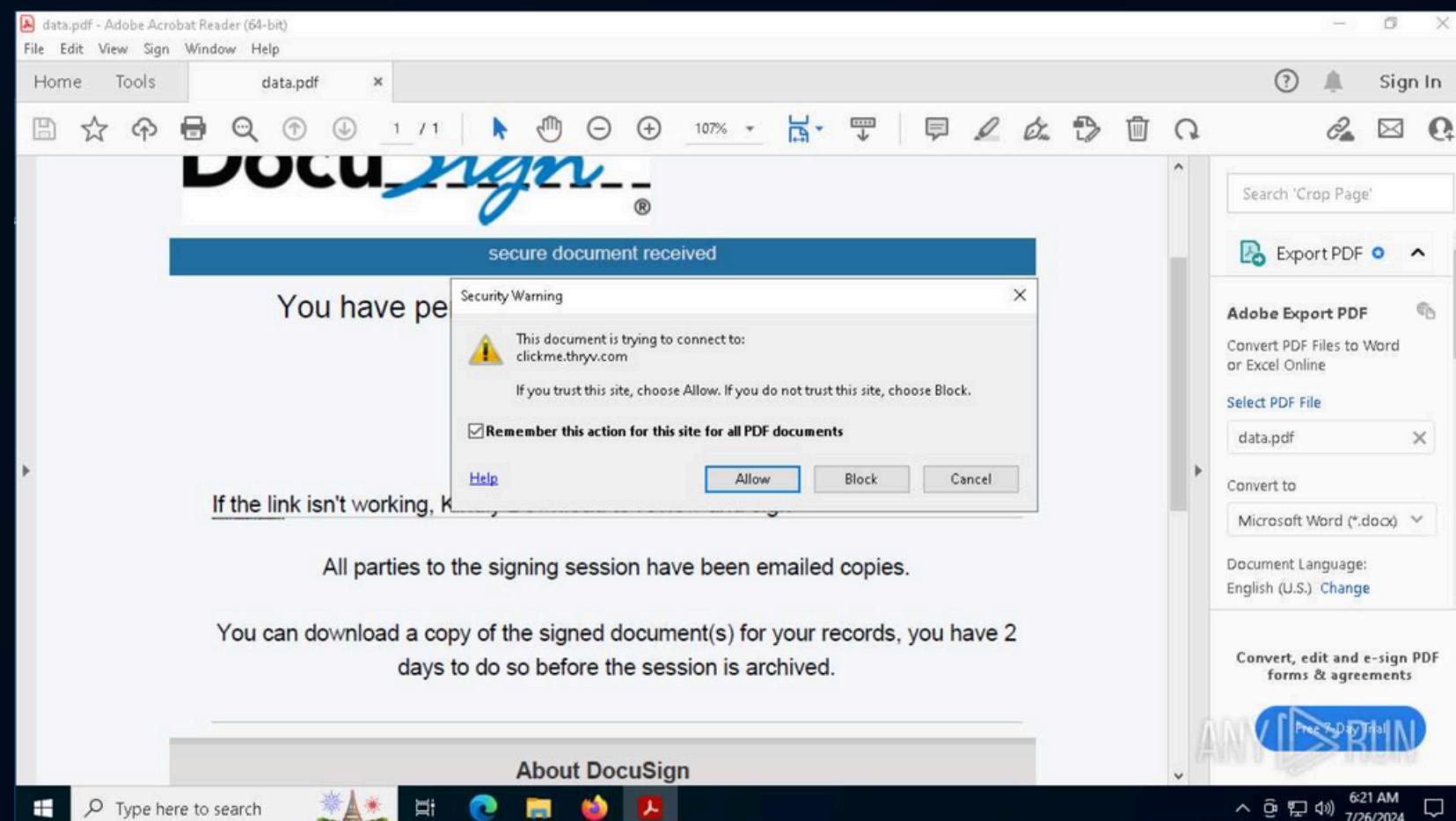
## Analisi del log

<https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6/>



Il file data.pdf si presenta all'apparenza un semplice foglio pdf ma in realtà ricade nella tipologia di attacchi phishing e generated-doc

Il file proverà a stabilire connessioni ad indirizzi IP malevoli e modificherà chiavi di registro Microsoft Office lanciando nuovi processi in automatico



## Connessione a domini e indirizzi IP potenzialmente dannosi



Advanced details of process [6268] Acrobat.exe C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe

Main information

Code signing	Expired
Process dump	0

Events

Modified files	1
Registry changes	12
Synchronization	35
HTTP requests	0
Connections	1
Network threats	0
Modules	119
Debug	0

Put the slider in the desired position or select the desired segment by yourself ?

9.162 s +19.15 s

Time	Type	Rep	CN	Src IP	Port	Dst IP	Port	ASN
+19157 ms	TCP	✓	NL	2.19.11.122	443	VM	49911	Elisa Oyj

## Cambiamento di chiavi di registro e creazione nuovi processi

Advanced details of process [6268] Acrobat.exe C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe

Main information

Code signing	Expired
Process dump	0

Events

Modified files	1
Registry changes	12
Synchronization	35
HTTP requests	0
Connections	1
Network threats	0
Modules	119
Debug	0

Put the slider in the desired position or select the desired segment by yourself ?

9.162 s +163 ms

Time	Operation	Name	Key and value
+163 ms	Write	DisplayName	HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15 934 Adobe Acrobat Reader Protected Mode
+7898 ms	Delete Value	ProductInfoCache	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AdobeViewer (value not set)
+10590 ms	Write	ProxyBypass	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+10590 ms	Write	IntranetName	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1

Verdetto



## Analisi del log

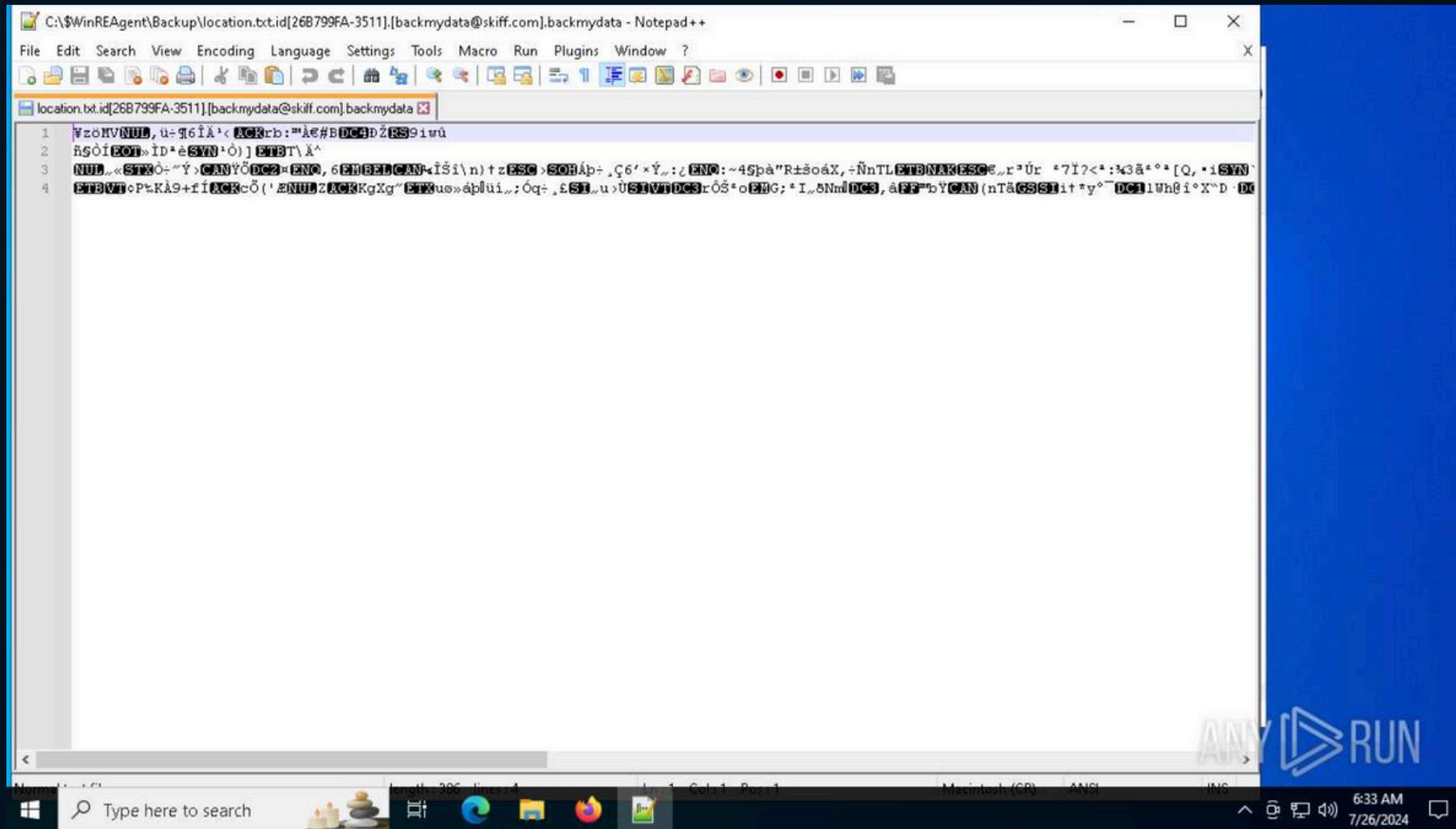
<https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2/>

L'attacco in questione si tratta di un ransomware. E' un tipo di malware, ovvero un software dannoso, che prende in ostaggio i dati o un dispositivo. In pratica, "sequestra" i file, criptandoli in modo da renderli illeggibili, oppure blocca l'accesso al computer o a parti di esso. In particolare il ransomware in questione è Phobos che critta i file presenti su un computer, rendendoli inaccessibili. Chiede quindi un riscatto in cambio della chiave di decrittazione. Questo tipo di ransomware è particolarmente pericoloso perché si diffonde rapidamente e può causare gravi danni ai dati.

The screenshot shows the Any.Run interface for analyzing a process. At the top left, it says "Process details ID 4432 Malicious" and lists the file path "396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe". Below this, it shows the "Username: admin", "Start: +0ms", and "Indicators: 5". The "Command line" field contains the same file path. A large red circle with the number "100 OUT OF 100" is prominently displayed in the center. To the right of the score, the word "Verdetto" is written with a red arrow pointing to the score. On the right side of the interface, there is a summary: "Il programma si avvia da solo e cambia delle variabili nei registri di sistema". Below this, under the heading "Danger 2", are two items: "T1547.001 Registry Run Keys / Startup Folder (1)" and "Changes the autorun value in the registry". Under the heading "Warning 1", there is one item: "Drops the executable file immediately after the start". Red arrows point from the text "Changes the autorun value in the registry" and "Drops the executable file immediately after the start" to their respective entries in the "Danger 2" section. At the bottom right of the interface, the number "09" is visible.

## Alcuni screen del comportamento del ransomware

Crittografia dei dati



Cambio permessi di accesso

