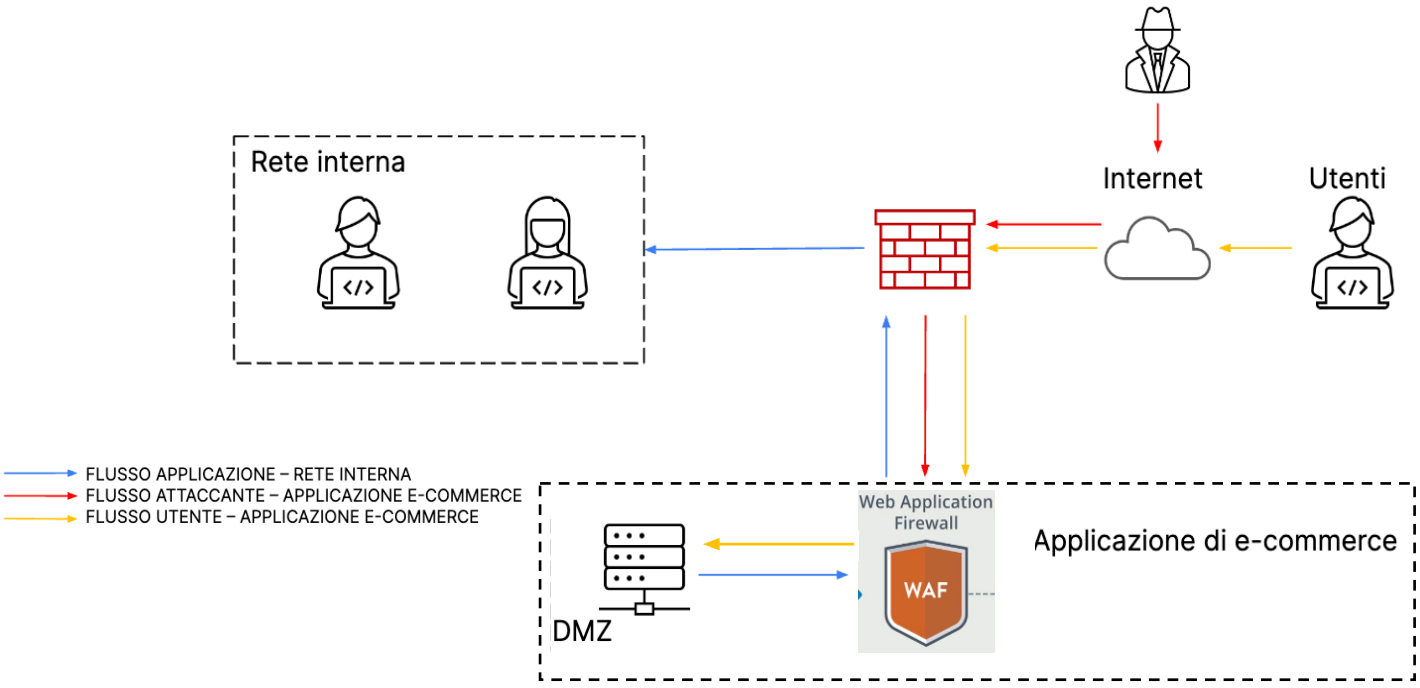
Edoardo Ceriani

ANALISI DEI LOG - CASO REALE

1. AZIONI PREVENTIVE

Per difendere l'applicazione web da attacchi di tipo SQLi o XSS da parte di un utente malintenzionato, si potrebbero implementare nel codice del sito web dei controlli su ciò che l'utente può inserire, così da evitare l'inserimento di codice malevolo, di eventuali script o, in casi estremi, di shell maligne per ottenere l'accesso al nostro sistema.
A livello di infrastruttura di rete, invece, si potrebbe aggiungere un **WAF**, Web Application Firewall, che rappresenta un dispositivo di sicurezza per proteggere le applicazioni proprio da attacchi SQLi e XSS.

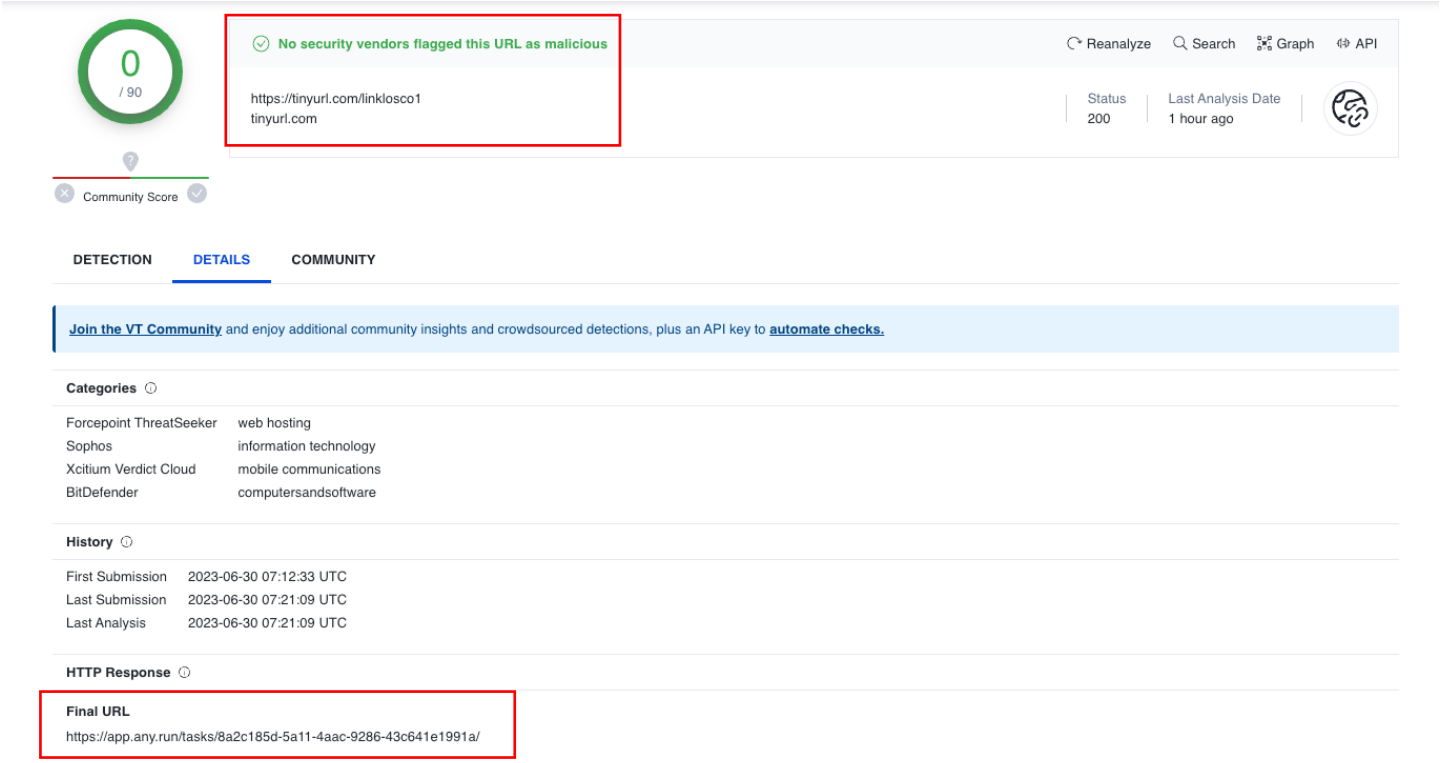
L'implementazione di tale dispositivo è raffigurata nell'immagine sottostante.



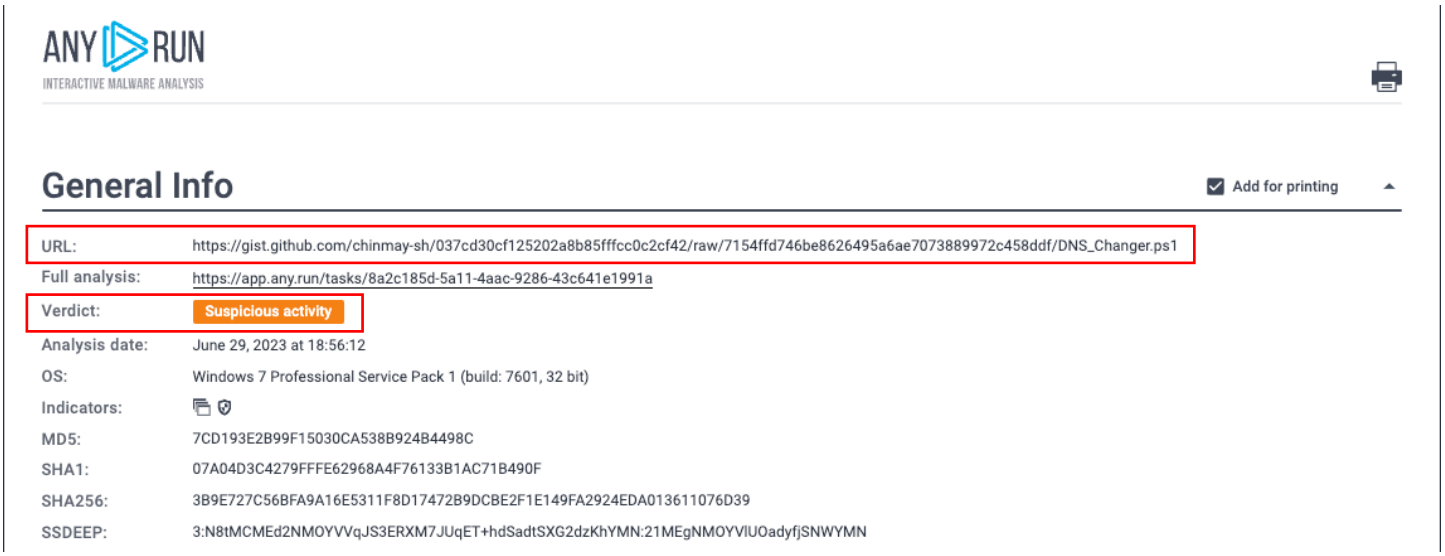
2. ANALISI ATTACCO

Analisi del link https://tinyurl.com/linklosco1:
Leggendo il link in questione, noto che si tratta di un tinyurl. Tinyurl è un servizio web che permette di convertire lunghi indirizzi web in brevi URL, così da permettere a possibili attaccanti di nascondere il vero indirizzo in uno meno "visibile".

Successivamente eseguo un'analisi del link tramite virustotal, noto sito web per l'analisi di file o url sospetti.



Da questa analisi non sembrerebbe niente di maligno, però riesco a risalire all'indirizzo originale e quindi passo ad analizzare quello. Noto che si tratta di link che riporta ad any run, servizio online che funge da sandbox per l'analisi interattiva di malware.



Raggiungo quindi il sito e vedo che in realtà il link sospetto è un link che riporta ad un codice su github che dal nome sembra che cambi i DNS. AnyRun, inoltre, lo classifica come "suspicious activity".

Continuando con l'analisi del report generato da AnyRun, si possono notare le attività svolte da questo codice, come il superamento delle policy di esecuzione per eseguire i comandi, l'esecuzione di script con Powershell, la lettura delle impostazioni di internet e altre attività riportate in figura.

Behavior activities

Add

MALICIOUS

Bypass execution policy to execute commands
- powershell.exe (PID: 3300)

SUSPICIOUS

The process executes Powershell scripts
- powershell.exe (PID: 2272)

The process bypasses the loading of PowerShell profile settings
- powershell.exe (PID: 2272)

Reads the Internet Settings
- powershell.exe (PID: 2272)
- powershell.exe (PID: 3300)

Application launched itself
- powershell.exe (PID: 2272)

Using PowerShell to operate with local accounts
- powershell.exe (PID: 3300)

Starts POWERSHELL.EXE for commands execution
- powershell.exe (PID: 2272)

INFO

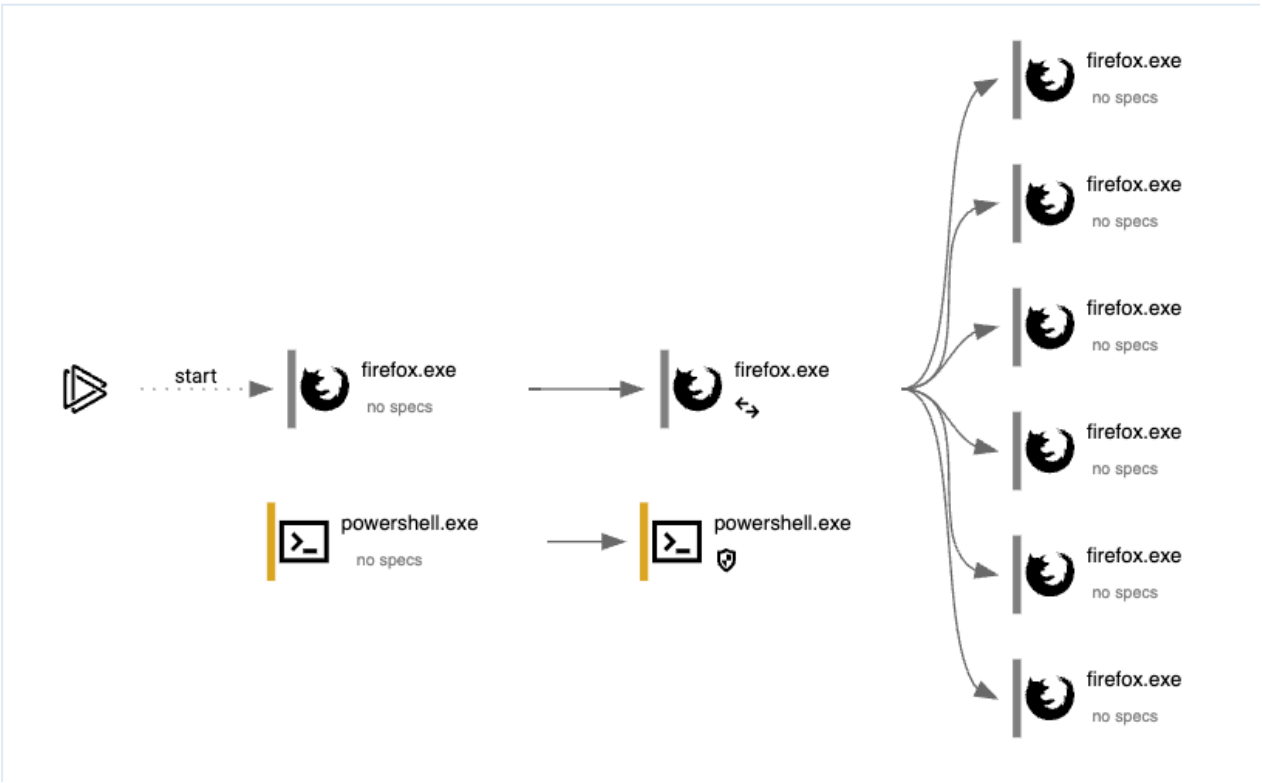
Application launched itself
- firefox.exe (PID: 2976)
- firefox.exe (PID: 3384)

The process uses the downloaded file
- powershell.exe (PID: 2272)
- firefox.exe (PID: 3384)

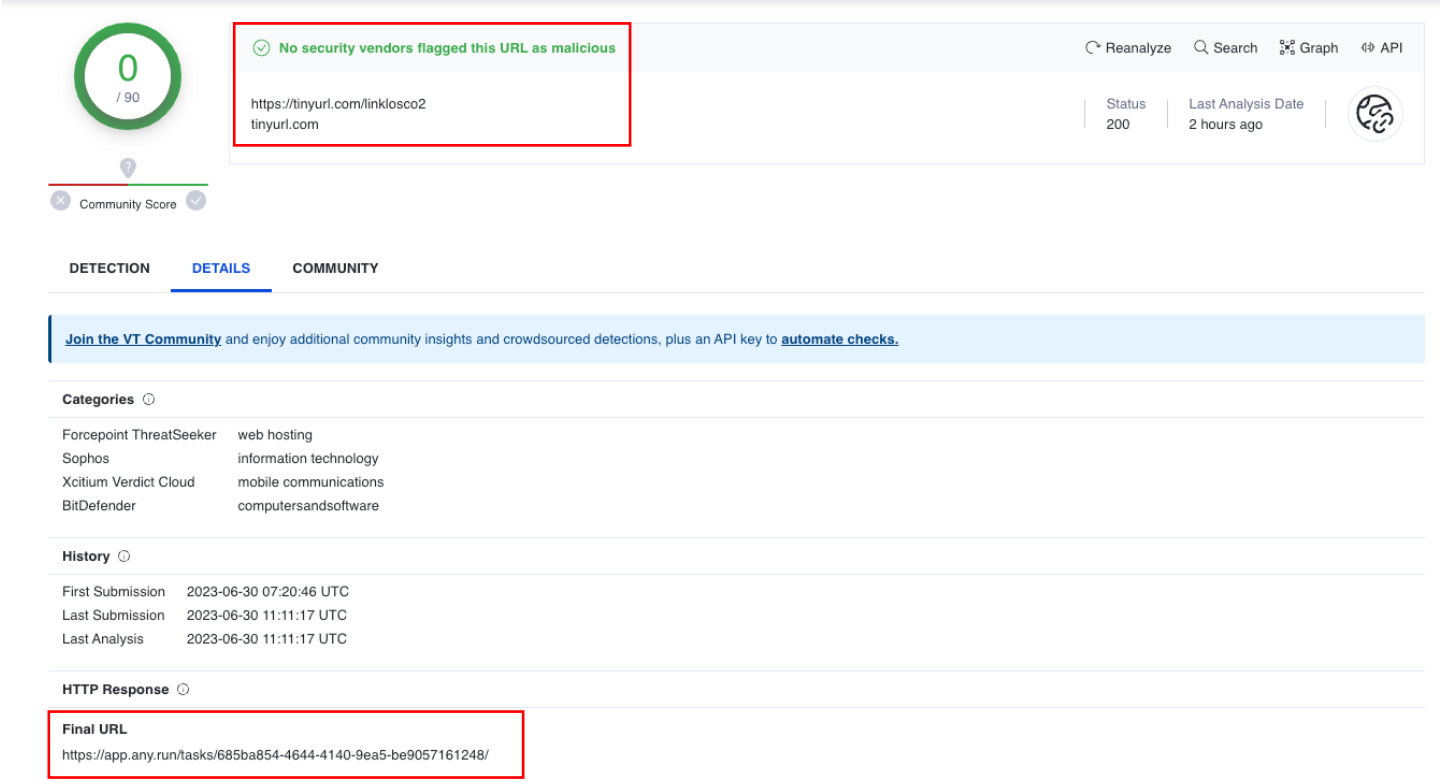
Manual execution by a user
- powershell.exe (PID: 2272)

Dal report, inoltre, si può notare il grafico del comportamento del codice per capire meglio il suo funzionamento.

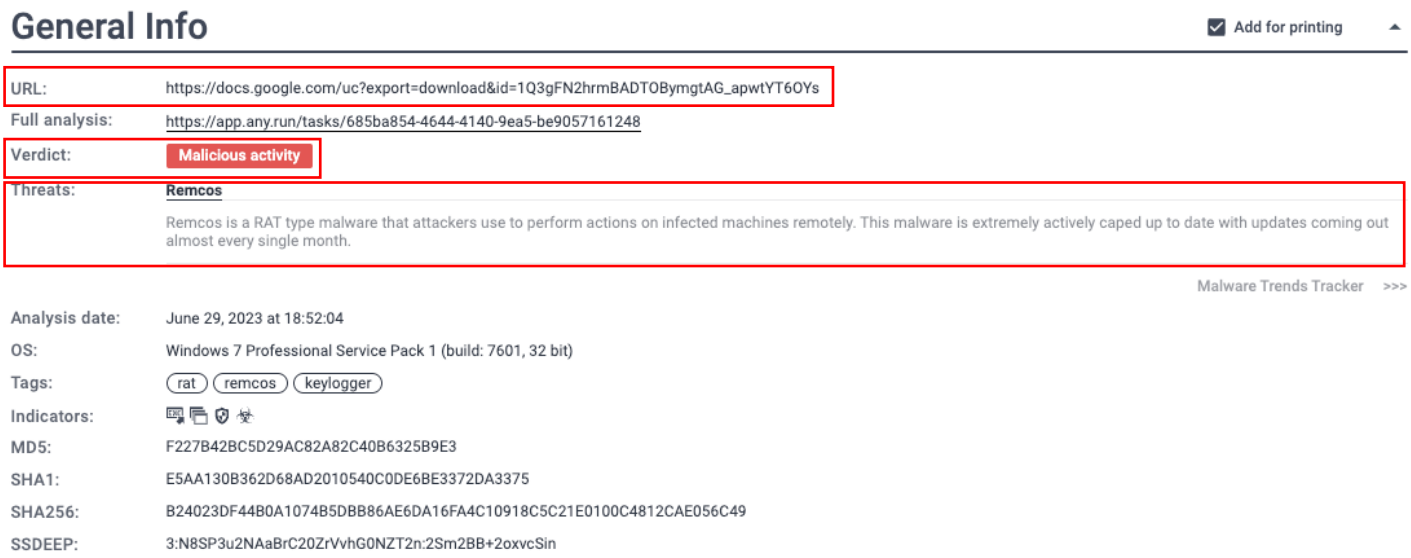
Behavior graph



Analisi del link https://tinyurl.com/linklosco2:
Come nel caso del link precedente, si tratta di un tinyurl. Eseguo quindi l'analisi con virustotal per risalire all'indirizzo originale.



Recuperato l'indirizzo originale, noto, anche questa volta, che rimanda ad AnyRun. Raggiungo quindi il sito per capire meglio cosa nasconde questo link losco2.



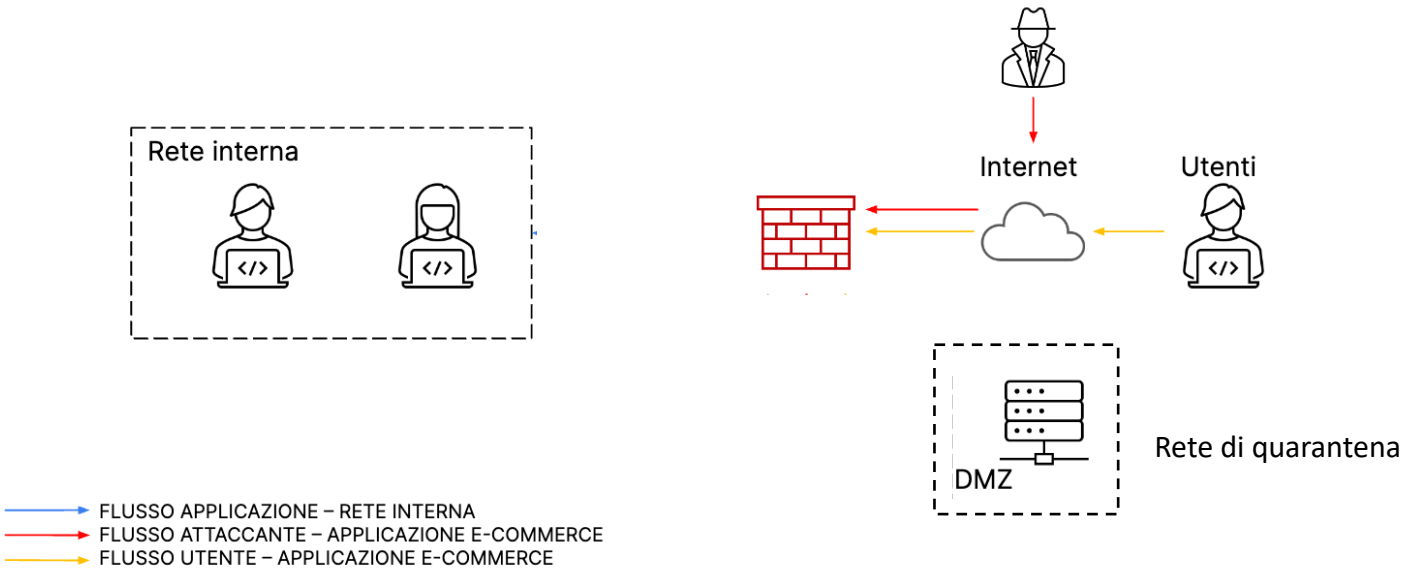
Dal report generato da AnyRun, si può notare che viene classificato come "malicious activity" e l'url rimanda ad un documento di Google da scaricare, probabilmente infetto.

Inoltre, viene identificata la minaccia in questione: **remcos**. Si tratta di un trojan apparso per la prima volta nel giugno 2016. Nello specifico è un malware di tipo RAT (remote access trojan) che gli aggressori utilizzano per eseguire azioni su macchine infette da remoto. Questo malware è aggiornato in modo estremamente attivo con aggiornamenti in uscita quasi ogni mese.

3. RESPONSE

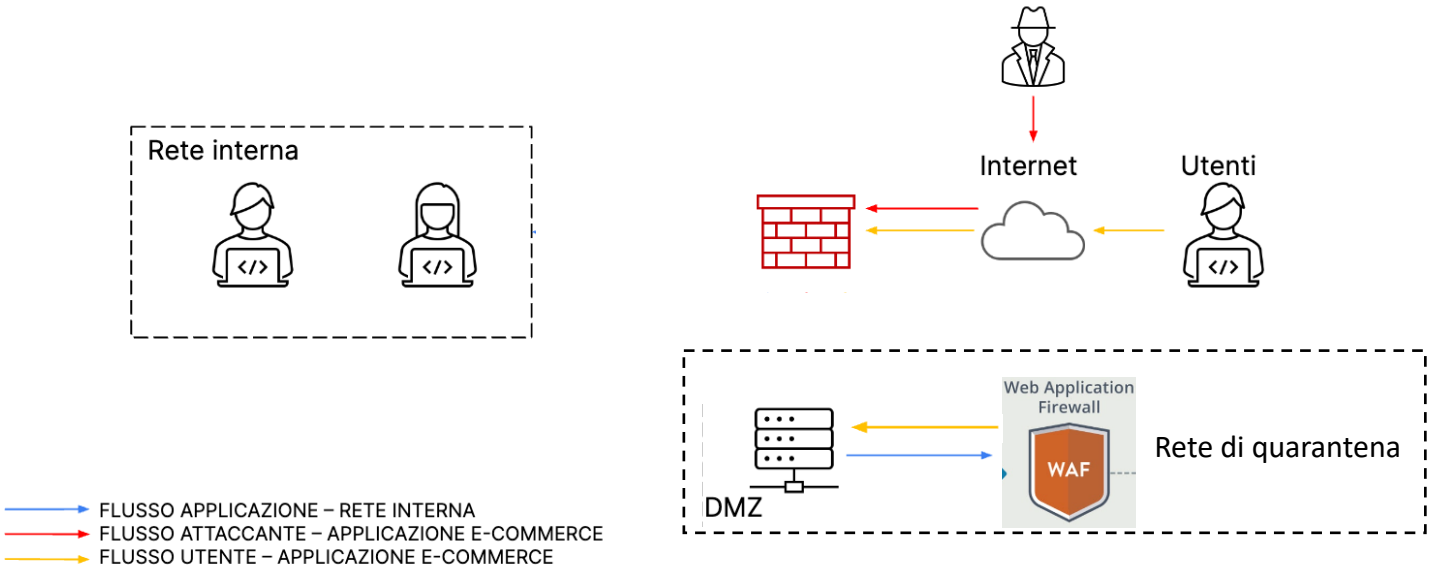
L'applicazione web è stata infettata da un malware.

La figura sottostante rappresenta una tecnica di contenimento per far sì che il malware non si propaghi sulla rete interna e che non vengano divulgate informazioni sensibili verso internet, rimuovendo così il sistema infetto sia dalla rete interna sia da internet.



4. SOLUZIONE COMPLETA

La figura sottostante rappresenta l'unione della soluzione al punto 1 e 3.



5. MODIFICA PIÙ AGGRESSIVA DELL'INFRASTRUTTURA

Per voler aumentare maggiormente la sicurezza dell'azienda e potendo disporre di un buon budget per tale scopo, si potrebbero aggiungere all'infrastruttura di rete alcuni dispostivi quali:

- **NGFW**: Next Generation Firewall, sostituzione del firewall tradizionale con uno di nuova generazione. Questo combina la tecnologia di quello tradizionale con altre funzioni di filtraggio dei dispositivi di rete per migliorare a sicurezza della rete aziendale, come il controllo inline delle applicazioni, un sistema integrato di prevenzione delle intrusioni (IPS), funzionalità di prevenzione delle minacce e protezione antivirus. Effettua una analisi su tutti i livelli della pila ISO/OSI, fino al livello 7.
- **UPS**: Uninterruptible Power Supply, apparecchiatura elettrica utilizzata per ovviare a repentine anomalie nella fornitura di energia elettrica. Consente di continuare a lavorare anche in caso di disservizi sulla linea elettrica.
- **Server di backup**: aggiunta di un secondo server per l'applicazione web così da evitare un disservizio come nel caso del punto 3. Se infatti il server principale venisse colpito da un malware, si potrebbe garantire il corretto funzionamento dell'applicazione web con il server di backup e intanto andare ad isolare il server infetto (come al punto 3).
- **NAS**: Network Attached Storage, offre un'archiviazione centralizzata in rete in cui memorizzare i dati. Utile per programmare ed effettuare backup per garantire la corretta disponibilità dei dati.