

# TRACCIA VENERDI

BY  
DATADEFENDERS





# CONTENTUTI

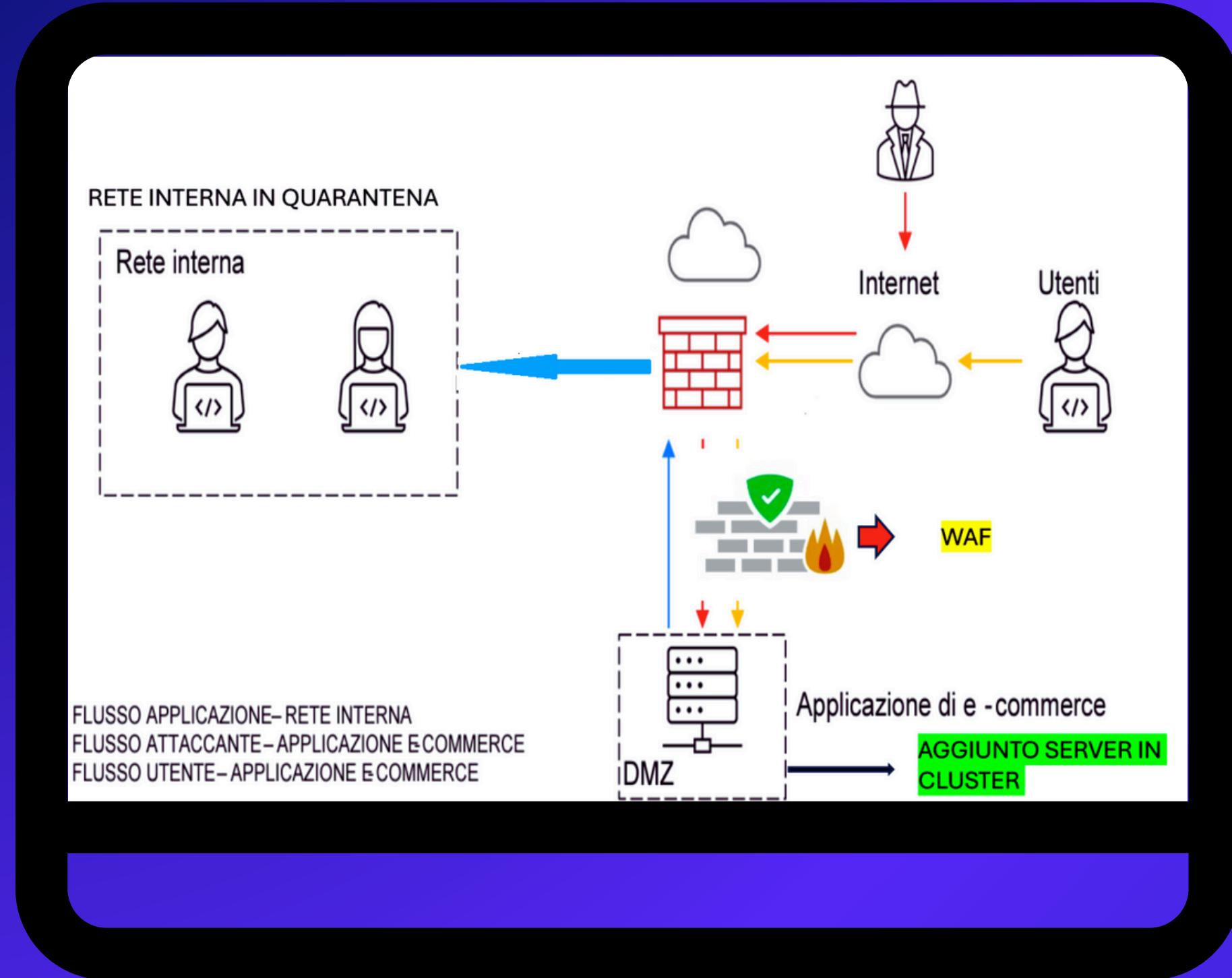
- Azioni preventive 01
- Architettura di rete 02
- Impatti sul business 03
- Tracce bonus 04



# PRESENTAZIONE RETE

"Benvenuti alla presentazione della nostra rete! Oggi vi condurremo in un viaggio attraverso le fondamenta, le prestazioni e le opportunità che la nostra rete offre. Scoprirete come questa infrastruttura sia progettata per connettere, ottimizzare e ampliare le nostre capacità, fornendo una base solida per il successo futuro. Preparatevi ad esplorare le potenzialità che questa rete ci offre e come possiamo sfruttarle per raggiungere nuovi traguardi e obiettivi aziendali."





## Migliorie aggiunte:

- Aggiunto WAF
- Aggiunti server in cluster

**Migliorie che possono essere aggiunte ma a costo superiore:**

- Zona hot site
- Servizio DRaaS

# LAVORO EFFETTUATO

## Consigli di prevenzione



Validazione dell'input: L'applicazione deve validare tutti i dati immessi dagli utenti prima di utilizzarli in query SQL o script lato client. Questo può essere fatto utilizzando librerie di validazione dedicate o espressioni regolari.

Sanificazione dell'output: L'applicazione deve sanificare tutti i dati che vengono visualizzati agli utenti prima di stamparli. Questo può essere fatto utilizzando funzioni di escape HTML o altre tecniche di sanificazione appropriate.

Lato server:

Dichiarazioni preparate: L'applicazione deve utilizzare dichiarazioni preparate per tutte le query SQL. Le dichiarazioni preparate separano i dati dal codice SQL, il che impedisce agli utenti malintenzionati di iniettare codice SQL dannoso.

Controllo degli accessi: L'applicazione deve implementare un rigoroso controllo degli accessi per garantire che gli utenti non possano accedere a dati o funzioni a cui non sono autorizzati.

Web Application Firewall (WAF): Un WAF può essere utilizzato per filtrare il traffico in entrata e bloccare le richieste dannose.

Altri consigli:

Mantenere aggiornato il software: Assicurarsi di utilizzare le ultime versioni di tutti i software, inclusi il sistema operativo, il server web e il framework di sviluppo web.

Effettuare regolarmente scansioni di sicurezza: Eseguire regolarmente scansioni di sicurezza dell'applicazione Web per identificare e correggere eventuali vulnerabilità.

Formare gli utenti: Formare gli utenti sui rischi delle minacce informatiche e su come proteggersi dagli attacchi.

# LAVORO EFFETTUATO

## Impatto sul business di un DDOS

### Impatto sul business di un attacco DDoS

Se l'applicazione Web subisce un attacco DDoS per 10 minuti, l'impatto sul business può essere significativo. Considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce, la perdita di fatturato durante l'attacco potrebbe essere di:

$$1.500 \text{ € al minuto} * 10 \text{ minuti} = 15.000 \text{ €}$$

Oltre alla perdita di fatturato, un attacco DDoS può anche danneggiare la reputazione dell'azienda e portare a una perdita di clienti.

### Azioni preventive per mitigare gli attacchi DDoS:

Utilizzare un servizio di bilanciamento del carico: Un servizio di bilanciamento del carico può distribuire il traffico su più server, il che può aiutare a mitigare gli attacchi DDoS.

Utilizzare un servizio di protezione DDoS: Un servizio di protezione DDoS può filtrare il traffico dannoso e proteggere l'applicazione Web dagli attacchi.

Aumentare la capacità della banda larga: Avere più banda larga disponibile può aiutare a gestire il traffico durante un attacco DDoS.



# LAVORO EFFETTUATO

## Response da Malware



Se l'applicazione Web viene infettata da un malware, la priorità è impedire che il malware si propaghi sulla rete. Questo può essere fatto isolando la macchina infetta dalla rete e impedendo l'accesso ai dati e alle risorse della rete.

Nella figura modificata è stata evidenziata la seguente soluzione:

Isolamento della macchina infetta: La macchina infetta viene isolata dalla rete utilizzando un firewall o un altro dispositivo di sicurezza.

Scansione antivirus: La macchina infetta viene scansionata con un antivirus per identificare e rimuovere il malware.

Ripristino del sistema: Se necessario, il sistema viene ripristinato da un backup pulito.

# LAVORO EFFETTUATO

Soluzioni per la  
cybersecurity



La soluzione completa per la sicurezza dell'applicazione Web deve combinare le azioni preventive con le misure di response. La figura precedente mostra una soluzione completa che include le seguenti componenti:

Firewall: Il firewall blocca il traffico non autorizzato e protegge la rete dagli attacchi esterni.

WAF: Il WAF filtra il traffico in entrata e blocca le richieste dannose.

Server di bilanciamento del carico: Il server di bilanciamento del carico distribuisce il traffico su più server e aiuta a mitigare gli attacchi DDoS.

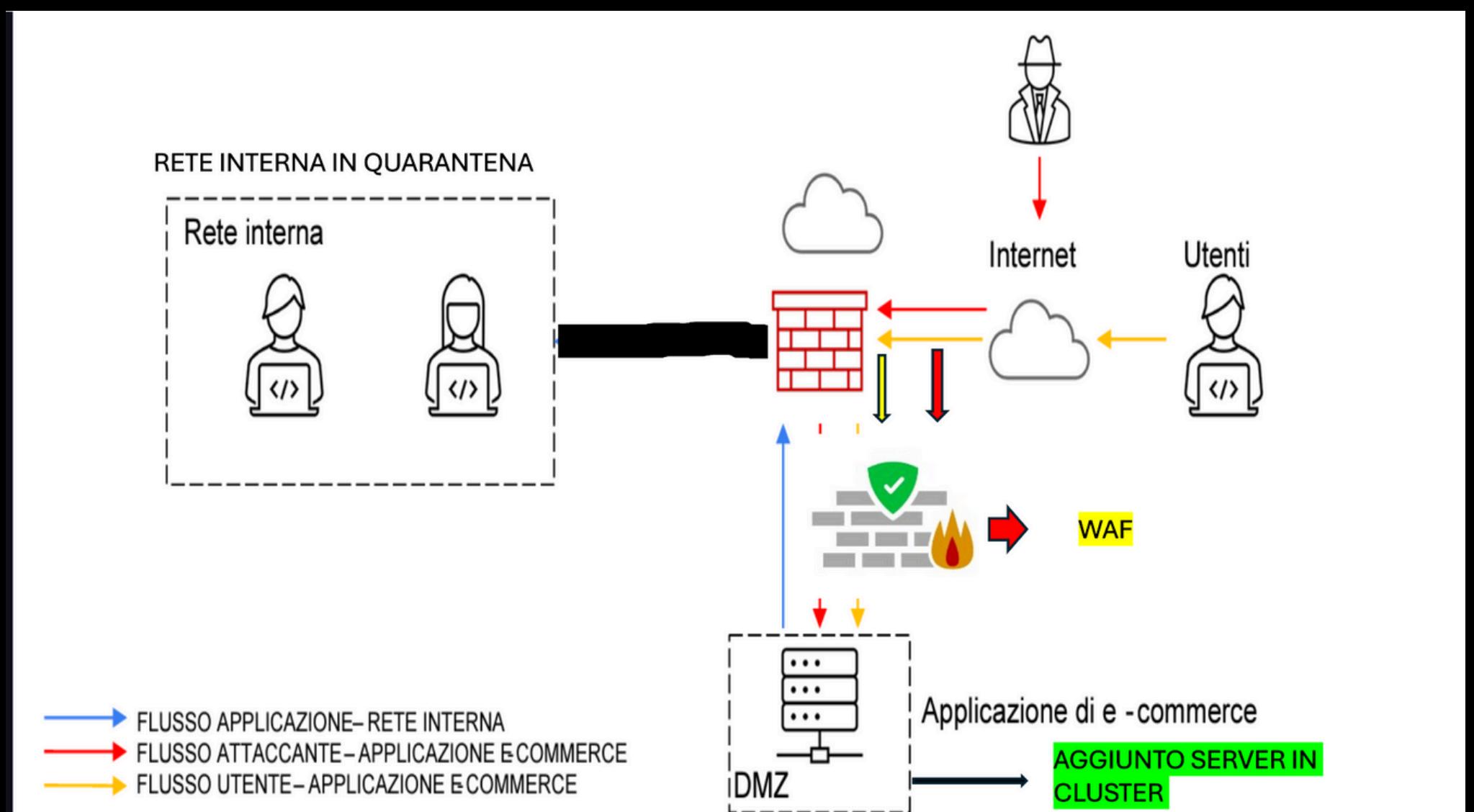
Sistema di rilevamento delle intrusioni (IDS): Un IDS monitora la rete per attività sospette e avvisa gli amministratori in caso di potenziali minacce.

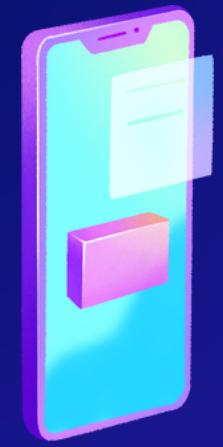
Segmentazione della rete: La rete viene segmentata in più zone per limitare la propagazione di malware.

Soluzioni di backup e ripristino: Vengono implementate soluzioni di backup e ripristino come dei server cluster.

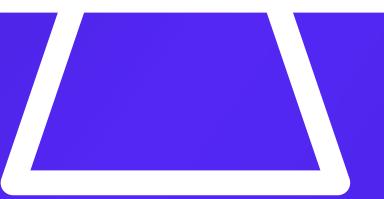
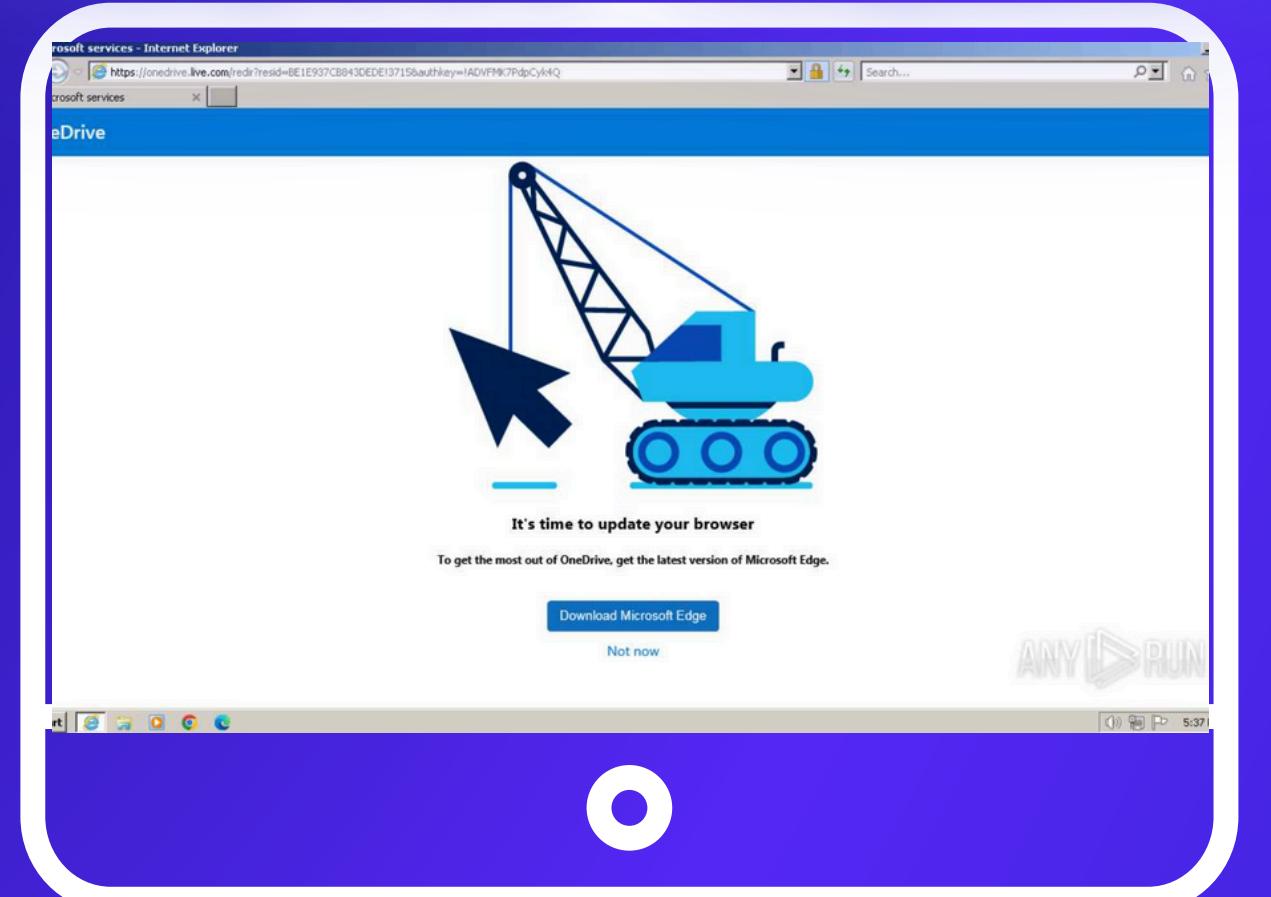
# Soluzioni per estrema emergenza

In caso di estrema emergenza come un accesso abusivo al sistema informatico per evitare la fuga di danni personali dei clienti e dei dipendenti puo' essere necessario staccare completamente i collegamenti alla rete interna. Ovviamente poi sara' necessario un notevole da parte del team CSIRT per mitigare il piu' celermente possibile la compromessa situazione.





# ANALISI MALWARE 1

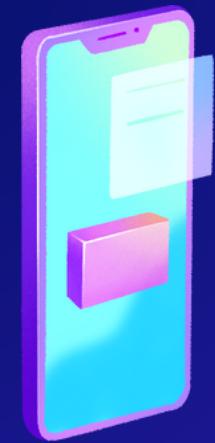


L'utente apre un finto iexplorer.exe che utilizza come vettore di replicazione il browser microsoft edge e sovrascrive file interni del browser.

## SISTEMI DI PROTEZIONE

Utilizzando una suite di protezione software, con sistema antivirus e tutti gli altri componenti necessari per proteggere il sistema operativo, e adottando un comportamento attento nella gestione del proprio PC (evitando ad esempio di installare software proveniente da fonti sconosciute), i rischi di imbattersi in un virus che sfrutta il nome SVCHost.exe sono limitatissimi o addirittura nulli.





# *ANALISI DEL MALWARE 2*



**l'utente apre un file PERFORMANCE\_BOOSTER\_v3.6.exe che esegue comandi da un file .bat che avvia cmd.exe per l'esecuzione dei comandi all'interno del file bat che cambia le policy sull'uso della powershell. Il malware si annida all'interno del sistema avviando un processo SVCHost.exe che viene definito, da Microsoft, come un nome generico che viene assegnato ad un processo Host di Windows.**

# SISTEMA DI PROTEZIONE

**Utilizzando una suite di protezione software, con sistema antivirus e tutti gli altri componenti necessari per proteggere il sistema operativo, e adottando un comportamento attento nella gestione del proprio PC (evitando ad esempio di installare software proveniente da fonti sconosciute), i rischi di imbattersi in un virus che sfrutta il nome SVCHost.exe sono limitatissimi o addirittura nulli**



GRAZIE PER LA  
VISUALIZZAZIONE

