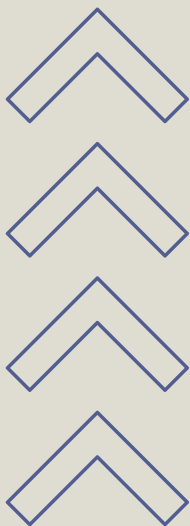




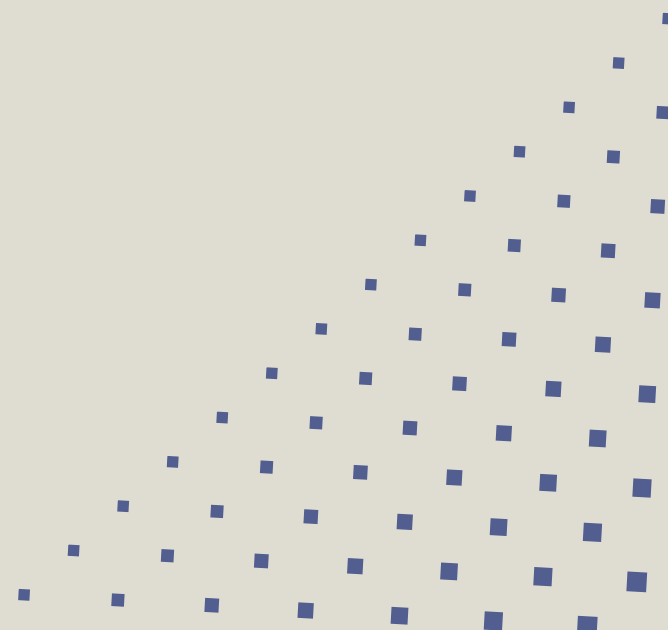
GIUGNO, 2024

ANALISI DEI RISCHI E SOLUZIONI

ARCHITETTURA SICUREZZA PER E-COMMERCE




Redatto da:
Anapaula Palacin





INDICE

Introduzione e Architettura di rete	3
Azioni preventive	4
Impatti sul Business	5
Response al Malware	6
Soluzione completa	7
Modifica aggressiva	8
Conclusioni	9
Anyrun / bonus	10



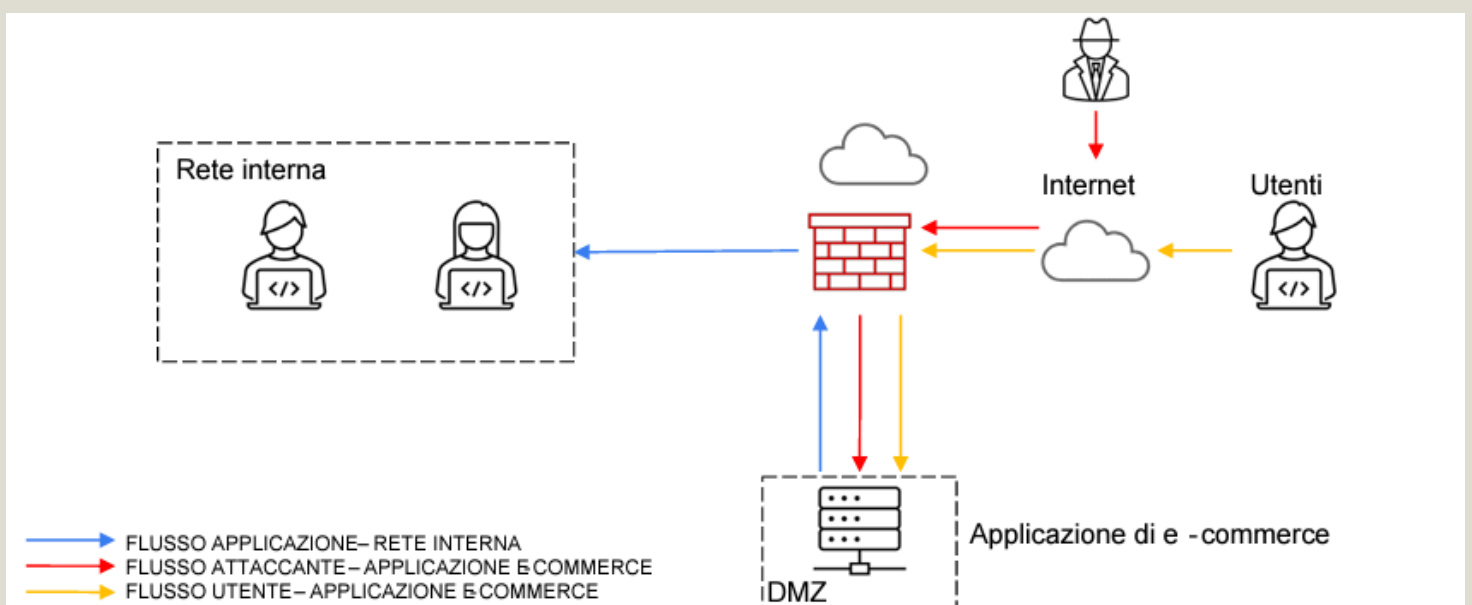
INTRODUZIONE

Architettura di Rete e Sicurezza per Applicazioni di E-commerce

- Importanza della sicurezza e la protezione dei dati sensibili nelle applicazioni di e-commerce.

Obiettivi della presentazione:

- Analizzare l'architettura di rete
- Identificare minacce comuni (SQLi, XSS)
- Azioni preventive
- Valutazione dell'impatto degli attacchi DDoS
- Strategie di risposta agli incidenti
- Soluzione completa e miglioramenti infrastrutturali



Architettura di rete: L'applicazione di e-commerce deve essere disponibile per gli utenti tramite la 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.

>>>> AZIONI PREVENTIVE (SQLI E XSS)

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

1 Convalida degli input:

convalidare e sanificare tutti gli input dell'utente per prevenire SQLi e XSS.

2 WAF:

implementare un WAF per filtrare e monitorare il traffico HTTP e bloccare gli attacchi dannosi.

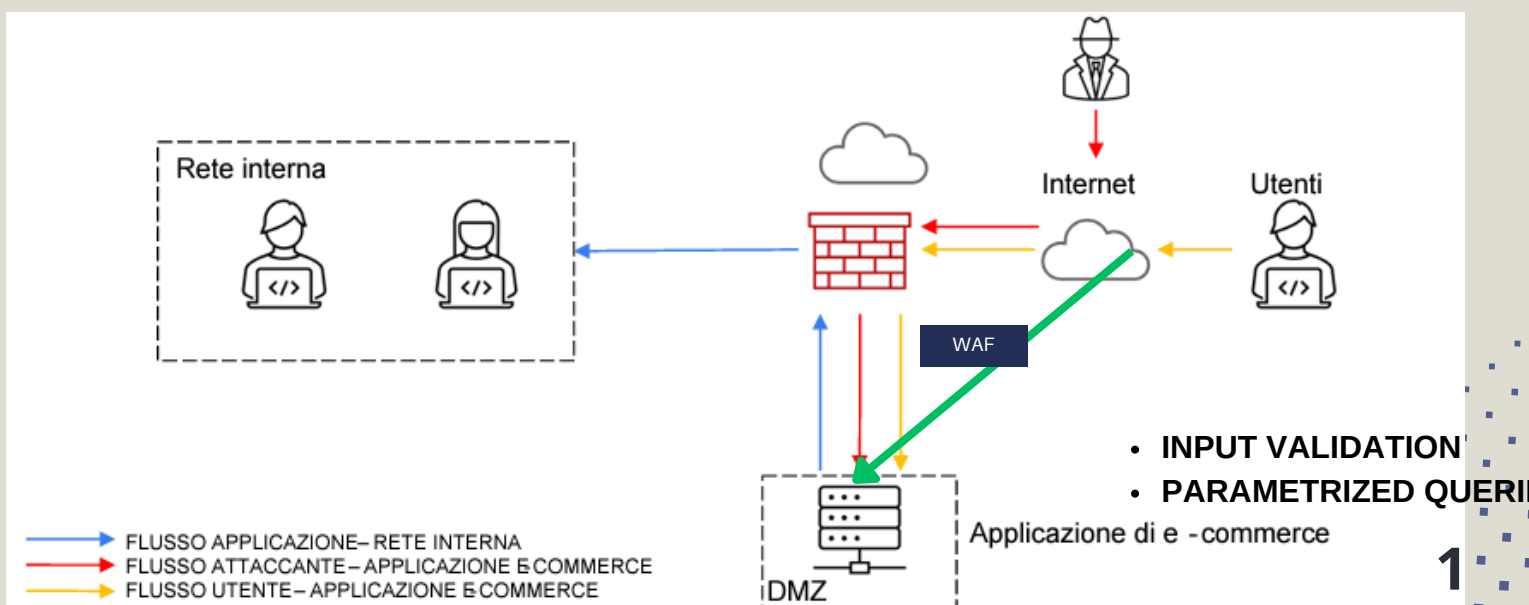
3 Query parametrizzate:

utilizzare query parametrizzate invece di concatenare stringhe SQL. (Questa tecnica garantisce che i dati degli utenti vengano trattati come semplici dati e non come parte della logica SQL, prevenendo così l'iniezione di codice malevolo.)

NO ---> `query = "SELECT * FROM utenti WHERE username = '" + user_input + "';"`

4 CSP (Content Security Policy):

implementare CSP per prevenire gli attacchi XSS. (Questa tecnica garantisce che i dati degli utenti vengano trattati come semplici dati e non come parte della logica SQL, prevenendo così l'iniezione di codice malevolo.)



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

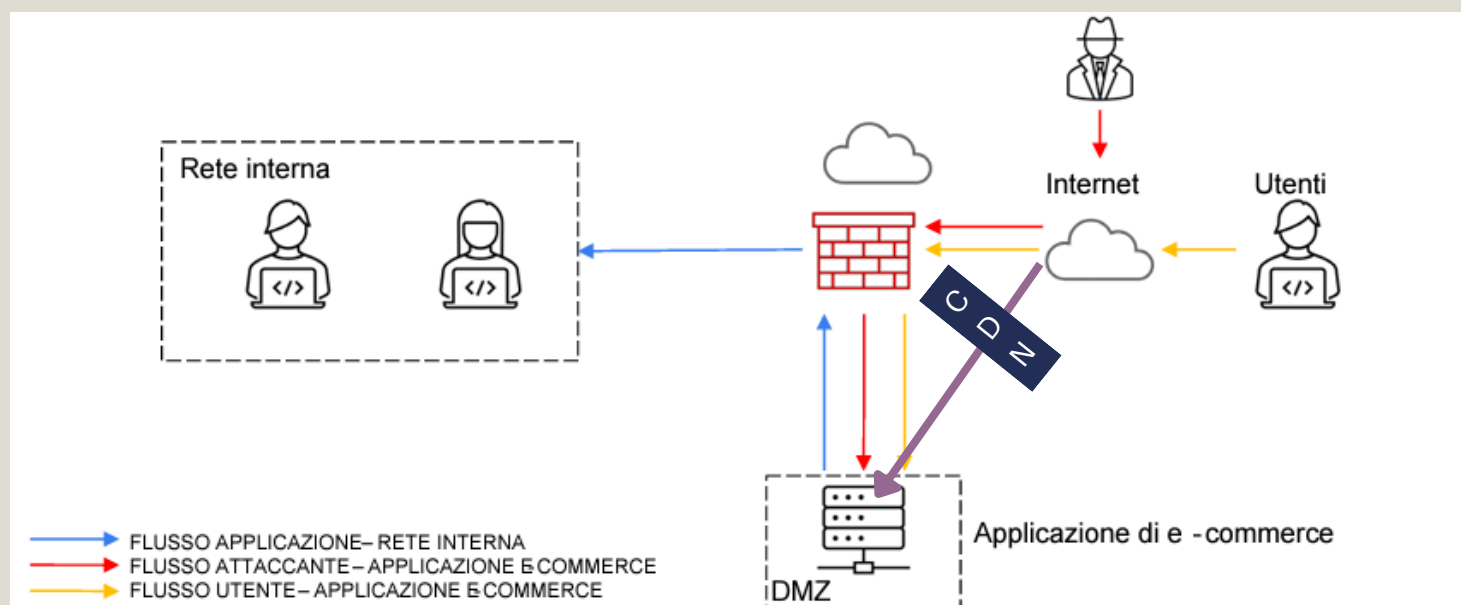
SPESSE AL MINUTO

1500 € al minuto quindi in 10 minuti saranno:

$1.500 \text{ €} \times 10 = 15.000 \text{ €}$ (IMPATTO TOTALE)

AZIONE PREVENTIVE

- **CDN (Content Delivery Network):** utilizzare CDN per distribuire il carico. (è una rete di server distribuiti geograficamente che lavorano insieme per fornire rapidamente contenuti internet agli utenti.) (Migliora la velocità di caricamento delle pagine web. "Riduce la latenza (ritardo) delle connessioni. /Distribuisce il carico di traffico, prevenendo sovraccarichi sui server principali."
- **Limitazione della velocità:** limitare il numero di richieste per IP. (il server può prevenire che una sola fonte sovraccarichi il sistema con troppe richieste in rapida successione.)
- **Servizi di protezione DDoS:** implementare servizi di protezione DDoS. (monitorano il traffico di rete in tempo reale e utilizzano algoritmi avanzati per identificare e filtrare il traffico dannoso. Questo per garantire che, anche durante un attacco il sito rimanga accessibile ai clienti)





RESPONSE AL MALWARE

Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra 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

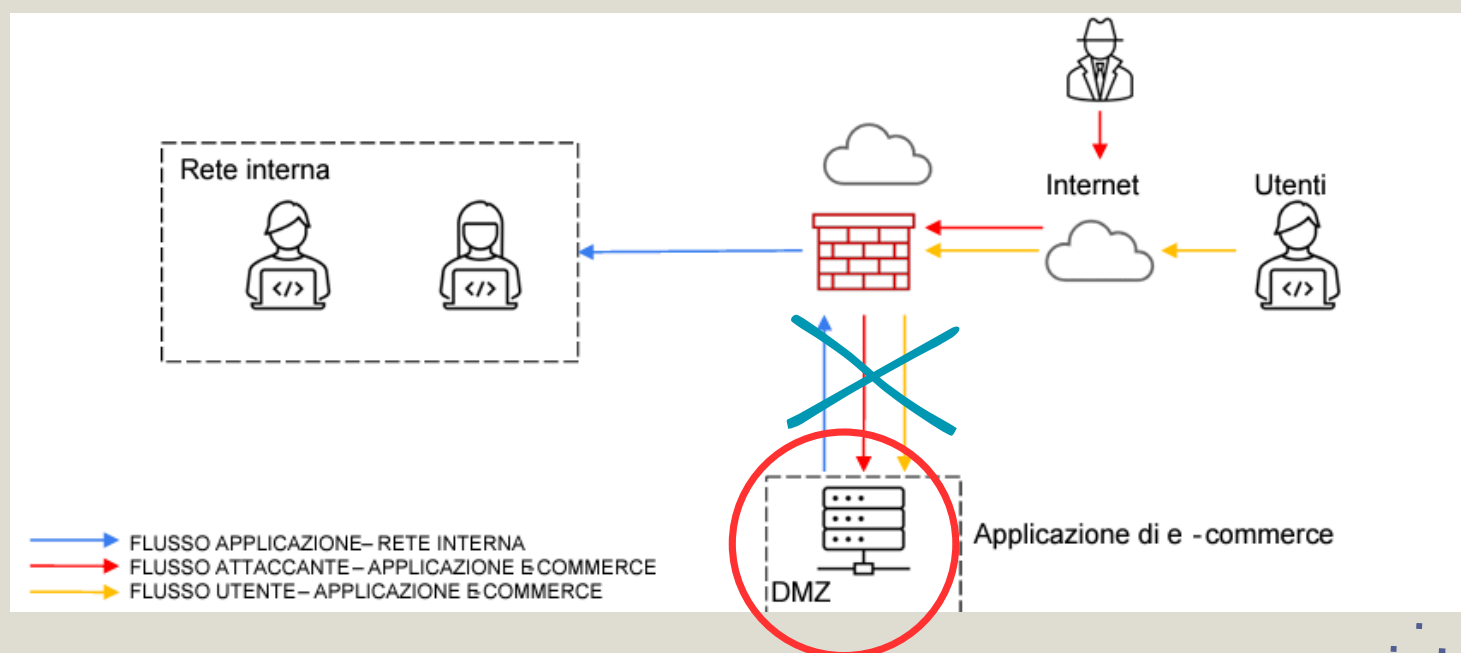
PRIORITÀ:

Impedire la diffusione di malware.

AZIONI:

1 Isolamento del server infetto: isolare il server compromesso. (per contenere un'infezione malware impedendo che il server compromesso comunichi con altri sistemi della rete.) Questo può essere fatto tramite configurazioni di firewall, sistemi di prevenzione delle intrusioni (IPS) o altre misure di rete.

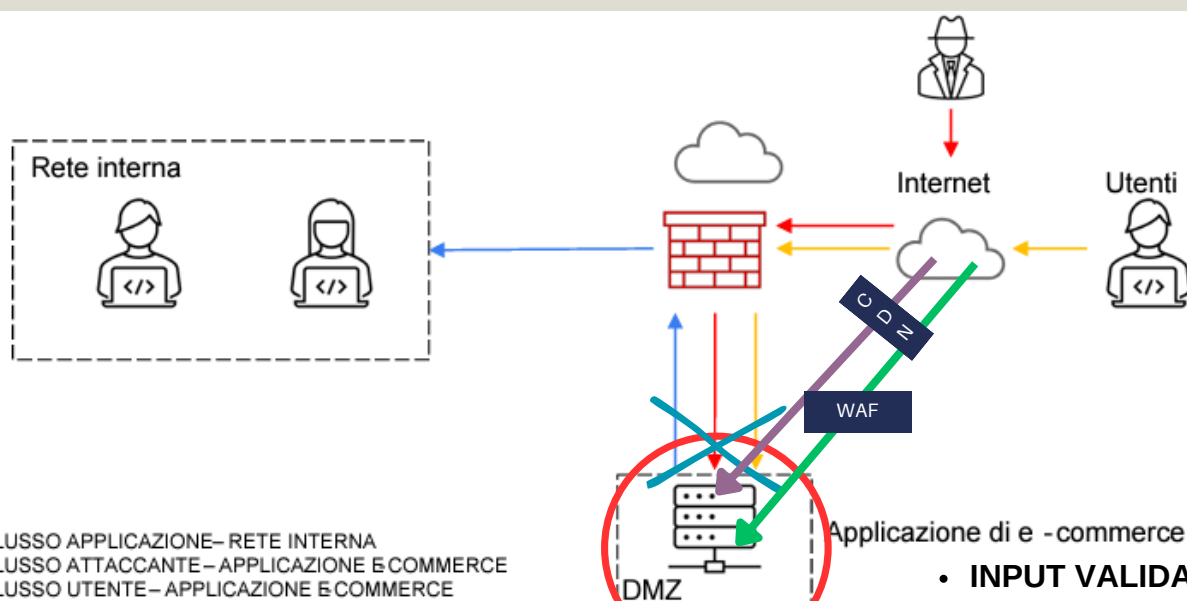
2 Segmentazione della rete: segmentare la rete per limitare il movimento laterale del malware. (divide una rete in segmenti più piccoli, ciascuno con i propri controlli di sicurezza) Ciascuno dei quali è isolato dagli altri tramite firewall o switch con regole di accesso specifiche. Riduce l'impatto di un'infezione o di un attacco, confinandolo a un solo segmento





SOLUZIONE COMPLETA

unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)



SERVER INFETTO

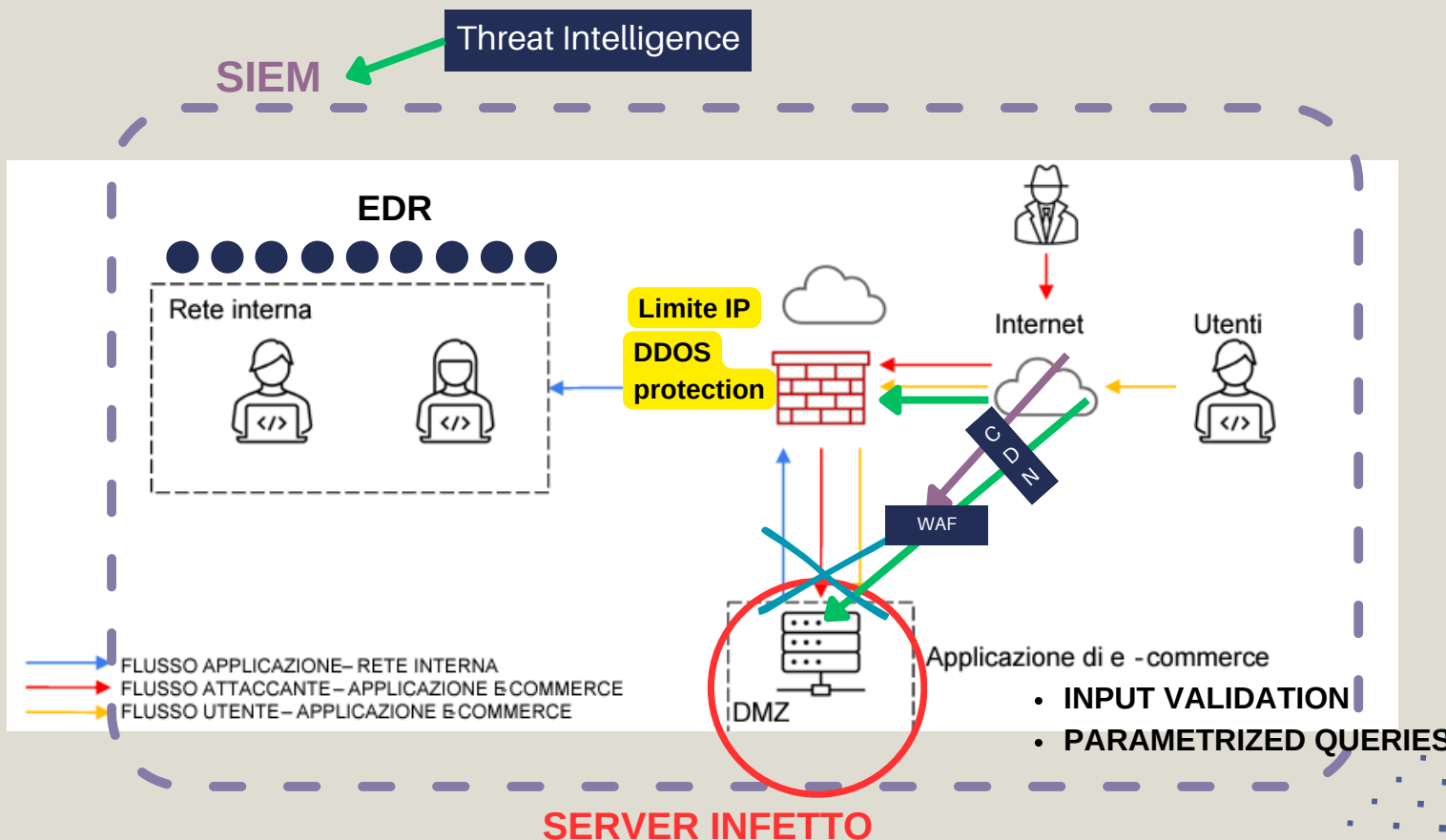


MODIFICA AGGRESSIVA

Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

ELEMENTI DI SICUREZZA:

- **EDR (Endpoint Detection and Response)** :rileva le minacce, isola il dispositivo infetto e avvia la rimozione del malware sugli endpoint (computer, server, dispositivi mobili).
- **SIEM (Security Information and Event Management)**: raccoglie log e dati di eventi da firewall, server, applicazioni, dispositivi di rete e altri sistemi. in tempo reale, quando rileva una minaccia, il SIEM genera avvisi e report per il team di sicurezza.
- **Threat Intelligence**: Fornisce informazioni sulle minacce per migliorare le difese e prevenire attacchi.





CONCLUSIONI

Protezione completa: implementando strumenti come EDR e SIEM e applicando tecniche come la segmentazione della rete, possiamo rilevare e rispondere rapidamente alle minacce, migliorando la sicurezza complessiva della nostra infrastruttura di e-commerce.

Prevenzione degli attacchi più comuni: misure preventive come l'uso di WAF, la convalida degli input e la parametrizzazione delle query sono essenziali per proteggere le nostre applicazioni web dagli attacchi SQLi e XSS, evitando così di compromettere la sicurezza.

Impatto sul business: utilizzando servizi di CDN, limitazione della velocità e protezione DDoS, possiamo ridurre al minimo l'impatto degli attacchi DDoS, garantendo che la nostra piattaforma di e-commerce rimanga accessibile e operativa anche durante un attacco.

Miglioramento continuo: l'integrazione di servizi di threat intelligence ci consente di essere sempre un passo avanti rispetto agli aggressori, aggiornando costantemente le nostre difese e adattandoci alle minacce nuove ed emergenti per proteggere meglio i nostri dati e le nostre operazioni.



ANYRUN

COSA É?

É un tool online interattivo per l'analisi del malware. Consente agli utenti di analizzare file e URL sospetti in tempo reale, interagendo direttamente con l'ambiente sandbox. È utile per studiare le minacce informatiche che richiedono l'interazione dell'utente, come fare clic su pulsanti o attivare macro.

Caratteristiche principali:

Interazione in tempo reale: gli utenti possono interagire con l'ambiente virtuale per attivare comportamenti specifici del malware.

Monitoraggio dettagliato: registra attività quali richieste di rete, creazione di processi, modifiche di file e cambiamenti del registro di sistema.

Database di intelligence sulle minacce: gestito da una comunità globale di ricercatori, aiuta a identificare gli indicatori di compromissione (IOC).

Configurazione flessibile: consente di selezionare il sistema operativo, le opzioni di connettività e il software precaricato per la sessione di scansione.

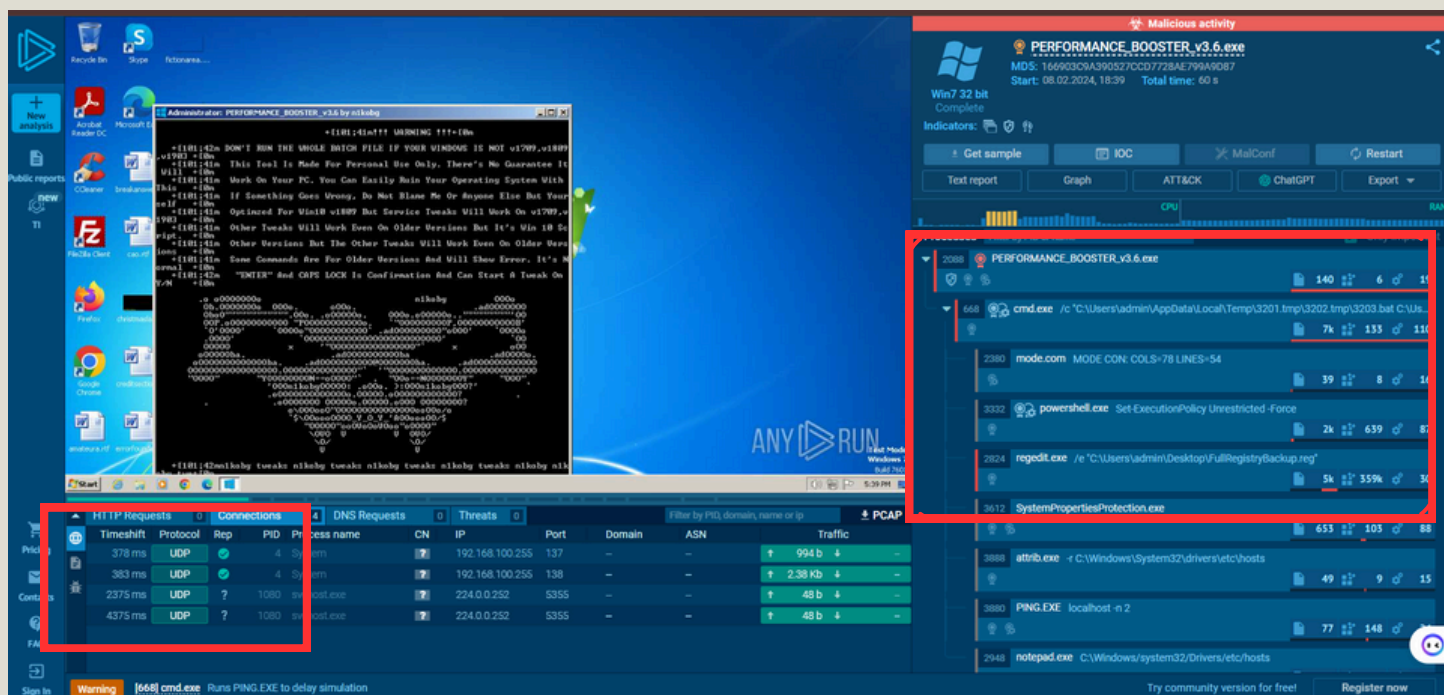


BONUS

TRACCIA

Analizzare le seguenti segnalazioni caricate su anyrun e 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:

- 1 <https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/>
- 2 <https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>



Analisi del malware: PERFORMANCE_BOOSTER_v3.6.exe

Tipo di attacco:

Sembra un malware che si maschera da strumento per migliorare le prestazioni del sistema. Le esecuzioni osservate includono comandi per modificare il registro di sistema e script PowerShell.

Modifica del registro: regedit.exe e altri processi modificano le impostazioni critiche del sistema.

Esecuzione di script: powershell.exe esegue comandi senza restrizioni.

Attività di rete: connessioni UDP sospette da svchost.exe.

Prevenzione per utenti e dirigenti:

- Mantenere il software aggiornato assicurandosi che tutti i sistemi e le applicazioni siano sempre aggiornati.
- Utilizzare software di sicurezza implementando solide soluzioni antivirus e antimalware.
- Formazione e sensibilizzazione, educando i dipendenti sui rischi dell'utilizzo di software provenienti da fonti non verificate.
- Limitazioni di esecuzione, limitando l'accesso alle funzioni critiche del sistema solo a personale addestrato e fidato.

The screenshot shows the Any.Run interface. On the left, a OneDrive notification states "It's time to update your browser" and "To get the most out of OneDrive, get the latest version of Microsoft Edge." Below this is a table of HTTP Requests, Connections, DNS Requests, and Threats. On the right, a "Malicious activity" panel shows a list of processes. A red box highlights the following processes:

- 1632 iexplore.exe "https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE"
- 3564 iexplore.exe SCODEF:1632 CREDAT:267521 /prefetch:2
- 3360 MicrosoftEdgeSetup.exe PE
- 3728 MicrosoftEdgeUpdate.exe PE /installsource taggedmi /install "appguid-{56EB1B...}
- 2476 MicrosoftEdgeUpdateSet... PE /installsource taggedmi /install "appguid-{56...

Below the highlighted processes, a table shows the traffic for MicrosoftEdgeUpdate.exe:

Process	Operation	Size	Direction
MicrosoftEdgeUpdate.exe	/regsvc	1k	175
MicrosoftEdgeUpdate.exe	/regserver	202	50
MicrosoftEdgeUpdate.exe	/regserver	180	90
MicrosoftEdgeUpdate.exe	/ping PD94bWwgdmiVyc2h0b0IM54w...	3408	

Analisi del malware: MicrosoftEdgeUpdate.exe

Tipo di attacco:

Finge di essere un aggiornamento legittimo di Microsoft Edge ma esegue attività dannose.

Modifica del registro: regedit.exe e altri processi apportano modifiche critiche.

Esecuzione di script: powershell.exe esegue comandi dannosi.

Connessioni di rete: vengono stabilite connessioni UDP e TCP sospette.

Download di file: richieste HTTP per scaricare file da server noti e sospetti.

HTTP Requests	13	Connections	44	DNS Requests	19	Threats	1	Filter by PID, name or url	PCAP
Timeshift	Protocol	Rep	PID	Process name	CN	URL	Content		
1602 ms	GET	304: Not Modifi...	?	3564	iexplore.exe	http://ctdl.windowsupdate.com/msdo...	-		
1606 ms	GET	304: Not Modifi...	?	3564	iexplore.exe	http://ctdl.windowsupdate.com/msdo...	-		
1624 ms	GET	200: OK	?	3564	iexplore.exe	http://ocsp.digicert.com/MFEWtZBNM...	471 b ↓ binary		
2564 ms	GET	200: OK	?	3564	iexplore.exe	http://ocsp.digicert.com/MFEWtZBNM...	471 b ↓ binary		
2616 ms	GET	304: Not Modifi...	?	1632	iexplore.exe	http://ctdl.windowsupdate.com/msdo...	-		
2617 ms	GET	304: Not Modifi...	?	1632	iexplore.exe	http://ctdl.windowsupdate.com/msdo...	-		

Warning [3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings

Richieste HTTP:

Visualizza le richieste effettuate dai processi (ad esempio, iexplore.exe) a vari URL.

GET, HEAD: Tipi di richieste HTTP.

Stati: 200: OK, Nessuna risposta.

Filter by PID, domain, name or ip												PCAP
HTTP Requests	13	Connections	44	DNS Requests	19	Threats	1					
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic		
576 ms	UDP	✓	4	System	?	192.168.100.255	137	–	–	↑ 694 b	↓ –	
585 ms	UDP	?	1080	svchost.exe	?	224.0.0.252	5355	–	–	↑ 48 b	↓ –	
589 ms	UDP	✓	4	System	?	192.168.100.255	138	–	–	↑ 1.66 Kb	↓ –	
1563 ms	TCP	✗	3564	ieexplore.exe	🇺🇸	13.107.42.12	443	1drv.ms	MICROSOFT...	↑ 390 b	↓ 8.88 Kb	
1575 ms	TCP	✗	3564	ieexplore.exe	🇺🇸	13.107.42.12	443	1drv.ms	MICROSOFT...	↑ 747 b	↓ 9.43 Kb	
1592 ms	TCP	✓	3564	ieexplore.exe	🇬🇧	93.184.221.240	80	ctldl.window...	EDGECAST	↑ 285 b	↓ 289 b	
Warning [3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings												

Warning [3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings

Connessioni:

Elenco delle connessioni di rete stabilite dai processi.
Protocollo utilizzato (UDP, TCP), porta, IP di destinazione.

HTTP Requests13

Connections44

DNS Requests19

Threats1

Filter by IP or domain

PCAP

Timeshift	Status	Rep	Domain	IP
539 ms	Responded	✖	1drv.ms	13.107.42.12
1545 ms	Responded	✔	ctldl.windowsupdate.com	93.184.221.240
1546 ms	Responded	✔	ocsp.digicert.com	192.229.221.95
2549 ms	Responded	✖	onedrive.live.com	13.107.137.11
				13.107.139.11
2550 ms	Responded	✔	p.sfx.ms	51.105.104.217

Warning

[3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings

Warning [3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings

Richieste DNS:

Domini richiesti e relative risposte.
Indica la risoluzione dei nomi di dominio in indirizzi IP.

HTTP Requests

13

Connections

44

DNS Requests

19

Threats

1

Filter by message

PCAP

Timeshift	Class	PID	Process name	Message
32509 ms	Potential Corporate Privacy Violation	856	svchost.exe	ET POLICY PE EXE or DLL Windows file download HTTP

Warning

[3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings

Warning [3408] MicrosoftEdgeUpdate.exe Checks Windows Trust Settings

Minacce:

Possibili violazioni della privacy aziendale rilevate.
Messaggi di avviso specifici.

Prevenzione per utenti e dirigenti:

- Aggiornare il software e mantenere aggiornati i sistemi e le applicazioni.
- Utilizzare l'antivirus e formazione degli utenti
- Limitare le autorizzazioni: Limitare le modifiche al sistema agli utenti autorizzati.
- Monitorare le connessioni e il DNS monitorando il traffico di rete e le richieste DNS per rilevare attività sospette e prevenire gli attacchi di rete.



GRAZIE!