

PROGETTO S9L5

SECURITY OPERATION CENTER PROCESS AND PROCEDURE



Simone La Porta
CS0424IT

Table of contents

01

Azioni preventive SQLi e XSS WebApp

02

Impatti sul business DDoS attack WebApp

03

Malware Response WebApp

04

Soluzione completa

05

Modifica più "aggressiva" dell'infrastruttura

06

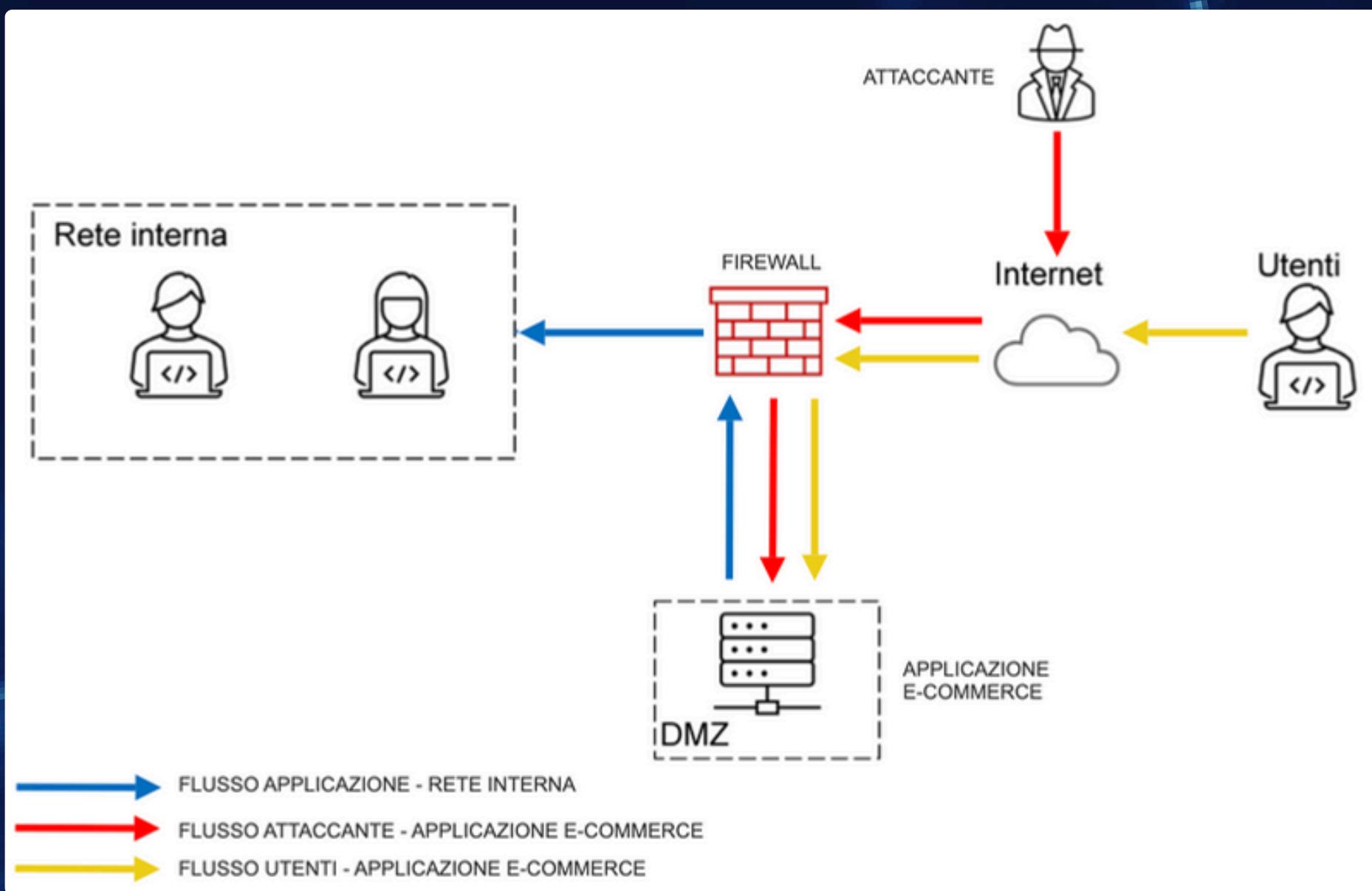
BONUS: Analisi log con AnyRun

1

Azioni preventive SQLi e XSS WebApp

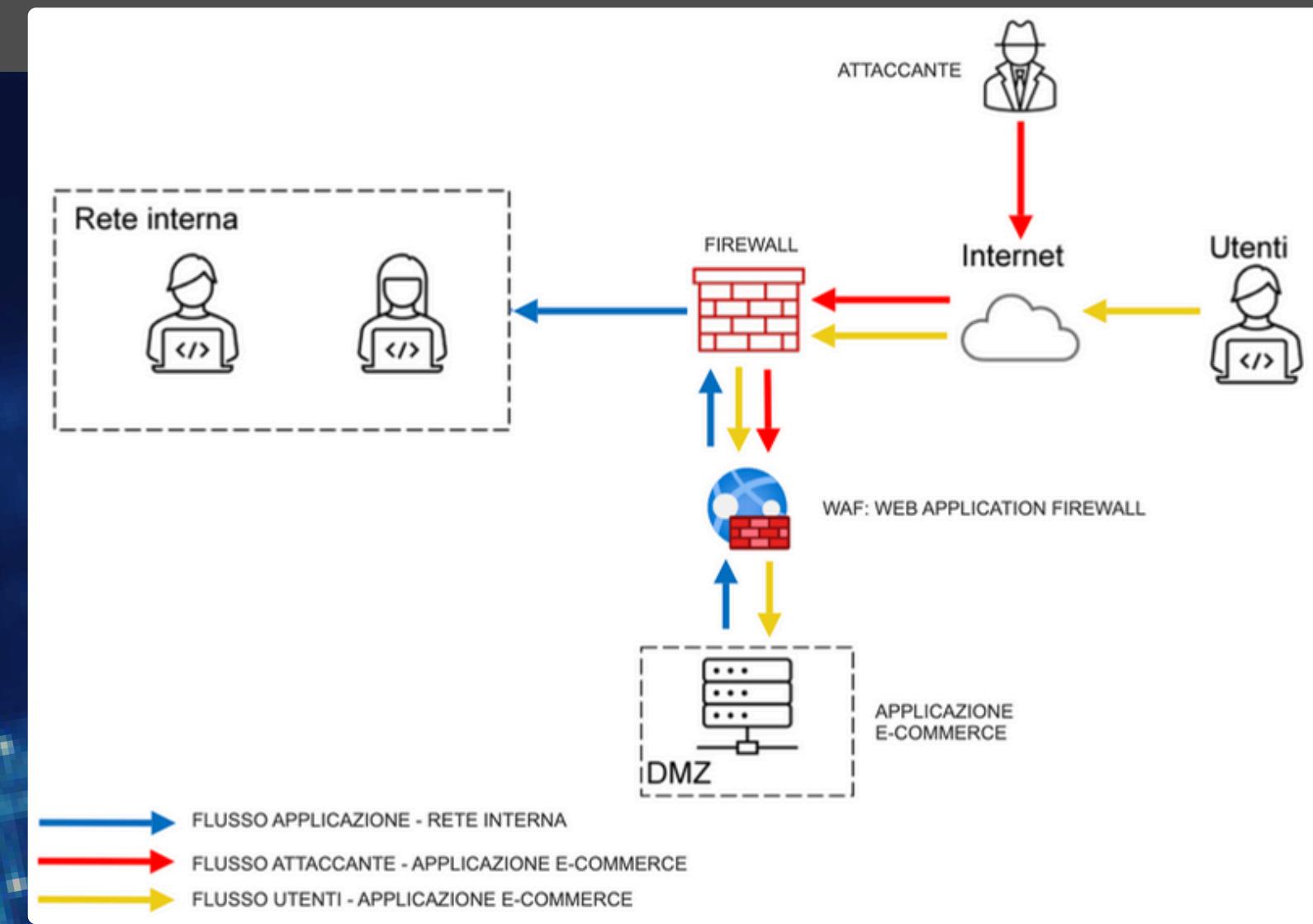
Traccia

Riferendosi alla figura, quali azioni preventive potrebbero essere implementate per proteggere un'applicazione web da attacchi di tipo SQL Injection (SQLi) o Cross-Site Scripting (XSS) da parte di utenti malintenzionati? Si prega di modificare la figura per evidenziare tali implementazioni. È richiesta una sola modifica.



Azioni preventive

- Per proteggere la Web App da minacce come XSS e SQLi, è possibile adottare preventivamente una soluzione basata su un **Web Application Firewall (WAF)**. A differenza dei firewall standard, i WAF sono specificamente progettati per difendere le applicazioni web da attacchi di tipo XSS e SQLi.
- Il WAF deve essere posizionato per filtrare il traffico in entrata verso la WebApp proveniente da internet (utenti e potenziali attaccanti) e bloccare le possibili attività malevoli (attaccanti).



Azioni preventive WAF e WebApp

Implementazione WAF:

- Filtrare e monitorare tutto il traffico HTTP che passa attraverso al WAF, per **bloccare in tempo reale** tentativi di attacco SQLi e XSS, proteggendo così l'applicazione web da minacce esterne.

Configurazione sicura WebApp:

- **Validazione/sanitizzazione** di tutti i campi di input per garantire che i dati inseriti dagli utenti siano conformi alle aspettative e che eventuali caratteri pericolosi vengano filtrati, così da impedire agli attaccanti di inserire codice malevolo.
- **Query parametrizzate** per gestire le interazioni con il DB, così che i dati dell'utente non vengano mai trattati come comandi SQL.
- **Codifica di tutti i dati in output** prima di renderli visibili agli utenti, per impedire l'esecuzione di script dannosi nel browser dell'utente, prevenendo efficacemente gli attacchi XSS.
- **Aggiornare** e applicare regolarmente patch all'applicazione web e ai sistemi di database.
- Implementare **meccanismi di autenticazione robusti e controlli di accesso**, così da garantire che solo gli utenti autorizzati possano accedere a funzionalità specifiche dell'applicazione, migliorando la sicurezza complessiva del sistema.

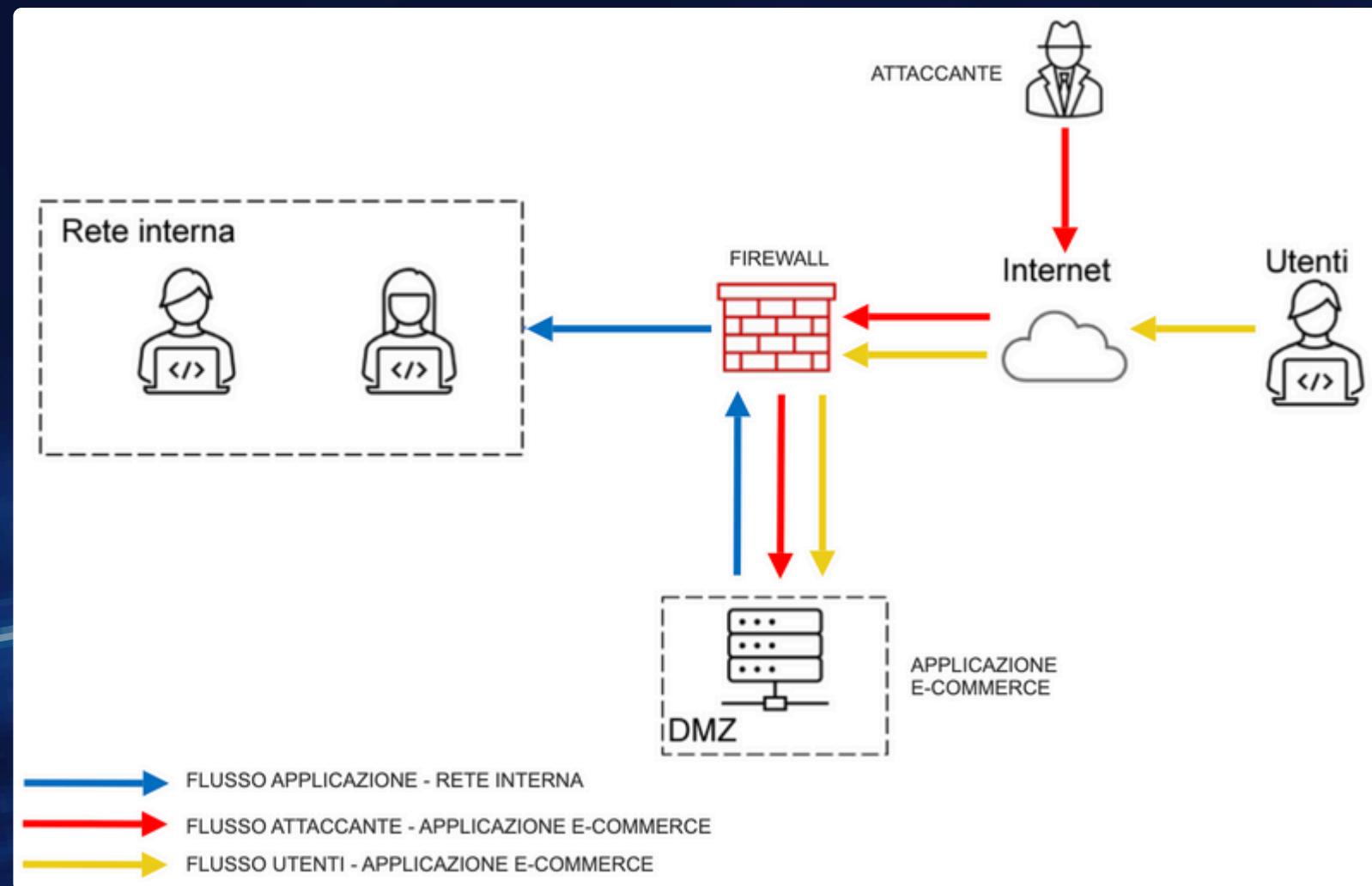
2

Impatti sul business DDoS attack WebApp

Traccia

Si suppone che la nostra applicazione web subisca un attacco di tipo Distributed Denial of Service (DDoS) dall'esterno, rendendola non raggiungibile per 10 minuti. Calcolare l'impatto economico di questa interruzione sul business, considerando che in media ogni minuto gli utenti spendono 1200€ sulla piattaforma di e-commerce.

Valutare eventuali azioni preventive per mitigare tali problematiche in futuro.



Impatti sul business

- **Perdita diretta a causa delle mancate vendite:**
 - Tempo di inattività: 10 min.
 - Spesa media degli utenti: 1.200 €/min.
 - Perdita economica diretta: $1.200 \text{ €/min} * 10 \text{ min} = 12.000\text{€}$.

Per una stima più realistica necessario considerare altri fattori (stimati):

- **Perdita di clienti e reputazione:** supponendo una perdita dell'1% dei clienti abituali a causa dell'inattività e circa 5000 clienti abituali/giorno, ognuno dei quali spende in media 100€/giorno, si avrebbe un'ulteriore perdita di 5.000 €.
- **Costi di recupero e gestione dell'incidente:** supponendo una tariffa oraria per il team IT di 100€/h e un tempo di recupero di 3h, si avrebbe un'ulteriore perdita/spesa di 300€.
- Molti altri fattori in gioco come il valore delle opportunità di vendita perse, ecc.

Azioni preventive

- **Soluzioni anti-DDoS:**

- Scegliere un fornitore affidabile di soluzioni anti-DDoS, come Cloudflare, Akamai, o AWS Shield.
- Configurare il servizio anti-DDoS per monitorare e filtrare il traffico verso il sito web. Questo può includere la protezione a livello di rete e applicazione.
- Integrare la soluzione anti-DDoS con il firewall esistente e altri sistemi di sicurezza per garantire una protezione completa.
- Eseguire test periodici per verificare l'efficacia della protezione e per aggiornare le regole di mitigazione in base ai nuovi tipi di attacco.

- **Ridondanza e failover:**

- Impostare server di backup in diversi data center per garantire la disponibilità del servizio anche se un data center diventa inaccessibile.
- Utilizzare servizi di failover DNS che reindirizzano automaticamente il traffico verso server alternativi in caso di indisponibilità del server principale.
- Implementare la replicazione dei database per garantire la consistenza dei dati tra i server primari e di backup.
- Eseguire test regolari per garantire che i meccanismi di failover funzionino correttamente e che il tempo di inattività sia minimizzato.

Azioni preventive

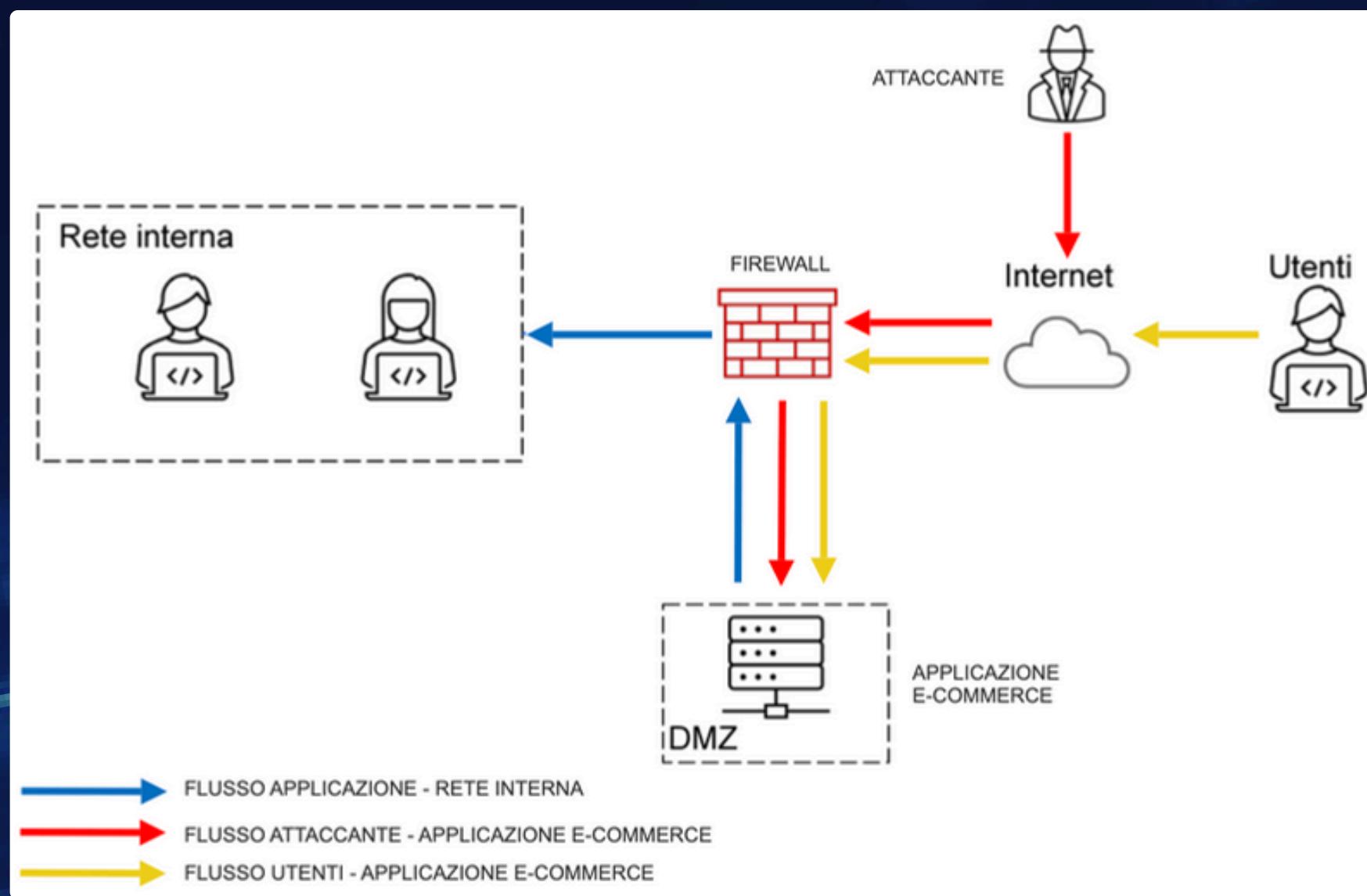
- **Monitoraggio del traffico:**
 - Utilizzare strumenti di monitoraggio come Wireshark, Nagios, o SolarWinds per analizzare il traffico di rete in tempo reale.
 - Configurare allarmi e avvisi per attività sospette o picchi di traffico anomali.
 - Implementare la raccolta e l'analisi dei log di rete per identificare e rispondere tempestivamente agli attacchi.
 - Aggiornare regolarmente gli strumenti di monitoraggio e rivedere le configurazioni di allarme per far fronte alle nuove minacce.
- **Limitazione del tasso di richieste:**
 - Utilizzare funzionalità del server web (come Apache mod_evasive o Nginx rate limiting) per impostare limiti sul numero di richieste per IP.
 - Configurare regole del firewall per limitare il traffico in base al volume delle richieste provenienti da singoli indirizzi IP.
 - Se l'applicazione offre API, implementare limiti sul tasso di richieste a livello di API.
 - Monitorare i limiti di richiesta e aggiustarli in base al comportamento dell'utente e ai carichi di lavoro normali.

3

Malware Response WebApp

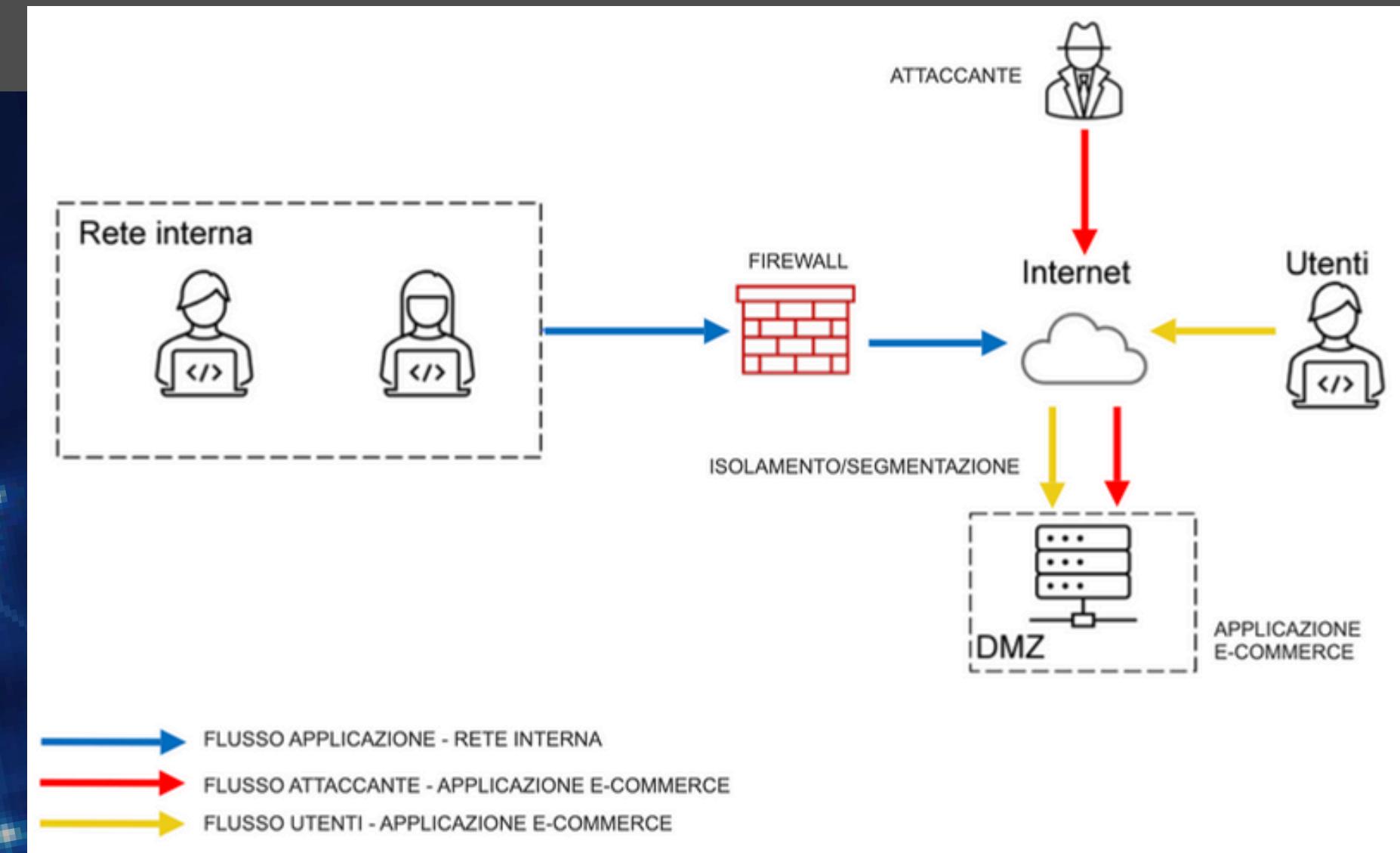
Traccia

L'applicazione web è stata infettata da un malware. La priorità è impedire che il malware si propaghi alla rete interna. Non si è interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificare la figura della rete per rappresentare la soluzione proposta.



Azioni preventive

- Isolare la macchina infetta:
 - Assicurarsi che la macchina infetta (l'applicazione di e-commerce nella DMZ) sia isolata dalla rete interna. Questo può essere fatto aggiornando le regole del firewall per bloccare qualsiasi traffico dalla DMZ verso la rete interna.
- Segmentare la rete:
 - Segmentare ulteriormente la DMZ da altre parti della rete. Ciò significa garantire che l'applicazione infetta non possa comunicare lateralmente con altri server o servizi all'interno della DMZ.

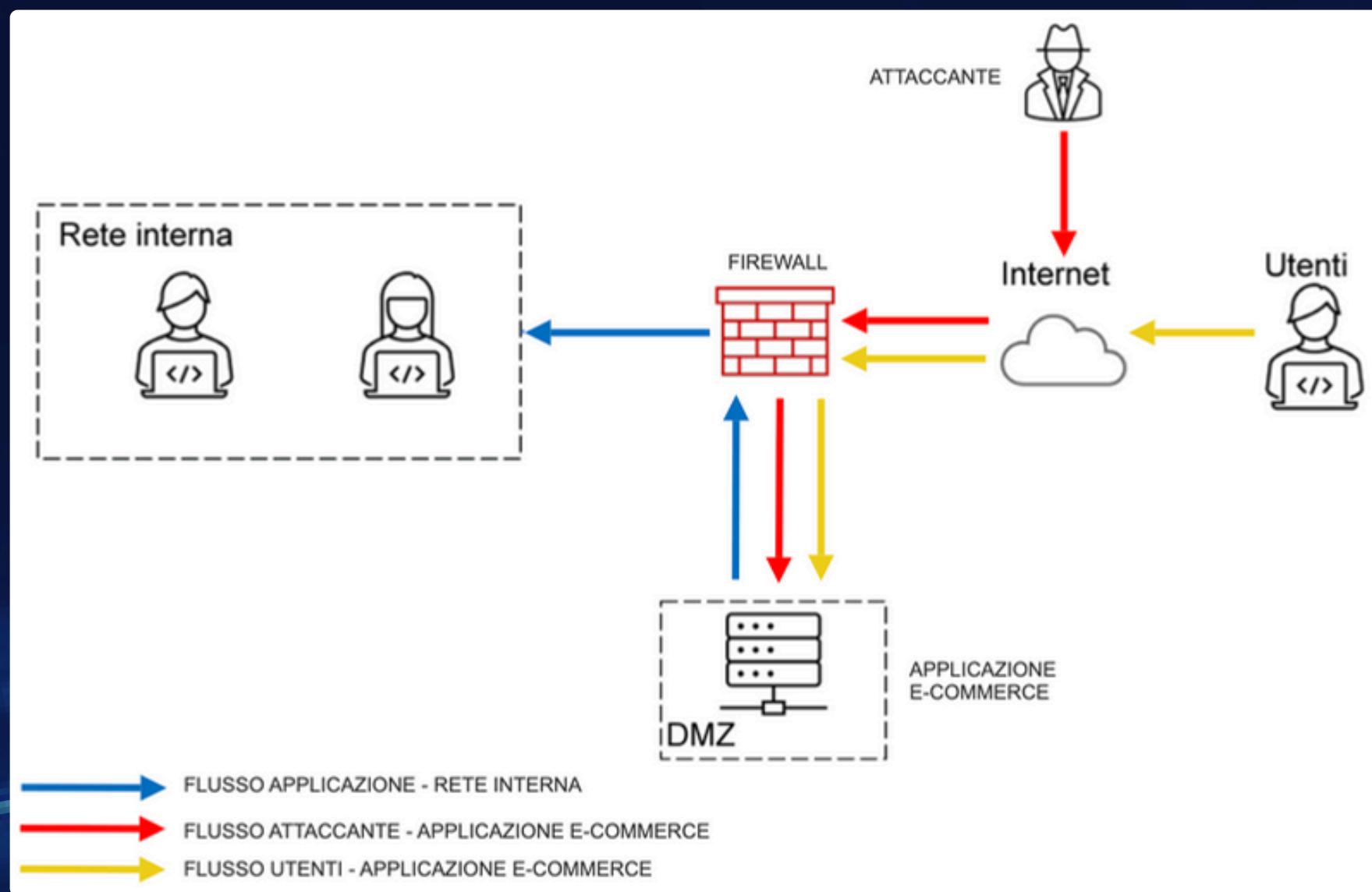


4

Soluzione completa

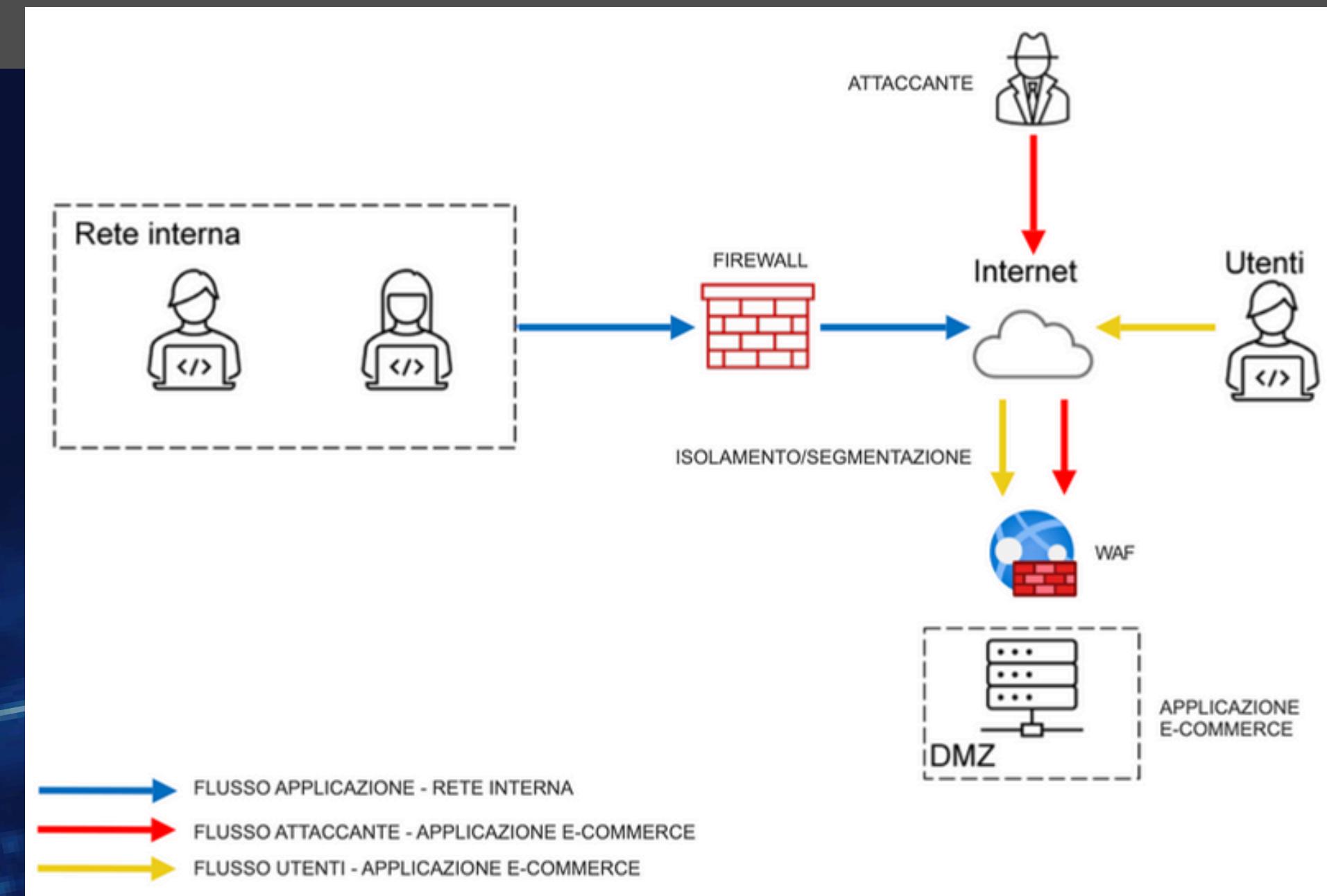
Traccia

Unire soluzione dei punti 1 e 3 per un'azione preventiva più completa.



Azioni preventive

- In questo caso la macchina sarà ancora collegata ad internet, raggiungibile dall'attaccante, non più connessa alla rete interna e con l'aggiunta del WAF.
- La figura mostra la soluzione con la strategia dell'isolamento della macchina infetta con un ulteriore filtraggio.

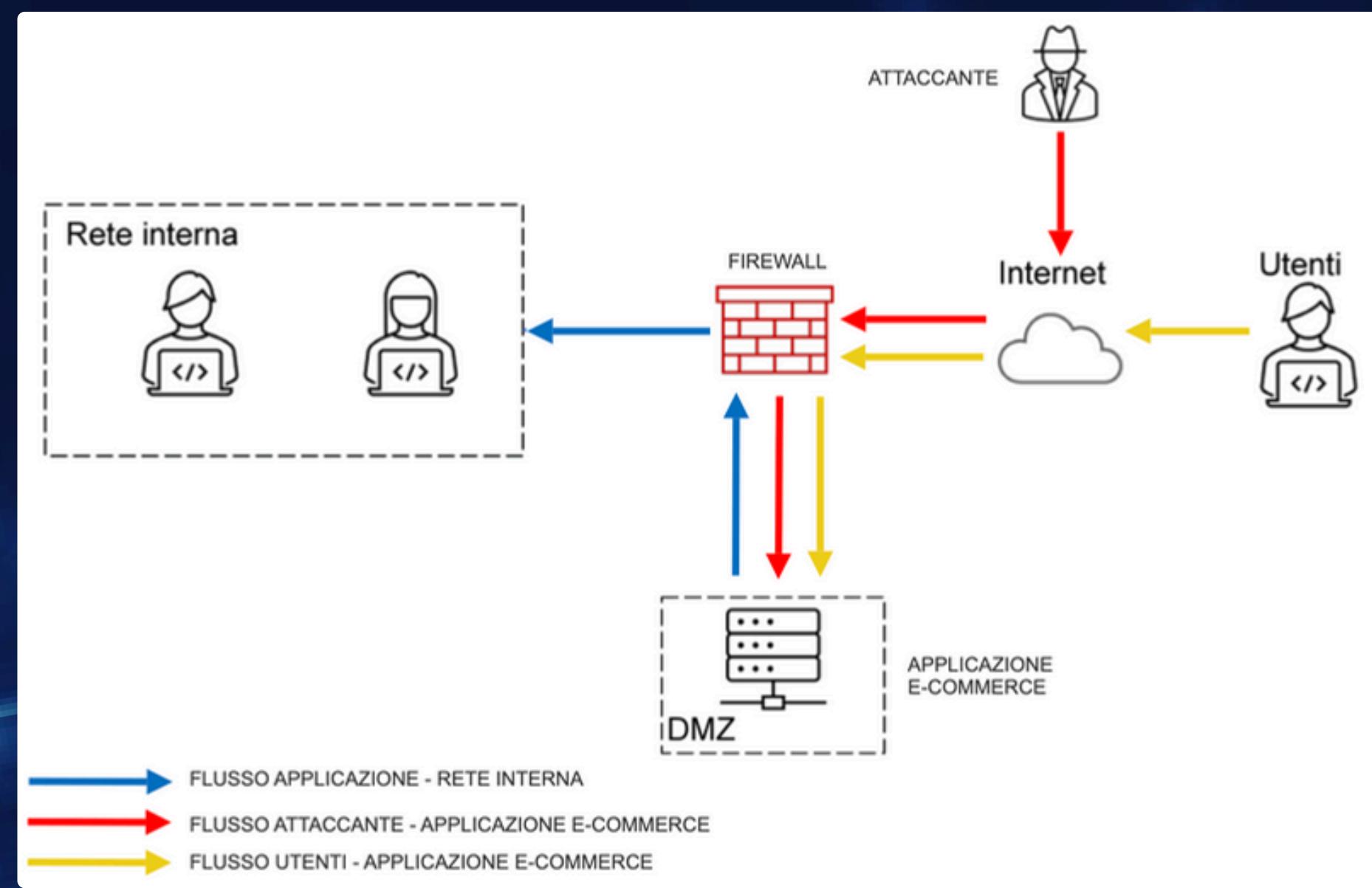


5

**Modifica più
"aggressiva"
dell'infrastruttura**

Traccia

Proporre una modifica «più aggressiva» dell'infrastruttura includendo soluzioni per i punti precedenti e integrando eventuali altri elementi di sicurezza (budget 5.000-10.000 €). Eventualmente fare più proposte di spesa.



Azioni preventive

Opzione 1: Suite di Sicurezza Completa (~5.000 €)

- **Firewall per Applicazioni Web (WAF)**
 - Costo: ~2.000 €
 - Protegge contro attacchi XSS/SQLi ispezionando e filtrando le richieste HTTP.
- **Servizio di protezione DDoS**
 - Costo: ~1.500 €
 - Mitiga gli attacchi DDoS, assicurando la disponibilità dell'applicazione durante un attacco.
- **Rilevamento e Risposta degli Endpoint (EDR)**
 - Costo: ~1.000 €
 - EDR offre visibilità sui dispositivi endpoint, rilevando attività sospette e fornendo strumenti per rispondere rapidamente a eventuali minacce.
- **Sistema di Backup e Failover**
 - Costo: ~1.000 €
 - Garantisce la disponibilità dei dati e la continuità operativa in caso di guasti.

Azioni preventive

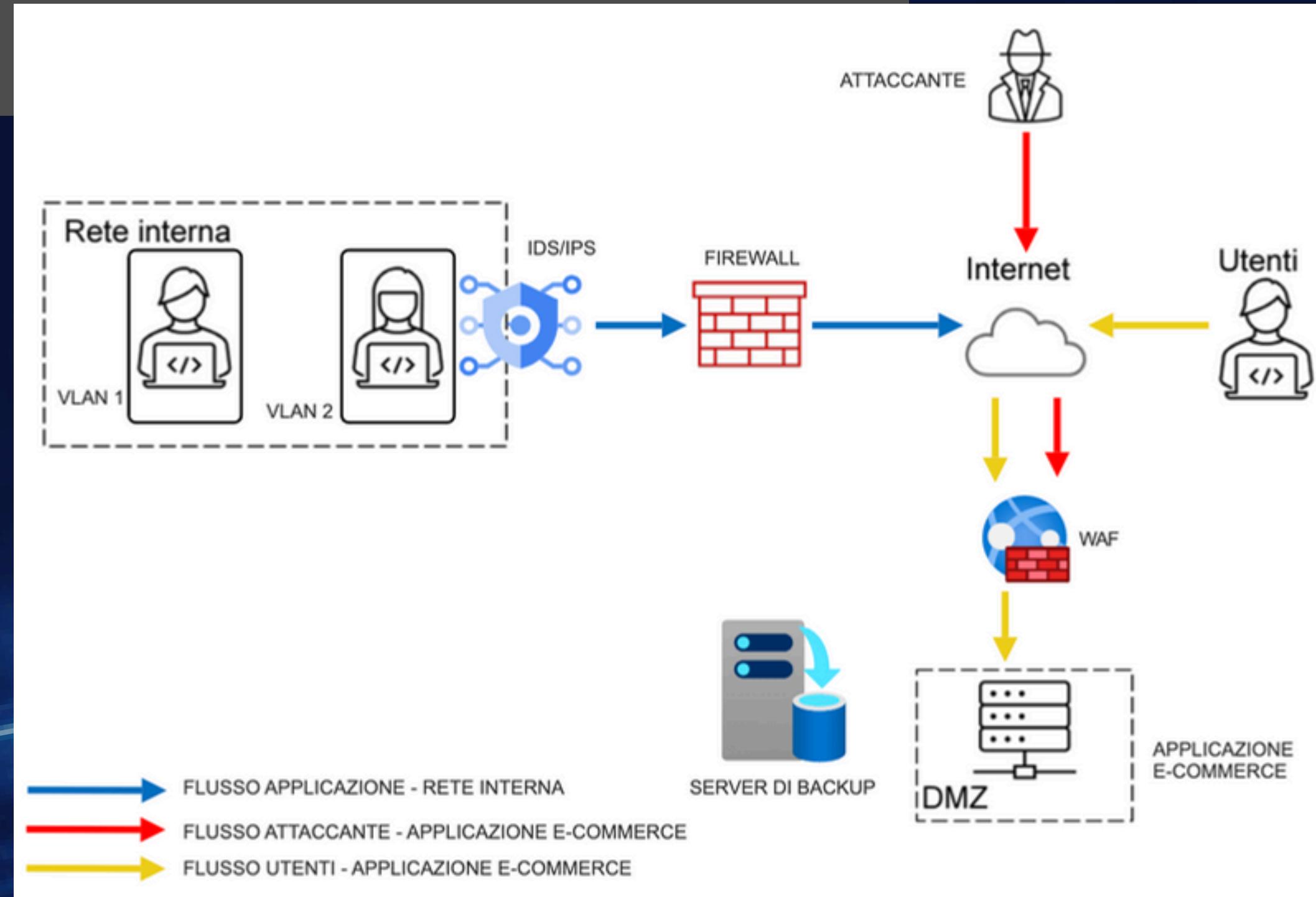
Opzione 2: Rilevamento e Prevenzione delle Minacce Avanzate (~10.000 €)

- **Sistema di Rilevamento delle Intrusioni (IDS) / Sistema di Prevenzione delle Intrusioni (IPS)**
 - Costo: ~3.000 €
 - Monitora e previene accessi non autorizzati e anomalie nel traffico di rete.
- Gestione delle Informazioni e degli Eventi di Sicurezza basata su Cloud (SIEM)
 - Costo: ~2500 €
 - Raccoglie e analizza log da diverse fonti, identificando e correlando eventi di sicurezza per una risposta più efficace.
- **WAF Avanzato con Capacità di Machine Learning**
 - Costo: ~2000 €
 - Utilizza algoritmi di machine learning per riconoscere e bloccare attacchi sconosciuti, migliorando la sicurezza adattiva.
- **Protezione DDoS con Funzionalità Avanzate**
 - Costo: ~2000 €
 - Fornisce una protezione completa, inclusa la pulizia del traffico e l'analisi in tempo reale per prevenire downtime.
- **Sistema di Backup e Failover Avanzato**
 - Costo: ~1000 €
 - Include copie ridondanti dei dati e infrastrutture di failover automatizzate per garantire il funzionamento continuo.

Azioni preventive

Miglioramenti alla configurazione di rete:

- Segmentazione rete interna e isolamento applicazione Web.
- IDS/IPS.
- Server di Backup.



6

BONUS

Analisi log con AnyRun

Traccia

Analizzare le seguenti segnalazioni caricate su AnyRun e fare un piccolo report di ciò che si scopre relativo all'eventuale attacco spiegando ad utenti e manager la tipologia di attacco e come evitare questi attacchi in futuro:

- <https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6/>
- <https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2/>

AnyRun

AnyRun: Piattaforma di Analisi Malware Interattiva

Caratteristiche principali:

- Analisi interattiva:
 - Consente interazione manuale con i file sospetti.
 - Rivela comportamenti nascosti non visibili in analisi automatizzate.
- Ambiente sicuro:
 - File eseguiti in una sandbox isolata.
 - Previene infezioni al sistema host e diffusione nella rete.
- Rilevamento di comportamenti sospetti:
 - Monitora e registra attività, processi, modifiche al file system, connessioni di rete e azioni sul registro di sistema.
 - Identifica rapidamente comportamenti malevoli.

AnyRun

ANY  RUN
INTERACTIVE MALWARE HUNTING SERVICE

MALWARE HUNTING WITH
LIVE ACCESS TO THE
HEART OF AN INCIDENT

Watch the epidemic as if it was on your computer,
but in a more convenient and secure way.
with a variety of monitoring features.

REGISTER FOR FREE

AnyRun è uno strumento potente e flessibile che consente ai professionisti della sicurezza di analizzare in profondità i comportamenti malevoli in un ambiente sicuro e controllato.

Analisi log 1

Scansione sull'Interactive Malware Sandbox per analizzare un eventuale un'attività dannosa di nome data.pdf su sistema Microsoft Windows 10 Pro.

ANYRUN
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Video Screenshots System events Network

General Info

File name: data.pdf
Full analysis: <https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6>
Verdict: **Malicious activity**
Analysis date: July 26, 2024 at 08:20:40
OS: Windows 10 Professional (build: 19045, 64 bit)
Tags: **(generated-doc) (phishing)**
Indicators:
MIME: application/pdf
File info: PDF document, version 1.7, 1 pages
MD5: 0D06D5045BC3B30E9CB90DE1D46EEF01
SHA1: C50A73C13C29A392BA00DC8E9DF7B44815E4EEAD
SHA256: AESC5FC7FDFFED3A2A19405B35FBAE8F3D82D285FC8516963E713171257F29060
SSDEEP: 3072:TMJMarKKzIWWSgoMqi/Hq+CGQQUf0wyah:IKGNzT9sxqcCGP0gh

[1560] msedge.exe C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Threat Verdict
100 OUT OF 100
Malicious
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators:

Timeline of the process
0 s 34.08 s 68.37 s

Danger 1
T1566.002 Spearphishing Link (1)
Phishing has been detected

Other 2
T1012 Query Registry (1)
Reads Microsoft Office registry keys

Application launched itself

Process information
Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 34.08 s

File information
Company: Microsoft Corporation
Description: Microsoft Edge
Version: 122.0.2365.59

Command line
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://clickme.thryv.com/s/click?upnv=001-a-28yHGRfBzjgPYQnB3fzo0t6brPyCAIVBxmb-2fNrGKny-2f3jMpc8U5LisWgcfdU_4wslj8OKpOm07zUjWicHluyUyJntNlgdP9s0-2f8tLXX0D72Qgv2tveAJBLyV1AeB-283DwRaLJ4t6OyYT6R1uyBVQd04xsY5vie2BnTIAfylkeo03qYK-2fxtvw-2f2c-29Y2R6cgOknDXazt6-2fQ2DEesMbsPTZVipbtLYGwAII3X0G-2fX-2Bt6S79bFofC0R2NmxIzuxzg0PgV8t9B-2Bt6pjk0fWkFrJ78f2e44659g1hg1TwuJoTg-2f9p0w0Jz2AWAJVYIWIisuzWhQxu7mQ2oYb05-2Bp0dlNaeUbLgxUfITmre-2Bt6ys5z2KmnAangRbATXNAHnvVpjzdg4Ay73IP9LddUtzf9QHm6wBSDDmssVWnMofof0AxzJ7Wg8-2BwZmI4BhapSLQh0x2fIm7low-3D-#/?dm9sb2R5b0yLmrhrc2VuZW5rb08jYW5wYWWhLmNbQ--

Overview log 1

Tramite menu ATT&CK sono mostrate le azioni malevole rilevate:

- Attività di rete: connessioni effettuate a URL potenzialmente malevoli.
- Numerose letture/modifiche alle chiavi di registro dell'utente.

The screenshot displays three cards from the ATT&CK interface, each detailing a specific threat technique:

- Spearphishing Link (T1566.002)**: A red card indicating a **Danger (1)** level threat. It shows a single subtechnique: **Phishing has been detected (1)**, associated with process **1560 msedge.exe (1)**.
- System Information Discovery (T1082)**: A blue card indicating an **Other (4)** level threat. It lists four subtechniques:
 - Reads the computer name (1) - associated with process **8952 identity_helper.exe (1)**
 - Reads Environment values (1) - associated with process **8952 identity_helper.exe (1)**
 - Checks supported languages (2)
 - 7320 acrobat_sl.exe (1)
 - 8952 identity_helper.exe (1)
- Query Registry (T1012)**: A green card. It shows six subtechniques:
 - Reads Microsoft Office registry keys (2)
 - 6268 Acrobat.exe (1)
 - 1560 msedge.exe (1)
 - Reads the computer name (1) - associated with process **8952 identity_helper.exe (1)**
 - Reads Environment values (1) - associated with process **8952 identity_helper.exe (1)**
 - Checks supported languages (2)
 - 7320 acrobat_sl.exe (1)
 - 8952 identity_helper.exe (1)

Operazioni log 1

Dettaglio delle operazioni eseguite dal malware:

- **Phishing**
 - Tecnica: Spearphishing Link (T1566.002)
 - Descrizione: gli attaccanti inviano email di spearphishing con un link malevolo per ottenere accesso ai sistemi delle vittime. Questa tecnica utilizza link per scaricare malware invece di allegare file malevoli.
 - Attività rilevata:
 - Il processo msedge.exe (PID: 1560) ha aperto un link di phishing identificato come malevolo.

Techniques details
Get to know what this threat is about

Subtechniques ▾ [T1566.002](#)

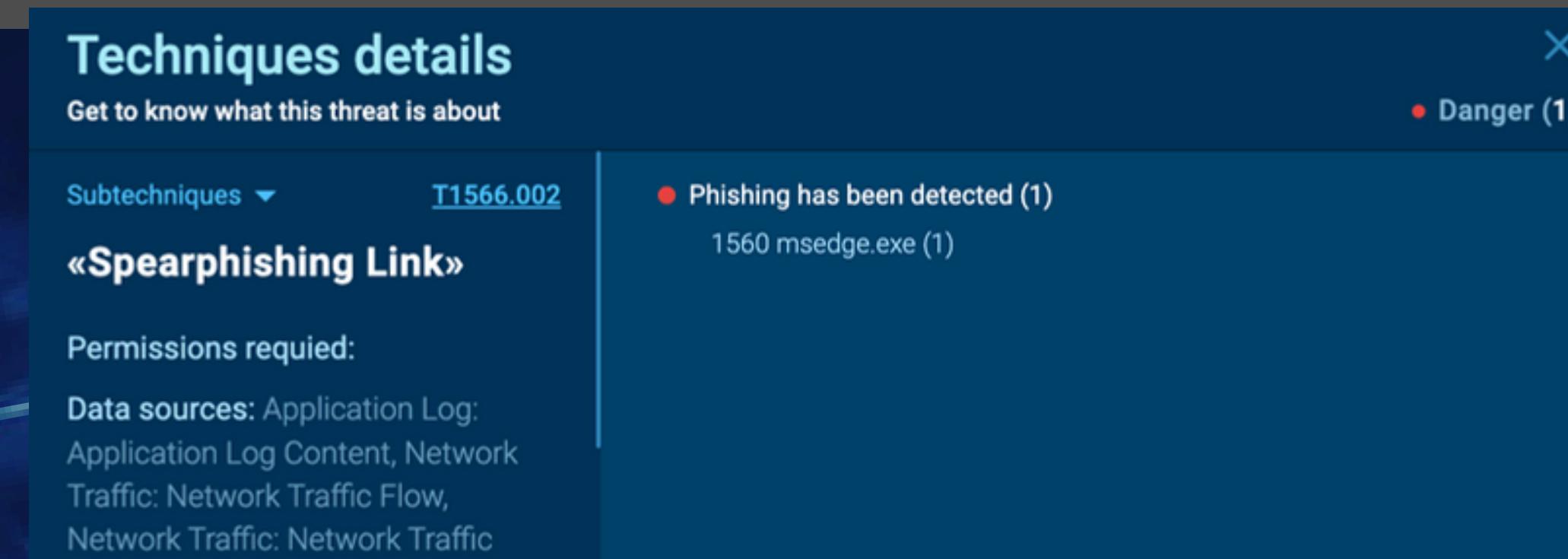
«**Spearphishing Link»**

Permissions required:

Data sources: Application Log:
Application Log Content, Network Traffic: Network Traffic Flow,
Network Traffic: Network Traffic

● Phishing has been detected (1)
1560 msedge.exe (1)

● Danger (1)



Operazioni log 1

- Query Registry
 - Tecnica: Query Registry (T1012)
 - Descrizione: gli attaccanti possono interagire con il registro di Windows per raccogliere informazioni sul sistema, configurazione e software installato.

Techniques details
Get to know what this threat is about

X
• Other (6)

T1012

«Query Registry»

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access

- Reads Microsoft Office registry keys (2)
6268 Acrobat.exe (1)
1560 msedge.exe (1)
- Reads the computer name (1)
8952 identity_helper.exe (1)
- Reads Environment values (1)
8952 identity_helper.exe (1)
- Checks supported languages (2)
7320 acrobat_sl.exe (1)
8952 identity_helper.exe (1)

- Attività rilevata:
 - Processi coinvolti:
 - Acrobat.exe (PID: 6268)
 - msedge.exe (PID: 1560)
 - identity_helper.exe (PID: 8952)
 - acrobat_sl.exe (PID: 7320)
 - Azioni:
 - Lettura delle chiavi di registro di Microsoft Office.
 - Lettura del nome del computer e dei valori dell'ambiente.
 - Controllo delle lingue supportate.

Operazioni log 1

- System Information Discovery
 - Tecnica: System Information Discovery (T1082)
 - Descrizione: gli attaccanti tentano di ottenere informazioni dettagliate sul sistema operativo e l'hardware, inclusi versione, patch, hotfix, service pack e architettura.

Techniques details

Get to know what this threat is about

T1082

«System Information Discovery»

Permissions required:

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution

- Reads the computer name (1)
8952 identity_helper.exe (1)
- Reads Environment values (1)
8952 identity_helper.exe (1)
- Checks supported languages (2)
7320 acrobat_sl.exe (1)
8952 identity_helper.exe (1)

• Other (4)

- Attività rilevata:
 - Processi coinvolti:
 - identity_helper.exe (PID: 8952)
 - acrobat_sl.exe (PID: 7320)
 - Azioni:
 - Lettura del nome del computer e dei valori dell'ambiente.
 - Controllo delle lingue supportate.

Operazioni log 1

- System Information Discovery
 - Tecnica: System Information Discovery (T1082)
 - Descrizione: gli attaccanti tentano di ottenere informazioni dettagliate sul sistema operativo e l'hardware, inclusi versione, patch, hotfix, service pack e architettura.

Techniques details

Get to know what this threat is about

T1082

«System Information Discovery»

Permissions required:

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution

- Reads the computer name (1)
8952 identity_helper.exe (1)
- Reads Environment values (1)
8952 identity_helper.exe (1)
- Checks supported languages (2)
7320 acrobat_sl.exe (1)
8952 identity_helper.exe (1)

• Other (4)

- Attività rilevata:
 - Processi coinvolti:
 - identity_helper.exe (PID: 8952)
 - acrobat_sl.exe (PID: 7320)
 - Azioni:
 - Lettura del nome del computer e dei valori dell'ambiente.
 - Controllo delle lingue supportate.

Analisi log 2

Scansione sull'Interactive Malware Sandbox per analizzare un eventuale un'attività dannosa di un file eseguibile su sistema Microsoft Windows 10.

ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Video Screenshots System events Network  

General Info

File name: 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6
Full analysis: <https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2>
Verdict: **Malicious activity**
Threats: **Phobos** Ransomware Stealer
Phobos is a ransomware that locks or encrypts files to demand a ransom. It uses AES encryption with different ex...
Analysis date: July 26, 2024 at 08:31:20
OS: Windows 10 Professional (build: 19045, 64 bit)
Tags: **phobos** **ransomware** **stealer**
Indicators: 
MIME: application/x-dosexec
File info: PE32 executable (GUI) Intel 80386, for MS Windows
MD5: CA52EF8F80A99A01E97DC8CF7D3F5487
SHA1: D4BF7B56D1F022E14A870D724E8DA274288BC50B
SHA256: 396A2F2DD09C936E93D250E8467AC7A9C0A923EA7F9A395E63C375B877A399A6
SSDEEP: 768:UyVHL0Nw1ALXbLwHi/WEhFOYQj7zs7ERdxmEeQ/9BLQ6XGHFG9laLNTrMh5Xgh6D:UymNrLwC/WPYQ3CU

[4432] 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe
C:\Users\admin\Desktop\396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe

Threat Verdict
100 OUT OF 100 
Malicious
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators: 

Timeline of the process 
0 s 5.17 s 309.42 s
5.17 s 309.42 s

Danger 2
T1547.001 Registry Run Keys / Startup Folder (1)
Changes the autorun value in the registry
Drops the executable file immediately after the start

Warning 1
Application launched itself

Other 2
T1012 Query Registry (2)
Reads the computer name
Checks supported languages
T1082 System Information Discovery (2)
Reads the computer name
Checks supported languages

Overview log 2

Tramite menu ATT&CK sono mostrate le azioni malevole rilevate:

- Il ransomware Phobos cifra i file utilizzando la crittografia AES e richiede un riscatto per la chiave di decrittazione.
 - Phobos può anche rubare informazioni sensibili e condurre attacchi DDoS.



Operazioni log 2

- **Accesso Iniziale**

- Esecuzione del file malevolo da parte dell'utente.

- **Esecuzione**

- Il malware viene eseguito (PID: 4432).
- Avvio di servizi di sistema critici (PID: 5616, 356, 7036).
- Utilizzo della shell dei comandi di Windows (cmd.exe, PID: 1256).

- **Persistenza**

- Boot o autostart all'Accesso/Login: modifica delle chiavi di registro e delle cartelle di avvio per garantire la persistenza (PID: 4432).
- Creazione di file di avvio: file eseguibili piazzati nelle directory di avvio (C:\Users\admin\AppData\Local).

Malicious File ▾

- Manual execution by a user (1)

7016 notepad++.exe (1)

Service Execution ▾

- Executes as Windows Service (3)

5616 VSSVC.exe (1)

7036 wbengine.exe (1)

356 vds.exe (1)

Windows Command Shell ▾

- Starts CMD.EXE for commands execution (1)

4180 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

Registry Run Keys / Startup Folder ▾

- Changes the autorun value in the registry (2)

4432 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (2)

Operazioni log 2

- Escalation dei privilegi

- Modifica delle chiavi di registro: alterazioni nelle chiavi di avvio per acquisire privilegi elevati (PID: 4432).
- Uso di bcdedit.exe: modifica delle opzioni di ripristino e cancellazione delle copie shadow (cmd.exe, PID: 1256).

- Evasione delle difese

- Mascheramento: rinomina delle utility di sistema per nascondere le attività malevoli.
- Evasione della Sandbox/Virtualizzazione: utilizzo di tecniche di evasione basate sul tempo.

- Accesso alle credenziali

- Accesso a file contenenti credenziali non sicure.

Registry Run Keys / Startup Folder ▾

- Changes the autorun value in the registry (2)

4432 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (2)

Rename System Utilities ▾

- Process drops legitimate windows executable (1)

4180 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

Time Based Evasion ▾

- Reads the date of Windows installation (1)

2348 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

Credentials In Files ▾

- Actions looks like stealing of personal data (608)

4180 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (608)

Operazioni log 2

• Discovery

- Query del registro: lettura e modifica delle chiavi di registro di Windows (PID: 4432, 2348).
- Raccolta di informazioni sul sistema (PID: 2348).
- Verifica delle impostazioni di localizzazione del computer.

● Process checks computer location settings (1)

2348 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

● Actions looks like stealing of personal data (608)

4180 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (608)

● Reads the software policy settings (3)

5920 slui.exe (3)

● Checks proxy server information (2)

5920 slui.exe (2)

● Reads the computer name (2)

4432 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)
2348 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

● Reads the date of Windows installation (1)

2348 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

● Reads security settings of Internet Explorer (1)

2348 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

● Checks supported languages (2)

4432 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)
2348 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (1)

● Deletes shadow copies (1)

1256 cmd.exe (1)

● Using BCDEDIT.EXE to modify recovery options (2)

1256 cmd.exe (2)

● Renames files like ransomware (101)

4180 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (101)

● PHOBOS has been detected (10)

4180 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b87
7a399a6.exe (10)

• Impatto

- Inibizione del recupero del sistema: modifiche per impedire il ripristino del sistema (cmd.exe, PID: 1256).
- Cifratura dei dati per creare un impatto significativo (PID: 4180).

Summary log 2

Il ransomware Phobos funziona cifrando i file presenti nel sistema infetto utilizzando la crittografia AES, rendendo i file inaccessibili senza una chiave di decrittazione.

Dopo l'infezione, il malware rinomina i file con estensioni specifiche e richiede il pagamento di un riscatto per ottenere la chiave di decrittazione.

Il malware può eliminare le copie shadow del sistema per impedire il recupero dei file e accedere a credenziali memorizzate nel sistema. Phobos spesso viene distribuito attraverso campagne di phishing.

Procedure di mitigazione

Dopo aver analizzato e compreso le minacce, possibile valutare azioni di mitigazione:

- **Isolamento del sistema infetto:**
 - Disconnettere immediatamente il sistema infetto dalla rete per prevenire ulteriori diffusioni del malware e ridurre il rischio di esfiltrazione di dati.
- **Analisi e rimozione del Malware:**
 - Eseguire una scansione completa del sistema utilizzando software antivirus e strumenti di rimozione malware.
 - Rimuovere tutti i file e processi identificati come malevoli.
 - Controllare e ripristinare le modifiche sospette nel registro di sistema.
- **Ripristino del sistema:**
 - Verificare l'integrità dei backup per assicurarsi che non siano infetti.
 - Ripristinare il sistema utilizzando backup puliti e funzionanti.
- **Aggiornamenti e patch di sicurezza.**
- **Rafforzamento delle politiche di sicurezza:**
 - Configurare e rafforzare le politiche di sicurezza delle email, inclusi filtri anti-phishing.
 - Implementare l'uso di autenticazione a due fattori (2FA).
 - Educare i dipendenti su come riconoscere email e link sospetti.



Thank you!

