

S9 / L5

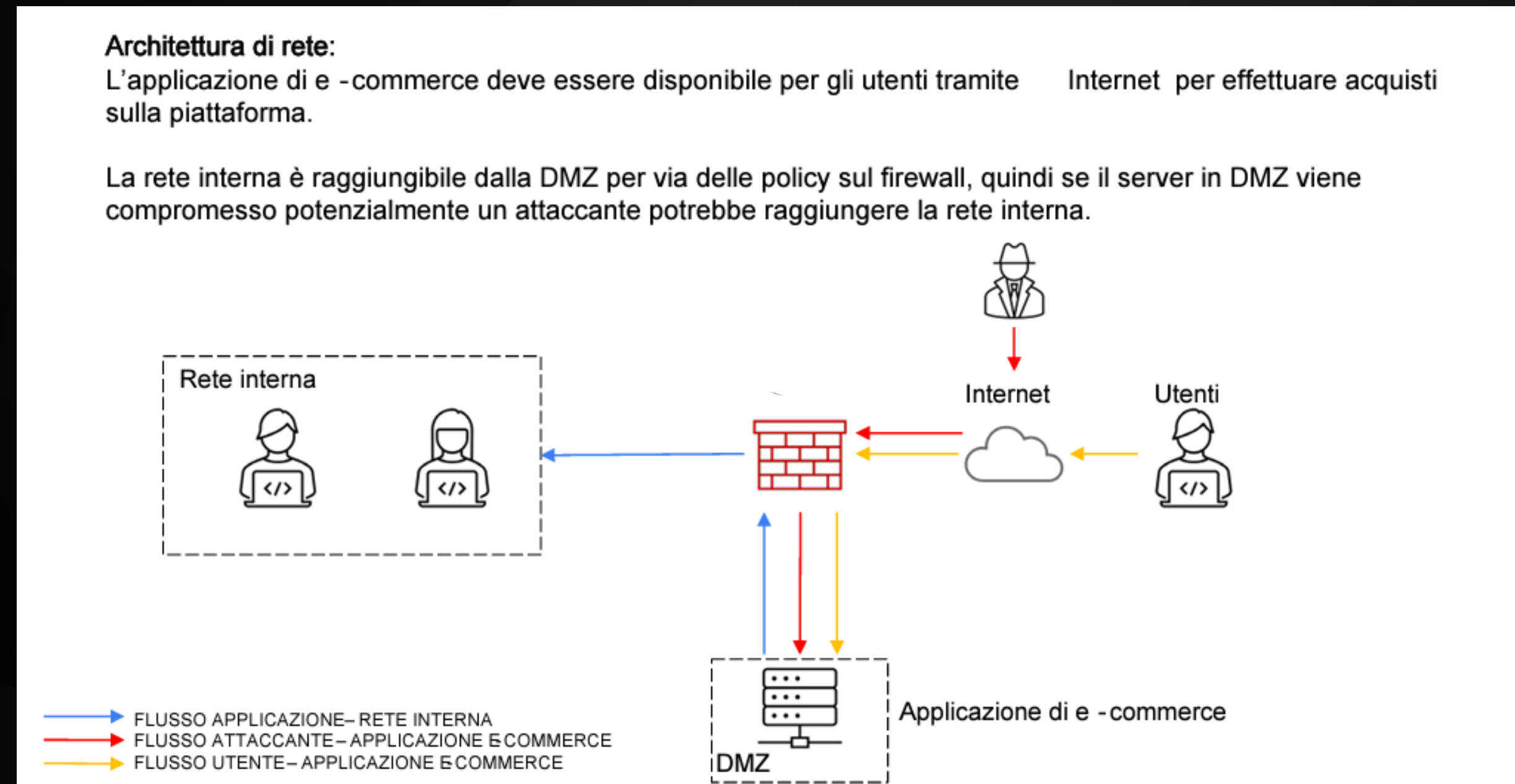
Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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?
Modificate la figura in modo da evidenziare le implementazioni
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 1.500 €** sulla piattaforma di e-commerce . **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**
3. **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 .
4. **Soluzione completa** : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. **Modifica «più aggressiva» dell'infrastruttura:** integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

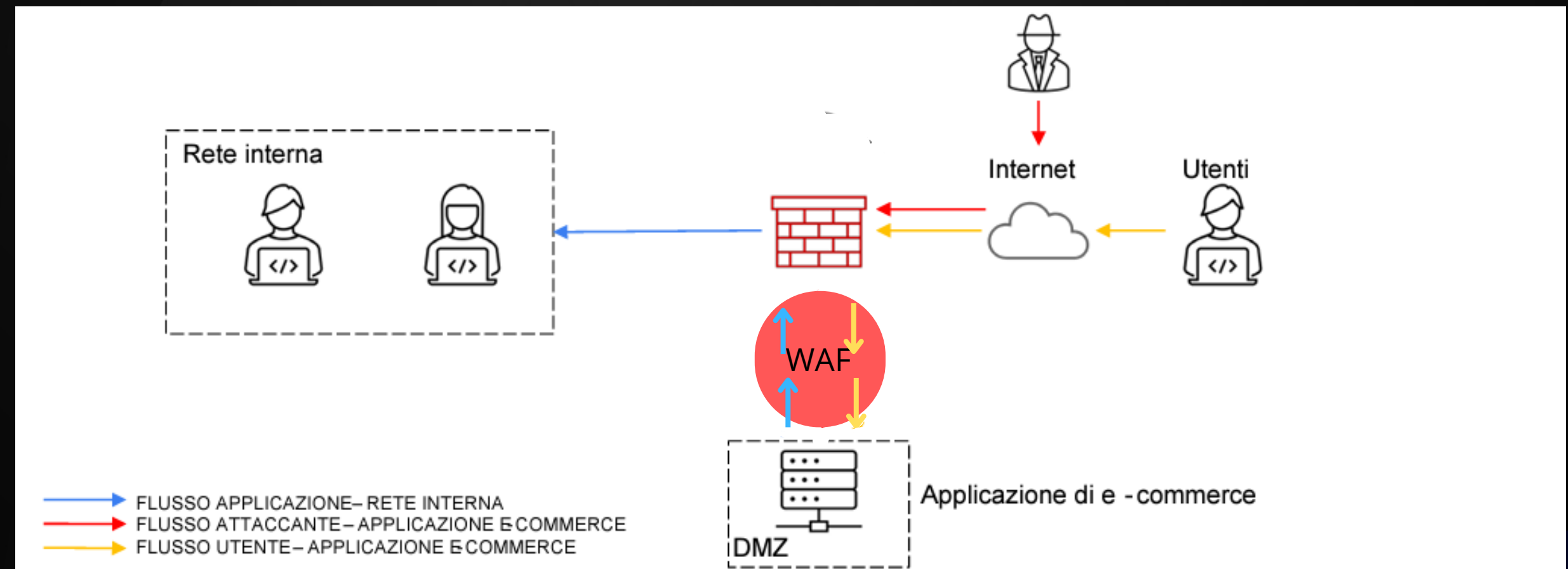
Architettura di rete: L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

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.



AZIONE PREVENTIVA

L'azione preventiva migliore è l'uso del WAF, acronimo di Web Application Firewall. Una soluzione di sicurezza informatica progettata per proteggere le applicazioni web da una serie di minacce, tra cui attacchi di tipo injection SQLi, cross-site scripting (XSS), e altri exploit che mirano alle vulnerabilità delle applicazioni web.



IMPATTO SUL BUSINESS

L'applicazione Web subisce un attacco di tipo DDoS dall'esterno. COSTO TOTALE: 15.000 EURO

Un attacco DDoS (Distributed Denial of Service) mira a sovraccaricare un servizio, rendendolo inaccessibile ai suoi utenti legittimi.

Ecco alcune misure per mitigare l'attacco:

- Firewall e Filtri di Traffico

Configurazione del tuo firewall per bloccare il traffico sospetto o indesiderato. Uso anche di filtri di traffico per riconoscere e bloccare pacchetti dannosi basandoti su criteri specifici

- Monitoraggio del Traffico

Implementa sistemi di monitoraggio del traffico (WIRESHARK) per rilevare anomalie e attacchi DDoS in tempo reale

- Aggiornamenti del Software e dei Firmware

Assicurati che il software e i firmware dei tuoi dispositivi di rete siano sempre aggiornati. Gli attaccanti potrebbero sfruttare vulnerabilità noti per compromettere la tua infrastruttura.

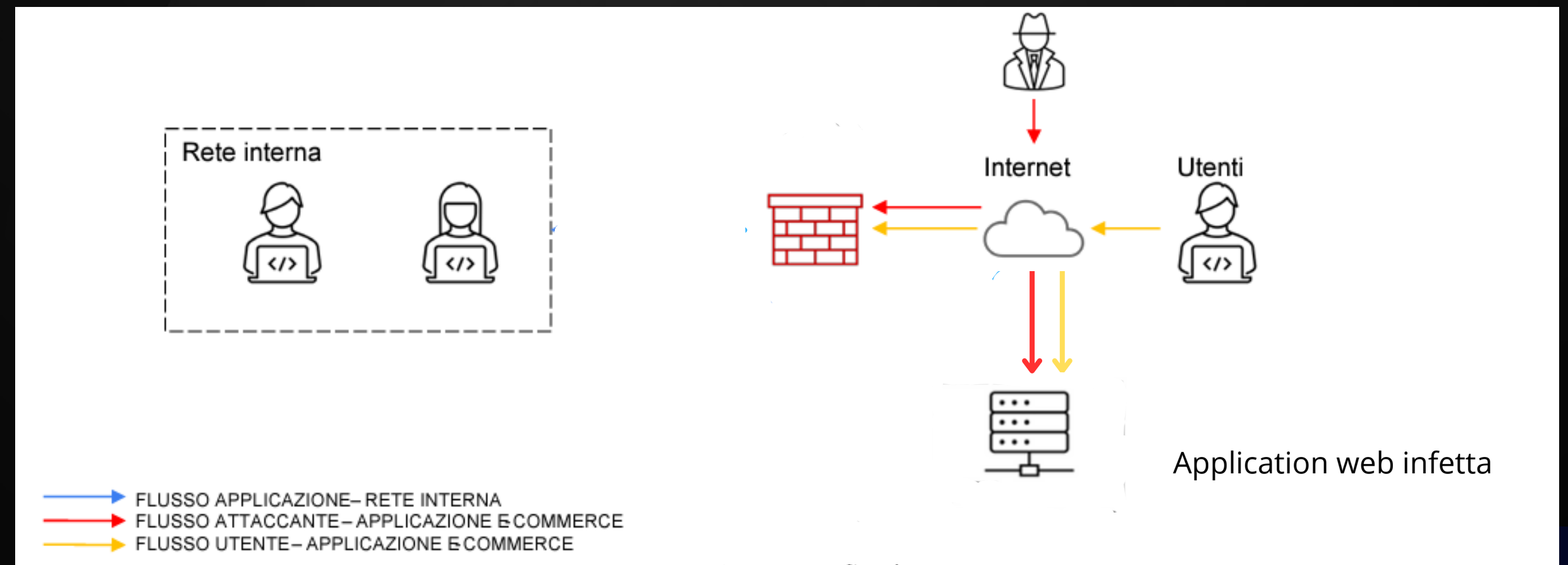
- Pianificazione per la Continuità Operativa (BCP) e Recupero di Disastro (DR)

Sviluppo piani di continuità operativa e recupero di disastro per assicurarsi di poter ripristinare le operazioni il più rapidamente possibile in caso di un attacco DDoS riuscito.

RESPONSE

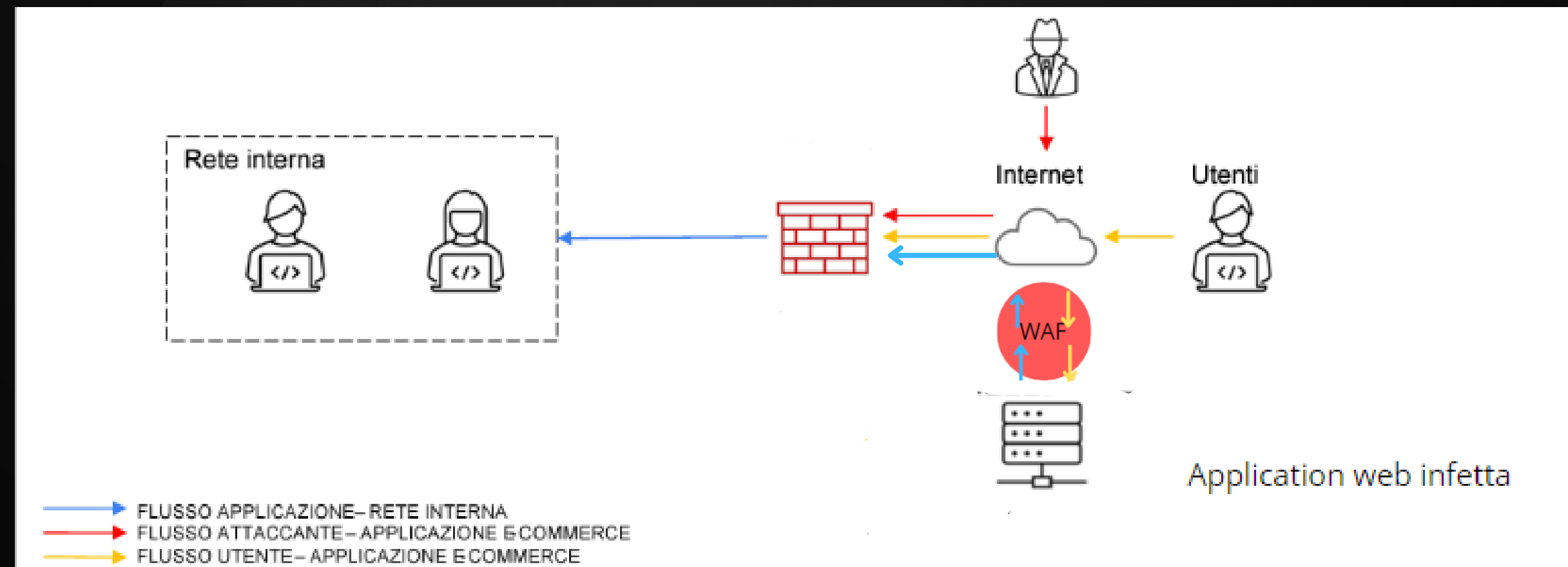
L'isolamento consiste nella completa disconnessione del sistema infetto (in questo caso l'application web) dalla rete, per restringere quasi del tutto l'accesso alla rete interna da parte dell'attaccante.

In ogni caso in tale scenario l'attaccante mantiene l'accesso all'application web e ovviamente anche gli utenti.



SOLUZIONE COMPLETA, unione RESPONSE e ISOLAMENTO

Così facendo
tramite l'uso di WAF
e tecnica di
isolamento il
malware non si
potrà propagare, la
application web
continuerà a
comunicare con la
rete interna e
l'attaccante non
avrà nessun accesso
alla rete interna.

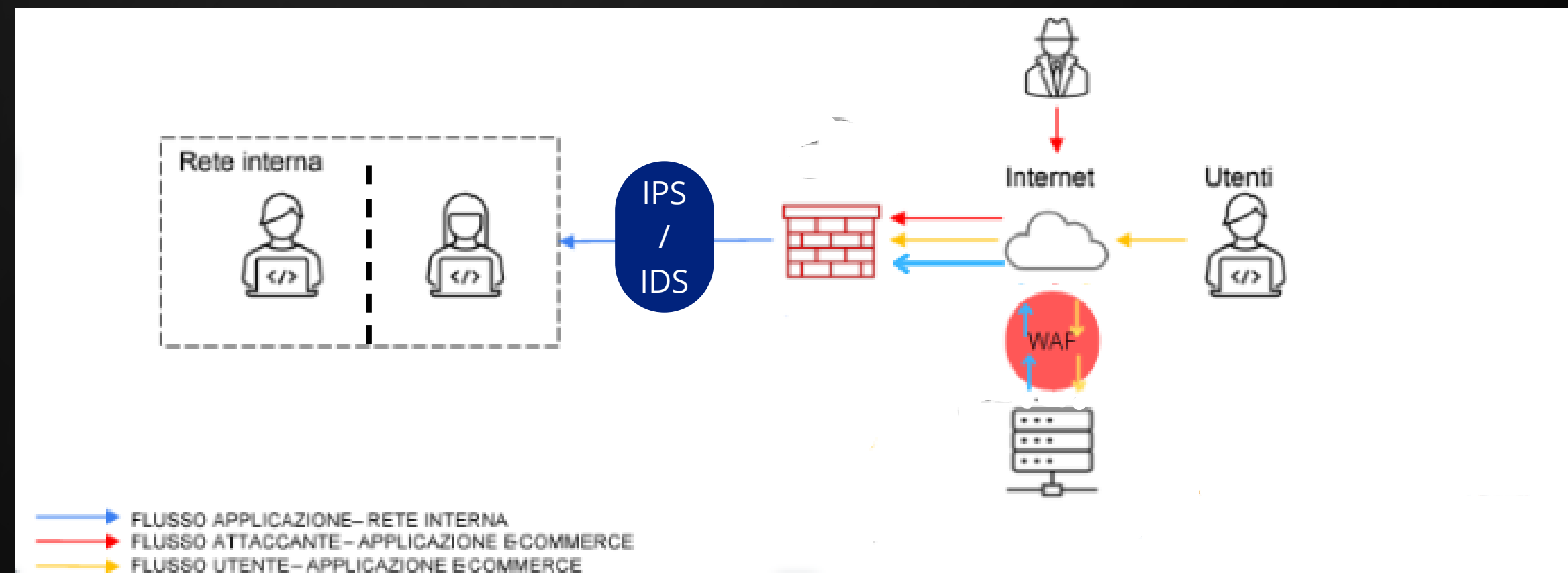


MODIFICA <<AGGRESSIVA>> DELL' INFRASTRUTTURA

BUDGET 7000 EURO

Con tecnica di SEGMENTAZIONE vado ad aumentare notevolmente il livello di sicurezza della rete interna. Il prezzo si aggira sui 4000 euro

Con il budget rimanente installiamo dispositivi IPS/IDS e va a coprire all'incirca 3000 euro. Un' ulteriore implementazione della sicurezza, in quanto svolgono la funzione di filtro.





ANALISI DI ANYRUN

PERFORMANCE BOOSTER programma mascherato
che incrementa le performance del computer

Process details ID 2088 **Malicious**

PERFORMANCE_BOOSTER_v3.6.exe

Username: admin
Start: +0ms Indicators:  

100
OUT OF 100

Command line

"C:\Users\admin\AppData\Local\Temp\PERFORMANCE_BOOSTER_v3.6.exe"

More Info

Danger 1




Drops the executable file immediately after the start

Malicious activity

PERFORMANCE_BOOSTER_v3.6.exe

MD5: 166903C9A390527CCD7728AE799A9D87
Start: 08.02.2024, 18:39 Total time: 60 s

Win7 32 bit
Complete

Indicators:   

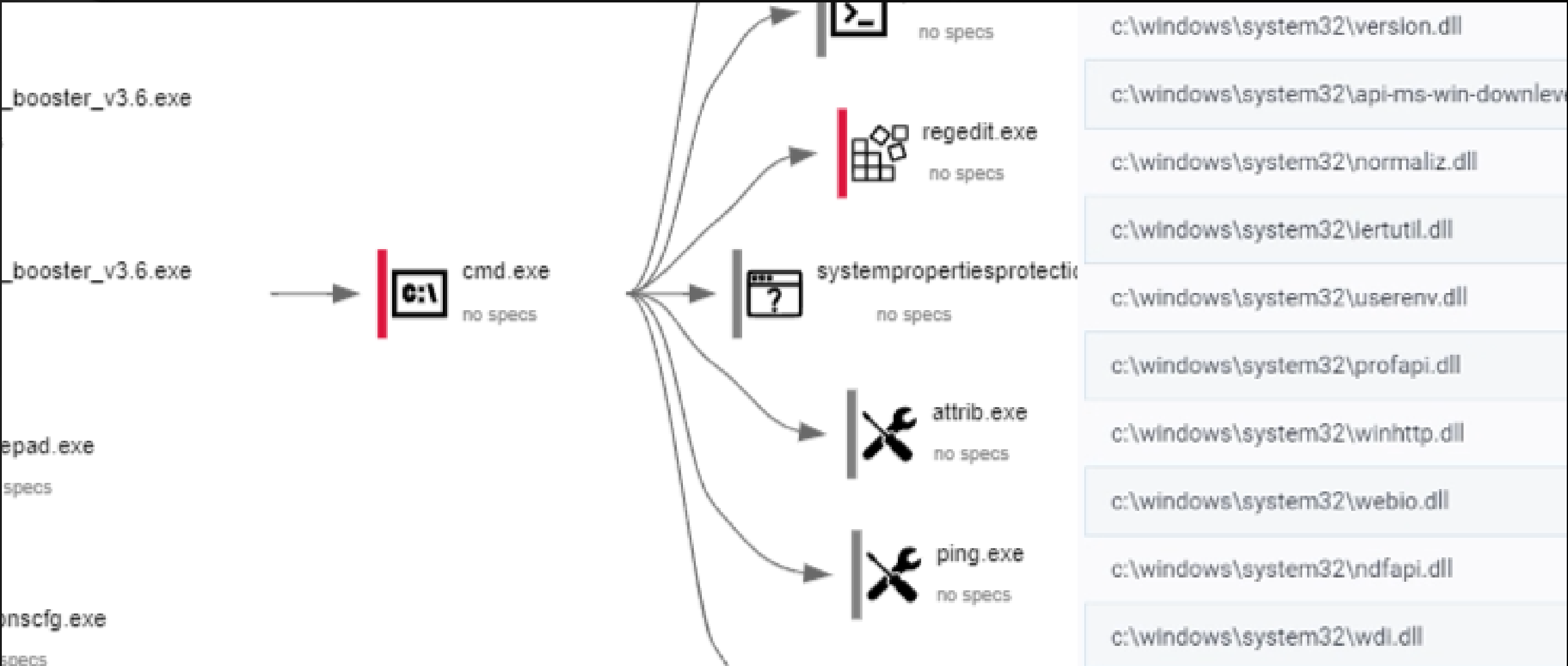
Get sample **IOC** **MalConf** **Restart**

Text report **Graph** **ATT&CK** **ChatGPT** **Export**

Processes Filter by PID or name ☒ Only important

2088	PERFORMANCE_BOOSTER_v3.6.exe	140	6	19
668	cmd.exe /c "C:\Users\admin\AppData\Local\Temp\3201..."	7k	133	110
2380	mode.com MODE CON: COLS=78 LINES=54	39	8	16
3332	powershell.exe Set-ExecutionPolicy Unrestricted -For...	2k	639	87
2824	regedit.exe /e "C:\Users\admin\Desktop\FullRegistryBack...	5k	359k	30
3612	SystemPropertiesProtection.exe	653	103	88
3888	attrib.exe -r C:\Windows\System32\drivers\etc\hosts	49	9	15

L'attaccante ha infettato la vittima con un malware, il quale si esegue appena avviato un programma. Creando così una shell tramite il payload. L'indicazione che un file infetto "starts CMD.EXE for commands execution" significa che il file sta cercando di eseguire comandi tramite il prompt dei comandi di Windows (CMD.EXE). Questa attività potrebbe essere sospetta, poiché alcuni malware o script malevoli cercano di sfruttare il prompt dei comandi per eseguire operazioni dannose sul sistema. Inoltre questo malware agisce sulle librerie DLL le quali contengono codice e dati che utilizzati da più di un'applicazione contemporaneamente, consentendo la condivisione di risorse e la riduzione dello spazio su disco. Tipico degli attacchi DoS.



Behavior activities

MALICIOUS

Changes powershell execution policy (Unrestricted)

- `cmd.exe` (PID: 668)

Drops the executable file immediately after the start

- `PERFORMANCE_BOOSTER_v3.6.exe` (PID: 2088)

SUSPICIOUS

Starts `CMD.EXE` for commands execution

- `PERFORMANCE_BOOSTER_v3.6.exe` (PID: 2088)

Using PowerShell to operate with local accounts

- `powershell.exe` (PID: 3332)

Starts `POWERSHELL.EXE` for commands execution


- `cmd.exe` (PID: 668)

R I S O L U Z I O N E





Soluzioni migliori sono l'eliminazione completa del file, scansione con antivirus.

BONUS 2

Malicious activity



Win7 32 bit
Complete

Indicators:    

https://1drv.ms/u/s!A17eQ7h8kx6-nQM1R...

Open in browser

Start: 08.02.2024, 18:37 Total time: 60 s

IOC

MalConf

Restart

Text report

Graph

ATT&CK

ChatGPT

Export

CPU

RAM

Processes

Filter by PID or name

Only important

2476	MicrosoftEdgeUpdateSet...	PE	/installsource tag...	447	12	21
4040	MicrosoftEdgeUpdate.exe	PE	/installsource t...	1k	175	56
2436	MicrosoftEdgeUpdate.exe	PE	/regsvc	202	50	28
4012	MicrosoftEdgeUpdate.exe	PE	/regserver	380	90	31
3408	MicrosoftEdgeUpdate.exe	PE	/ping PD9...	713	3k	86
2812	MicrosoftEdgeUpdate.exe	PE	/handoff *...	329	57	40
3796	SER MicrosoftEdgeUpdate.exe	PE	/svc	840	4k	65

Microsoft Edge

Download Microsoft Edge

To install the browser, you must be the PC administrator and might need to download updates to your Windows PC and restart it.

HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE SOFTWARE.

1. MICROSOFT EDGE FOR WINDOWS DEVICES

1.1. Windows License Terms . Your installation and use of the Software on any Windows platform shall be governed by the license terms for your Microsoft Windows Operating System software ("Windows License Terms") on which you are using the Software, and those terms are incorporated by reference. If the Software is downloaded from Microsoft and labeled preview, insider, beta or pre-release, or is otherwise indicated as not being a final retail version of the Software, the applicable terms in Section 1.2 also apply to your use of the Software. Section 1.3 applies to your use of other services that may be made available for use through your use of the Software.

1.1.1. Updates . Notwithstanding above Section 1.1 as applied to Windows 7, 8, and 8.1, the terms of the applicable Windows License Terms, or any Windows update settings you have configured, the Software periodically checks for updates, and downloads and installs them for you. You may obtain updates only from Microsoft or authorized sources, and Microsoft may need to update your system to provide you with those updates. By accepting this agreement, you agree to receive these types of automatic updates without any additional notice.

1.2. Previews . Microsoft may make preview, insider, beta or other pre-release versions of the Software ("Previews") available to you. You may use Previews only up to the Software's expiration date (if any) and so long as you comply with the applicable Windows License Terms. Previews are experimental, which means that Previews may not operate correctly and may

Privacy statement

Accept and download








La directory C:\Windows\System32 è una directory cruciale del sistema operativo Windows, e i file al suo interno sono fondamentali per il corretto funzionamento del sistema. KernelBase.dll è una libreria di sistema di Windows che contiene funzioni essenziali per le applicazioni basate su Windows.

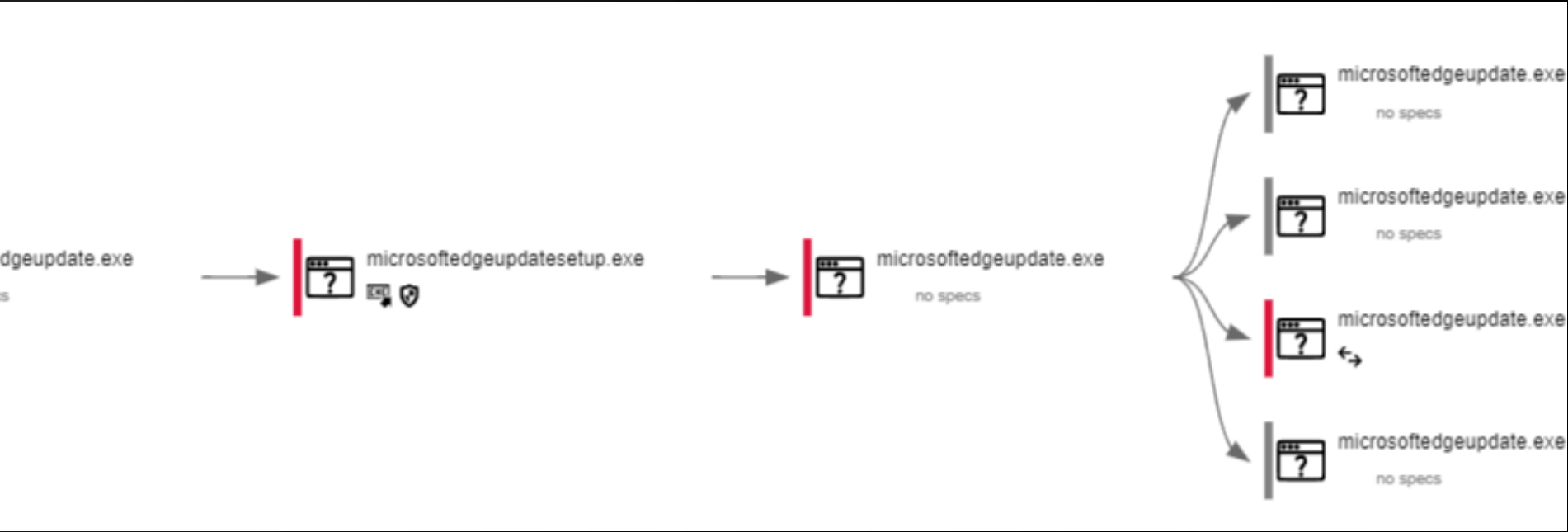
Se un attaccante ha agito su C:\Windows\System32\KernelBase.dll, ciò potrebbe avere gravi conseguenze, poiché potrebbe compromettere il funzionamento stabile del sistema operativo e delle applicazioni. Una grave conseguenza è l'instabilità del Sistema in quanto la manipolazione di KernelBase.dll potrebbe causare instabilità nel sistema operativo, comportando arresti anomali o crash delle applicazioni.

L'attaccante potrebbe aver sostituito KernelBase.dll con una versione dannosa, consentendo l'esecuzione di codice malevolo o l'attuazione di azioni dannose.

La modifica di KernelBase.dll potrebbe essere finalizzata a raccogliere informazioni sensibili o a facilitare l'accesso non autorizzato al sistema.

Una possibile azione è quella di creare una backdoor e attivare un meccanismo di accesso remoto nel sistema, consentendo l'accesso continuato e non autorizzato.

BEFORE	LOAD		C:\Users\admin\AppData\Local\Temp\EU9F13.tmp\MicrosoftEdgeUpdateSetup.exe
BEFORE	LOAD		C:\Windows\System32\ntdll.dll
BEFORE	LOAD		C:\Windows\System32\kernel32.dll
BEFORE	LOAD		C:\Windows\System32\KernelBase.dll
BEFORE	LOAD		C:\Windows\System32\advapi32.dll
+15 ms	LOAD		C:\Windows\System32\msvcrt.dll
+15 ms	LOAD		C:\Windows\System32\sechost.dll



RISOLUZIONE

Campagna anti phishing
Istruire utenti a intuire se i siti sono attendibili.

Utilizzo di firewall efficienti o proxy
Impedire così pacchetti malevoli tramite filtraggio.