S9/L5

ANALISI DEI LOG

ELEONORA VIOLA

TABLE OF CONTENT

INTRODUCTION

Traccia:

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. È richiesta sola modifica.

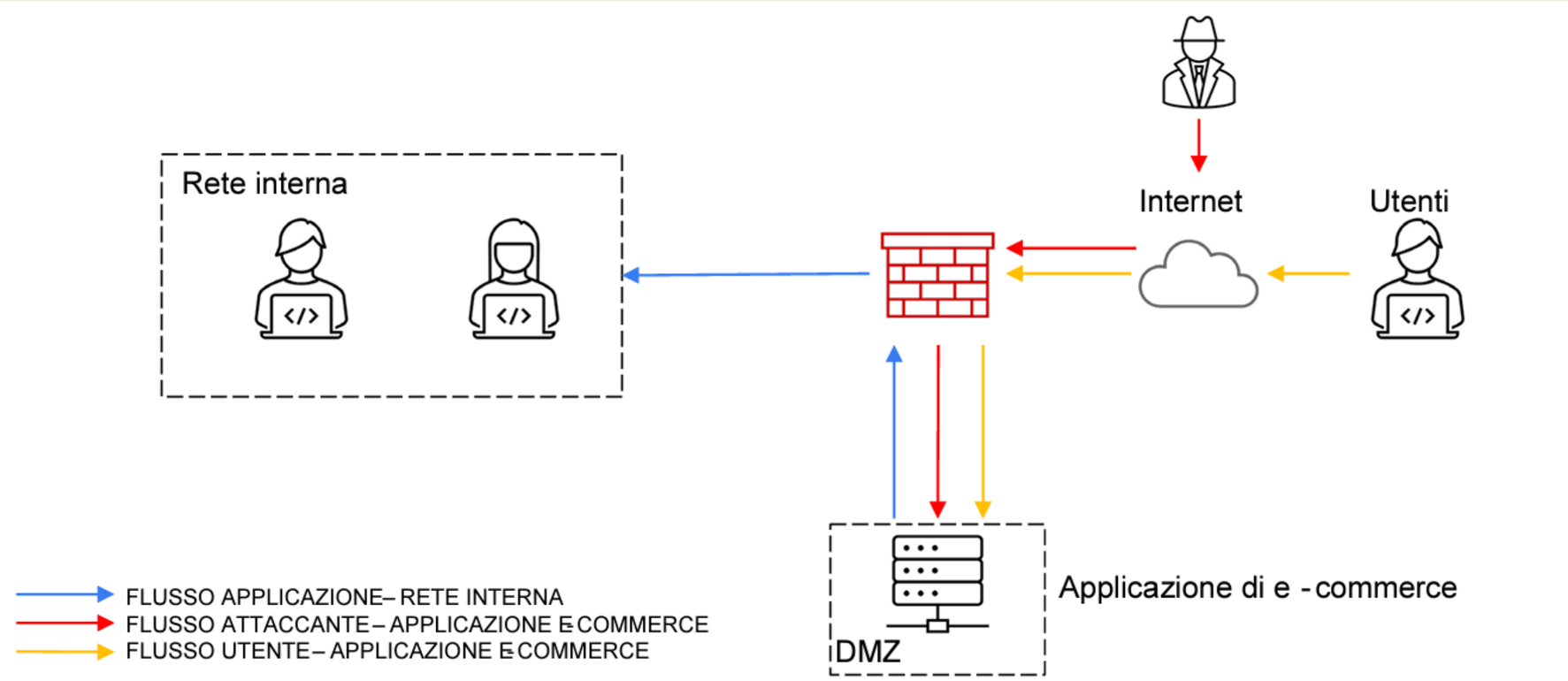
2. Impatti sul business : l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma 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 vostre 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 (integrando anche una soluzione al punto 2). Budget 5000-10000 euro. Eventualmente fare più proposte di spesa

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.



AZIONI PREVENTIVE

Misure preventive contro gli attacchi di SQLi e XSS

Affinché un'applicazione web sia protetta da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), è necessario adottare una serie di misure preventive volte a proteggere i punti di accesso dell'applicazione.

Le principali azioni preventive possono includere:

- **Validazione e Sanitizzazione degli Input:** in modo che non siano presenti caratteri pericolosi, è obbligatorio convalidare e pulire attentamente ogni input fornito dagli utenti. Consigliamo ulteriormente di utilizzare le funzioni di librerie apposite per filtrare gli input e prevenire l'inserimento o il potenziale danneggiamento dei caratteri. Inoltre bisogna verificare che gli input dei campi accettino solo i tipi di dati corretti (ad esempio, numeri in campo numerico, indirizzi email nei campi email, ecc.).

- **Utilizzo di Query Parametrizzate:** è necessario parametrizzare le query SQL per evitare che i comandi SQL vengano interpretati come input degli utenti. Infatti l'utilizzo dei parametri nelle query consente di mantenere separato il codice SQL dai dati forniti dagli utenti, evitando così l'iniezione di comandi malevoli.

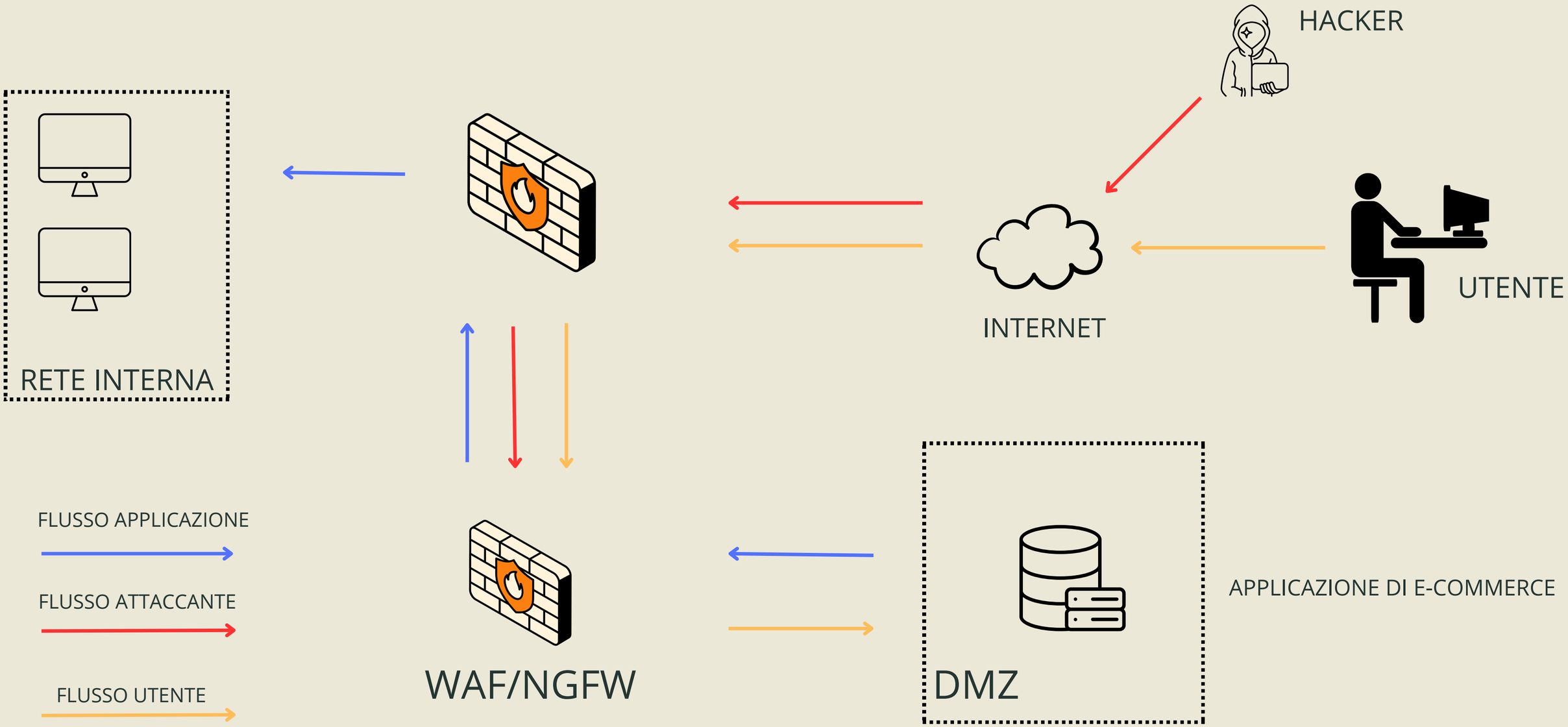
- **Content Security Policy (CSP):** si può impostare una CSP per restrizioni delle origini da cui il browser è autorizzato a caricare risorse come script, stili e immagini. La configurazione accurata di una CSP consente di prevenire numerosi attacchi XSS impedendo l'esecuzione di script non autorizzati.

- **Web Application Firewall (WAF):** un Application Firewall (WAF) è in grado di controllare e sorvegliare il flusso delle richieste HTTP verso l'applicazione web, riconoscendo e impedendo la propagazione del traffico dannoso. I Web Application Firewall possono rilevare schemi di attacco già noti e il loro riconoscimento può essere aggiornato per individuare anche nuovi rischi.

- **Firewall di Nuova Generazione (NGFW): s**e non ci sono problemi di budget al posto del WAF si potrebbe pensare di implementare un NGFW, che integra il filtraggio del traffico di rete con una serie di altre funzioni di sicurezza, come la prevenzione delle intrusioni (IPS), il controllo delle applicazioni, l'ispezione del contenuto, la protezione contro le minacce e la visibilità del traffico crittografato.

WEB APPLICATION FIREWALL

Quest’ultimo punto è quello che utilizzeremo nella parte grafica:



IMPATTI SUL BUSINESS

In questa situazione l’applicazione Web subisce un attacco di tipo DDoS dall’esterno che rende l’applicazione non raggiungibile per 10 minuti.

DDOS

Un attacco Distributed Denial of Service (DDoS) è un tentativo malevolo di interrompere il normale traffico di un server, servizio o rete sovraccaricandolo con un flusso di traffico Internet travolgente. Gli attacchi DDoS sfruttano più sistemi informatici compromessi come fonti di traffico di attacco. Le macchine sfruttate possono includere computer e altre risorse di rete come dispositivi IoT.

Calcolo dell'Impatto Economico

Se gli utenti spendono mediamente 1.200 € al minuto sulla piattaforma di e-commerce, un'interruzione di 10 minuti può comportare una perdita di entrate come segue:

Perdita totale = 10minuti x 1.200€= 12.000€

Le azioni preventive per mitigare questo rischio possono includere:

1. **Soluzioni Anti-DDoS:** sono servizi di mitigazione DDoS forniti da provider specializzati (come Cloudflare, Akamai, ecc.), possono rilevare e bloccare traffico anomalo prima che raggiunga l'infrastruttura interna.
2. **Load Balancer:** i load balancer sono utili per distribuire il traffico tra diversi server, prevenendo sovraccarichi e migliorando la resilienza.
3. **Scalabilità Automatica:** infine se si configurano sistemi di scalabilità automatica per aumentare temporaneamente le risorse dell'infrastruttura durante picchi di traffico.

In seguito vedremo nel dettaglio i dispositivi proposti.

RESPONSE

Malware e tipologie comuni:

Il termine malware nasce dalla combinazione delle parole “malicious” (malevolo) e “software” e si riferisce a qualsiasi tipo di software progettato per danneggiare, compromettere o alterare il funzionamento di un sistema informatico, di un dispositivo o di una rete, senza il consenso o la conoscenza da parte dell’utente.

I tipi più comuni di malware sono:

- **Virus**: si diffonde passando da computer a computer, senza azione diretta o autorizzazione da parte dei sistemi infetti. Si copiano in sezioni particolari all’interno del file system e i più sofisticati cercano di nascondersi dalle analisi dei vari sistemi di sicurezza (come antivirus o anti malware).

- **Trojan:** un tipo di malware che si nasconde all’interno di un file apparentemente innocuo, come un documento office oppure un PDF, si attiva quando la vittima apre il file. Tra i trojan più comunemente utilizzati troviamo le backdoor, che sono generalmente utilizzate per fornire agli attaccanti delle shell sui sistemi infetti.

- **Rootkit:** un malware progettato per nascondersi dagli utenti e dagli antivirus per prendere il controllo completo del sistema operativo. Un rootkit permette di mantenere privilegi elevati su una macchina senza essere notati.

- **Bootkit:** sono dei rootkit che aggirano le protezioni del sistema operativo in quanto entrano in funzione prima dell’avvio completo del sistema operativo, in particolar modo prima dell’attivazione dei moduli di sicurezza di un sistema operativo.

- **Adware:** sono dei programmi fastidiosi che mostrano pubblicità agli utenti di un pc.

- **Spyware:** programmi che si usano per raccogliere informazioni sulle attività degli utenti di un sistema, ad esempio: il tipo di sistema operativo installato sulla macchina, i siti visitati, le password. Queste informazioni vengono inviate successivamente ad un server sotto il controllo dell’attaccante.

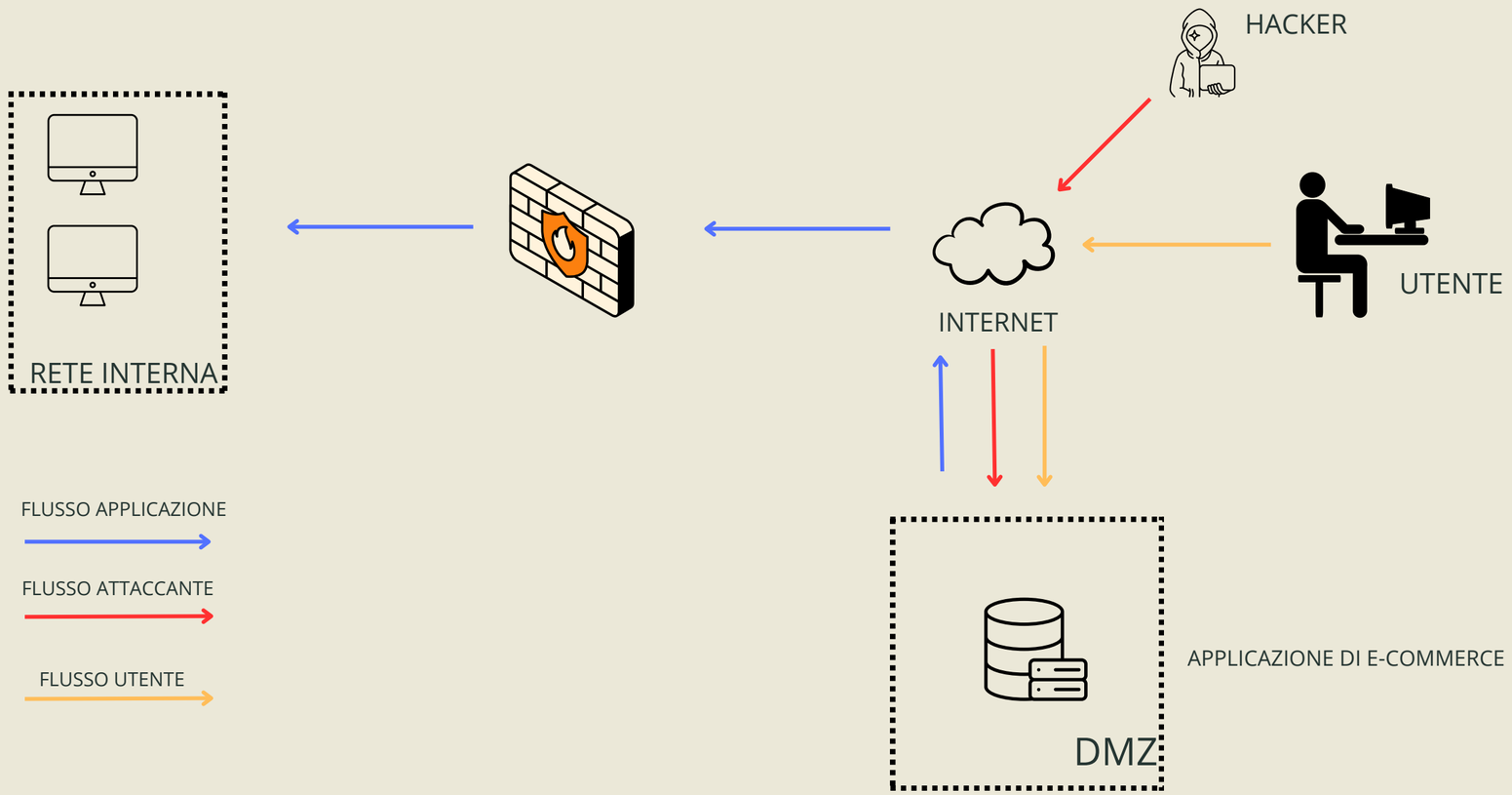
- **Dialer:** un programma che cerca di chiamare numeri telefonici a pagamento per guadagnare soldi.

- **Keylogger:** programma che registra ogni tasto premuto sulla macchina della vittima, salvano poi queste informazioni in un file di log che spediscono ad un server controllato dall’attaccante.

PROPOSTA SOLUZIONE RESPONSE

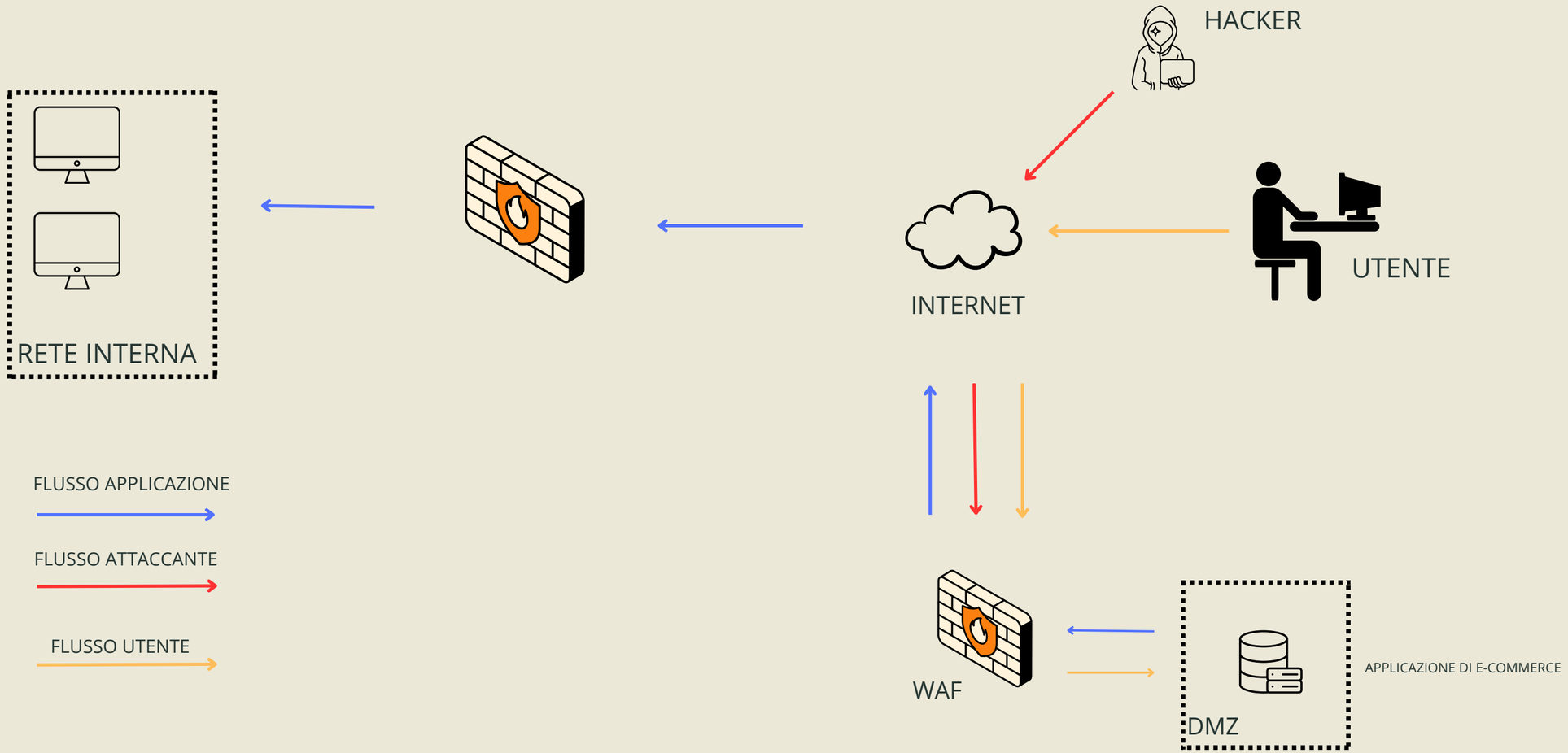
Considerando che la nostra priorità è impedire la diffusione di malware nella nostra rete, riteniamo che la scelta più efficace sia quella di mettere in quarantena la macchina infettata.

L'attaccante potrà raggiungere la suddetta macchina poiché essa resterà collegata ad internet, tuttavia, non è più collegata alla nostra rete interna come mostrato nella Figura 3.



SOLUZIONE COMPLETA

Combinando le misure preventive contro SQLi e XSS con le azioni di risposta per contenere il malware, otteniamo una soluzione completa per proteggere l'infrastruttura IT. La figura seguente rappresenta tutte le misure preventive e di risposta implementate insieme:



MODIFICA INFRASTRUTTURA

Adesso che abbiamo analizzato le debolezza dell'infrastruttura, possiamo dunque proporre delle soluzioni che rientrano nel budget richiesto per proteggere al meglio l'azienda:

1. **Firewall di Nuova Generazione (NGFW)**
- Esempio: Fortinet FortiGate 60F
- Prezzo: 1.000 €
- Scopo: protezione avanzata contro attacchi di rete, inclusi quelli DDoS, con funzionalità di filtraggio dei contenuti, controllo delle applicazioni e protezione contro le minacce.
2. **Web Application Firewall (WAF)**
- Esempio: AWS WAF
- Prezzo: Circa 20 € al mese per il servizio base, più costi aggiuntivi basati sul numero di regole e richieste.
- Scopo: protegge le applicazioni web da attacchi comuni, consentendo la creazione di regole personalizzate per filtrare il traffico HTTP/HTTPS. (Soluzione più economica rispetto a NGFW)
3. **Sistema di Prevenzione delle Intrusioni (IPS)**
- Esempio: Snort (Software Open Source) o Cisco Secure IPS
- Prezzo: Snort gratuito, Cisco Secure IPS 2.000 €
- Scopo: monitoraggio e analisi del traffico di rete per identificare e prevenire attacchi in tempo reale, utile per difendere da exploit come SQLi e XSS.
4. **Servizio di Protezione DDoS (Cloud-based)**
- Esempio: Cloudflare Business
- Prezzo: 4.000 € all'anno
- Scopo: protezione continua contro attacchi DDoS, mitigando il traffico malevolo e mantenendo il sito operativo.
5. **Sistema di Backup e Ripristino Avanzato**
- Esempio: Veeam Backup & Replication
- Prezzo: 1.500 €
- Scopo: esecuzione di backup regolari e ripristino rapido dei dati in caso di attacco malware o perdita dei dati.
6. **Sistema di Monitoraggio e Analisi del Traffico**
- Esempio: SolarWinds Network Performance Monitor
- Prezzo: 2.500 €
- Scopo: monitoraggio in tempo reale del traffico di rete per rilevare anomalie e rispondere rapidamente a eventuali attacchi o problemi di prestazioni.

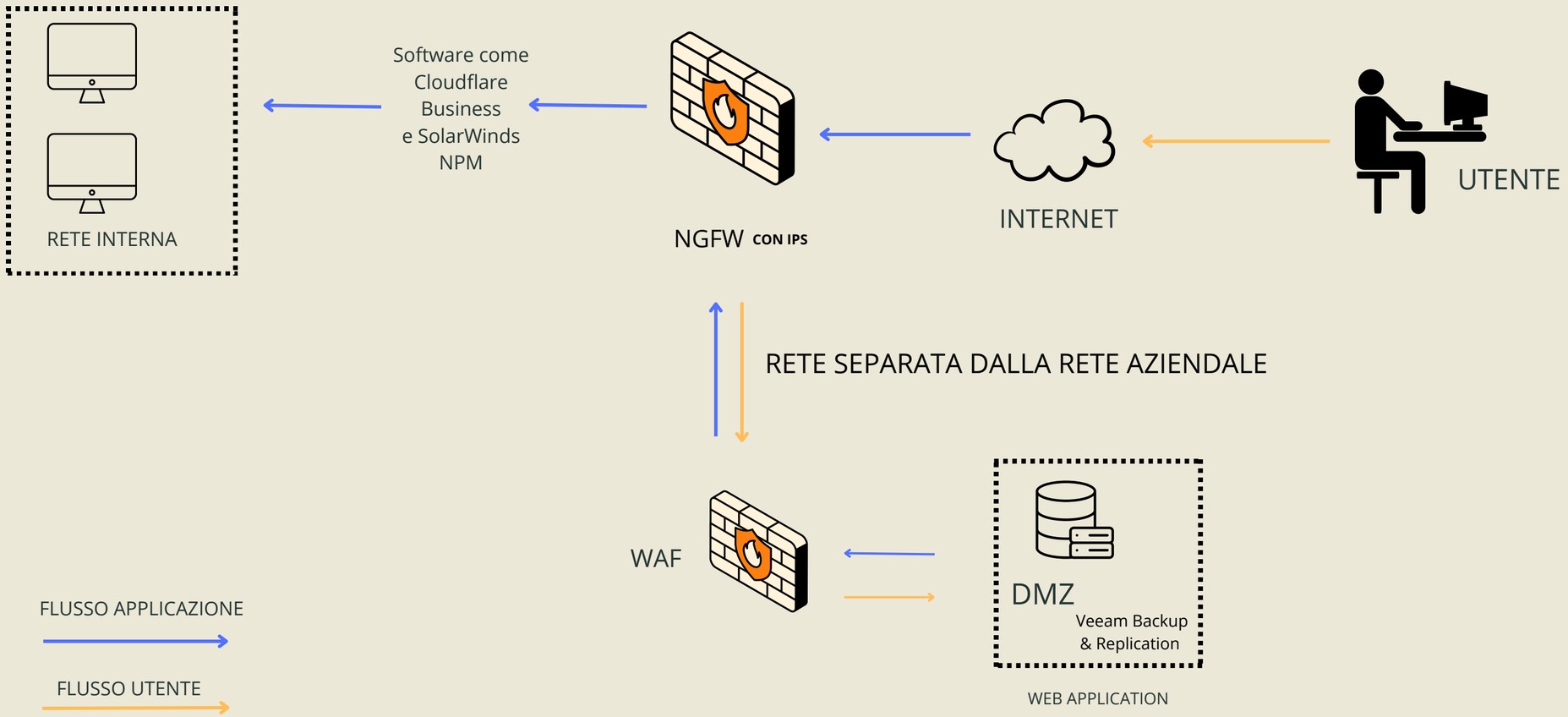
TOTALE STIMATO

Opzione Economica: Circa 7.000 euro
Opzione Completa: Fino a 11.000 euro

CONCLUSIONE

- **Firewall e IPS:** fondamentali per proteggere e monitorare la rete. Quello citato ovvero il Fortinet FortiGate 60F fornisce protezione avanzata, che con l'IPS aiuta a identificare e prevenire exploit.
- **Servizio DDoS:** Cloudflare Business è cruciale per mantenere la disponibilità del sito durante attacchi DDoS, minimizzando il rischio di downtime.
- **Backup e Ripristino:** Veeam Backup & Replication garantisce il recupero rapido dei dati in caso di attacco malware, riducendo l’impatto delle perdite di dati.
- **Monitoraggio del Traffico:** SolarWinds Network Performance Monitor è essenziale per rilevare anomalie e rispondere tempestivamente a problemi di sicurezza o di prestazioni.

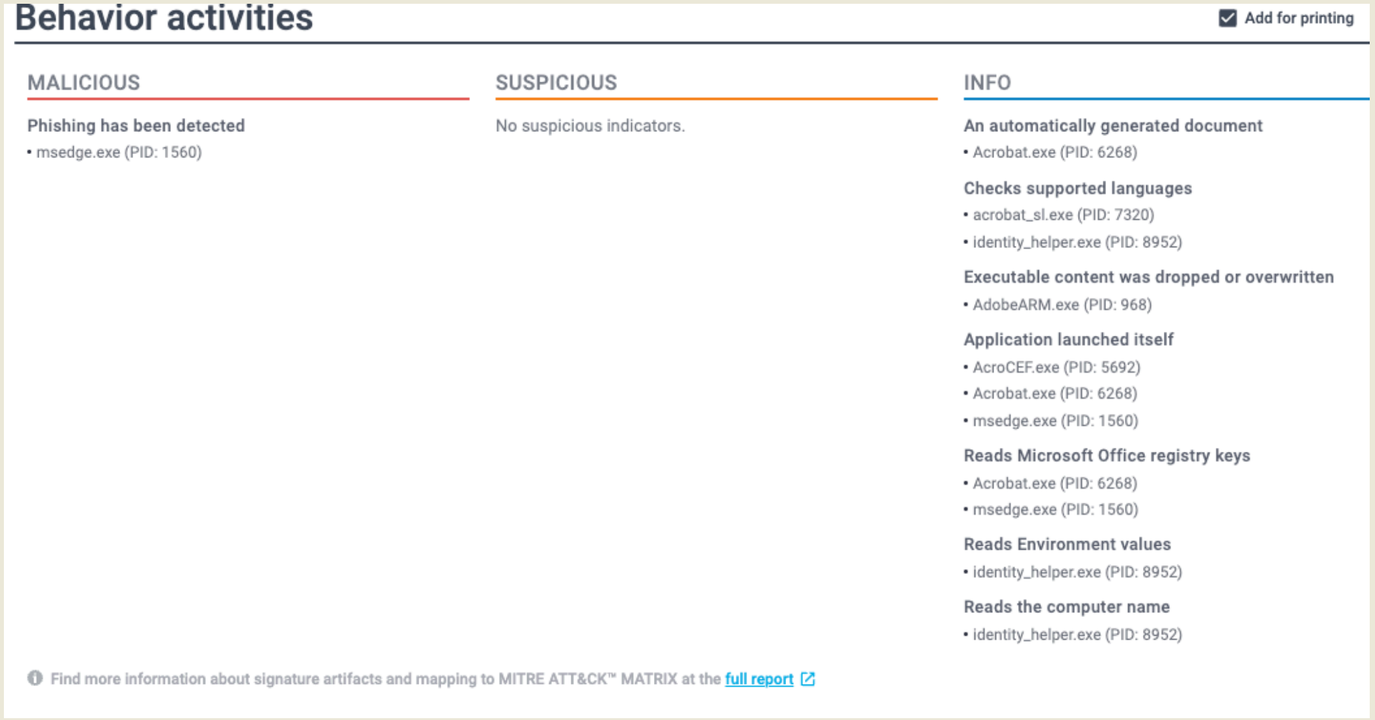
RAPPRESENTAZIONE GRAFICA:



ANALISI ANYRUN (BONUS 1)

Ho esaminato il file "data.pdf" con l'hash **MD5 0D06D5045BC3830E9CB90DE1D46EEF01** su ANYRUN, vedendo l’analisi il pdf sembra essere malevolo, Il file esegue script potenzialmente dannosi quando viene aperto.

Come si può vedere dal report è un phishing che quando viene aperto genera un processo denominato AcroCEF.exe viene avviato, che potrebbe essere responsabile della gestione dei contenuti web all'interno del PDF.



Possiamo vedere che ci sono molte richieste “GET” per tentativi di connessione.

Network activity

Add for printing

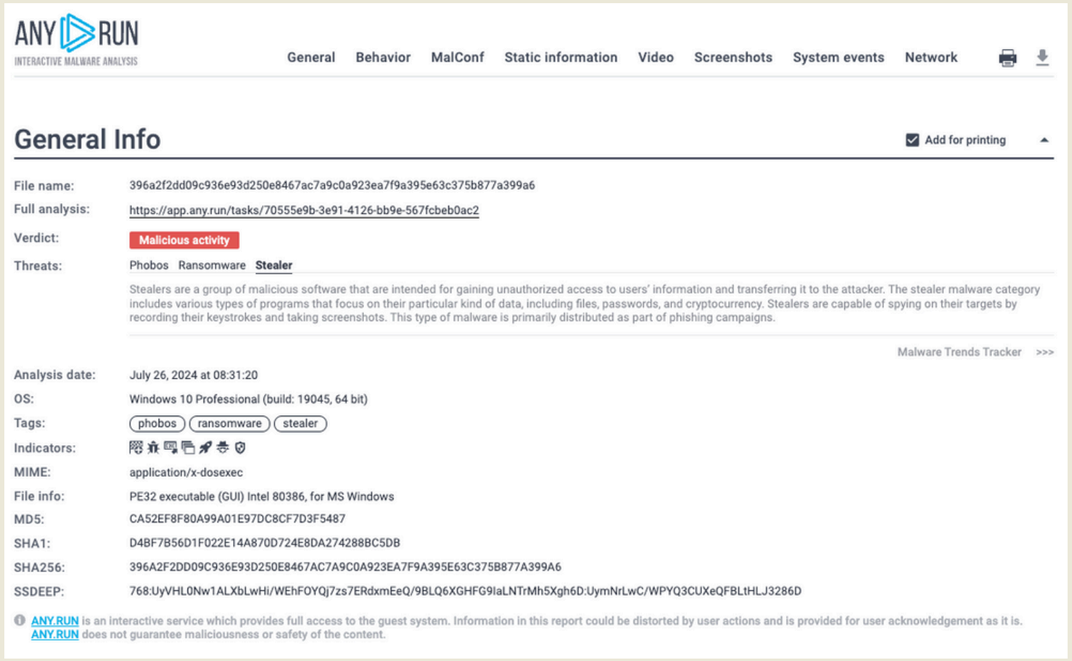
HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
15	71	51	0

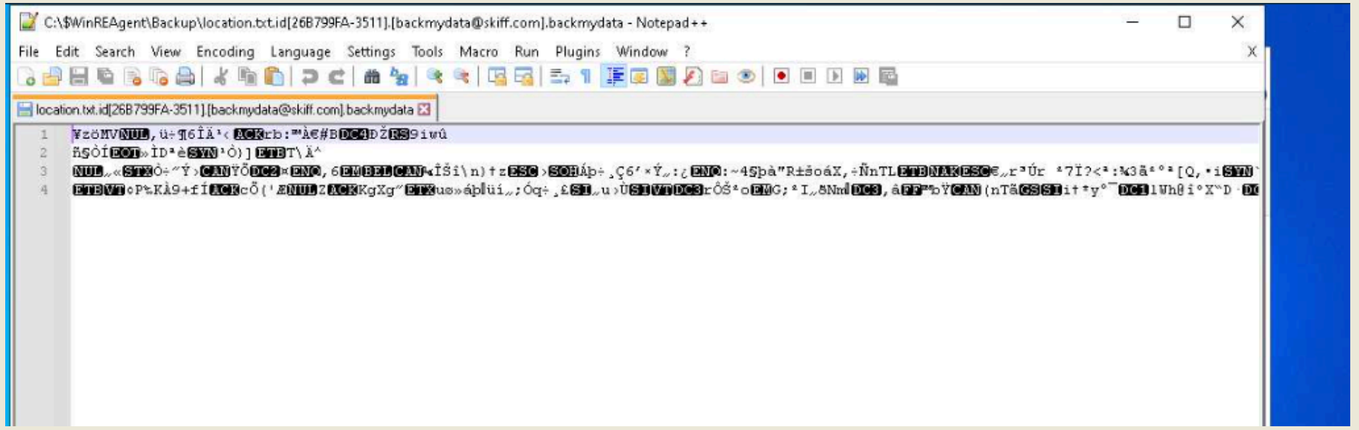
HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
968	AdobeARM.exe	GET	304	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/ReportOwner.txt	unknown	–	–	unknown
968	AdobeARM.exe	GET	304	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/ProcessMAU.txt	unknown	–	–	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEA0aNA9419AA4In9uq1Ilt8%3D	unknown	–	–	unknown
968	AdobeARM.exe	GET	404	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/2024/7/UC/Other.txt	unknown	–	–	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA6bGI750C3n79tQ4ghAGFo%3D	unknown	–	–	unknown
4424	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfIs%2BLjDtGwQ09XEB1Yeq%2BtX%2BBgQQU7NfjgtJxXWRM3y5nP%2Be6mK4cD08CEAitQLJg0pxMn17Nqb2Trtk%3D	unknown	–	–	unknown
968	AdobeARM.exe	GET	404	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/2024/7/OwnerAPI/Rdr.txt	unknown	–	–	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1	unknown	–	–	unknown

ANALISI ANYRUN (BONUS 2)

In questa seconda analisi possiamo vedere che il computer è stato attaccato da un ransomware, infatti tutti i file sono stati criptati.





Nel report possiamo leggere che ci sono diversi comportamenti sospetti tra cui “droppare” i file eseguibili subito dopo l’avvio oppure la rinomina dei file ed altro ancora come da immagine.

Behavior activities

Add for printing

MALICIOUS

Drops the executable file immediately after the start
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Changes the autorun value in the registry
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)

PHOBOS has been detected
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Using BCDEDIT.EXE to modify recovery options
- cmd.exe (PID: 1256)

Deletes shadow copies
- cmd.exe (PID: 1256)

Renames files like ransomware
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Actions looks like stealing of personal data
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

SUSPICIOUS

Application launched itself
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Reads security settings of Internet Explorer
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Executable content was dropped or overwritten
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Reads the date of Windows installation
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Starts CMD.EXE for commands execution
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Executes as Windows Service
- VSSVC.exe (PID: 5616)
- vds.exe (PID: 356)
- wbengine.exe (PID: 7036)

The process creates files with name similar to system file names
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Process drops legitimate windows executable
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Write to the desktop.ini file (may be used to cloak folders)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

INFO

Checks supported languages
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Reads the computer name
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)

Process checks computer location settings
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Creates files in the program directory
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Creates files or folders in the user directory
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Checks proxy server information
- slui.exe (PID: 5920)

Reads the software policy settings
- slui.exe (PID: 5920)

Manual execution by a user
- notepad++.exe (PID: 7016)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report