



26.07.2025

REPORT PROGETTO S9/L5

ADAM DERRO

INTRODUZIONE

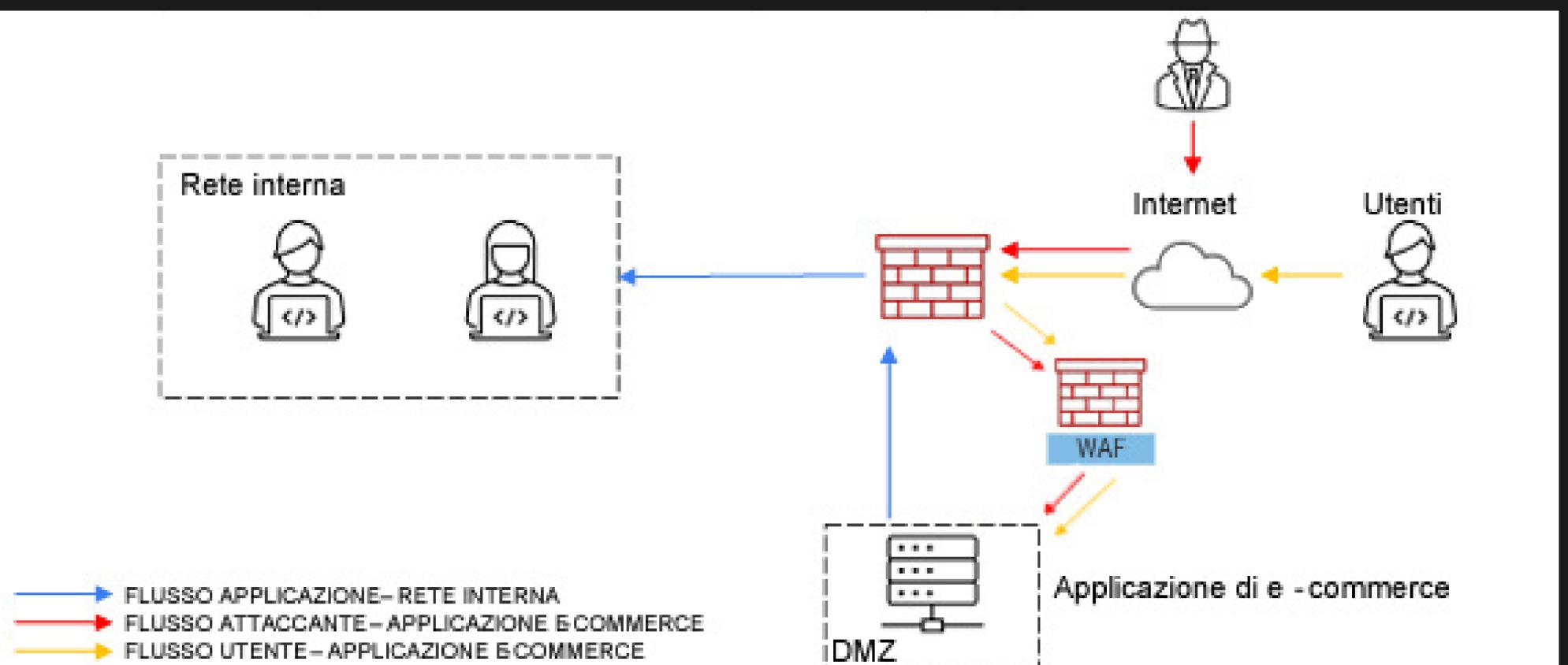
Questo report si propone di affrontare un esercizio di sicurezza informatica basato su una traccia specifica. L'obiettivo principale è analizzare e proporre soluzioni preventive e correttive per difendere un'applicazione di e-commerce da vari tipi di attacchi informatici.

1. AZIONI PREVENTIVE

Obiettivo: Implementare misure preventive per difendere l'applicazione Web da attacchi SQLi (SQL Injection) e XSS (Cross-Site Scripting).

Azioni Preventive:

- Web Application Firewall (WAF): Implementare un WAF per proteggere le applicazioni web da attacchi SQLi e XSS. Il WAF filtra il traffico HTTP/S e blocca le richieste dannose.
- Validazione dell'Input: Assicurarsi che tutti i dati inviati dagli utenti vengano convalidati e sanificati. Questo include la rimozione di caratteri speciali e l'uso di whitelist per i dati accettabili.



2. IMPATTI SUL BUSINESS

Scenario: L'applicazione Web subisce un attacco DDoS (Distributed Denial of Service) dall'esterno che rende l'applicazione non raggiungibile per 10 minuti.

Calcolo dell'Impatto sul Business:

- Danno Economico: L'attacco DDoS causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti. Durante questo periodo, gli utenti non possono effettuare acquisti, causando una perdita di guadagno. Considerando che in media gli utenti spendono 1200 euro al minuto sulla piattaforma, possiamo calcolare il danno totale:

$$\text{Impatto sul business} = 1200 \text{ euro} \times 10 \text{ minuti} = 12000 \text{ euro}$$

Conclusione: Per 10 minuti di indisponibilità, la compagnia ha perso 12000 euro di potenziali acquisti.

Per prevenire o mitigare gli effetti di un attacco DDoS, è possibile adottare diverse misure di sicurezza:

Servizi di Mitigazione DDoS:

- Descrizione: Implementare servizi di mitigazione DDoS forniti da provider specializzati. Questi servizi possono rilevare e bloccare il traffico DDoS prima che raggiunga l'applicazione.

Load Balancer:

- Descrizione: Utilizzare un load balancer per distribuire il traffico su più server. Questo può aiutare a gestire grandi volumi di traffico e prevenire il sovraccarico di un singolo server.

Ridondanza della Rete:

- Descrizione: Creare ridondanza nella rete utilizzando più data center distribuiti. In caso di attacco DDoS su un data center, il traffico può essere reindirizzato ad altri data center.

Monitoring e Alerting:

- Descrizione: Implementare soluzioni di monitoraggio per rilevare anomalie nel traffico in tempo reale. Configurare sistemi di alerting per notificare immediatamente i responsabili IT in caso di attacco.

Rate Limiting e Throttling:

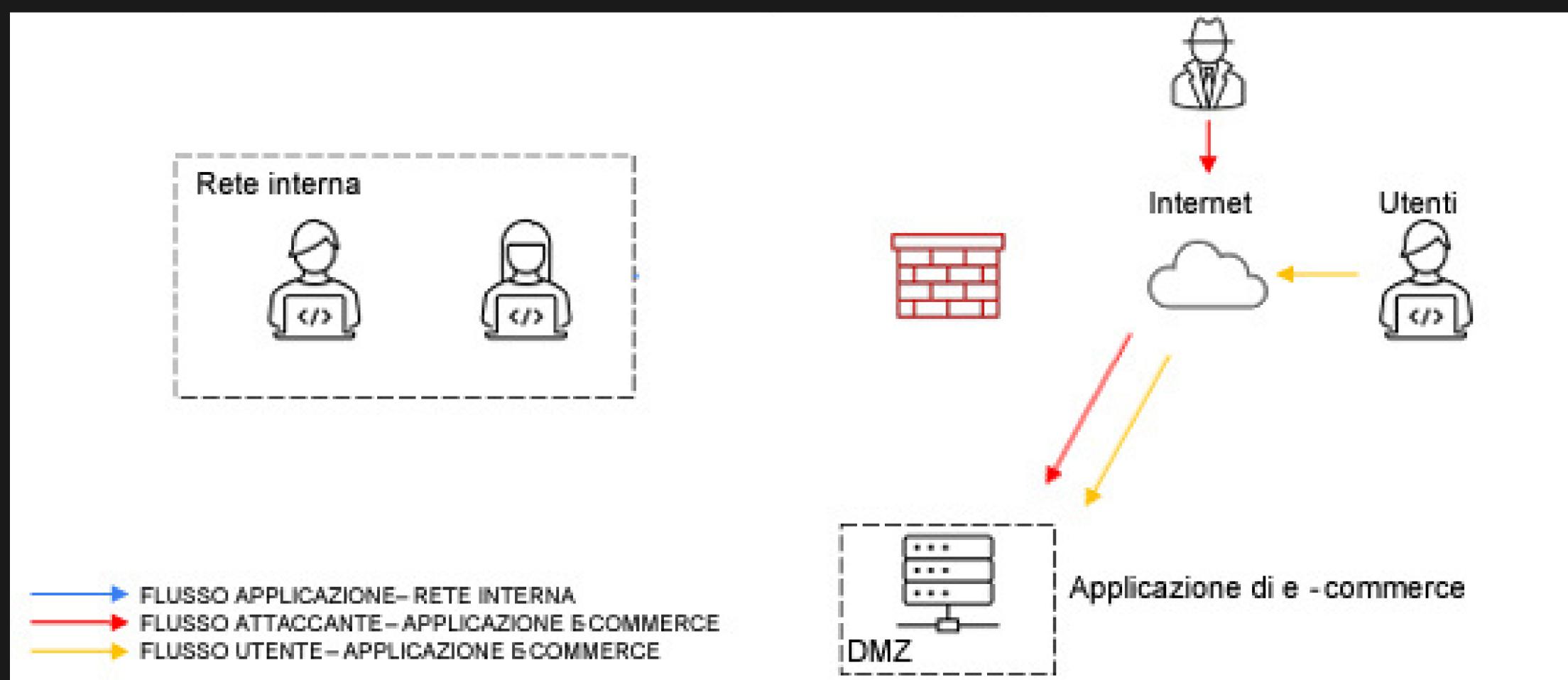
- Descrizione: Configurare rate limiting e throttling per limitare il numero di richieste che un singolo IP può fare in un determinato periodo di tempo.

3. RESPONSE

Scenario: L'applicazione Web viene infettata da un malware. La priorità è evitare che il malware si propaghi sulla rete interna, senza preoccuparsi di rimuovere immediatamente l'accesso dell'attaccante alla macchina infetta.

Strategia di Risposta:

- Isolamento della Macchina Infetta: La macchina infetta viene immediatamente isolata dalla rete interna e collegata direttamente a Internet. Questo impedisce al malware di propagarsi ad altri sistemi nella rete interna, limitando il danno potenziale.

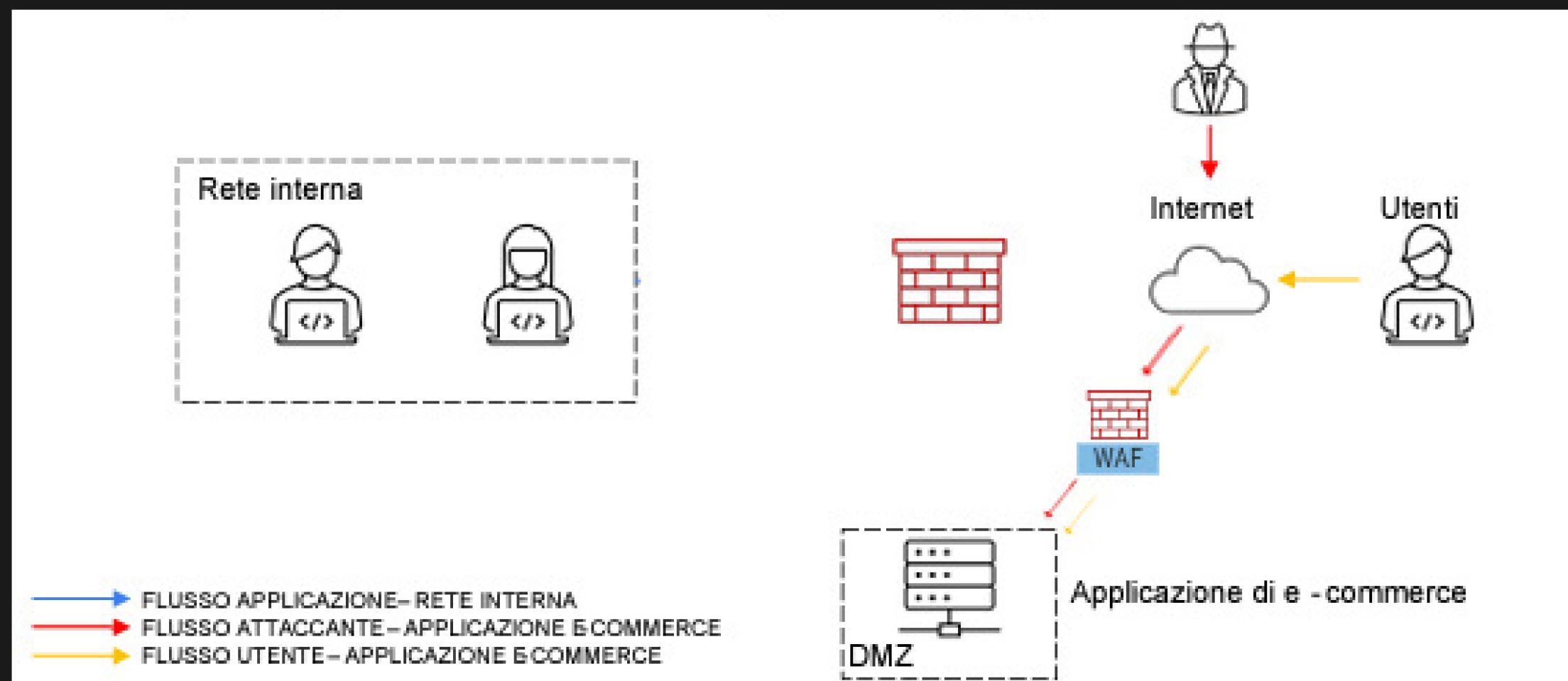


4. SOLUZIONE COMPLETA

Obiettivo: Unire i disegni delle azioni preventive e della risposta per fornire una soluzione di sicurezza integrata.

Soluzione Completa:

- Prevenzione: L'implementazione del WAF e altre misure preventive come la validazione dell'input.
- Risposta: La strategia di isolamento della macchina infetta, garantendo che il malware non si propaghi sulla rete interna.



5. MODIFICA "PIÙ AGGRESSIVA" DELL'INFRASTRUTTURA

Obiettivo: Integrare altri elementi di sicurezza nell'infrastruttura esistente con un budget di 5000 - 10000 euro.

Proposte di Spesa:

1. Implementazione di un IDS/IPS (Intrusion Detection System/Intrusion Prevention System):

- Descrizione: Un IDS/IPS monitora il traffico di rete per identificare e prevenire attacchi.
- Costo Stimato: 3000 - 5000 euro.

2. Backup e Ripristino dei Dati:

- Descrizione: Implementazione di una soluzione di backup regolare per garantire il ripristino rapido dei dati in caso di attacco. Questo include backup giornalieri automatici e soluzioni di storage off-site.

- Costo Stimato: 2000 - 4000 euro.

3. Formazione del Personale:

- Descrizione: Addestramento continuo del personale sulla sicurezza informatica e le migliori pratiche, inclusi corsi su come riconoscere e rispondere a minacce comuni come phishing e malware.

- Costo Stimato: 1000 - 2000 euro.

CONCLUSIONE

Queste misure garantiranno una protezione più robusta e una risposta efficace agli incidenti di sicurezza. L'integrazione di un IDS/IPS rafforzeranno le difese contro attacchi avanzati, mentre il backup dei dati e la formazione del personale aumenteranno la resilienza complessiva dell'organizzazione.





BONUS

BONUS 1.

Analisi di Sicurezza del File "data.pdf"

Questo report analizza le segnalazioni caricate su AnyRun riguardanti il file "data.pdf". L'obiettivo è spiegare agli utenti e ai manager la tipologia di attacco rilevata e fornire raccomandazioni su come evitare futuri attacchi simili.

DETTAGLI DELL'ANALISI

L'analisi del file "data.pdf" su AnyRun ha indicato la presenza di attività malevole, specificamente un attacco di phishing. Di seguito vengono riportati i principali risultati dell'analisi:

- Verdetto: Attività malevola (Malicious activity)
- Data di Analisi: 26 luglio 2024
- Sistema Operativo: Windows 10 Professional

Comportamenti Rilevati

Durante l'analisi, sono stati osservati i seguenti comportamenti del file:

Attività Malevole:

- **Phishing:** È stata rilevata un'attività di phishing, evidenziata dall'esecuzione del processo mesedge.exe.

TIPOLOGIA DI ATTACCO

L'attacco identificato è un attacco di **phishing**, in cui il file PDF malevolo tenta di ingannare l'utente per ottenere informazioni sensibili o per eseguire codice malevolo sul sistema target. Questo tipo di attacco è spesso usato per rubare credenziali, dati personali o per installare malware.

Raccomandazioni per Evitare Futuri Attacchi

Per proteggersi da futuri attacchi di phishing e altre attività malevoli, si raccomandano le seguenti misure:

Formazione del Personale:

- Educare i dipendenti a riconoscere email e documenti sospetti.
- Sensibilizzare riguardo ai pericoli del phishing e alle tecniche comuni usate dagli attaccanti.

Aggiornamento dei Sistemi di Sicurezza:

- Assicurarsi che tutti i software e i sistemi operativi siano aggiornati con le ultime patch di sicurezza.
- Utilizzare soluzioni antivirus e antimalware aggiornate.

Implementazione di Filtri Email:

- Utilizzare filtri antispam e antiphishing sui server di posta elettronica per ridurre il rischio che email malevole raggiungano gli utenti finali.

Monitoraggio e Risposta alle Minacce:

- Implementare sistemi di monitoraggio per rilevare attività sospette in tempo reale.
- Stabilire procedure di risposta agli incidenti per gestire rapidamente eventuali compromissioni.

CONCLUSIONE

Il file "data.pdf" è stato identificato come malevolo a causa di un attacco di phishing. Implementando le raccomandazioni precedentemente descritte, le organizzazioni possono migliorare la loro sicurezza e ridurre il rischio di essere vittime di attacchi simili in futuro.



BONUS 2.

Analisi di Sicurezza del File

"396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a3
95e63c375b877a399a6".

L'obiettivo è spiegare agli utenti e ai manager la tipologia di attacco rilevata e fornire raccomandazioni su come evitare futuri attacchi simili.

DETTAGLI DELL'ANALISI

L'analisi del file "396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6"

Di seguito vengono riportati i principali risultati dell'analisi:

- Verdetto: Attività malevola (Malicious activity)
- Minacce: Phobos, Ransomware, Stealer
- Data di Analisi: 26 luglio 2024
- Sistema Operativo: Windows 10 Professional
- Tag: phobos, ransomware, stealer

Comportamenti Rilevati

Durante l'analisi, sono stati osservati i seguenti comportamenti del file:

Attività Malevole (MALICIOUS)

- Il file eseguibile viene rilasciato immediatamente dopo l'avvio.
- Modifica il valore di autorun nel registro di sistema.
- Rilevato il ransomware Phobos.
- Utilizza BCEDIT.EXE per modificare le opzioni di ripristino.
- Elimina le copie shadow.
- Rinomina i file come farebbe un ransomware.

TIPOLOGIA DI ATTACCO

L'attacco è un attacco di ransomware, specificamente il ransomware Phobos. Questo tipo di malware cifra i file della vittima e richiede un riscatto per la decifrazione. Inoltre, il file presenta comportamenti di furto di dati personali e altre attività malevole tipiche dei malware di tipo stealer.

Per proteggersi da futuri attacchi di ransomware e altre attività malevole, si raccomandano le seguenti misure:

1. Backup Regolari:

- Effettuare backup regolari dei dati importanti e conservarli offline o su una rete separata.
-

2. Formazione del Personale:

- Educare i dipendenti a riconoscere email e documenti sospetti.
- Sensibilizzare riguardo ai pericoli del ransomware e alle tecniche comuni usate dagli attaccanti.

3. Aggiornamento dei Sistemi di Sicurezza:

- Assicurarsi che tutti i software e i sistemi operativi siano aggiornati con le ultime patch di sicurezza.
- Utilizzare soluzioni antivirus e antimalware aggiornate.

4. Implementazione di Filtri Email:

- Utilizzare filtri antispam e antiphishing sui server di posta elettronica per ridurre il rischio che email malevole raggiungano gli utenti finali.

5. Monitoraggio Continuo:

- Implementare sistemi di monitoraggio per rilevare attività sospette in tempo reale.
- Stabilire procedure di risposta agli incidenti per gestire rapidamente eventuali compromissioni.

CONCLUSIONE

Il file

*"396a2f2dd09c936e93d250e8467ac7a9c0a
923ea7f9a395e63c375b877a399a6"* è stato
identificato come malevolo a causa della
presenza del ransomware Phobos e
comportamenti di furto di dati personali.

*Implementando le raccomandazioni
precedentemente descritte, le organizzazioni
possono migliorare la loro sicurezza e ridurre
il rischio di essere vittime di attacchi simili in
futuro.*





GRAZIE

ADAM DERRO