ESERCIZI S9-L5

Traccia:

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

Esercizio Traccia e requisiti 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 l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende 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)

Report sulla Sicurezza dell'Applicazione e-commerce

Introduzione
Questo report analizza le azioni preventive e di risposta necessarie per proteggere l'applicazione e-commerce da attacchi informatici, valutare l'impatto sul business in caso di downtime, e proporre una soluzione completa e migliorata per l'infrastruttura di rete.

1. Azioni Preventive: Difesa contro Attacchi SQLi e XSS

Per difendere l'applicazione Web da attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS), si raccomandano le seguenti azioni preventive:

-utilizzo di Prepared Statements: Utilizzare statement preparati per le query SQL per prevenire l'iniezione di codice SQL malevolo.

-sanitizzazione e Validazione degli Input: Assicurarsi che tutti gli input degli utenti siano correttamente sanitizzati e validati per prevenire attacchi XSS.

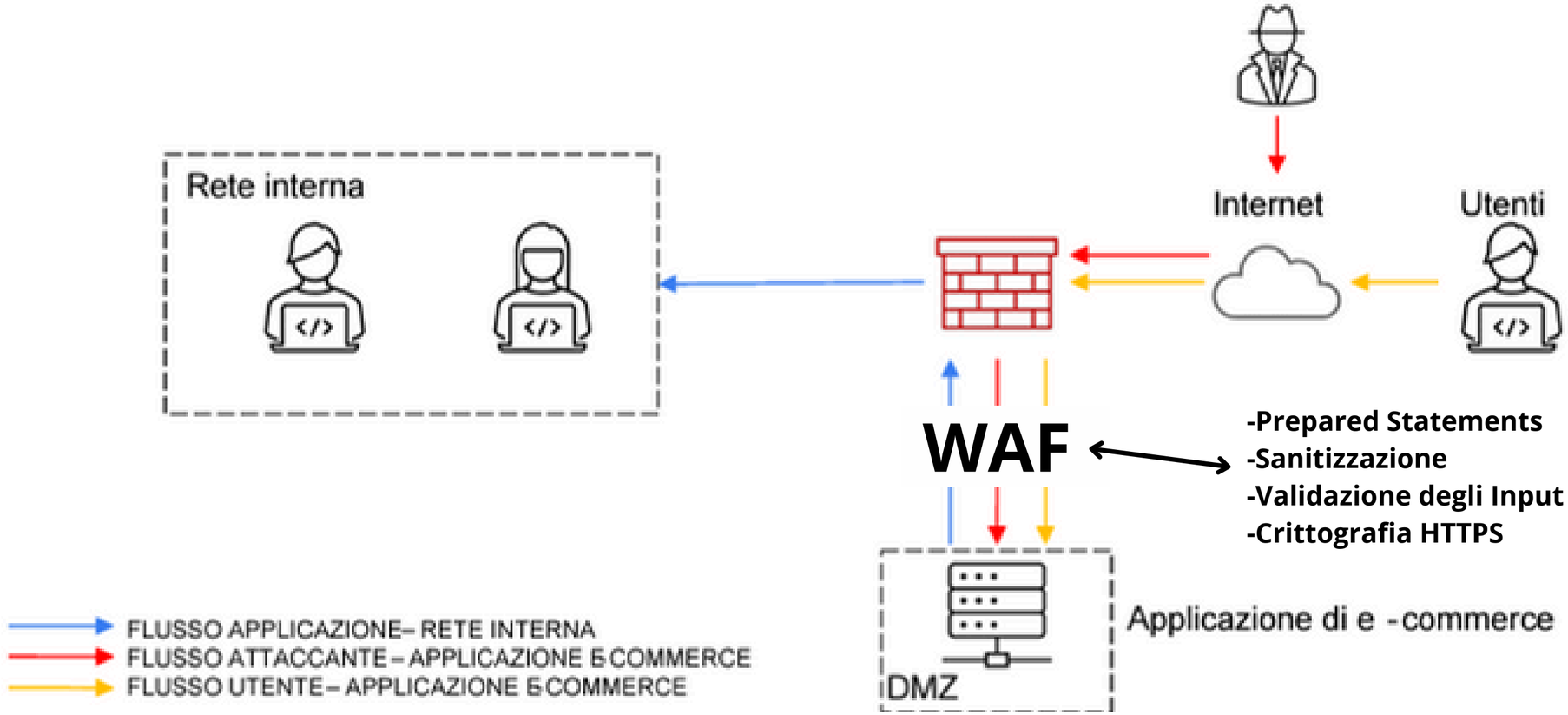
-firewall per Applicazioni Web (WAF): Implementare un WAF per rilevare e bloccare tentativi di attacco SQLi e XSS.

-crittografia delle Comunicazioni (HTTPS): Utilizzare HTTPS per garantire la trasmissione sicura dei dati.

-aggiornamenti e Patch: Mantenere aggiornato il software dell'applicazione e i suoi componenti per proteggersi dalle vulnerabilità conosciute.

Modifica alla Figura:

aggiunta di un WAF tra Internet e l'applicazione e-commerce nella DMZ.
Note sull'uso di statement preparati, sanitizzazione degli input e crittografia HTTPS.



Web Application Firewall (WAF):

Il Web Application Firewall si posiziona come uno scudo
avanzato per le applicazioni web, operando direttamente al confine tra internet e le risorse digitali che si intende proteggere.

Questo dispositivo specializzato è progettato per scrutare e analizzare il traffico HTTP/HTTPS in ingresso, utilizzando un insieme di regole e politiche di sicurezza per identificare e bloccare le richieste potenzialmente dannose prima che possano raggiungere il server dell'applicazione.
Attraverso un processo di filtraggio accurato, il WAF è in grado di rilevare e neutralizzare tentativi di attacco come iniezioni SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), e molte altre minacce che sfruttano le vulnerabilità comuni delle applicazioni web.

2. Impatti sul Business: Attacco DDoS

In caso di un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, l'impatto sul business è calcolato come segue:

-entrate per Minuto: €1200
-tempo di Inattività: 10 minuti
-impatto Totale: €1200 × 10 = €12,000

Azioni Preventive per Mitigare un Attacco DDoS:

-servizi di Mitigazione DDoS: Utilizzare servizi come Cloudflare o AWS Shield.
-bilanciamento del Carico: Implementare sistemi per distribuire il traffico in modo equilibrato.
-aumento della Capacità di Banda: Incrementare la capacità di banda per resistere a picchi di traffico.

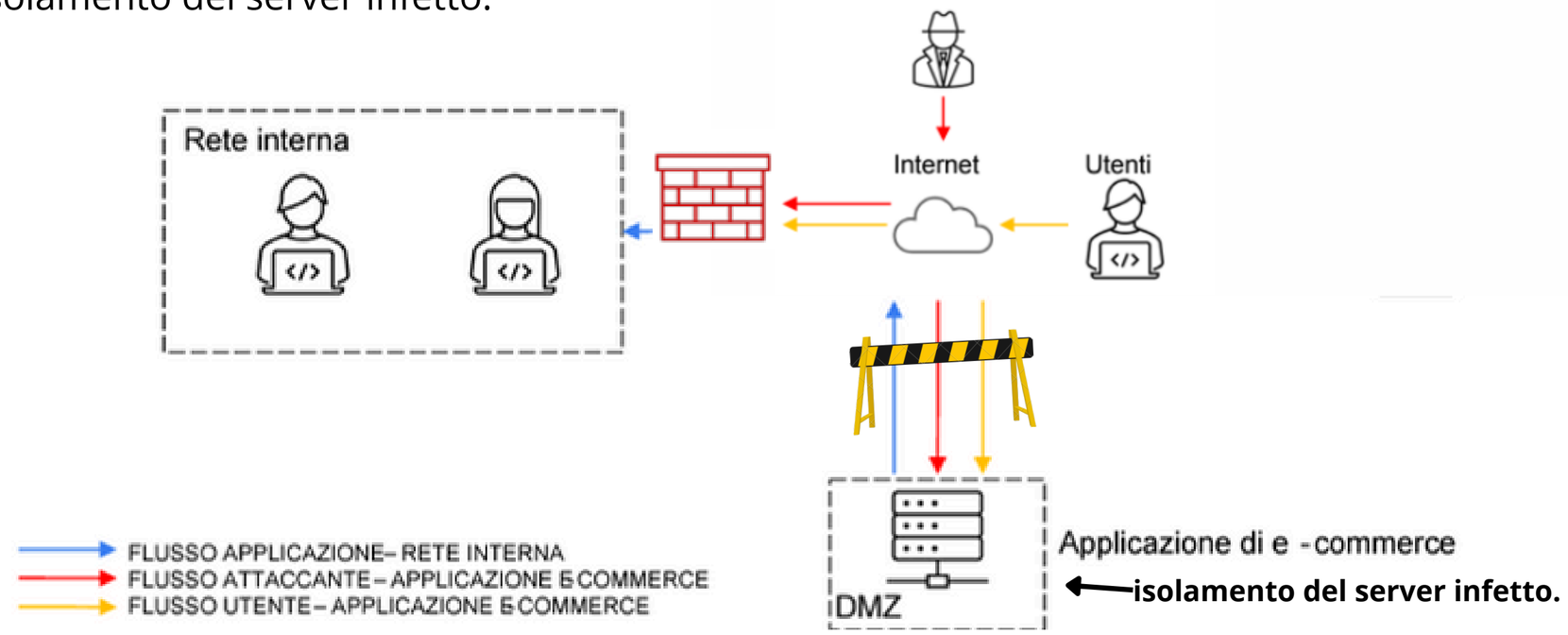
3. Response: Contenimento di un Malware

Se l'applicazione viene infettata da un malware, la priorità è evitare la propagazione sulla rete interna. Le seguenti azioni sono consigliate:

-isolamento del Server Infetto: Disconnettere il server infetto dalla rete interna.
-segmentazione della Rete: Limitare l'accesso del malware ad altre parti della rete tramite segmentazione.

Modifica alla Figura:

-aggiunta di segmentazione tra la DMZ e la rete interna.
-indicazione dell'isolamento del server infetto.

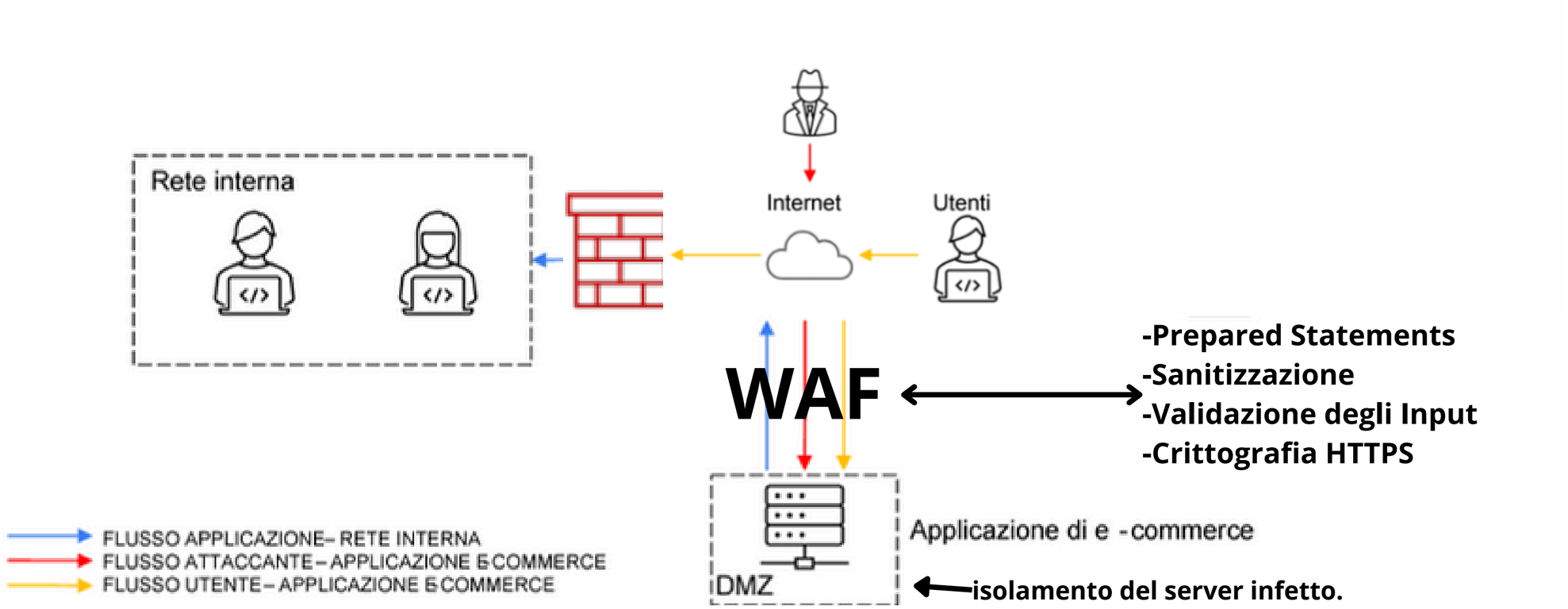


4. Soluzione Completa: Unione di Azioni Preventive e di Response

La soluzione completa combina le azioni preventive con le risposte al contenimento del malware.

Modifica alla Figura:

inclusione di tutte le modifiche descritte nei punti precedenti, mostrando chiaramente il WAF, la segmentazione della rete e l'isolamento del server infetto**.**



5. Modifica "Più Aggressiva" dell'Infrastruttura

Con un budget di €5000-€10000, le seguenti proposte possono essere implementate per migliorare ulteriormente la sicurezza:

Proposta 1:

-servizio di Mitigazione DDoS (Cloudflare/AWS Shield): €2000-€5000 annui.
-WAF Gestito (Cloudflare/AWS WAF): €2000-€3000 annui.
-segmentazione di Rete e Aggiornamenti Hardware: €1000-€2000.

Proposta 2:

-aumento della Capacità di Banda: €3000-€5000.
-sistemi di Bilanciamento del Carico: €2000-€3000.
-servizio di Monitoraggio e Risposta agli Incidenti: €2000-€3000.

Proposta 1:

Descrizione:

I servizi di mitigazione DDoS (Distributed Denial of Service) sono progettati per proteggere le applicazioni web dagli attacchi che cercano di sovraccaricare i server con un'elevata quantità di traffico malevolo, rendendo il servizio inaccessibile agli utenti legittimi.

Servizi Noti:

Cloudflare: Offre una protezione DDoS avanzata che rileva e mitiga automaticamente il traffico dannoso prima che raggiunga il server di destinazione.
AWS Shield: Un servizio di protezione DDoS integrato con AWS che offre protezione standard gratuita e una versione avanzata (AWS Shield Advanced) con monitoraggio e mitigazione più sofisticati.

Come Funzionano:

Rilevamento del Traffico Dannoso: Identificano automaticamente i pattern di traffico anomali che indicano un attacco DDoS.
Filtraggio del Traffico: Bloccano o mitigano il traffico malevolo prima che possa raggiungere e sovraccaricare l'infrastruttura del sito.
Distribuzione del Carico: Reindirizzano il traffico legittimo attraverso una rete distribuita di data center, riducendo la pressione sul server di destinazione.

Proposta 1:

2. Bilanciamento del Carico: Implementare sistemi per distribuire il traffico in modo equilibrato

Descrizione:

Il bilanciamento del carico è una tecnica utilizzata per distribuire il traffico di rete o le richieste di elaborazione attraverso più server, garantendo che nessun singolo server sia sovraccaricato.

Strumenti Comuni:

-hardware Load Balancers: Dispositivi fisici installati tra i server e l'internet per distribuire il traffico.
-software Load Balancers: Applicazioni che eseguono lo stesso lavoro, spesso integrate nelle infrastrutture cloud (es. --AWS Elastic Load Balancing).

Come Funziona:

-distribuzione delle Richieste: Le richieste degli utenti vengono distribuite tra diversi server in base a vari algoritmi (es. round-robin, least connections, IP hash).
-monitoraggio della Salute dei Server: I bilanciatori di carico monitorano costantemente lo stato dei server per reindirizzare il traffico solo ai server funzionanti.
-scalabilità: Permettono di aggiungere o rimuovere server in base alla domanda di traffico.

Proposta 1:

3. Aumento della Capacità di Banda: Incrementare la capacità di banda per resistere a picchi di traffico

Descrizione:

l'aumento della capacità di banda implica l'espansione della quantità di dati che possono essere trasmessi attraverso la rete in un determinato periodo di tempo. Questo è essenziale per gestire i picchi di traffico elevati e prevenire il sovraccarico della rete.

Implementazione:

-acquisto di Maggior Larghezza di Banda: Collaborare con il proprio ISP (Internet Service Provider) per aumentare il limite di banda disponibile.
-ottimizzazione delle Risorse di Rete: Configurare correttamente le risorse di rete per massimizzare l'efficienza della larghezza di banda esistente.
-utilizzo di CDN (Content Delivery Network): CDN come Cloudflare o Akamai distribuiscono il contenuto attraverso vari nodi globali, riducendo la latenza e il carico sul server principale.

Proposta 2

Descrizione:

L'aumento della capacità di banda implica l'espansione della quantità di dati che possono essere trasmessi attraverso la rete in un determinato periodo di tempo. Questo è essenziale per gestire picchi di traffico elevati e prevenire il sovraccarico della rete.

Implementazione:

-collaborazione con il Fornitore di Servizi Internet (ISP): Negoziare con l'ISP per aumentare la larghezza di banda disponibile.

-ottimizzazione della Rete: Configurare adeguatamente le risorse di rete per massimizzare l'efficienza della larghezza di banda esistente.

-uso di CDN (Content Delivery Network): Utilizzare CDN come Cloudflare o Akamai per distribuire il contenuto attraverso vari nodi globali, riducendo la latenza e il carico sul server principale.

2. Sistemi di Bilanciamento del Carico (€2000-€3000)

Descrizione:

Il bilanciamento del carico è una tecnica utilizzata per distribuire il traffico di rete o le richieste di elaborazione attraverso più server, garantendo che nessun singolo server sia sovraccaricato.

Strumenti Comuni:

-hardware Load Balancers: Dispositivi fisici installati tra i server e l'internet per distribuire il traffico.
-software Load Balancers: Applicazioni che eseguono lo stesso lavoro, spesso integrate nelle infrastrutture cloud (es. AWS Elastic Load Balancing).

Come Funziona:

-distribuzione delle Richieste: le richieste degli utenti vengono distribuite tra diversi server in base a vari algoritmi (es. round-robin, least connections, IP hash).
-monitoraggio della Salute dei Server: i bilanciatori di carico monitorano costantemente lo stato dei server per reindirizzare il traffico solo ai server funzionanti.
-scalabilità: permettono di aggiungere o rimuovere server in base alla domanda di traffico.

3. Servizio di Monitoraggio e Risposta agli Incidenti (€2000-€3000)

Descrizione:

Il monitoraggio e la risposta agli incidenti coinvolgono l'uso di strumenti e servizi che rilevano, analizzano e rispondono a eventi di sicurezza in tempo reale. Questo aiuta a mitigare rapidamente gli effetti di un attacco e a proteggere l'infrastruttura IT.

Componenti Principali:

-monitoraggio continuo: utilizzo di strumenti di monitoraggio della sicurezza che controllano costantemente il traffico di rete, i log dei server e altre attività per individuare comportamenti anomali.
-risposta automatica: implementazione di sistemi che possono rispondere automaticamente a determinati tipi di minacce (es. blocco di IP sospetti, disconnessione di sessioni).
-team di Risposta agli Incidenti (IRT): un team dedicato di esperti che analizza e risponde agli incidenti di sicurezza.

S9-L5 Bonus Emanuele Di Stefano

Bonus: Esercizio Traccia e requisiti 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 /

1. Analisi del Primo Report

Tipologia di Attacco:

L'analisi del primo report rivela che si tratta di un attacco basato su un file eseguibile dannoso. Il file è stato eseguito in un ambiente virtuale dove ha mostrato comportamenti sospetti come tentativi di connessione a server remoti e modifiche al registro di sistema.

Comportamenti Osservati:

-tentativi di connessione a indirizzi IP esterni non riconosciuti.
-modifiche a chiavi di registro critiche.
-creazione di file temporanei nel sistema.
-consigli per Prevenire Futuri Attacchi:

Utilizzare Software Antivirus e Antimalware:

-assicurarsi che tutti i dispositivi abbiano installato e aggiornato software antivirus.
-monitoraggio della Rete: implementare sistemi di monitoraggio della rete per rilevare tentativi di connessione non autorizzati.
-controlli di Integrità del Sistema: utilizzare strumenti che monitorano e segnalano modifiche non autorizzate ai file di sistema e alle chiavi di registro.

2. Analisi del Secondo Report

Tipologia di Attacco:

Il secondo report mostra un attacco basato su un documento PDF contenente macro dannose. Quando il documento è stato aperto in un ambiente controllato, ha attivato una serie di macro che hanno tentato di scaricare ulteriori payload dannosi da Internet.

Comportamenti Osservati:

-esecuzione automatica di macro all'apertura del documento.
-tentativi di scaricare file aggiuntivi da server remoti.
-comunicazione con server Command and Control (C2).

Consigli per Prevenire Futuri Attacchi:

-Disabilitare Macro: Configurare i software di Office per disabilitare l'esecuzione automatica delle macro.
-Educazione degli Utenti: Formare gli utenti per riconoscere email e documenti sospetti e evitare di aprirli.
-Filtri di Contenuti: Implementare filtri che esaminano gli allegati email e bloccano quelli sospetti prima che raggiungano gli utenti finali.