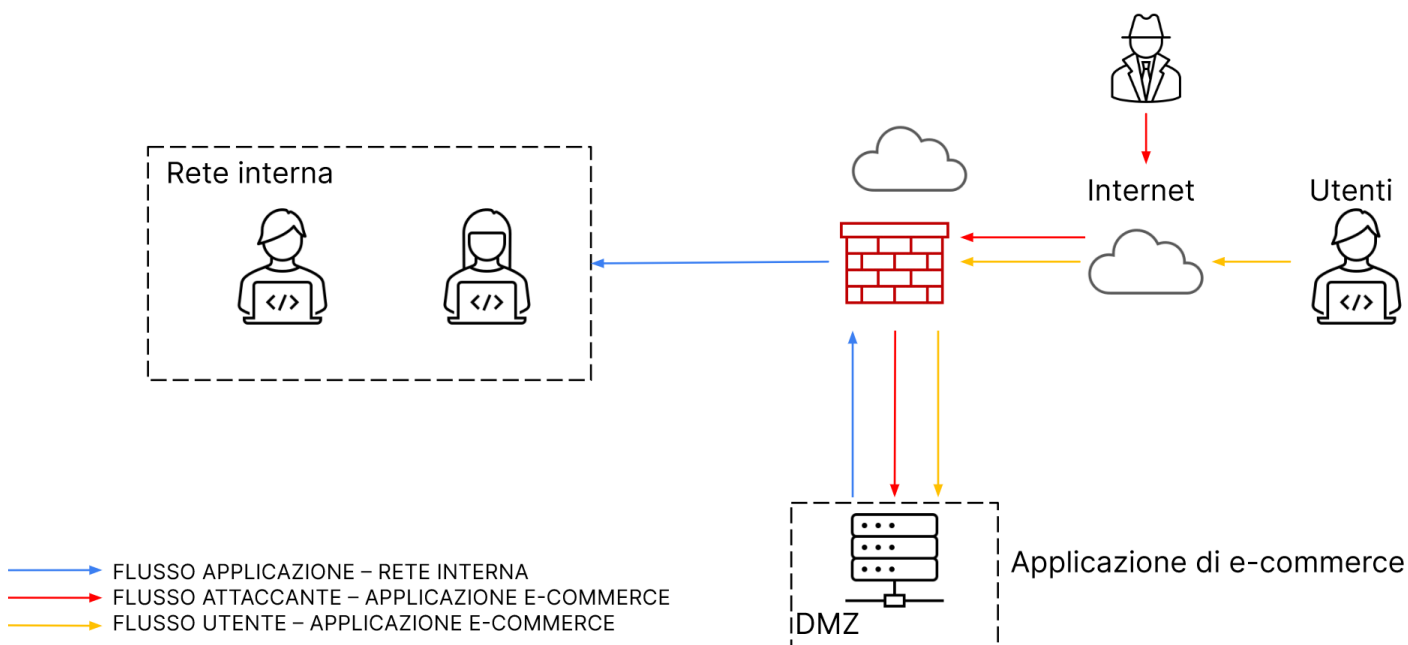


Report progetto UNIT 3 WEEK 9

Analisi dei log

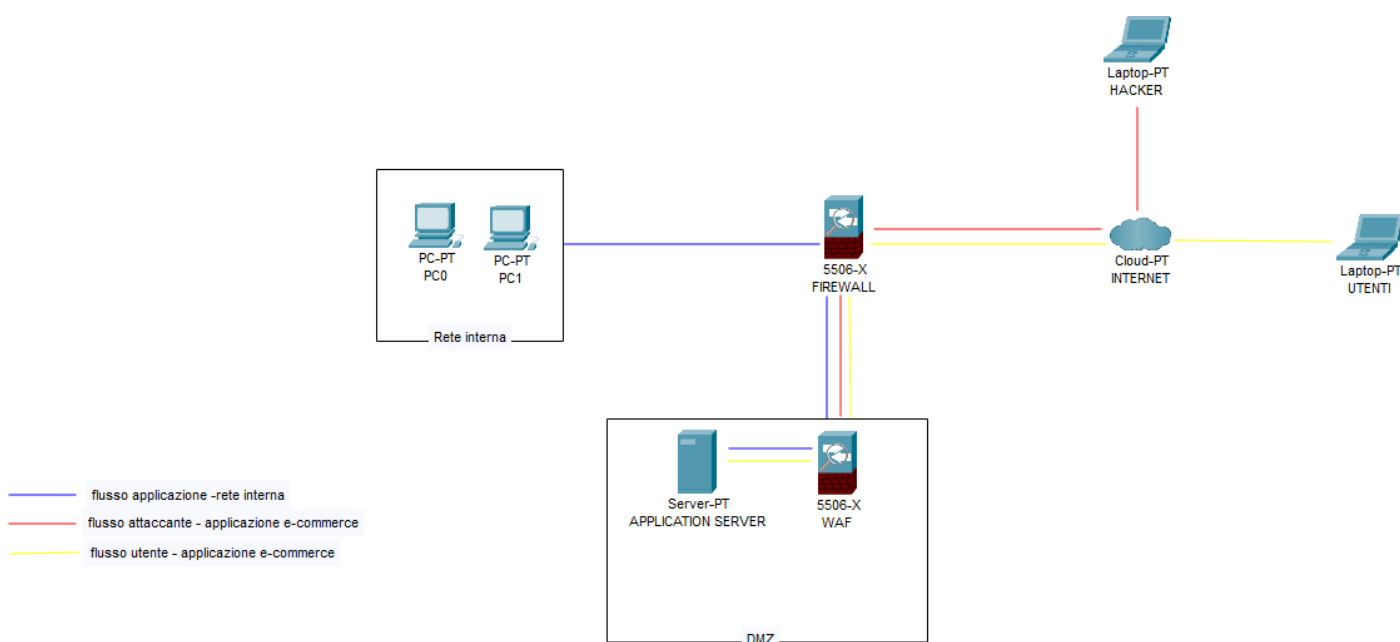
L'applicazione di e-commerce deve essere disponibile per tutti gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interne 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.



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?



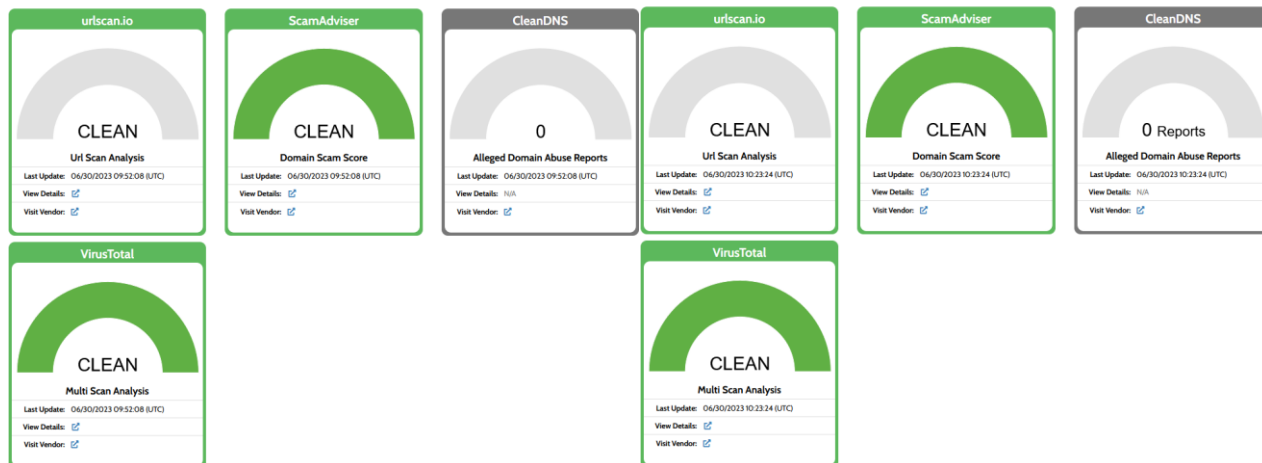
Per difendere un'applicazione web dagli attacchi di tipo SQLi (SQL injection) e XSS (cross-site scripting) da parte di utenti malintenzionati, è possibile implementare diverse azioni preventive.

- **Utilizzo di firewall e software di sicurezza (WAF)**
Configurare il firewall per filtrare il traffico indesiderato e utilizzare un software di sicurezza aggiuntivo come WAF (Web Application Firewall) per rilevare e bloccare attacchi comuni come SQLi e XSS.
- **Utilizzo di meccanismi di autenticazione e autorizzazione**
Implementazione sistema di autenticazione forte per consentire l'accesso solo agli utenti autorizzati con assegnazione di privilegi accesso appropriati ai diversi ruoli utente.
- **Sanitizzazione e validazione input**
Rimuovere o neutralizzare caratteri (tag HTML, JavaScript ed altri potenzialmente dannosi) nei dati inseriti dagli utenti utilizzando librerie o funzioni di sanitizzazione e validazione dell'input.
- **Escape e codifica corretta dati di output**
Eseguire la corretta escape e codifica dei caratteri speciali ("<, >, &", ecc) per evitare l'esecuzione involontaria di codice HTML o JavaScript, utilizzando codifiche appropriate fornite dal framework o linguaggio di programmazione utilizzato.
- **Parametrizzazione query SQL**
Utilizzo query parametriche o prepared statements con parametri posizionali o nominativi per eseguire le operazioni di database, evitando di concatenare i valori di input nelle query SQL e l'interpretazione errata degli input malevoli.
- **Validazione dei dati input**
Lato server con convalida tipo dei dati, limitazione lunghezza e gestione stringhe escape per prevenire l'inserimento di codice dannoso.
Lato client utilizzando HTML5 e JavaScript per un'interazione immediata e rilevare errori input comuni.
- **Educazione e consapevolezza**
Promuovere l'uso di best practice di sicurezza e la gestione corretta dei dati di input e output.
- **Implementazione CSP (Content Security Policy)**
Specificare le origini considerate affidabili e consentite per il caricamento di risorse nell'applicazione web, limitando le origini dei contenuti che possono essere caricati e visualizzati nell'applicazione.
- **Aggiornamento regolare e patching**
Mantenere il sistema ed i componenti software aggiornati con le ultime versioni e patch di sicurezza.
- **Controllo messaggi di errore**
Evitare di fornire agli utenti messaggi di errore dettagliati, che potrebbero rivelare informazioni sensibili, utilizzando messaggi di errore generici che non rivelano informazioni specifiche.

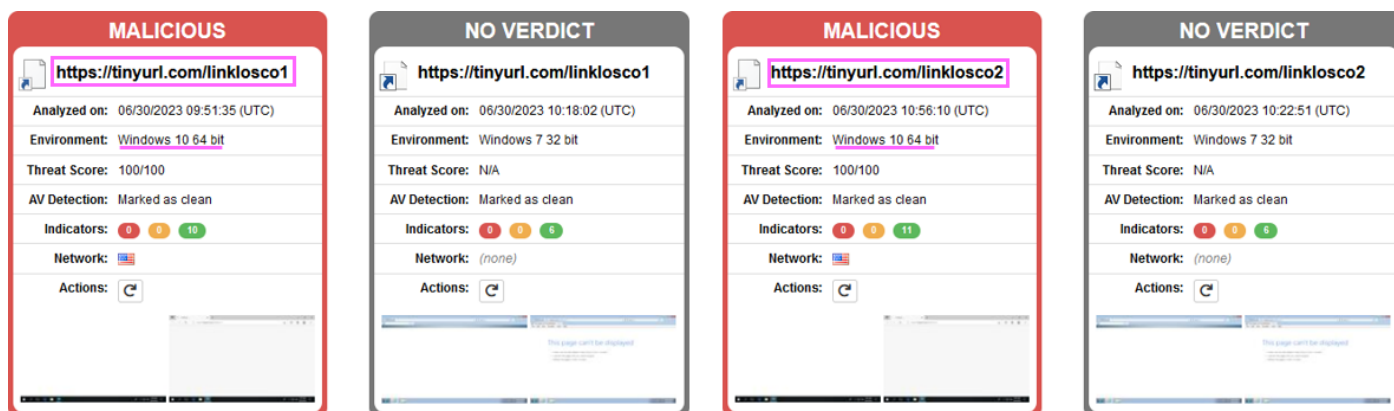
2) ANALISI ATTACCO

Analizzare i seguenti link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco <https://tinyurl.com/linklosco1> <https://tinyurl.com/linklosco2>

Per l'analisi dei link ho scelto di utilizzare il sito **Hybrid Analysis**, un servizio online che fornisce funzionalità di analisi avanzata di file sospetti o link potenzialmente dannosi. Questo fornisce una piattaforma per l'analisi dinamica e statica dei malware creando report dettagliati.



Entrambi i link hanno passato la scansione antivirus risultando “CLEAN” su [urlscan.io](#), [ScamAdviser](#) e [VirusTotal](#).



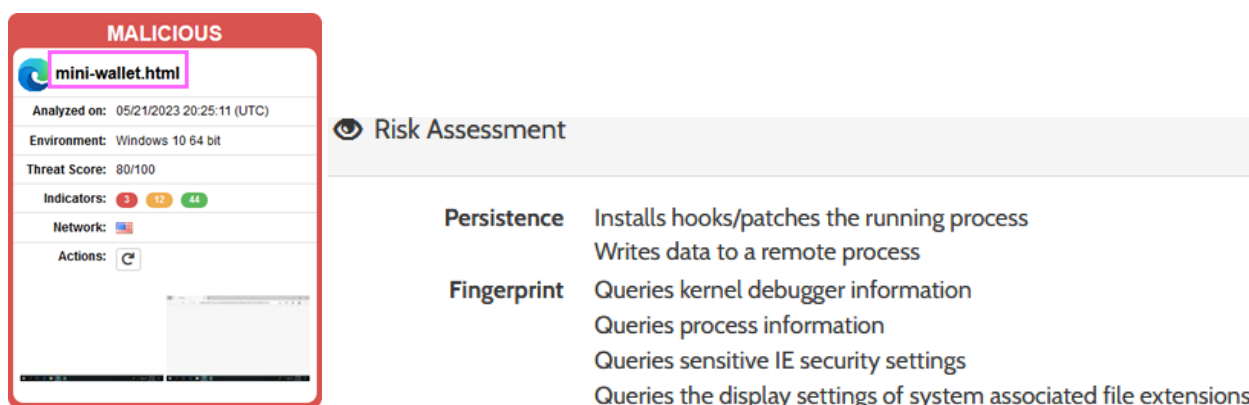
Dalla sandbox report invece i risultati sono diversi.

mini-wallet.html	df47aac0fa71fbcecc16685ad4024965491e601880daf1fefa3735e769df661b	malicious
shopping_iframe_driver.js	456369ffe3542bb3ab1288484cfb909820a76f35e4d635a8638baf44ac6d3028	suspicious
bnpl_driver.js	b7aef5068ff4fab58e377effaa6119c21378c3730dc2ec8f4b4bcd18556787b9	suspicious
notification.bundle.js	7903741a9cc830873ed3d700504ee519dd88952c1747aad277c5e5d801d03543	suspicious

Nella sezione dei file estratti durante la detonazione vengono elencati i file estratti e rilevati durante l’analisi dinamica all’interno del sandbox, fornendo informazioni sulle risorse create o modificate durante l’esecuzione.

In entrambi i link si ritrovano “[mini-wallet.html](#)”, “[shopping_iframe_driver.js](#)”, “[bnpl_drivers.js](#)”, “[notification.bundle.js](#)”.

Vado ad analizzare ogni azione rilevata per comprenderne il comportamento.




In questo caso **mini-wallet.html** potrebbe cercare di ottenere una persistenza nel sistema, ad esempio installando hook o patch nel processo in esecuzione. Questo può consentire al file di rimanere attivo anche dopo un riavvio del sistema. Inoltre, il file potrebbe scrivere dati in un processo remoto, ovvero inviare informazioni o eseguire azioni su un processo in esecuzione su un altro sistema. Questo potrebbe intraprendere azioni per raccogliere informazioni sul sistema e sulle sue impostazioni di sicurezza come:

- cercare di identificare se è presente un kernel debugger sul sistema. Un kernel debugger è uno strumento diagnostico che consente agli sviluppatori di analizzare e debuggare il kernel del sistema operativo.
- interrogare informazioni sui processi in esecuzione nel sistema, come i processi attivi e le loro proprietà.
- interrogare le impostazioni di sicurezza sensibili di Internet Explorer, il browser web di Microsoft, per identificare eventuali configurazioni che potrebbero essere sfruttate a fini maligni.
- cercare di ottenere informazioni sulle impostazioni di visualizzazione associate alle estensioni dei file nel sistema. Queste informazioni possono essere utilizzate per scopi vari, inclusi potenziali attacchi o manipolazioni dei file.

In generale, queste azioni indicano che il file sospetto potrebbe cercare di ottenere accesso, raccogliere informazioni sensibili o sfruttare vulnerabilità nel sistema.

SUSPICIOUS

 shopping_iframe_driver.js

Analyzed on: 06/22/2023 01:50:32 (UTC)


Environment: Windows 10 64 bit


Threat Score: 45/100

AV Detection: Marked as clean

Indicators: 1 2 93

Network: (none)

Actions: 



Malicious Indicators

Network Related

Making HTTPS connections using insecure TLS/SSL version

Suspicious Indicators

General


Executes a JavaScript file

Unusual Characteristics

Found decoded javascript strings

Le indicazioni suggeriscono che **shopping_iframe_driver.js** potrebbe avere comportamenti potenzialmente dannosi o sospetti, come l'utilizzo di connessioni TLS/SSL insicure, l'esecuzione di codice JavaScript esterno e l'utilizzo di tecniche di codifica per nascondere informazioni sensibili o il codice malevolo stesso.

SUSPICIOUS

 bnpl_driver.js

Analyzed on: 06/22/2023 01:44:03 (UTC)


Environment: Windows 10 64 bit


Threat Score: 40/100

AV Detection: Marked as clean

Indicators: 1 1 95

Network: (none)

Actions: 



Malicious Indicators

Network Related

Making HTTPS connections using insecure TLS/SSL version

Suspicious Indicators

General

Executes a JavaScript file

In questo caso si può dedurre che il file **bnpl_drivers.js** potrebbe comportarsi in modo simile al file precedentemente menzionato, ovvero stabilire connessioni HTTPS insicure ed eseguire codice JavaScript esterno.

SUSPICIOUS

notification.bundle.js

Analyzed on: 06/24/2023 08:07:26 (UTC)

Environment: Windows 10 64 bit

Threat Score: 35/100

Indicators: 0 2 103

Network: (none)

Actions:

Suspicious Indicators

General

Executes a JavaScript file

Spyware/Information Retrieval

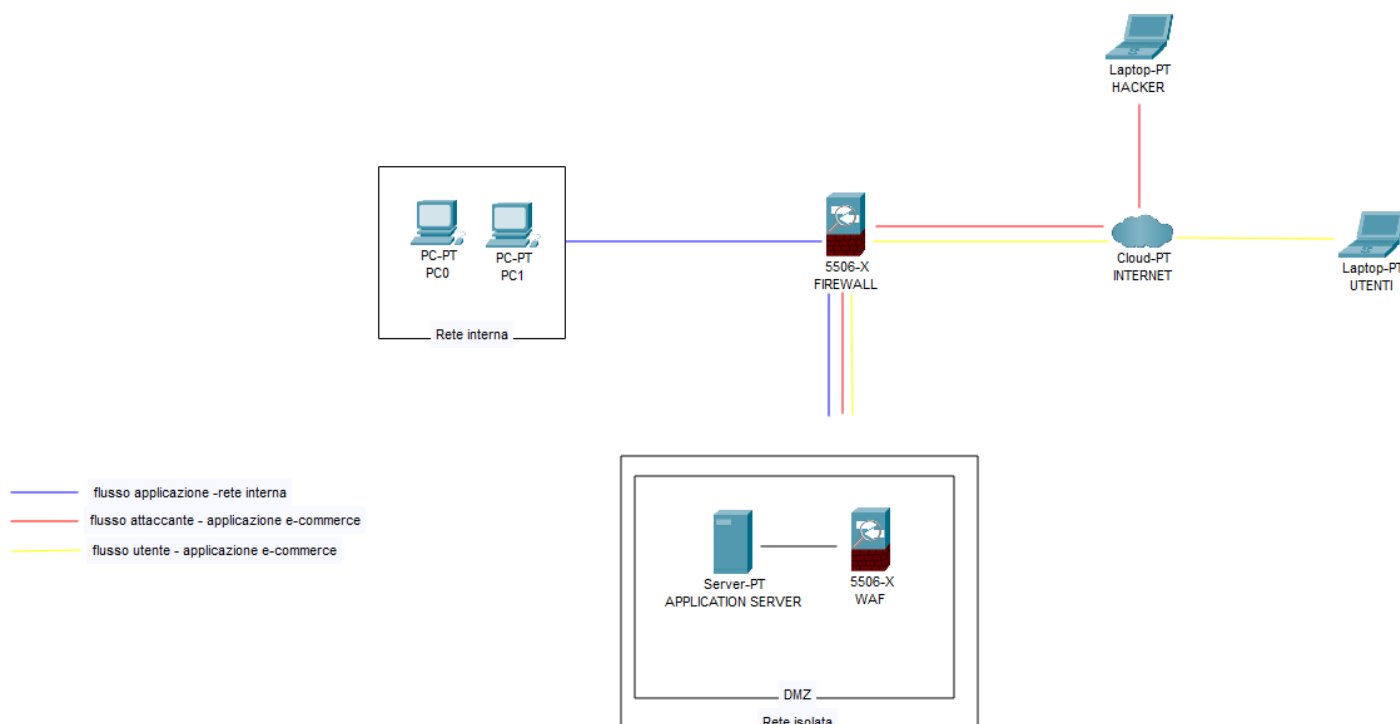
Found an instant messenger related domain

Il file **notification.bundle.js** potrebbe contenere istruzioni o codice aggiuntivo che potrebbe avere scopi dannosi o eseguire ulteriori azioni nel contesto dell'applicazione o del sistema. Inoltre, è stata rilevata un'associazione con un dominio relativo a un servizio di messaggistica istantanea. Questo potrebbe indicare che il file è coinvolto nell'interazione con un servizio di messaggistica istantanea o può comportare azioni che coinvolgono tale servizio.

3) RESPONSE

L'applicazione Web viene infettata da un malware.

La vostra priorità è che il malware non si propaghi sulla vostra rete, ma è altrettanto importante non divulgare informazioni sensibili verso Internet.

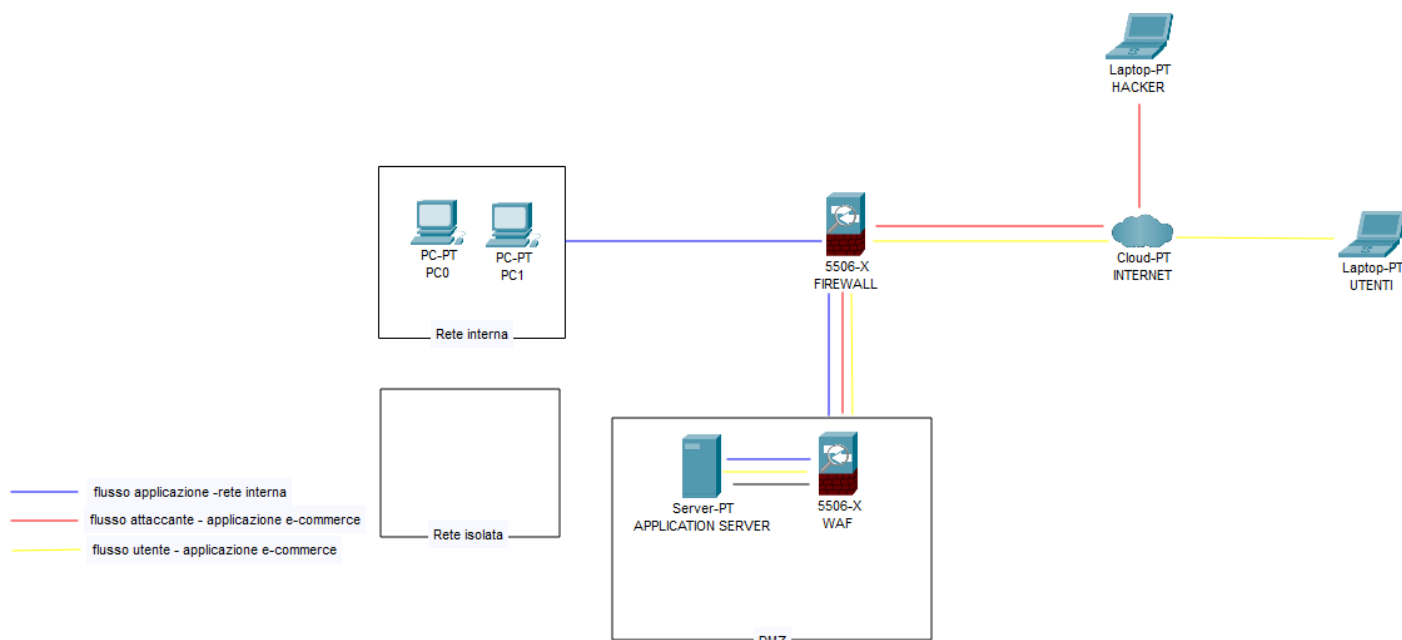


Quando un'applicazione Web viene infettata da un malware, la protezione della rete e la prevenzione della divulgazione di informazioni sensibili sono priorità importanti. Per questo si possono adottare più strategie:

- Isolamento applicazione
- Disconnessione della rete
- Analisi del malware
- Rimozione del malware
- Patch e aggiornamenti
- Monitoraggio e logging

4) SOLUZIONE COMPLETA

Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

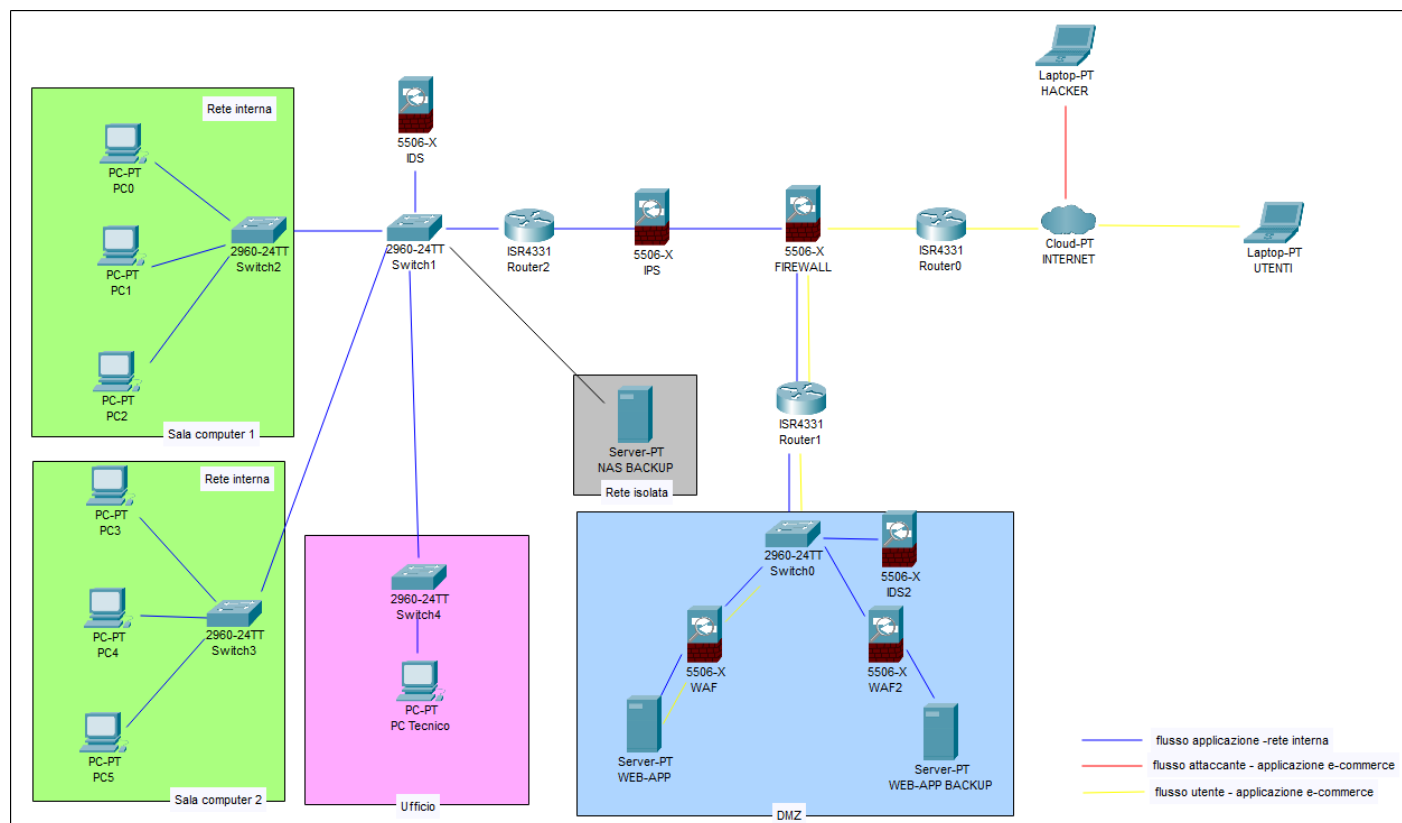


Mitigata la minaccia con le soluzioni precedentemente espote, procedo con una pulizia o reinstallazione completa.

Una volta rimosso il malware ed aver confermato che il server è stato ripulito si può procedere con una configurazione di sicurezza ottimizzata e ripristinare i dati da backup sicuri, sottoponendo il server a un'attenta valutazione della sicurezza per assicurarsi che sia protetto da future infezioni.

5) MODIFICA PIÙ AGGRESSIVA DELL'INFRASTRUTTURA

Integrando eventuali altri elementi di sicurezza.



- 1) Ho aggiunto switch separati per reti diverse in modo di segmentare la rete limitando la propagazione di minacce. In questo modo si aggiunge protezione per i dati sensibili e si migliora la sicurezza delle reti.
- 2) Ho aggiunto un NAS per il backup nella rete isolata che permette di isolare i dati di backup dalla rete principale, proteggendolo da potenziali attacchi o compromissioni.
- 3) Ho aggiunto un secondo router tra il firewall e la rete DMZ come ulteriore strato di protezione per limitare l'accesso non autorizzato ai sistemi, migliorando la sicurezza dell'ambiente.
- 4) Ho implementato un IDS collegato a un router nella rete DMZ e switch con IDS nella rete interna. Questo permette di rilevare e monitorare le attività sospette o potenzialmente dannose nella rete, con notifiche tempestive degli eventi di sicurezza, migliorando la sicurezza complessiva.
- 5) Ho aggiunto l'IPS tra router e firewall per il monitoraggio e blocco attivo di potenziali intrusioni.
- 6) Ho implementato due WAF per avere protezione contro attacchi mirati alle applicazioni web e da possibili vulnerabilità.

Si consiglia inoltre:

Aggiornare regolarmente dispositivi e software

Mantenere tutti i dispositivi di rete, i sistemi operativi e le applicazioni aggiornati con le ultime patch di sicurezza.

Implementare autenticazione a più fattori (MFA)

Autenticazione tramite qualcosa di cui l'utente è in possesso (come un codice generato da un'app sullo smartphone) oltre alle credenziali di accesso tradizionali.

Eseguire regolari pen-test

Per identificare vulnerabilità nel sistema.

Implementare una gestione degli accessi basata su privilegi (RBAC)

Privilegi di accesso assegnati in base ai ruoli e alle responsabilità degli utenti in modo che solo le persone autorizzate abbiano accesso ai dati e alle risorse sensibili.

Educazione e consapevolezza sulla sicurezza

Formazione e sensibilizzazione al personale sull'importanza delle pratiche di sicurezza informatica, come l'utilizzo di password forti, l'identificazione di attività sospette e l'evitare di cliccare su link o allegati sospetti nelle e-mail.

Monitoraggio e rilevamento delle minacce

Soluzioni di monitoraggio continuo della sicurezza, come sistemi SIEM (Security Information and Event Management) o soluzioni di threat intelligence, per rilevare e rispondere alle potenziali minacce in tempo reale.

Backup regolari e pianificati

Eseguire backup regolari dei dati critici e di archivarli in un luogo sicuro. I backup consentono di ripristinare i dati in caso di incidente o compromissione.

Aggiunta di UPS

Per fornire energia di backup in caso di interruzioni di corrente, proteggendo i dispositivi di rete da danni causati da improvvisi blackout o picchi di tensione.