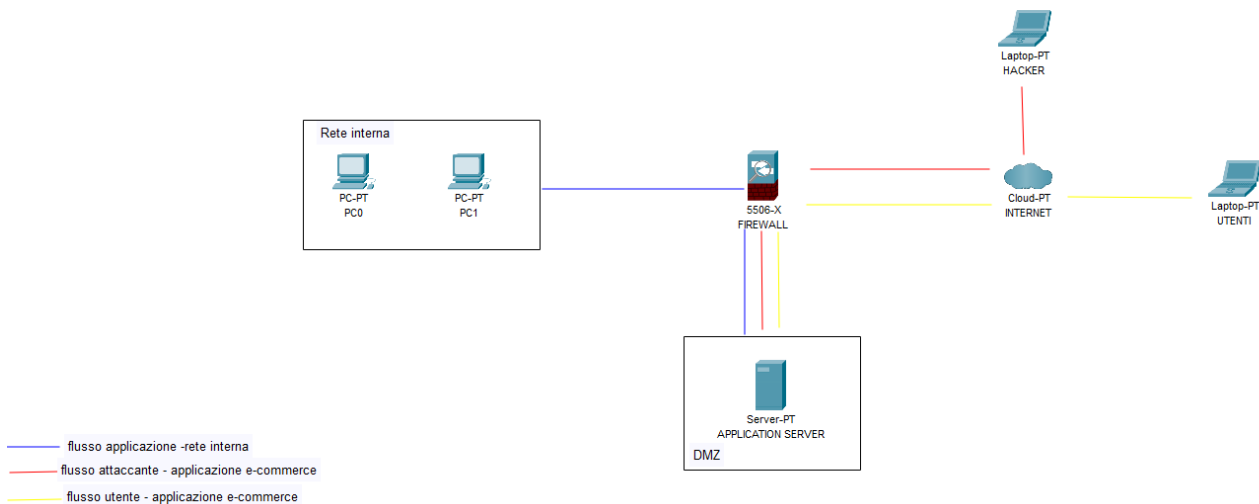


Progetto settimanale – Week 9

Analisi dei log – caso reale

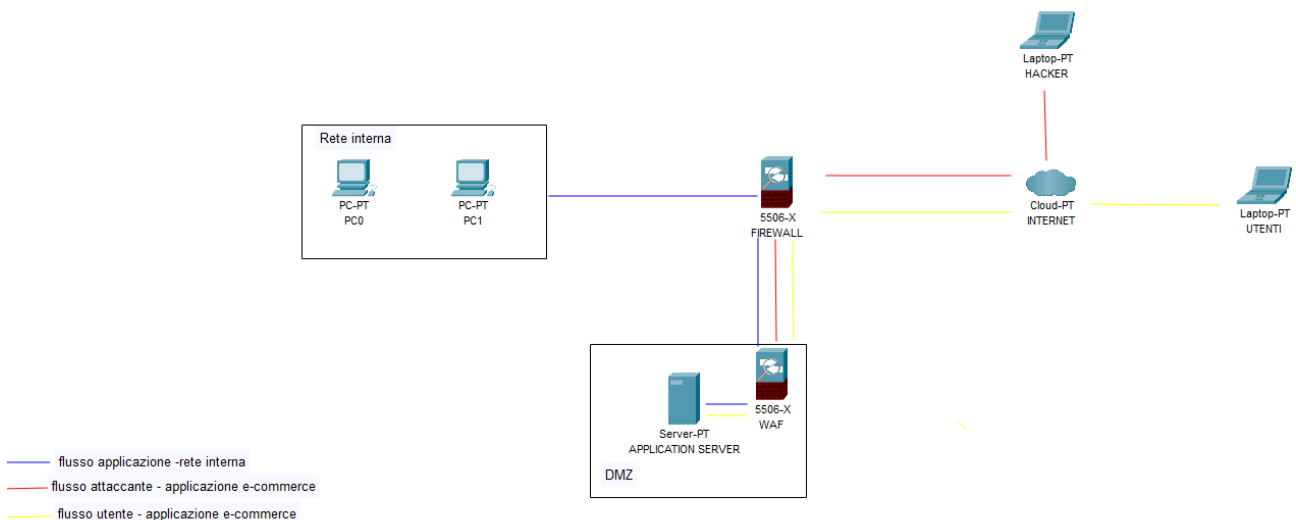
Architettura di rete

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.



1)Azioni preventive

In caso di attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato, come azione preventiva possiamo inserire un controllo di network, in questo caso un WAF, il quale è un firewall che protegge le app, dagli attacchi sopracitati. In questo caso tutti i flussi, arrivano al WAF e successivamente all'application server. In questo modo l'hacker, con questi attacchi, non accede all'application server e il suo flusso si interrompe al WAF.

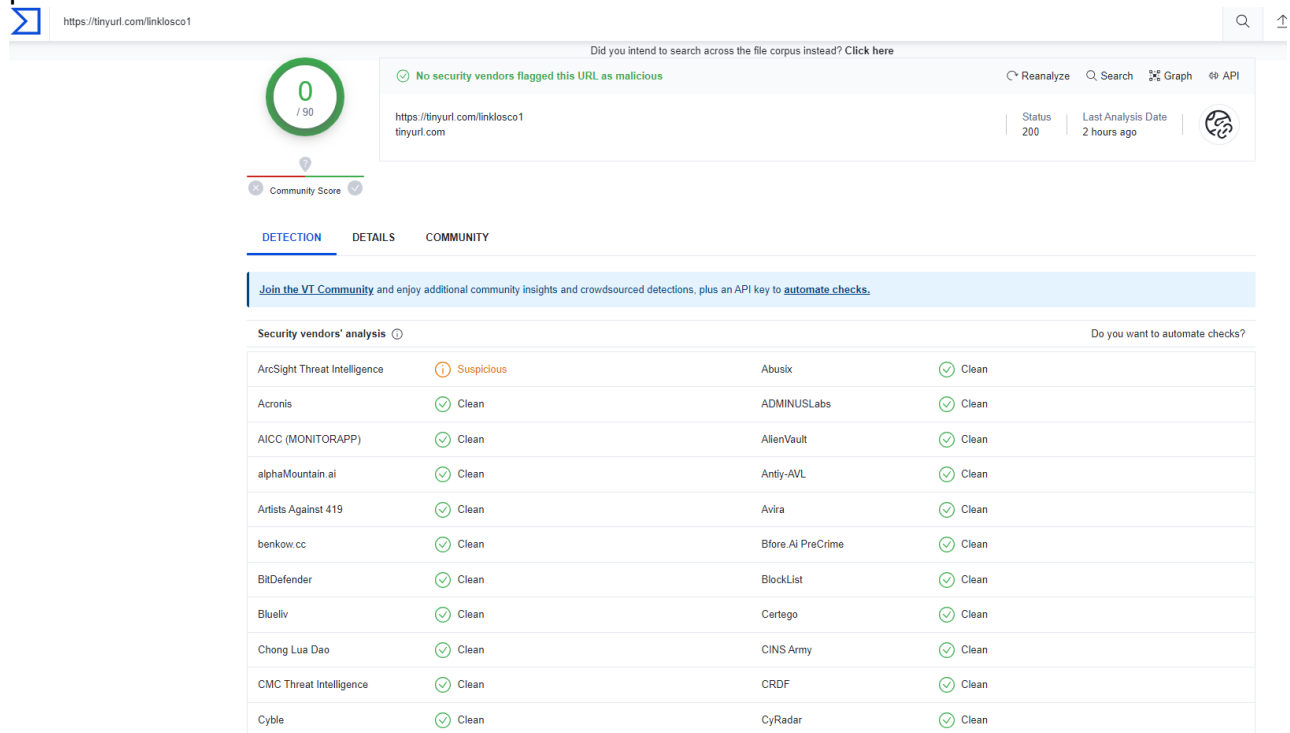


2)Analisi attacco

L'obiettivo di questo punto è di analizzare due link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco.

Link 1

Quindi vado alla ricerca di informazioni sui link, utilizzando un open source intelligence (osint), in questo caso VirusTotal. Il programma ci dice che il link è pulito e non sono presenti virus al suo interno.



Did you intend to search across the file corpus instead? Click here

Reanalyze Search Graph API

https://tinyurl.com/linklosco1
Status: 200 | Last Analysis Date: 2 hours ago

Community Score: 0 / 90

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

ArcSight Threat Intelligence	⚠ Suspicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AICC (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
alphaMountain.ai	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
benkow.cc	✓ Clean	Bfcore.AI PreCrime	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Cartago	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean
CMC Threat Intelligence	✓ Clean	CRDF	✓ Clean
Cyble	✓ Clean	CyRadar	✓ Clean

Provo ad utilizzare altri programmi, tra cui Hybrid analysis e ci riporta che è un link maligno, con un threat score di 100/100.

Submission name: hxxps://tinyurl.com/linklosco1

malicious

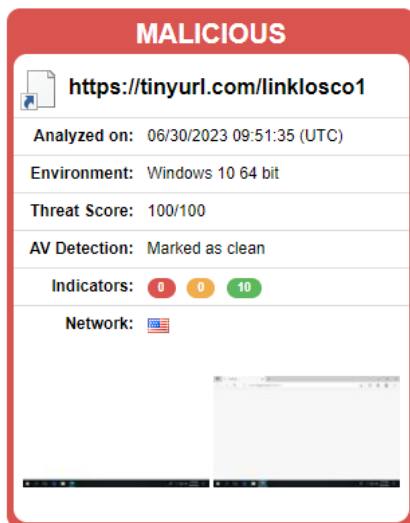
Infatti il file mini-wallet.html (file approfondito nel secondo link), risulta malevolo e potrebbe esserci del codice malevolo al suo interno o potrebbe subire un attacco, vista la vulnerabilità.

Files extracted during detonation

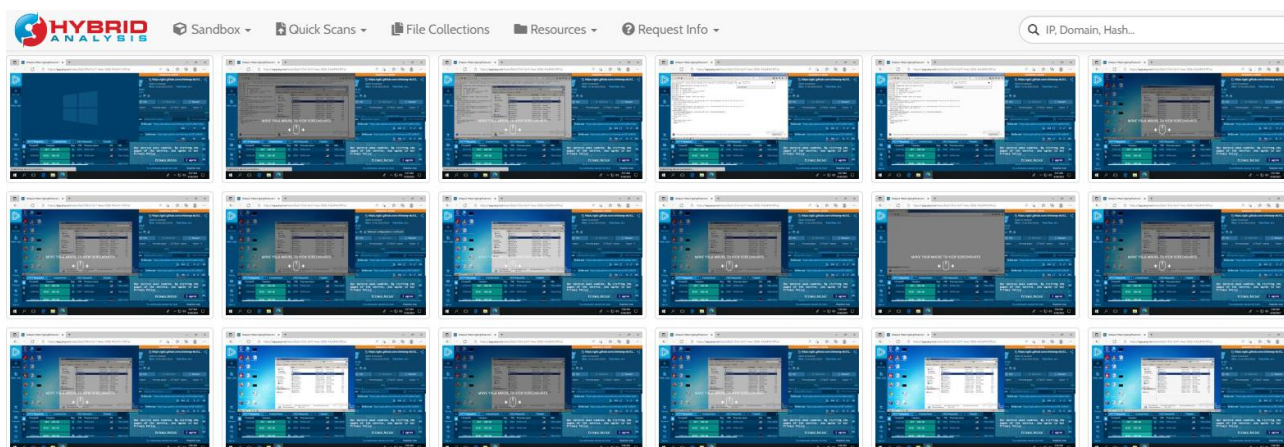
Name	Sha256	Verdict
mini-wallet.html	df47aac0fa71fbcecc16685ad4024965491e601880daf1fefa3735e769df661b	malicious
load-ec-i18n.bundle.js	4cac69d0545740f35cb9b1c4a473875a1f4064f087eb8ea119baf98059a417e	no specific threat
miniwallet.bundle.js	78a7e765ffd6dffaf3b92b6234271fdOdddf5945f38e70dOe22324c1ec06eca	no specific threat
urlref_httpstinyurl.comlinklosco1	7e53c9a37b9548d5268fc41f49362ab5958f9fc8596758aa5f885ecd76b815b1	no specific threat
shopping_iframe_driver.js	456369ffe3542bb3ab1288484cfb909820a76f35e4d635a8638baf44ac6d3028	suspicious
edge_driver.js	4cb3db7a9fbaec8d6607d051b4b704d5a5689d4db6b19426f6b182c571308642	no specific threat

Questo programma esegue anche un Falcon Sandbox Reports, quindi esegue l'url. Infatti nel report dell'analisi, ci sono gli screenshot dell'esecuzione dell'any.run.

Falcon Sandbox Reports



Quindi procedo con lo studio degli screenshot fatti dal software, così da **non aprire sul mio browser l'url che risulta essere malevolo**.



Nella sandbox, l'utente accedendo sul browser, si dirige su github e scarica un codice che permette di modificare le impostazioni del server DNS per il wifi. Il file è un eseguibile che apre una powershell, dalla quale si possono effettuare modifiche di domini e può essere utilizzato da un malintenzionato per raggiungere i suoi scopi.

Link 2

Effettuo anche per il secondo link delle ricerche incrociate, per verificare se il link è malevolo o meno. Anche in questo caso, VirusTotal riporta che il link è pulito, a differenza di Hybrid Analysis che ci mostra questi risultati:

Submission name: [hxxps://tinyurl.com/linklosco2](https://tinyurl.com/linklosco2)
 Size: 54B
 Type:

malicious

Threat Score: 100/100

Falcon Sandbox Reports

MALICIOUS

<https://tinyurl.com/linklosco2>

Analyzed on: 06/30/2023 10:56:10 (UTC)

Environment: Windows 10 64 bit

Threat Score: 100/100

AV Detection: Marked as clean

Indicators: 0 0 11

Network:

Risalta all'occhio anche in questo caso il file mini-wallet.html che risulta esser maligno ed entrando nei dettagli dell'analisi posso vedere la valutazione del rischio(come segue nel prossimo screen):

- Installa hook/patch del processo in esecuzione;
- Scrive i dati in un processo remoto;
- Fingerprinting:
- Richiede informazioni sul debugger del kernel;
- Le query elaborano le informazioni;
- Interroga le impostazioni di sicurezza sensibili di IE;
- Interroga le impostazioni di visualizzazione delle estensioni di file associate al sistema;

mini-wallet.html

This report is generated from a file or URL submitted to this webservice on May 21st 2023 20:25:11 (UTC) and action script: Default browser analysis
Guest System: Windows 10 64 bit, Professional, 10.0 (build 16299),
Report generated by Falcon Sandbox v10.12 © Hybrid Analysis

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Hash Seen Before | No similar samples | Report False-Positive | Request Report Deletion

malicious

Threat Score: 80/
AV Detection: Marked as cl

Link | Twitter | Facebook

Incident Response

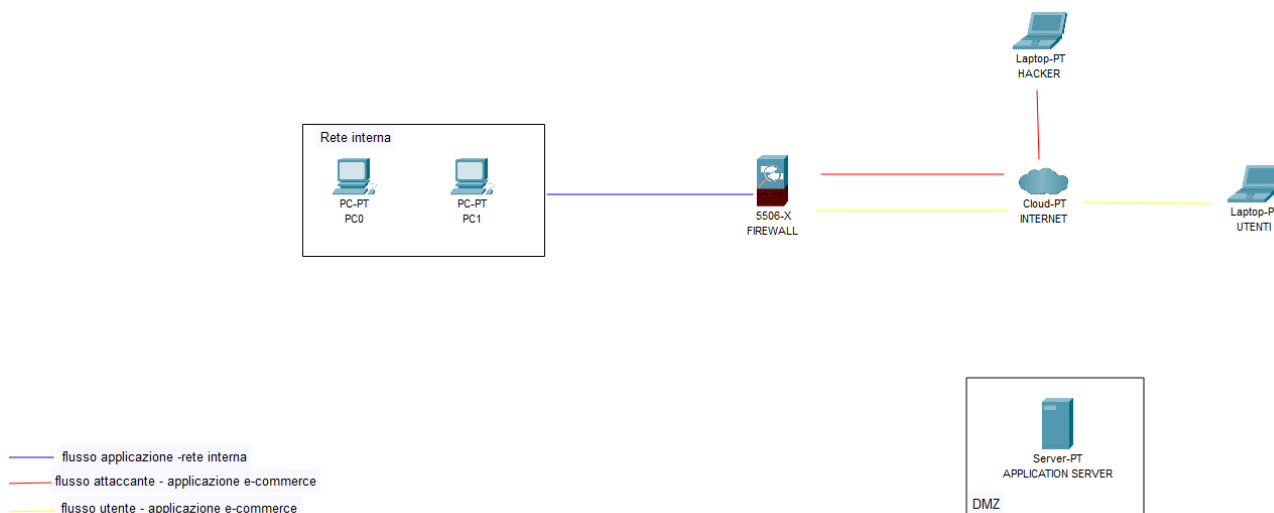
Risk Assessment

Persistence	Installs hooks/patches the running process Writes data to a remote process
Fingerprint	Queries kernel debugger information Queries process information Queries sensitive IE security settings Queries the display settings of system associated file extensions
Network Behavior	Contacts 1 domain and 2 hosts. View all details

Utilizzando il tool su questo secondo link, il software non elabora gli screenshot del programma, per questo ho approfondito i vari risk assesment e sono andato alla ricerca di quest'ultimi per avere una panoramica maggiore sui rischi del link stesso. Per questo, ho evitato di aprire il link sul mio pc, per evitare possibili minacce trovate dal tool open source.

3)Response

L'applicazione Web viene infettata da un malware. La priorità è che il malware non si propaghi sulla rete interna, ma è altrettanto importante non divulgare informazioni sensibili verso internet. Visto che in questo caso, con l'isolamento, il server web potrebbe divulgare informazioni su internet, l'unico modo per non permettere ciò è la rimozione completa del server Web, distaccandola dal router/firewall.

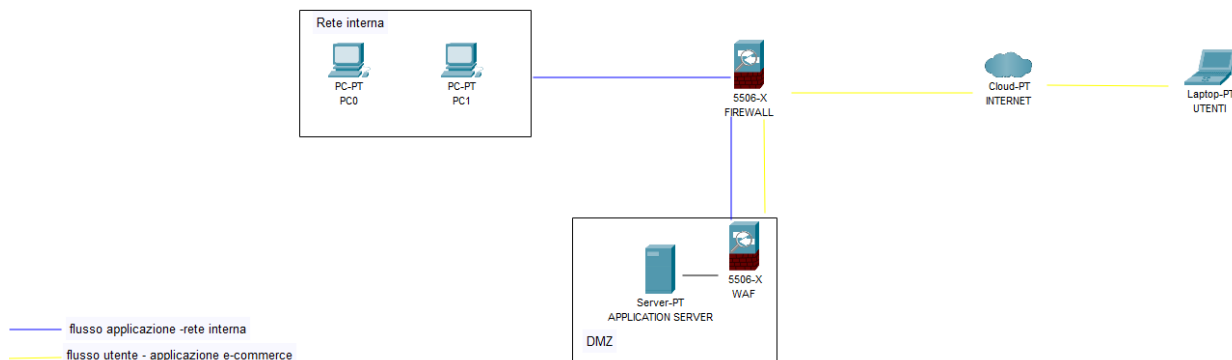


4) Soluzione completa

Dopo che il server web è stato infettato e isolato dalla rete, bisogna prima procedere con l'analisi dell'incidente per comprendere com'è avvenuta la compromissione. Quindi si raccolgono le informazioni sui log, si analizza il traffico di rete, si cercano file sospetti o modifiche non autorizzate e si individuano le vulnerabilità che hanno consentito l'accesso.

Si procede poi con il ripristino del server utilizzando una copia pulita dei dati di un backup e si effettua un aggiornamento di sistema con le ultime patch di sicurezza installate.

Ora, dopo aver effettuato i passaggi descritti poco fa, posso unire il server rimosso nel punto precedente e reintegrarlo come in figura 1 con un WAF, per impedire attacchi sqli e XSS.



5) Modifica <<più aggressiva>> dell'infrastruttura

All'infrastruttura base ho aggiunto i seguenti elementi:

- Router/Switch, al fine di ottimizzare la comunicazione tra i dispositivi e migliorare l'efficienza complessiva del sistema di rete;
- IPS, per proteggere la rete da intrusioni e attacchi informatici. L'obiettivo principale dell'IPS è rilevare e prevenire attività sospette o dannose, garantendo la sicurezza e l'integrità del sistema di rete;
- Web app aggiuntiva, L'obiettivo di questa aggiunta è garantire la continuità del servizio e ridurre al minimo gli eventuali tempi di inattività nel caso in cui si verifichi un'interruzione dell'applicazione principale. L'applicazione web aggiuntiva funge da backup.
- segmentazione della rete;
- pc tecnico, per la risoluzione dei problemi e analisi dei log.

