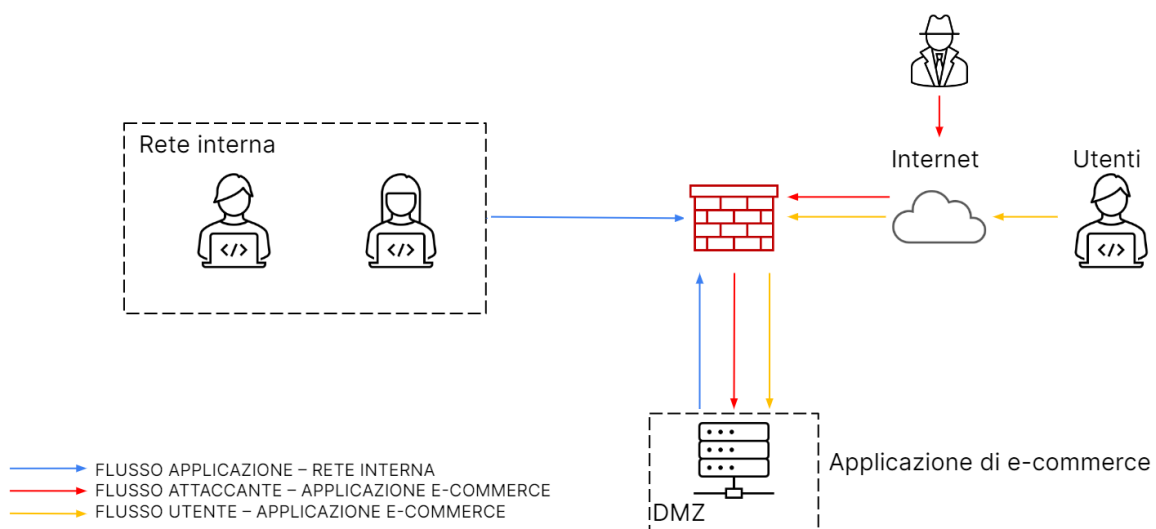


## Weekly Project Report

# ANALISI DEI LOG

Il progetto di questa settimana prevede l'intervento del team CSIRT durante un attacco per la gestione della rete prima che venga compromessa.

La situazione iniziale è quella che si vede in figura, dove abbiamo la seguente configurazione di rete: rete aziendale suddivisi in rete interna e DMZ. La rete interna è utilizzata dagli impiegati per poter svolgere le loro mansioni e comunica tramite un firewall con la DMZ dove si trova il webserver tramite cui si accede all'e-commerce. Ovviamente anche tutti i collegamenti dall'esterno passano attraverso il firewall prima di raggiungere l'e-commerce.

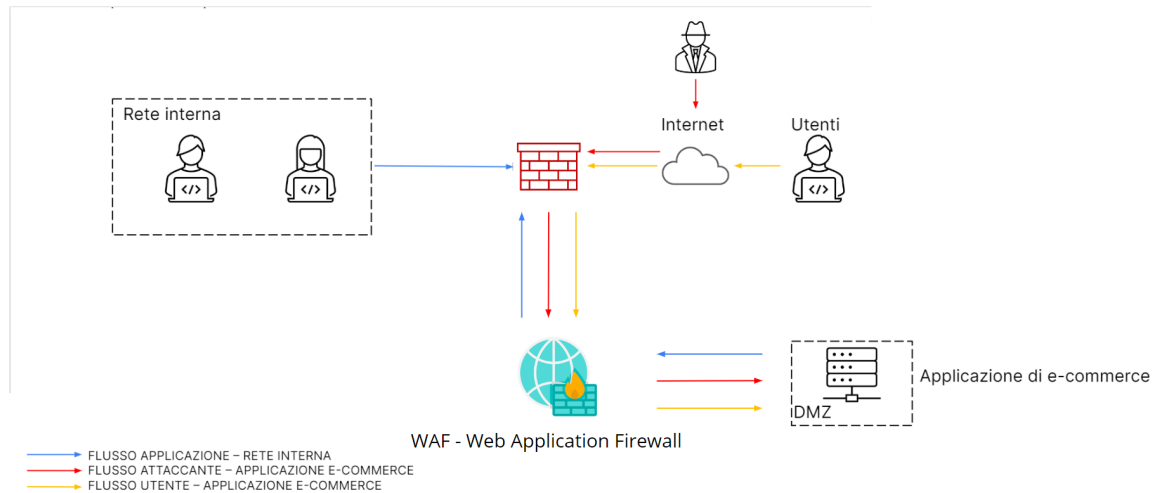


**Il compito del CSIRT si divide in 5 punti che sono:**

- 1) Proporre **azioni preventive** che si sarebbero potute **implementare per difendere l'applicazione Web da potenziali attacchi XSS e SQLi**
- 2) Effettuare un **analisi di due link sospetti** rinvenuti durante l'attacco e **fare un report** per ognuno su quanto ne viene fuori
- 3) **Incident response action** a seguito dell'attacco tramite malware all'applicazione Web
- 4) Mostrare la **configurazione di rete a valle delle response action applicate**
- 5) **Presentare una nuova configurazione di rete** con delle modifiche più concrete integrando altri eventuali dispositivi di sicurezza

## 1 - Azioni Preventive contro XSS e SQLi

Per quanto riguarda la configurazione di rete ciò che si poteva fare a livello di azione preventive era l'installazione di un **WAF** che sta per Web Application Firewall ovvero come si può dedurre dal nome un firewall dedicato alla protezione delle web app che **tramite l'analisi e filtraggio del traffico HTTP** in entrata e in uscita riesce a proteggere le app da attacchi quali cross site scripting, sql injection.



## 2 - Analisi Link Sospetti e Report

Durante l'attacco **vengono rinvenuti due link potenzialmente malevoli** che **dobbiamo analizzare** per capire **cosa sono e a cosa hanno potuto causare sul sistema**

I due link in questione sono:

- a) <https://tinyurl.com/linklosco1>
- b) <https://tinyurl.com/linklosco2>

Procediamo quindi ad **effettuare un'analisi preliminare con Virus Total** che è un sito web che permette l'analisi di files e/o URLs per scovarne virus o malware all'interno basandosi sui database dei maggiori antivirus in circolazione come Kaspersky, Avg ecc..

Una volta aperti, apparentemente **sembrano dei link innocui infatti Virustotal assegna uno score di 0 su 90**.

Ci spostiamo quindi nella **sezione Details**, per cercare di ottenere maggiori informazioni a riguardo ed ecco ci vengono mostrati **sia l'url originale, sia l'indirizzo IP di provenienza**.

### Screen Link 1

The screenshot shows the VirusTotal analysis interface for the URL <https://tinyurl.com/linklosco1>. The score is 0/90, indicating no security vendors flagged this URL as malicious. The 'DETAILS' tab is selected, showing the following information:

- Categories:** Forcepoint ThreatSeeker (web hosting), Sophos (information technology), Xcitium Verdict Cloud (mobile communications), BitDefender (computersandsoftware).
- History:**
  - First Submission: 2023-06-30 07:12:33 UTC
  - Last Submission: 2023-06-30 07:21:09 UTC
  - Last Analysis: 2023-06-30 07:21:09 UTC
- HTTP Response:**
  - Final URL: <https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a/>
  - Serving IP Address: 172.67.1.225

## Screen Link 2

The screenshot displays the Any.Run interface for analyzing the URL `https://tinyurl.com/linklosco2`. The interface includes a search bar at the top right and a navigation bar with tabs for DETECTION, DETAILS (highlighted), and COMMUNITY. A green circle with the number 0 indicates a score of 0/90. A green banner states "No security vendors flagged this URL as malicious". The URL is listed as `https://tinyurl.com/linklosco2` with a status of 200 and a last analysis date of 2 hours ago. Below the navigation bar, there is a section for "Join the VT Community" and a table of categories. The "History" section shows submission and analysis dates. The "HTTP Response" section is highlighted with a red box, showing the final URL `https://app.any.run/tasks/605ba854-4644-4140-9ea5-be9057161248/` and the serving IP address `172.67.1.225`.

Categories
Forcepoint ThreatSeeker
Sophos
Xcitium Verdict Cloud
BitDefender

History
First Submission
Last Submission
Last Analysis

HTTP Response
Final URL
Serving IP Address

Vediamo che **sono entrambi dei link di Any.Run** che è uno strumento per il rilevamento, il monitoraggio e la ricerca di minacce informatiche in tempo reale; mette a disposizione un sandbox interattivo online dotato di un'interfaccia intuitiva e che offre report altamente dettagliati.

Andiamo quindi a cliccare sul link e veniamo riportati su Any.Run e da qui **inizia il processo di studio e analisi del loro contenuto che verrà poi riportato in due report** generati automaticamente da Any.Run.

Notiamo inoltre che **provengono dallo stesso indirizzo IP**, quindi per approfondire le nostre conoscenze andiamo ad effettuare un'analisi anche di quest'ultimo. Cliccandoci sopra ne viene fuori che appartiene al provider Cloudflare e soprattutto che un produttore ha già segnalato questo indirizzo come malevolo.

The screenshot displays the Any.Run interface for analyzing the IP address `172.67.1.225`. The interface includes a search bar at the top right and a navigation bar with tabs for DETECTION, DETAILS (highlighted), RELATIONS, and COMMUNITY. A red circle with the number 1 indicates a score of 1/88. A red banner states "1 security vendor flagged this IP address as malicious". The IP address is listed as `172.67.1.225 (172.67.0.0/16)` with a status of 13335 (CLOUDFLARENET) and a last analysis date of 5 hours ago. Below the navigation bar, there is a section for "Join the VT Community" and a table of basic properties. The "Basic Properties" section is highlighted with a red box, showing the network details.

Basic Properties
Network
Autonomous System Number
Autonomous System Label
Regional Internet Registry
Country
Continent

Continuando poi all'interno della pagina ci viene riportata anche una schermata con WHOIS che contiene tutta una serie di informazioni dettagliate riguardante l'indirizzo IP e infine troviamo la **sezione delle "ricerche google"** che riporta invece i principali risultati contenenti tale indirizzo e possiamo notare **come primo risultato c'è quello del sito di "abuseipdb.com"** il quale contiene appunto un database con tutti gli abusi di IP e l'indirizzo in questione è stato già segnalato 61 volte.

The screenshot shows a web browser interface. At the top, there's a search bar with the IP address "172.67.1.225" entered. Below the search bar, there are two main sections. The first section is titled "Whois Lookup" and contains detailed information about the IP address, including its range, CIDR, netname, and organization (Cloudflare, Inc.). The second section is titled "Google results" and shows a list of search results. The first result is from "abuseipdb.com" and is highlighted with a red box. The text of the first result is: "172.67.1.225 | CloudFlare Inc. - AbuseIPDB www.abuseipdb.com IP Abuse Reports for 172.67.1.225: This IP address has been reported a total of 61 times from 20 distinct sources. 172.67.1.225 was first reported on ...".

**Questo la dice lunga sulla bontà del contenuto dei link provenienti da questo indirizzo.**

Analisi link 1:

Questo link mostra il processo di esecuzione di un file chiamato DNS\_Changer.ps1 il quale è un codice in power shell tramite il quale si possono andare a modificare le impostazioni di rete riguardanti il DNS.

Analisi link 2;

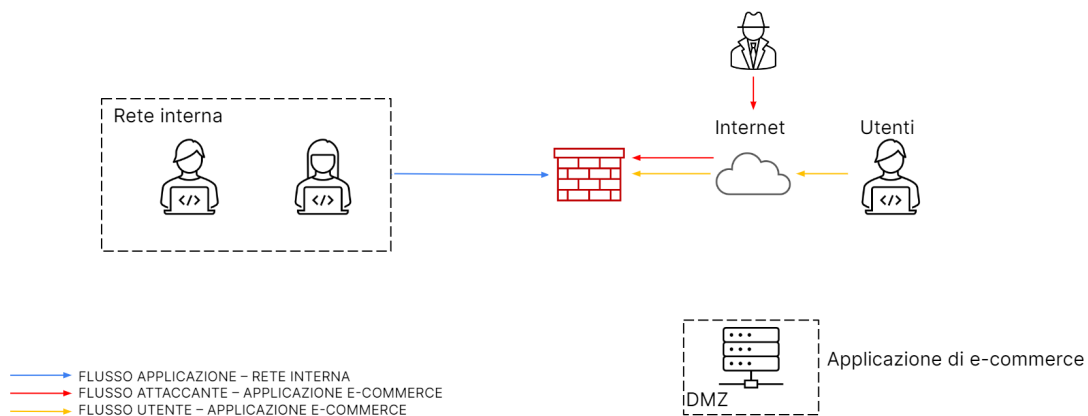
Questo link mostra invece il processo di .... iniziando dal download del tool Sysinternal che offre risorse tecniche e utilità per gestire, diagnosticare, risolvere i problemi e monitorare in ambiente Windows.

Dopodiché procede con il download di un altro file denominato DOCX\_SENTENCIA, il quale dopo essere stato estratto mostra l'icona di un file di Adobe ma in realtà è un eseguibile.

### 3 - Incident Response contro attacco malware

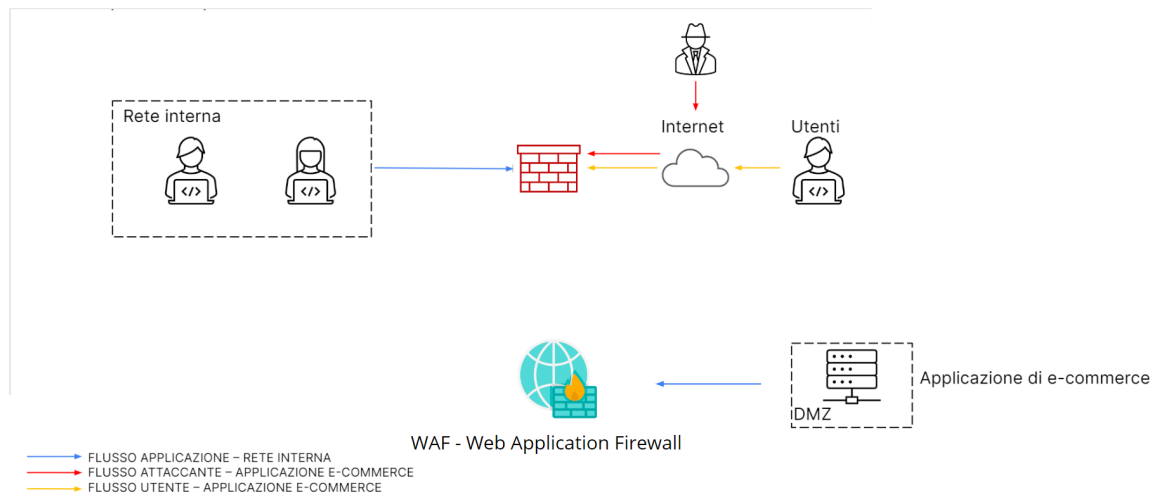
Dopodiché il team **deve occuparsi della gestione del web server** in quanto da analisi più dettagliate ne emerge che **è stato colpito da un malware**.

Di conseguenza come **da linee guida stabilite all'interno dell'incident response plan** si procede con la **rimozione completa della componente** disconnettendola totalmente dalla rete così che l'attaccante non vi abbia più accesso **per evitare** in primis **che il malware si propaghi** sul resto della rete andando a causare ulteriori danni agli altri componenti e poi per **evitare data-leaks verso l'esterno**.



## 4 - Configurazione di rete post response action

Dopo **aver provveduto alla rimozione del web server** la configurazione della rete aziendale è la seguente:



Come si può notare **al momento l'azienda non è in grado di fornire i suoi servizi** in quanto l'unico web server su cui gira l'e-commerce è stato rimosso dalla rete.

## 5 - Configurazione di rete “strong”

L'attività **post-incidente**, porta il team CSIRT a fare delle considerazioni su cosa si poteva fare per evitare l'incidente; **questa analisi prende il nome di lesson learned** e porta il team date le difficoltà trovatosi ad affrontare, a **ridisegnare la configurazione di rete** per renderla più robusta **ed evitare che si possano ripetere incidenti** come quello appena accaduto.

Viene quindi chiesto alla dirigenza uno stanziamento di budget per l'implementazione di ulteriori dispositivi e misure di sicurezza.

Nello specifico vengono aggiunti:

- **n.1 IPS** per la prevenzione delle minacce a monte della rete
- **n.1 Router interno** per l'eventuale creazione di altre sottoreti
- **n.1 Firewall** a difesa della rete interna
- **n.1 IDS** posizionato in rete interna per far sì che qualsiasi anomalia venga riconosciuta velocemente e avere così il tempo di intervenire
- **n.1 Switch interno** per arrivare ai singoli pc
- **n.1 Server Web** di ridondanza essendo l'e-commerce il core del business l'azienda non può permettersi di restare off. Nel caso dell'attacco appena subito se si avessero avuto a disposizione due serve si avrebbe potuto mettere in quarantena o eliminare il server colpito e garantire comunque la normale erogazione dei servizi aziendali.

