Analisi dei log caso reale

Traccia:

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

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

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

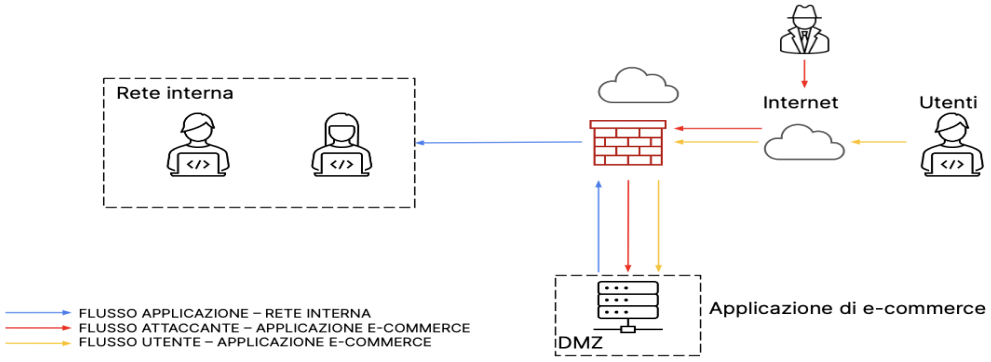
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, ma è altrettanto importante non divulgare informazioni sensibili verso Internet.
   Modificate la figura in slide 2 con la soluzione proposta.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

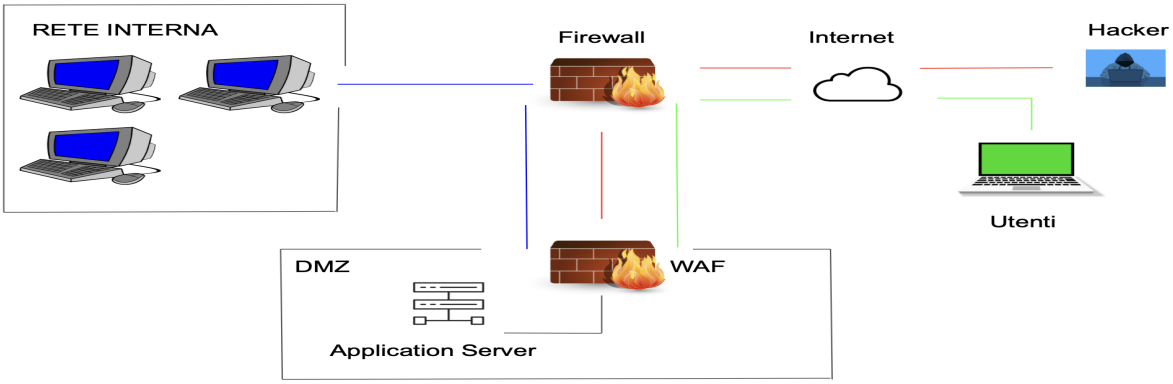
5. **Modifica «più aggressiva» dell'infrastruttura:** integrando eventuali altri elementi di sicurezza

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

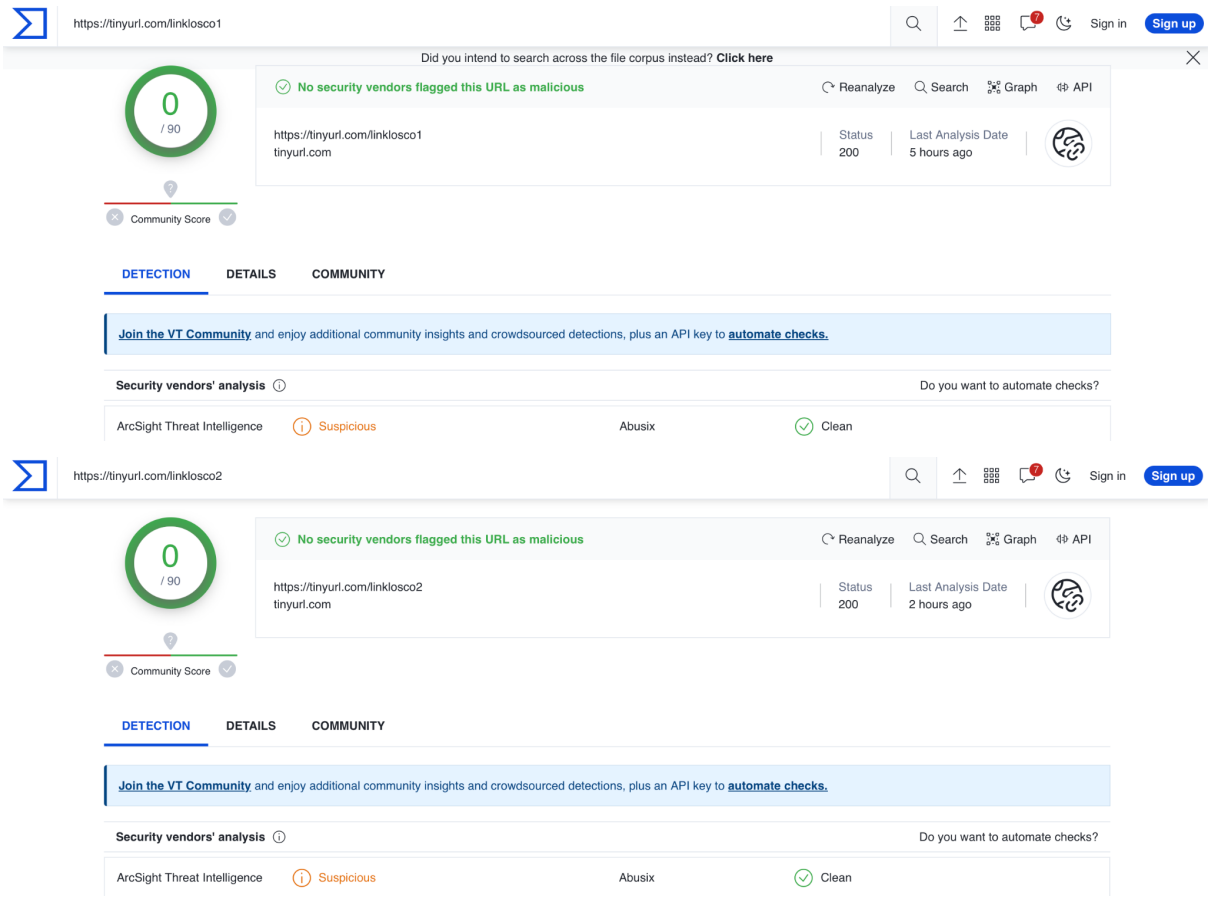
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



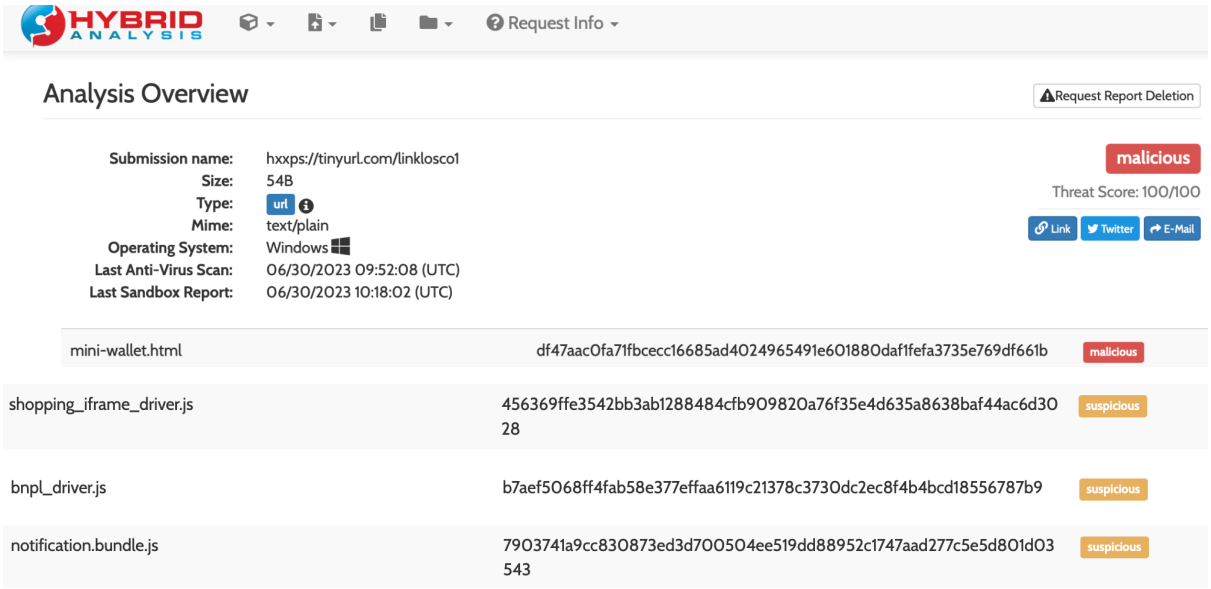
1 Come azione preventiva ho aggiunto il WAF (Web Application Firewall) che rileva e blocca attacchi di tipo SQL, XSS.

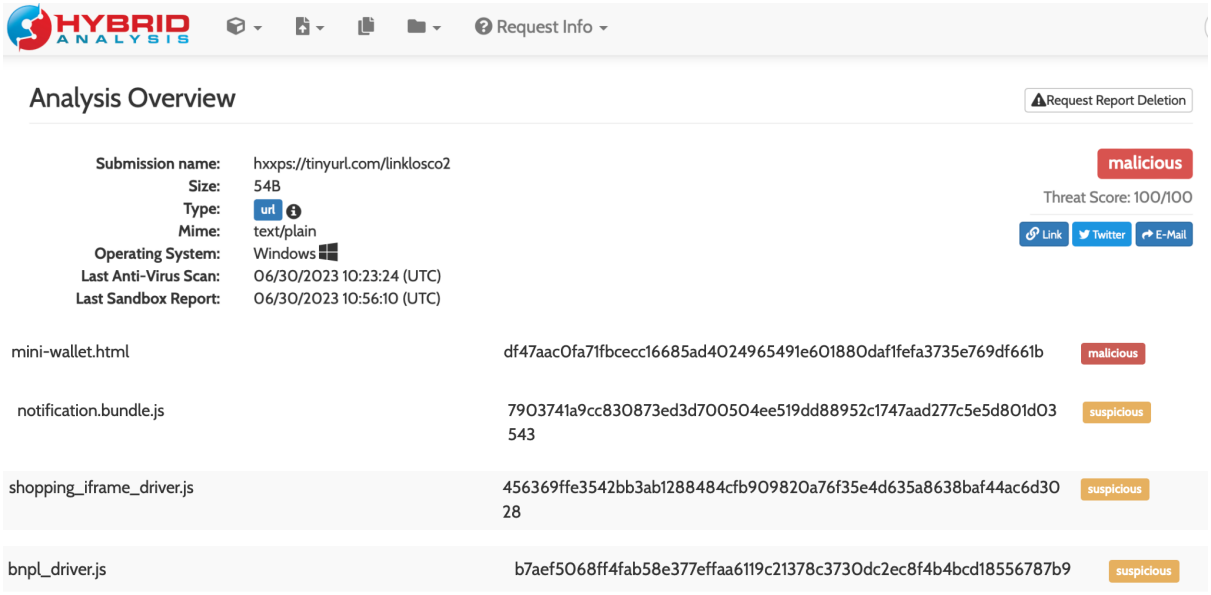


2 Per l'analisi dei link sospetti prima di aprirli ho effettuato una scansione prima su Virustotal, successivamente su Hybrid Analysis.



Virustotal non ha rilevato link malevoli mentre Hybrid Analysis ha rilevato la presenza di link malevoli

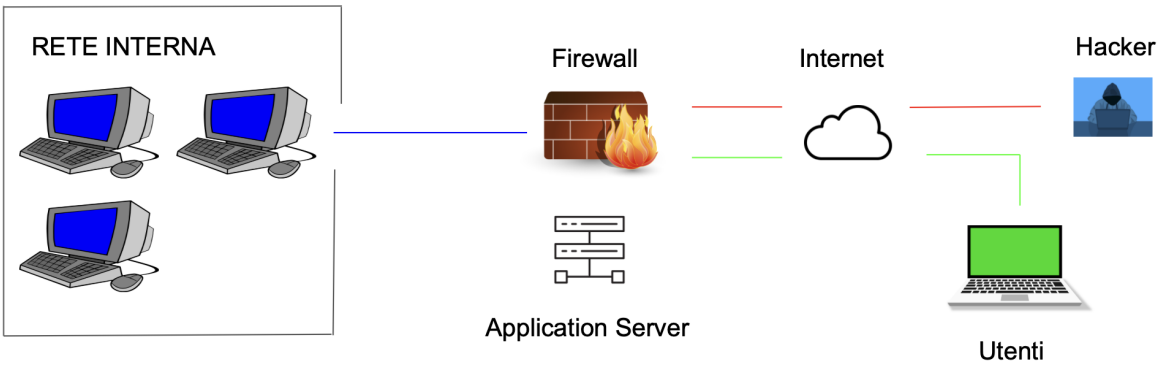




A fronte di queste analisi vediamo che i link sono malevoli e potrebbero contenere codice malevolo oppure virus all'interno.

3 Response

L'applicazione è stata infettata dal malware, se la priorità è quella che il malware non si propaghi sulla rete e su internet dobbiamo disconnetterlo del tutto



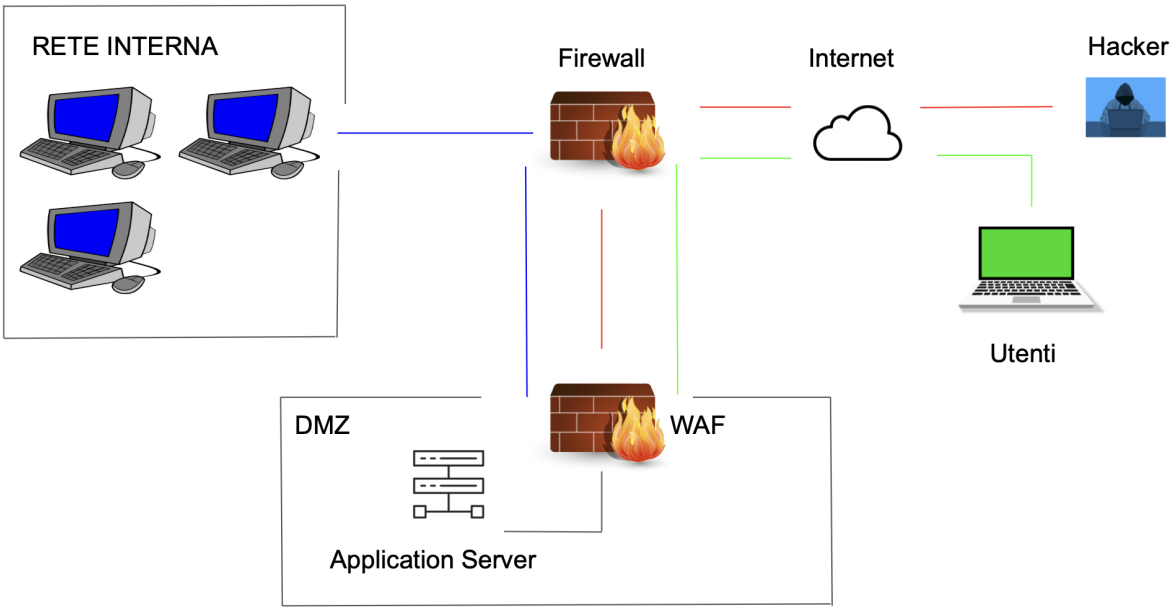
4 Soluzione completa

Una volta disconnesso l' Application Server il **CSIRT** deve passare alla fase di rimozione dell' incidente.

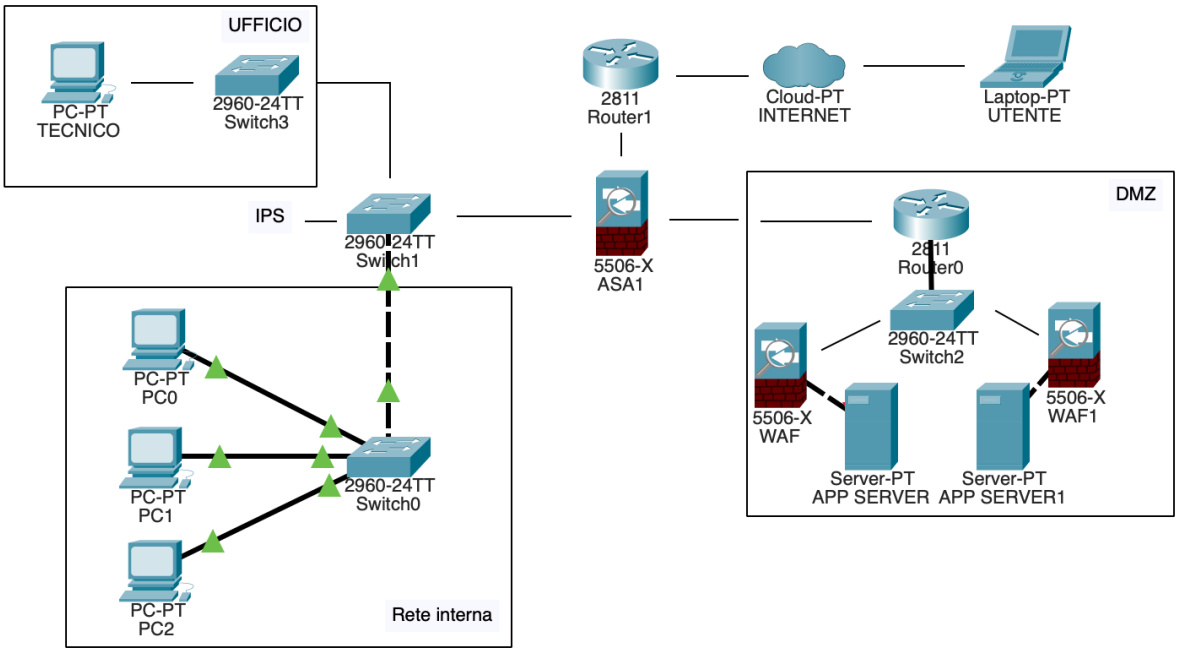
Questa fase dipende molto da che tipo di incidente è in corso, una lista con le attività da seguire la troviamo nei **playbook**

Una volta completata la fase di rimozione inizia la fase di recupero che consiste nel **recupero dei dati**, **l'applicazione delle patch**, **la revisione delle politiche dei firewall IPS** e **IDS** oppure **l'aggiornamento delle firme degli antivirus**

Con la tecnica **Reconstruction** andremo a recuperare le parti ancora affidabili di un sistema compromesso (Application Server)
Dopo aver rimosso la minaccia e aver fatto la patch del malware possiamo di nuovo mettere in collegamento l'application Server



5 Modifica più aggressiva



Ho aggiunto un secondo waf e un secondo app server e poi ho aggiunto ips per controllare le intrusione

Ciandri I