Report Compito 30/06/2023

Compito:

Compito di : Mendolia Valerio

Analisi dei Log, caso reale: -

Obiettivo

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

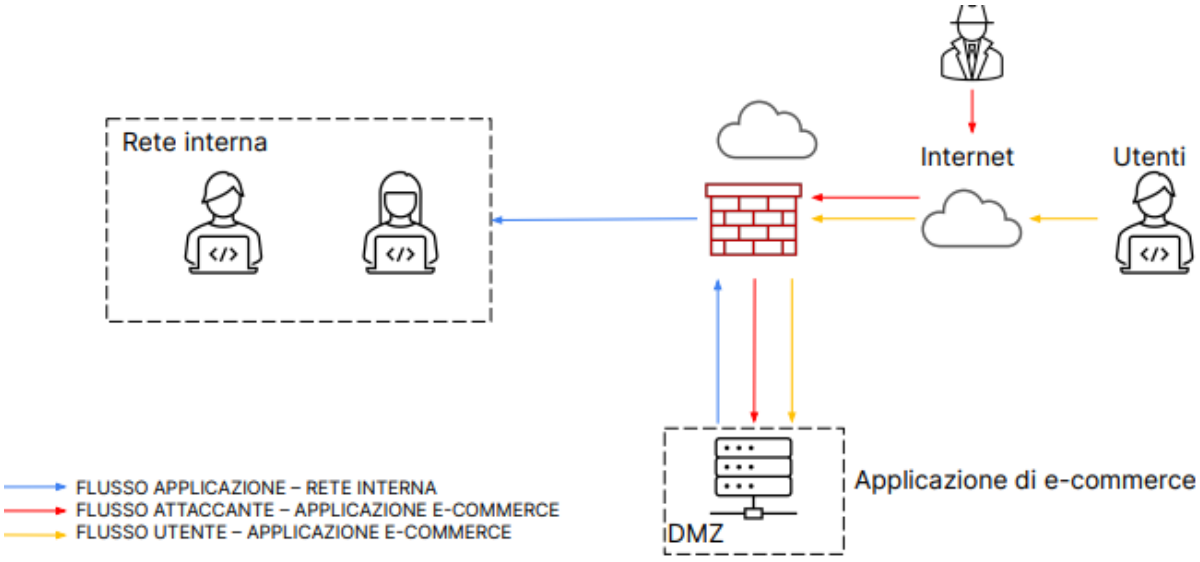
2. Analisi attacco: analizzare i seguenti link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco https://tinyurl.com/linklosco1 https://tinyurl.com/linklosco2

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

Immagine originale:



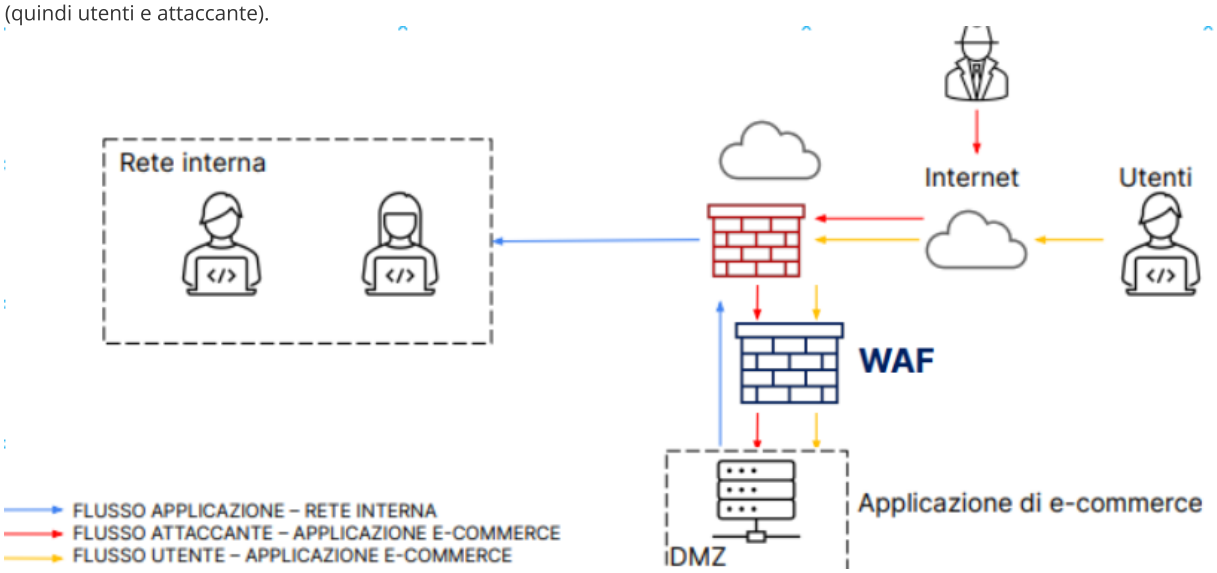
3

1. Azioni preventive

Come azioni preventive si può ovviamente implementare una soluzione come il Web Application Firewall che a differenza dei firewall standard sono costruiti per proteggere le webapp dagli attacchi XXS e Sql injections.

Quindi andiamo a modificare la figura proposta dall'esercizio dove abbiamo ipotizzato che il WAF sia a protezione del traffico in entrata sulla Web App da internet

(quindi utenti e attaccante).

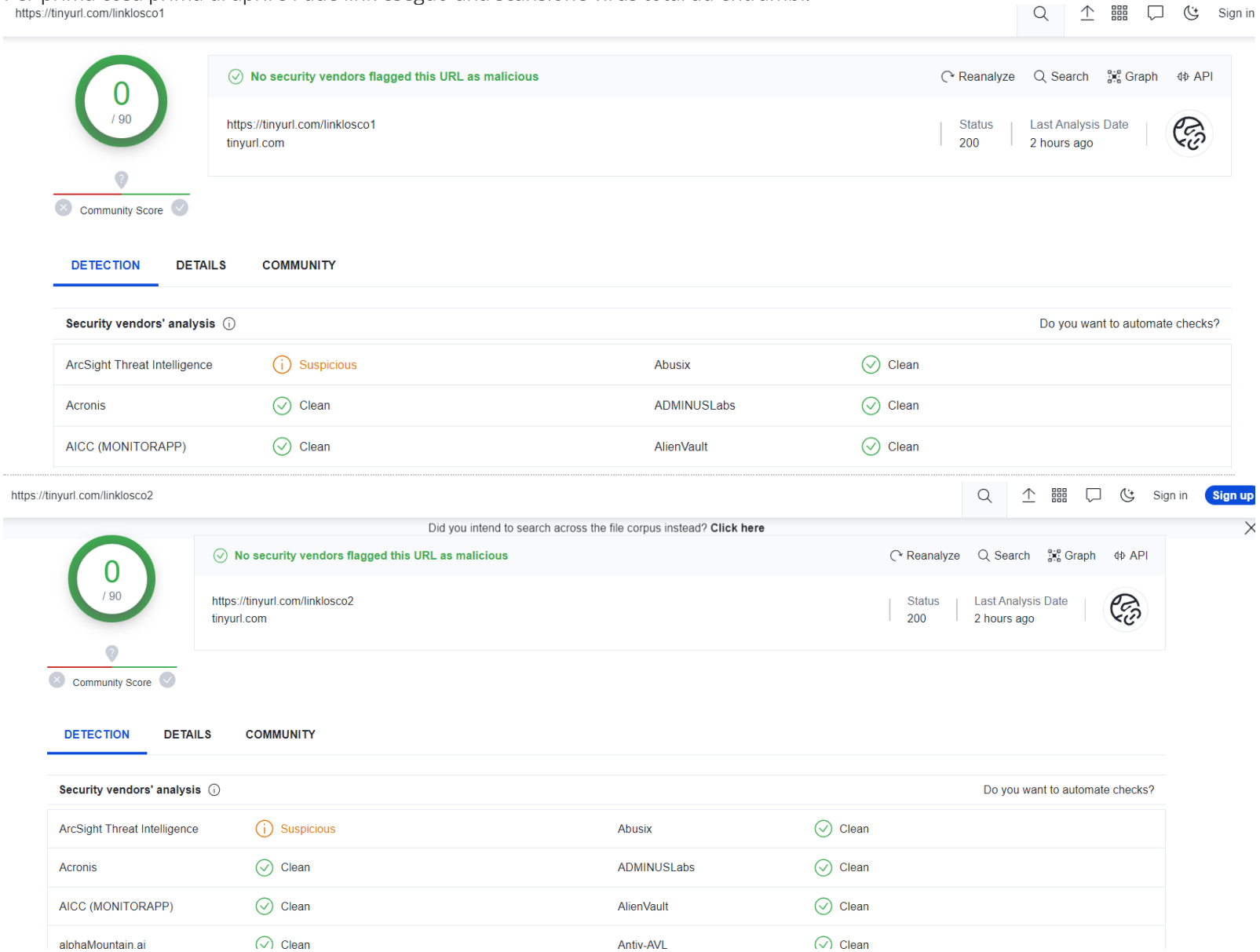


3

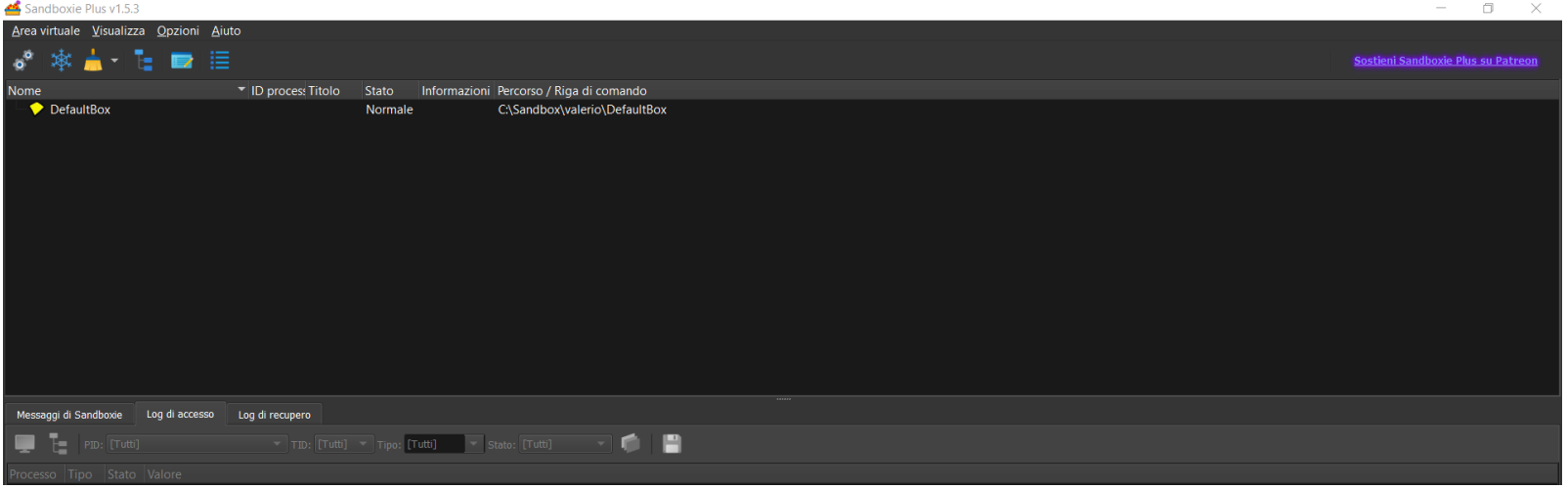
Inoltre l'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma,quindi la rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna. (Punto tre).
E' con ciò mi collego al punto tre richiesto che risolverò successivamente.

2. Analisi attacco:

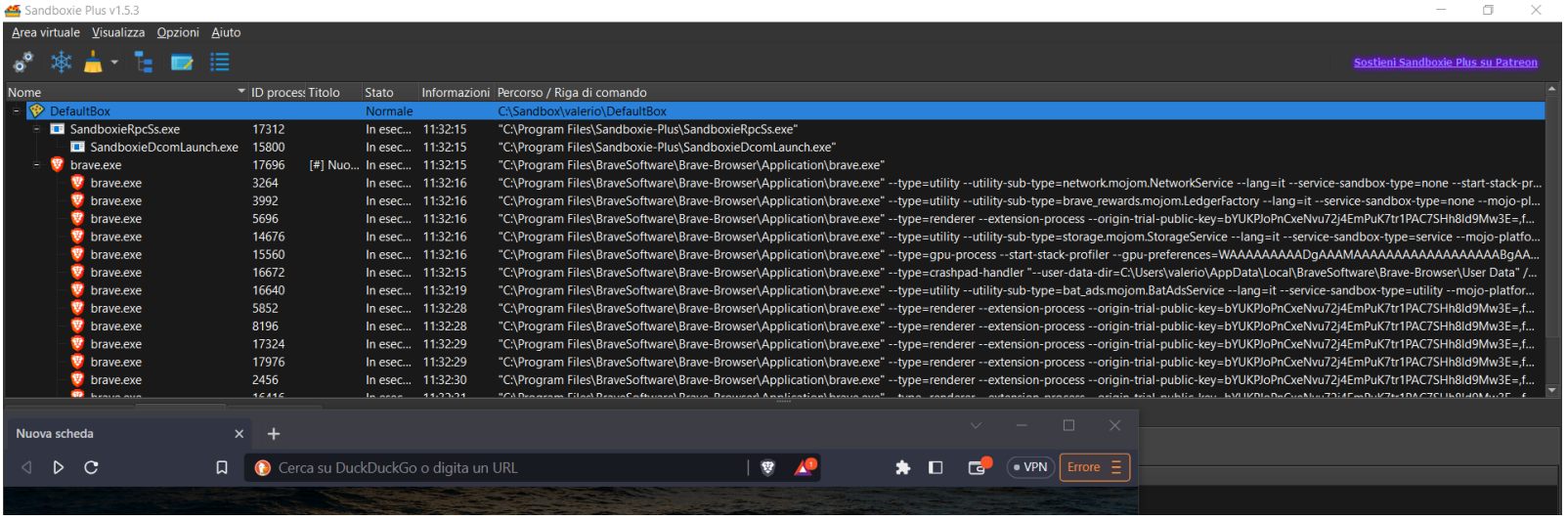
Per prima cosa prima di aprire i due link eseguo una scansione virus total ad entrambi:



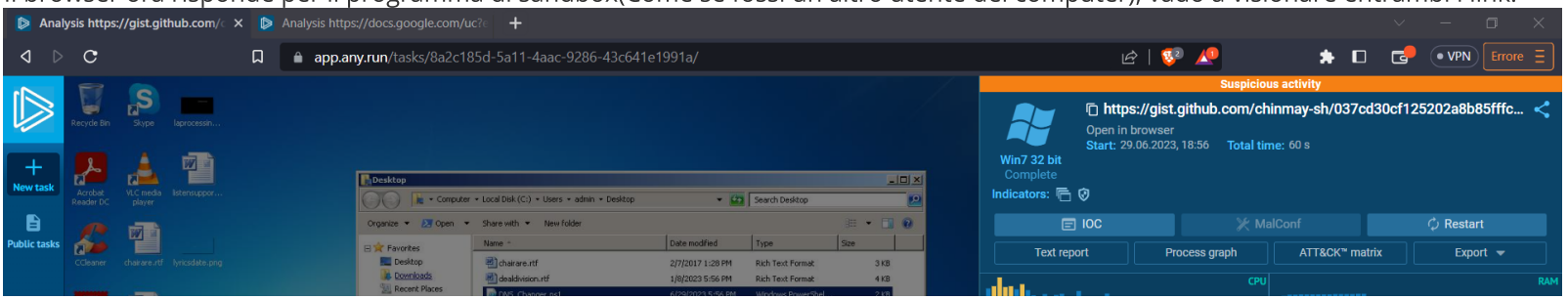
Successivamente utilizzo un programma che ti crea un ambiente protetto di lavoro(Sandbox) chiamato: Sandboxie Plus



Questo programma ti consente di effettuare un emulazione dei programmi in modo completamente sicuro simulando quasi completamente un sistema operativo.
Ma e' sicuro rispetto a virtualbox poichè viene incapsulato solo all'interno del programma e non esce in nessuna ragione, inoltre è molto comodo per vedere le log.
Ora vado ad avviare un browser in modalità sandbox:

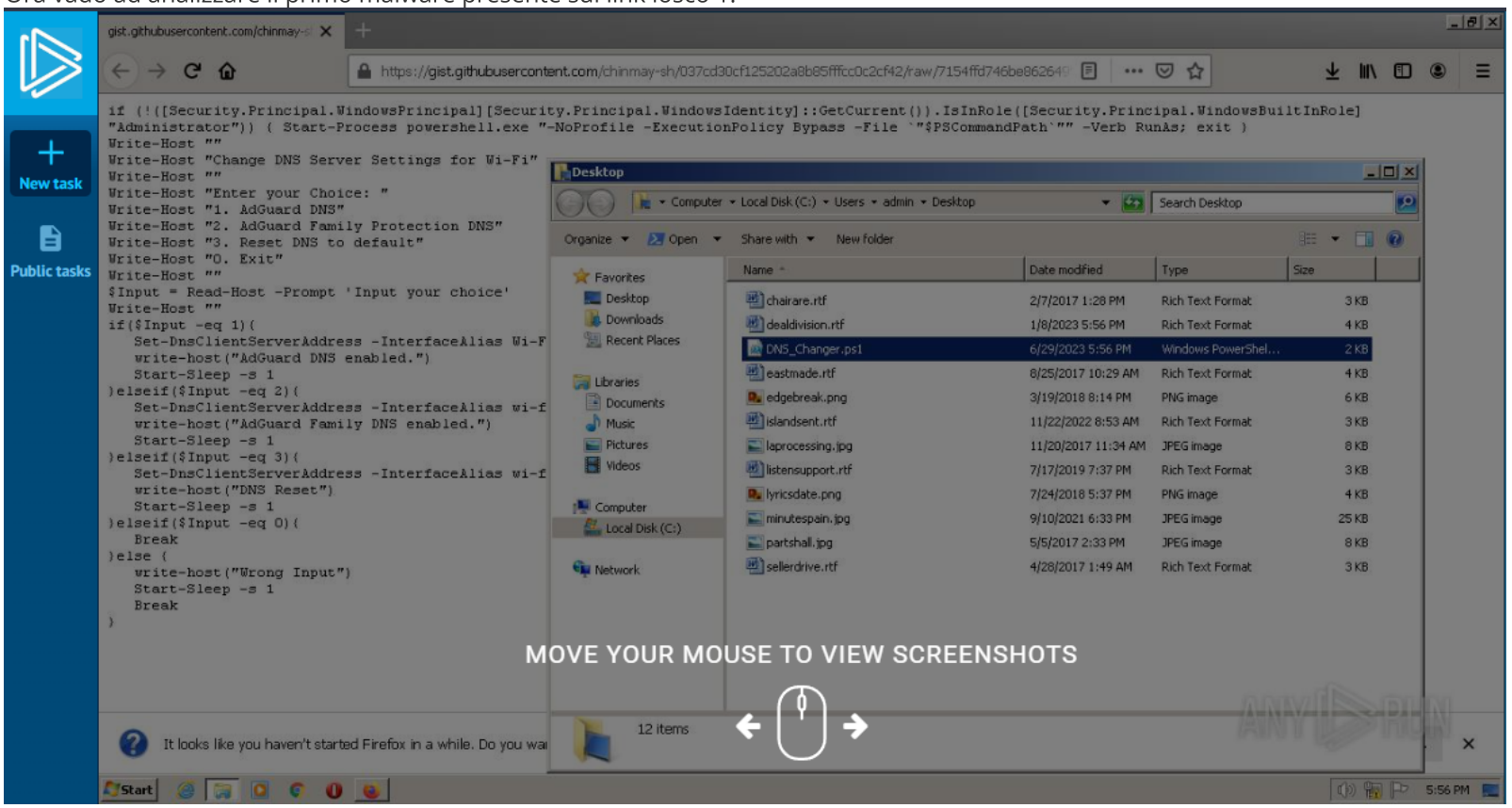


Il browser ora risponde per il programma di sandbox(Come se fossi un altro utente del computer), vado a visionare entrambi i link:



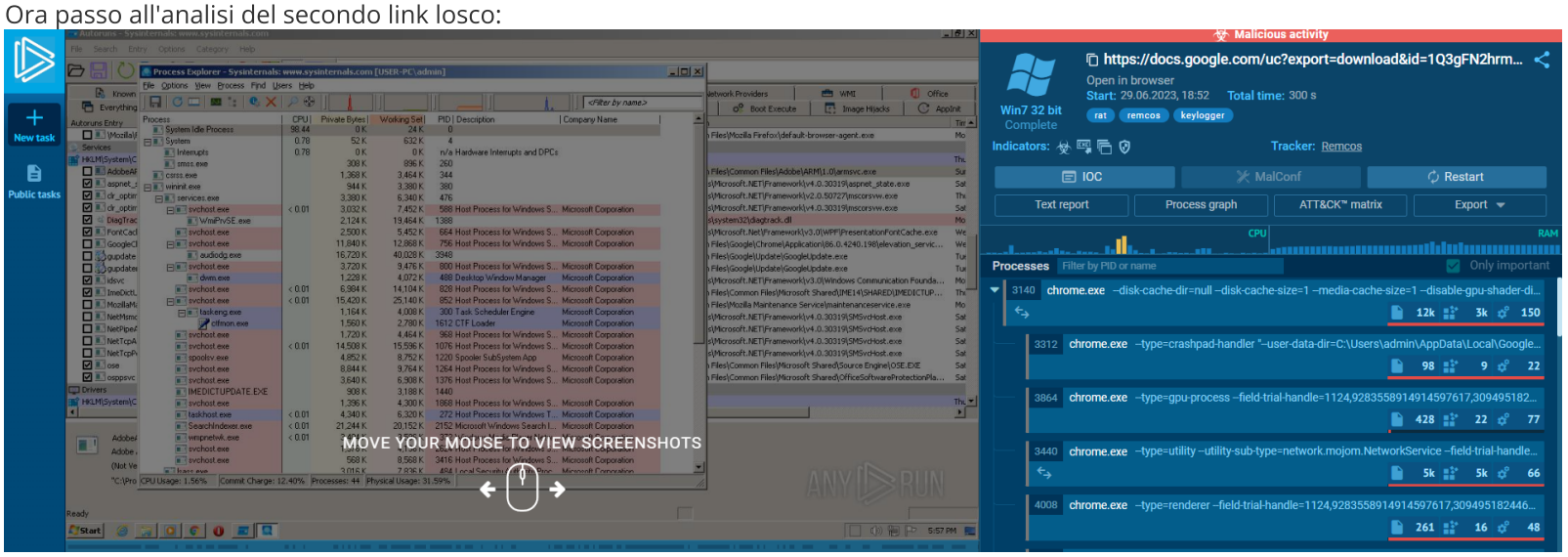
Scopro che sono due link del sito anyruns(Quindi sicuri), ma comunque ho eseguito le scansioni di prima perchè fidarsi è bene ma non fidarsi è meglio.

Ora vado ad analizzare il primo malware presente sul link losco 1:



In questo link possiamo vedere un tentativo sospetto di cambio dei DNS a favore comunque di un servizio anti ADS, quindi abbastanza lecito.
Ma l'azione di cambiare i dns deve essere sempre motivo di preoccupazione, poichè potreste cambiare i dns con server dns malevoli i quali vi reindirizzerebbero o modificherebbero la chiamata verso il sito in questione, magari cambiandogli gli ip.
Quindi catalogo questo tipo di malware "Sospetto" ma non letate, poichè se il servizio AdGuard è lecito e io voglio non vedere le pubblicità e mi fido di loro posso comunque impostare i loro dns, un pò come imposterei quelli di google.
Negli screenshoot viene scaricato un file .ps1 di scripting per Windows Power Shell,che risulta essere il file per modificare i dns .
Ovviamente bisogna comunque controllare il contenuto di ogni file script per Windows Power Shell(.ps1).

Ora passo all'analisi del secondo link losco:



Nel secondo link possiamo notare un attività molto pericolosa di un malware, da quello che ho notato penso sia un dirottamento dns verso domini malevoli integrati nel file hosts(Perchè vedo il coinvolgimento di svchost.exe) che reindirizzano l'utente che prova a scaricare dei file sul google DOCS su siti remoti, dove vengono scaricati dei malware pericolosi.
L'autore del video si prepara bene nell'analisi dei malware scaricando i programmi di SysInternals che servono per vedere meglio i processi e le eseguzioni all'avvio e anche per effettuare l'analisi del malware in modo dinamico.
Come possiamo vedere dopo il dirottamento dei dns(DNS hijacking) da google docs vengono scaricati due file ed eseguiti, come possiamo vedere il malware si posiziona subito per essere eseguito ad ogni avvio, e controlla principalmente il computer in modo totale, spacciandosi per altri programmi leciti all'interno del sistema operativo. Questo tipo di malware potrà essere utilizzato

dall'attaccante come zombie per determinate botnet, oppure semplicemente l'attaccante potrà usarlo come divertimento.

Threats

PID	Process	Class	Message
1076	svchost.exe	Potentially Bad Traffic	ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)
3824	csc.exe	Malware Command and Control Activity Detected	ET JA3 Hash - Remcos 3.x TLS Connection
–	–	A Network Trojan was detected	REMOTE [ANY.RUN] REMCOS JA3 Hash

3. Response:

Considerato che è un emergenza e bisogna essere veloci,si può adottare una strategia basata sull'isolamento della macchina infettata.
Come vediamo nell'immagine la rete locale dopo l'attacco è sicuramente esposta appunto dalla DMZ(Sito Ecommerce). Quindi bisogna isolare la rete interna in modo che non ci siano più leak dei dati.
Lasciando la macchina del webhost direttamente collegata ad internet, raggiungibile dall'attaccante e dagli utenti ma non più connessa alla rete interna, in questo modo isolo l'hacher in modo che non infetti altre macchine. Ecco come ho modificato la rete in base a questa emergenza:
Notate come non ci sia più comunicazione tra l'applicazione Web e la rete interna.

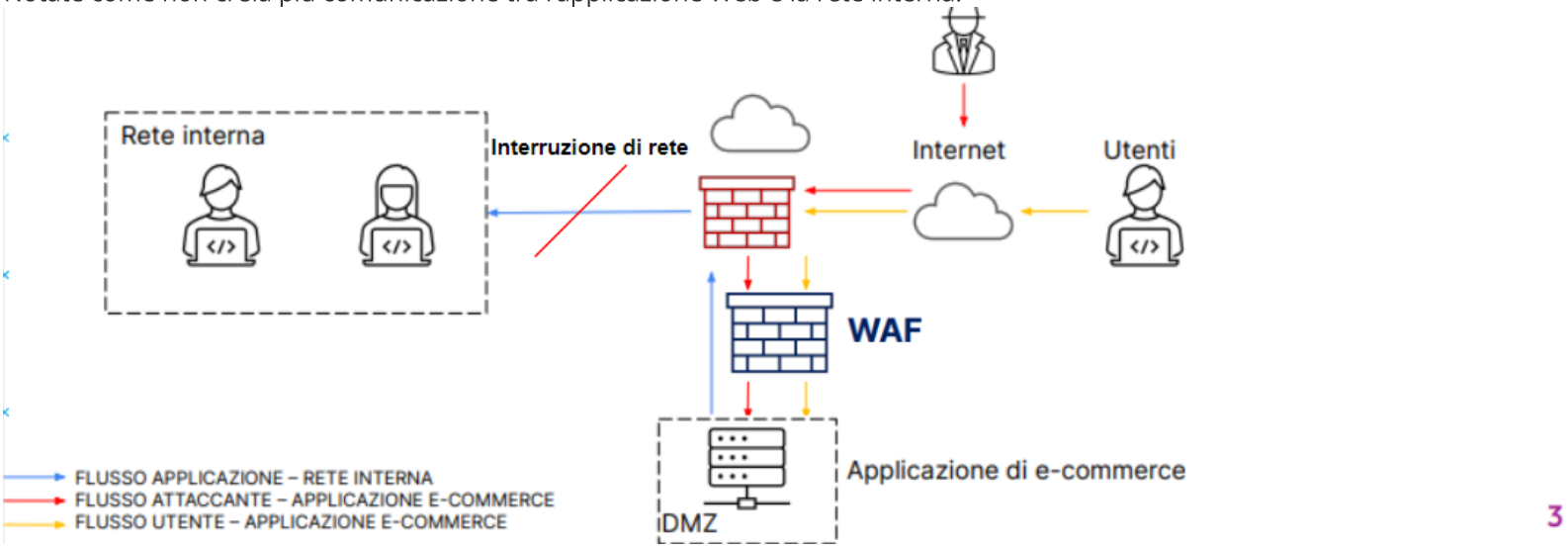
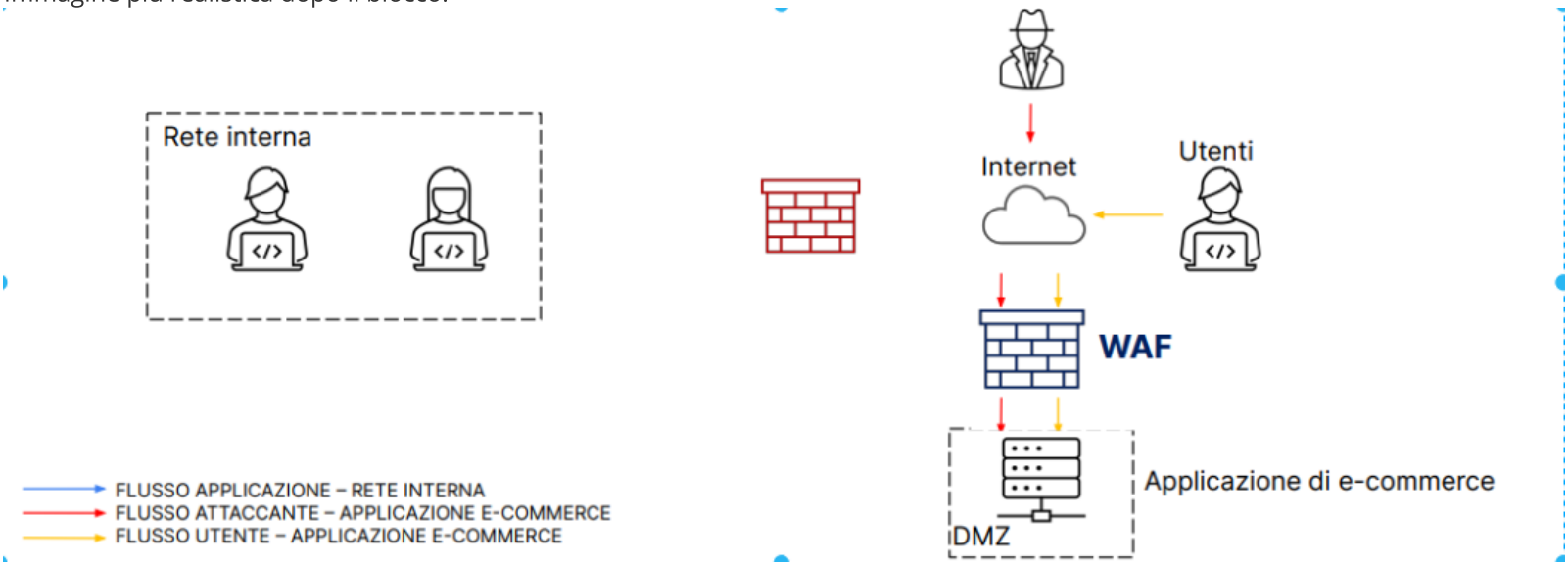
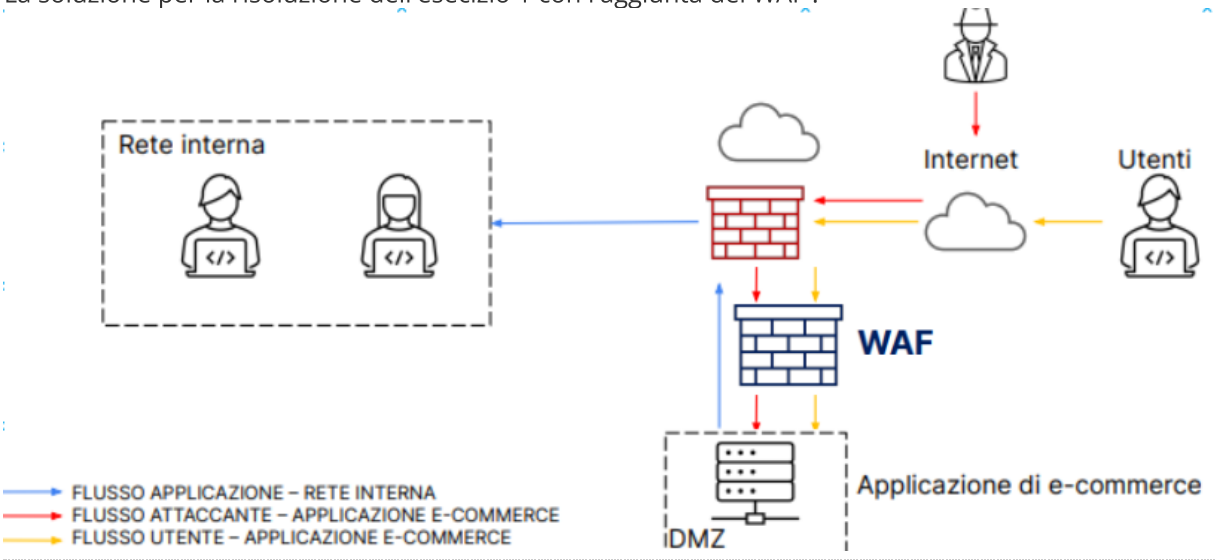


Immagine più realistica dopo il blocco:



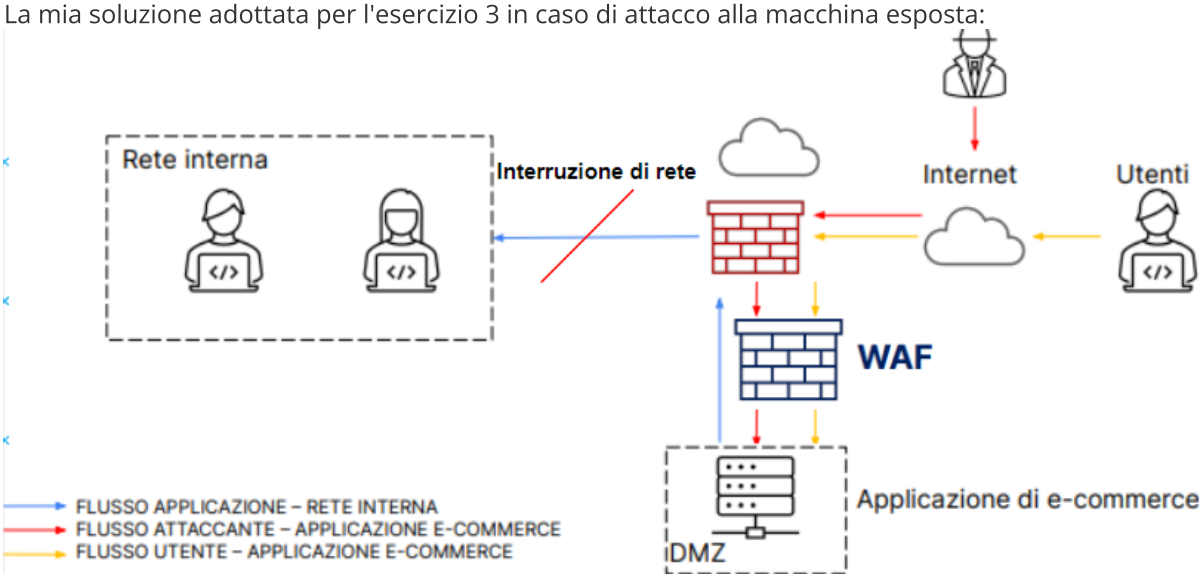
4. Soluzione Completa:

La soluzione per la risoluzione dell'esecizio 1 con l'aggiunta del WAF :



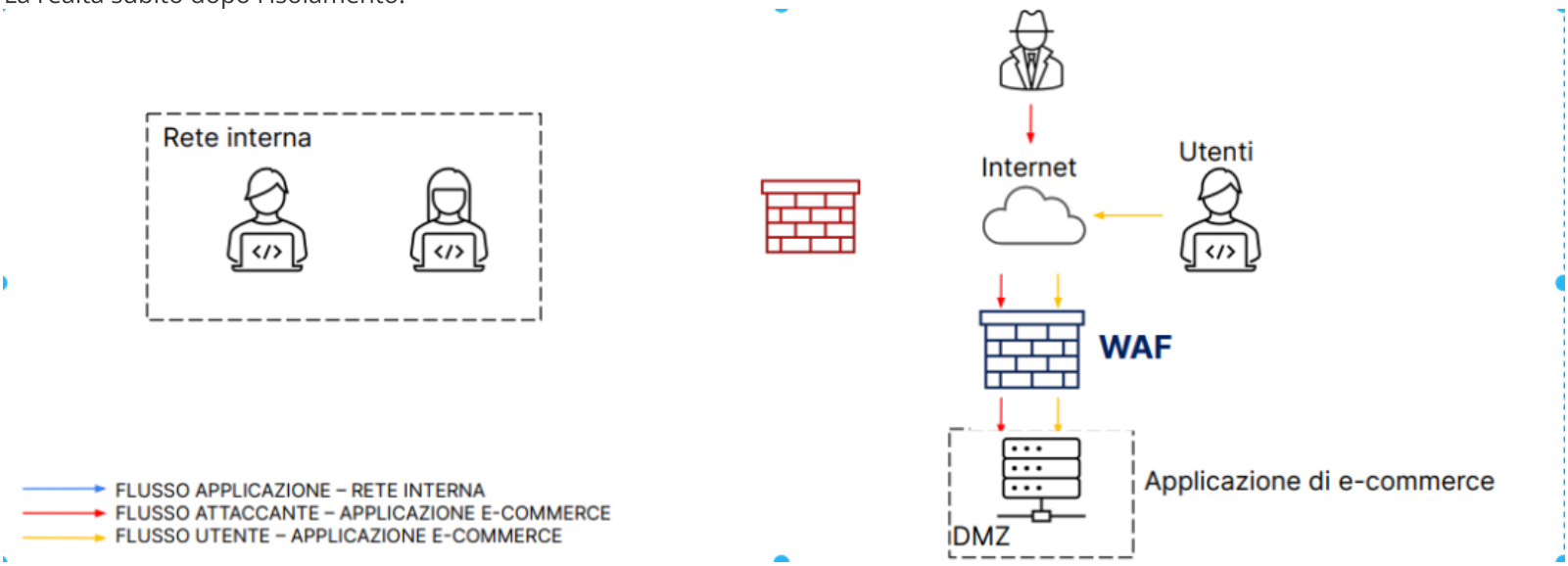
3

La mia soluzione adottata per l'esercizio 3 in caso di attacco alla macchina esposta:



3

La realtà subito dopo l'isolamento:



5. Modifica più aggressiva:

Può essere utile:
1) Aggiungere un IDS o IPS,nel prossimo attacco così sarai preparato.
2)Impostazioni di firewall più severe, in modo che blocchiamo da parte del webserver su ids l'accesso a determinate porte in locale.
3)Una segmentazione di reti potrebbe aiutare in questo caso poichè divide la rete in più sottoreti perchè isola i segmenti critici o sensibili da quelli pubblici o meno sicuri, impedendo così l'accesso non autorizzato ai dati sensibili.
4)Aggiornamenti dei vari sistemi operativi sia locali che del webserver.

5)Utilizzo di un server remoto blindato per l'accesso alla macchina che gestisce le connessioni dell'e-commerce, in questo modo con due server remoti sarà più facile configurare il firewall per entrambi e in caso di attacco, l'attaccante verrà reindirizzato in un server remoto blindato e sarà più facile gestire l'attacco in corso da li. Per blindato si intende una configurazione firewall o di iptables che consente l'accesso a determinate porte soltanto ad un determinato indirizzo ip.
6)Utilizzo di un honeypot per ingannare l'hacker.
7) Non utilizzare le password di default.
8)Monitoraggio delle reti costante da parte di persone qualificate.
9)Utilizzo della crittografia in ogni server/porta.

Compito di Mendolia Valerio