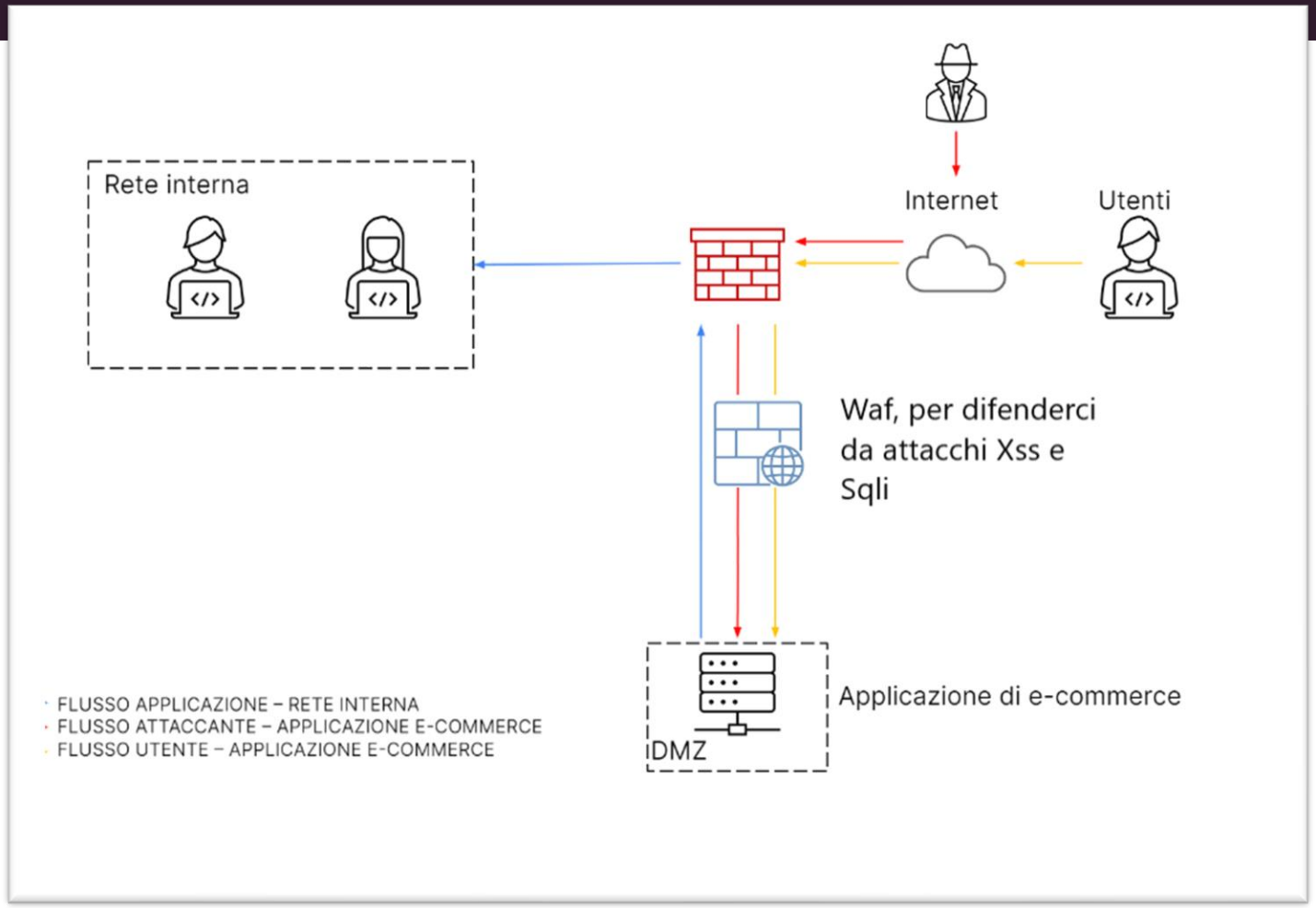
Progetto Epicode 30.06

Scopo principale del progetto: Data una rete già predisposta precedentemente, renderla sicura da certi tipi di attacchi e proporre soluzioni di response.

Punto 1: Protezione da Xss e Sqli

-I WAF (web application firewall) proteggono dagli attacchi a livello 7 del modello OSI, che è il livello applicativo. Questo include attacchi contro applicazioni come Ajax, ActiveX e JavaScript, nonché la manipolazione di cookie, l'iniezione SQL e gli attacchi URL.

-Un altro modo per controllare l'input utente è utilizzare un Html sanitizer, una parte di codice che controlla l'input inserito e verifichi che non sia codice malevolo.



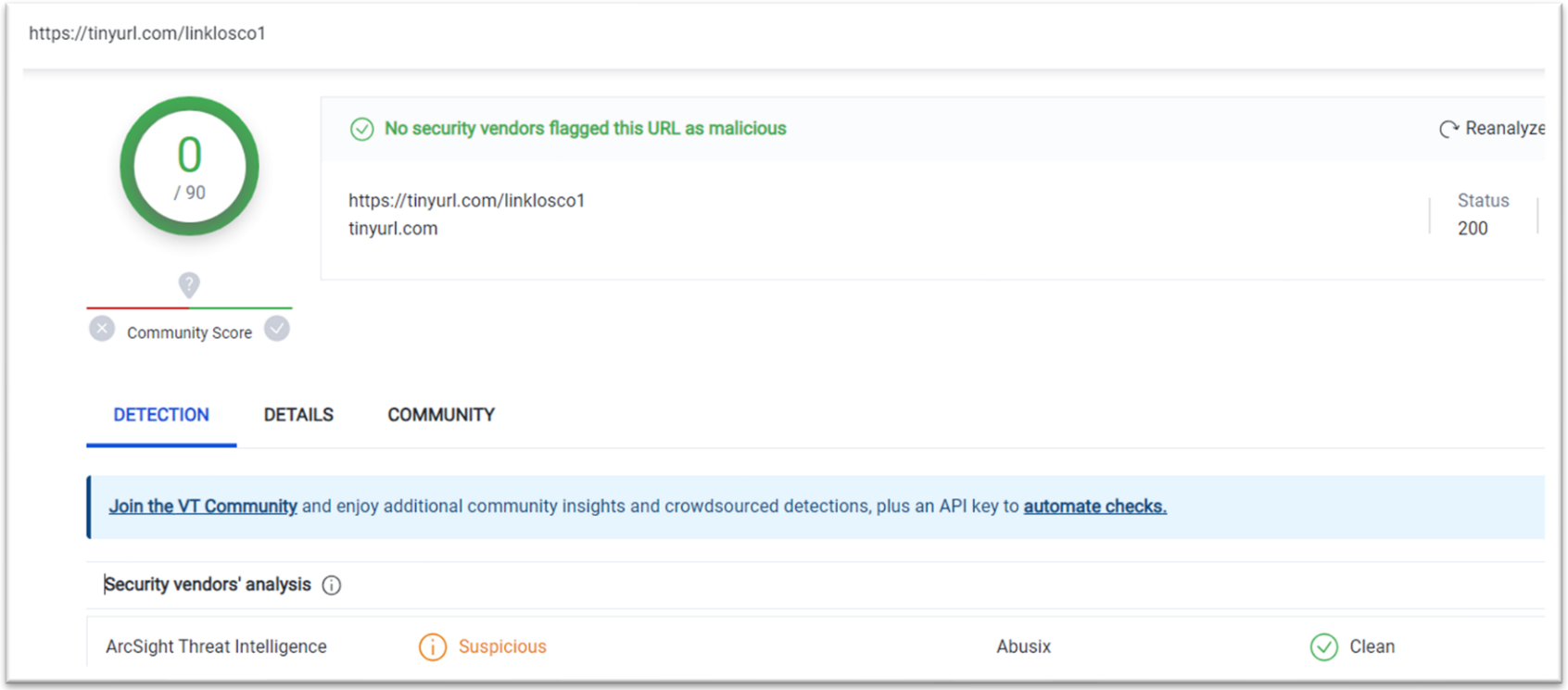
Metodi secondari per la sicurezza su Xss e Sqli

-Anche aumentare la sicurezza dei cookie può essere una soluzione agli attacchi Xss, per esempio uno degli attacchi più frequenti è quello di rubare il cookie di sessione di un utente per poi impersonarlo sulla pagina, la soluzione è attribuire il cookie e legarlo al Ip di un determinato utente, così che solo lui possa utilizzare quel cookie di sessione, perciò se un attaccante riuscisse a prenderlo non sarebbe in grado di usarlo con il suo ip.

-Soluzione più aggressiva invece per prevenire un attacco di questo tipo è quella di disabilitare gli script sulla pagina così da non permettere l'esecuzione di un codice

Task 2 , analisi dei link sottoposti

Per prima cosa analizzando entrambi i link su virus total vediamo solamente che sono degli url accorciati, il tool utilizzato li segnala come sospetti.



https://tinyurl.com/linklosco1

https://tinyurl.com/linklosco2

Anche il secondo link appunto è un link accorciato che porta a anyrun.

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

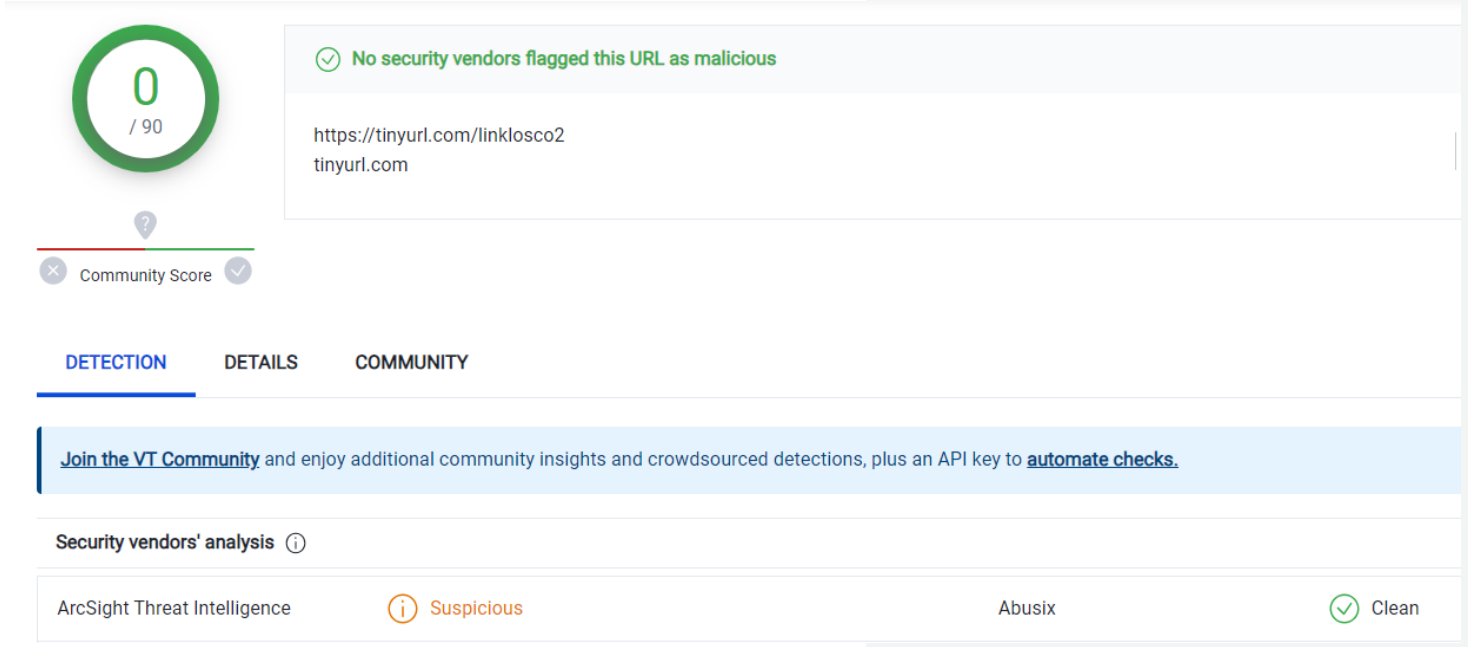
HTTP Response

Final URL

https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a/

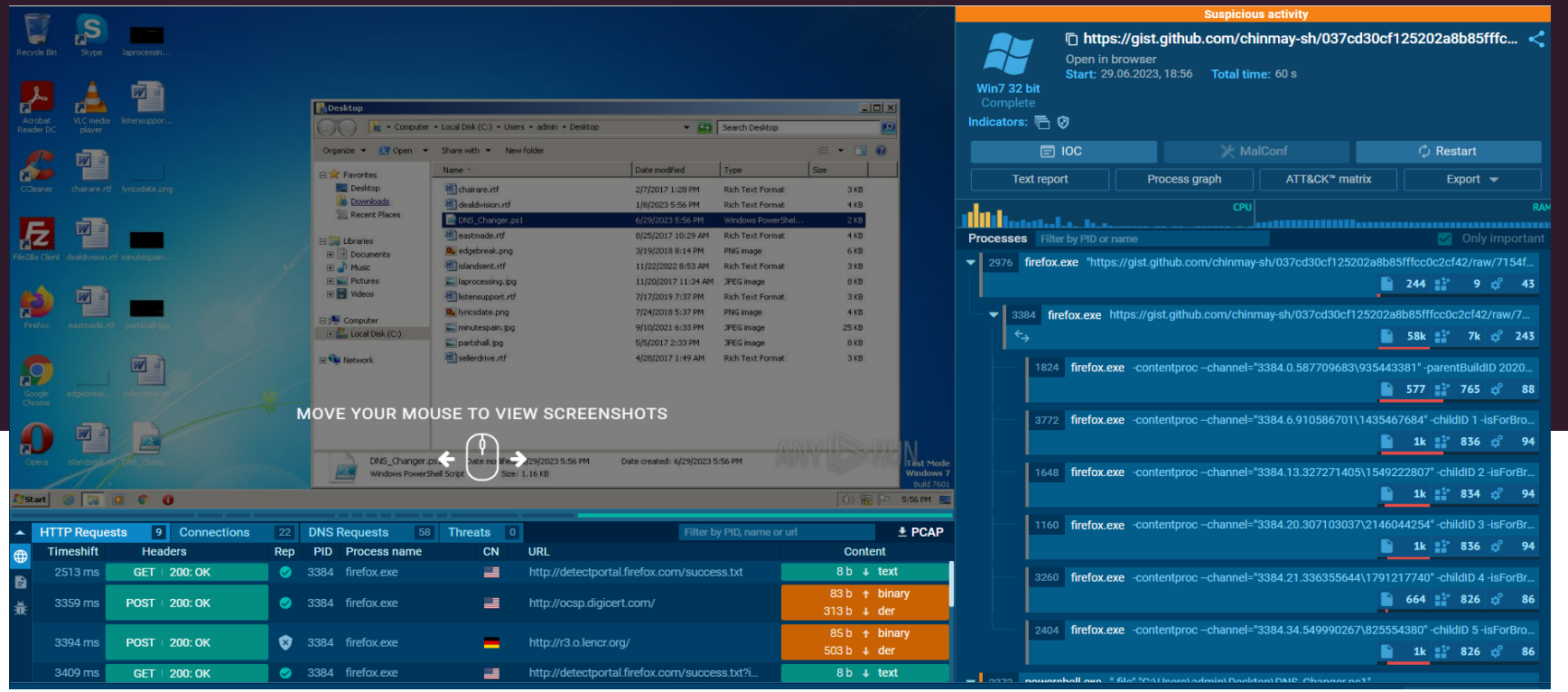
Serving IP Address

172.67.1.225



Link 1

Il virus visualizzato tramite il primo link, apre una shell in automatico sulla macchina target, e senza avere i permessi riesce ad aprire e visualizzare/modificare il un file DNS sulla macchina vittima.



MALICIOUS

Bypass execution policy to execute commands
- powershell.exe (PID: 3300)

SUSPICIOUS

The process executes Powershell scripts
- powershell.exe (PID: 2272)

The process bypasses the loading of PowerShell profile settings
- powershell.exe (PID: 2272)

Reads the Internet Settings
- powershell.exe (PID: 2272)
- powershell.exe (PID: 3300)

Application launched itself
- powershell.exe (PID: 2272)

Using PowerShell to operate with local accounts
- powershell.exe (PID: 3300)

Starts POWERSHELL.EXE for commands execution
- powershell.exe (PID: 2272)

INFO

Application launched itself
- firefox.exe (PID: 2976)
- firefox.exe (PID: 3384)

The process uses the downloaded file
- powershell.exe (PID: 2272)
- firefox.exe (PID: 3384)

Manual execution by a user
- powershell.exe (PID: 2272)

Questo può anche portare a:

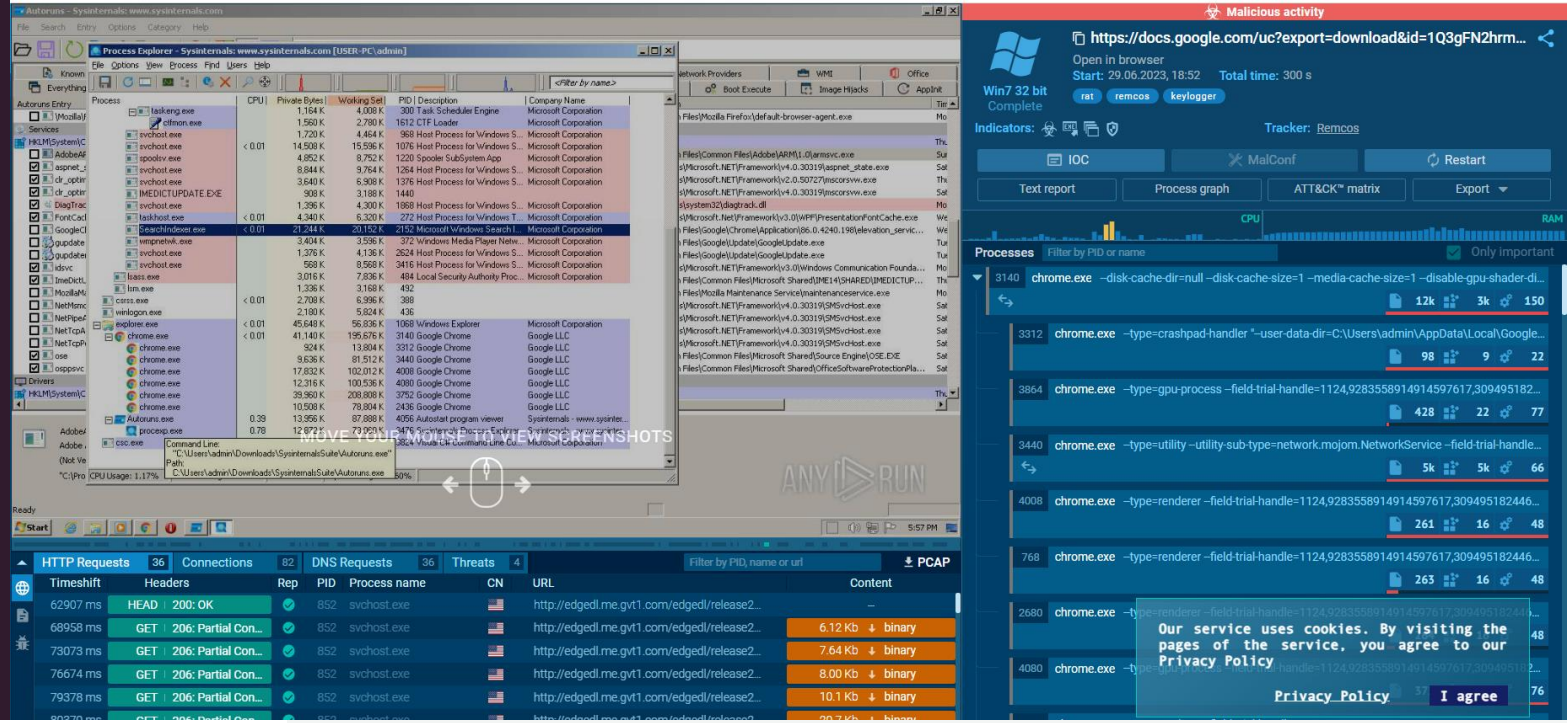
1.Reindirizzamento del traffico: modificando il DNS, il virus potrebbe reindirizzare il traffico di rete della macchina infetta verso server controllati dall'attaccante. Ciò potrebbe portare l'utente a siti web contraffatti, contenenti malware o progettati per raccogliere informazioni personali e di accesso.

2.Spoofing del DNS: il virus potrebbe sostituire i server DNS legittimi con server DNS falsi controllati dall'attaccante. In questo modo, l'attaccante può intercettare le richieste DNS e fornire risposte manipolate. Ad esempio, potrebbe indirizzare l'utente a siti web falsi che somigliano a quelli legittimi per rubare informazioni di accesso o installare malware.

3.Denial of Service (DoS): il virus potrebbe modificare il DNS in modo che la macchina infetta non riesca a raggiungere i server DNS corretti, impedendo l'accesso a Internet o a servizi specifici che dipendono dalla risoluzione DNS.

4.Controllo remoto: una volta che il virus ha modificato il DNS, l'attaccante potrebbe essere in grado di controllare la macchina infetta da remoto. Possono eseguire comandi, rubare dati o installare ulteriori malware.

Link 2



Il secondo invece riguarda un Remcos Rat, un programma più pericoloso.

Remcos o Remote Control and Surveillance, commercializzato come un software legittimo dalla società con sede in Germania Breaking Security per gestire in remoto i sistemi Windows, è ora ampiamente utilizzato in numerose campagne malevoli da parte di attori minacciosi. Remcos è un sofisticato Trojan di accesso remoto (RAT) che può essere utilizzato per controllare e monitorare completamente qualsiasi computer Windows da XP in poi.

MALICIOUS

Application was dropped or rewritten from another process
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Starts Visual C# compiler
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Uses Task Scheduler to run other applications
- cmd.exe (PID: 3604)
- cmd.exe (PID: 3200)
- cmd.exe (PID: 2628)
- cmd.exe (PID: 2960)

Remcos is detected
- csc.exe (PID: 3824)

REMCOS detected by memory dumps
- csc.exe (PID: 3824)

SUSPICIOUS

The process creates files with name similar to system file names
- WinRAR.exe (PID: 1944)

Drops a system driver (possible attempt to evade defenses)
- WinRAR.exe (PID: 1944)
- procexp.exe (PID: 3476)

Reads settings of System Certificates
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads security settings of Internet Explorer
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads the Internet Settings
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

Connects to unusual port
- csc.exe (PID: 3824)

INFO

The process uses the downloaded file
- chrome.exe (PID: 2064)
- chrome.exe (PID: 2356)
- chrome.exe (PID: 1140)
- WinRAR.exe (PID: 1944)
- chrome.exe (PID: 3868)
- WinRAR.exe (PID: 3092)
- chrome.exe (PID: 2880)

Application launched itself
- chrome.exe (PID: 3140)

Manual execution by a user
- WinRAR.exe (PID: 1944)
- Autoruns.exe (PID: 4056)
- WinRAR.exe (PID: 3092)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Altre funzionalità del Rat

1.Controllo remoto: permette all'attaccante di controllare il computer infetto da remoto. Possono eseguire comandi, accedere ai file, monitorare le attività dell'utente, registrare la tastiera e la webcam, e persino rubare informazioni sensibili.

2.Persistenza: Remcos RAT ha la capacità di mantenere la sua presenza nel sistema infetto, in modo da poter essere riattivato in futuro anche dopo un riavvio del computer.

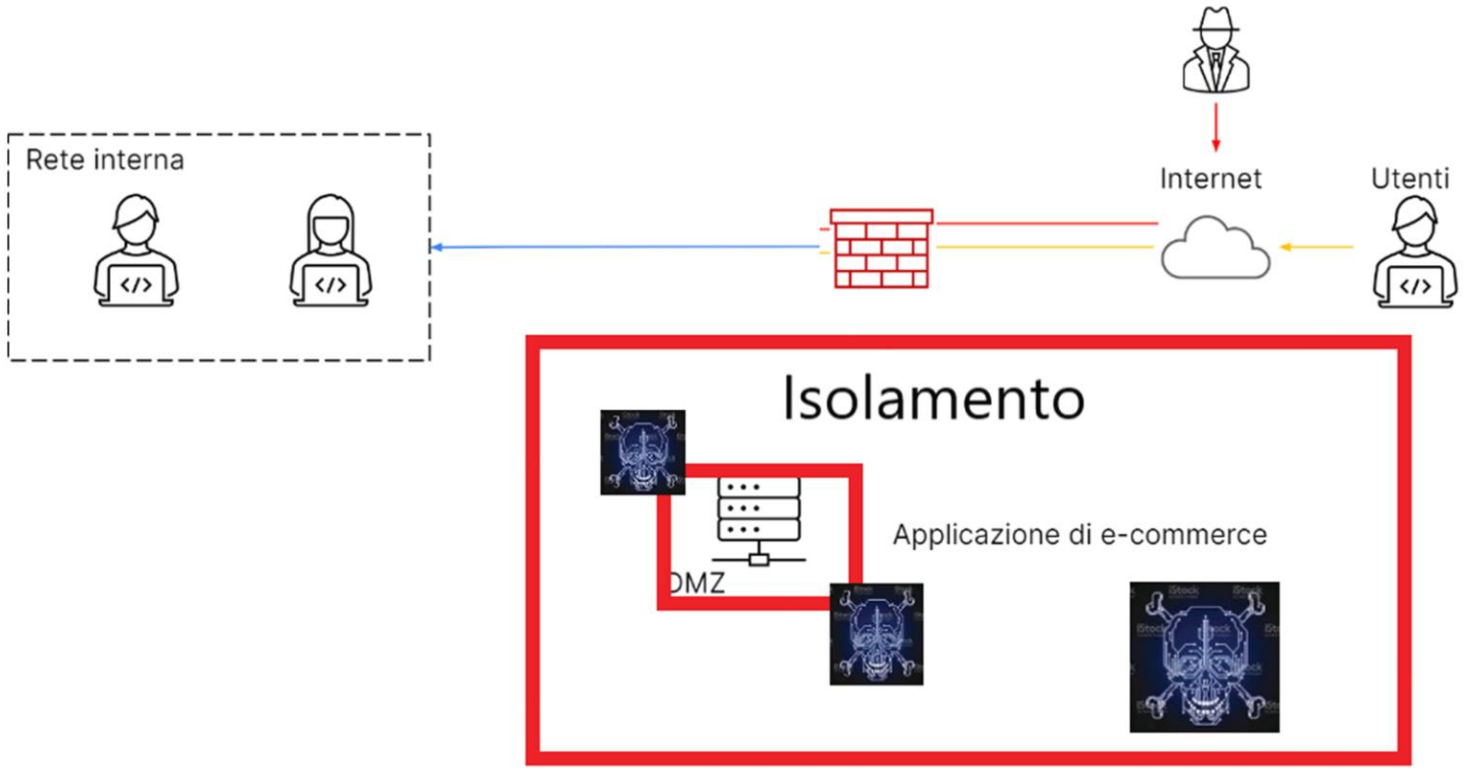
3.Keylogging: Remcos RAT può registrare tutte le pressioni di tasti effettuate dall'utente, consentendo all'attaccante di acquisire password, informazioni di accesso e altre informazioni sensibili.

4.File Manager: consente all'attaccante di accedere, copiare, modificare o eliminare i file sul computer infetto.

5.Webcam e microfono: Remcos RAT può attivare la webcam e il microfono del computer infetto senza che l'utente ne sia consapevole, consentendo all'attaccante di monitorare l'ambiente circostante o di registrare audio e video senza autorizzazione.

6.Distribuzione: Remcos RAT può essere distribuito attraverso diverse tecniche, come allegati di email malevoli, exploit di sicurezza, download da siti web compromessi o tramite altri malware.

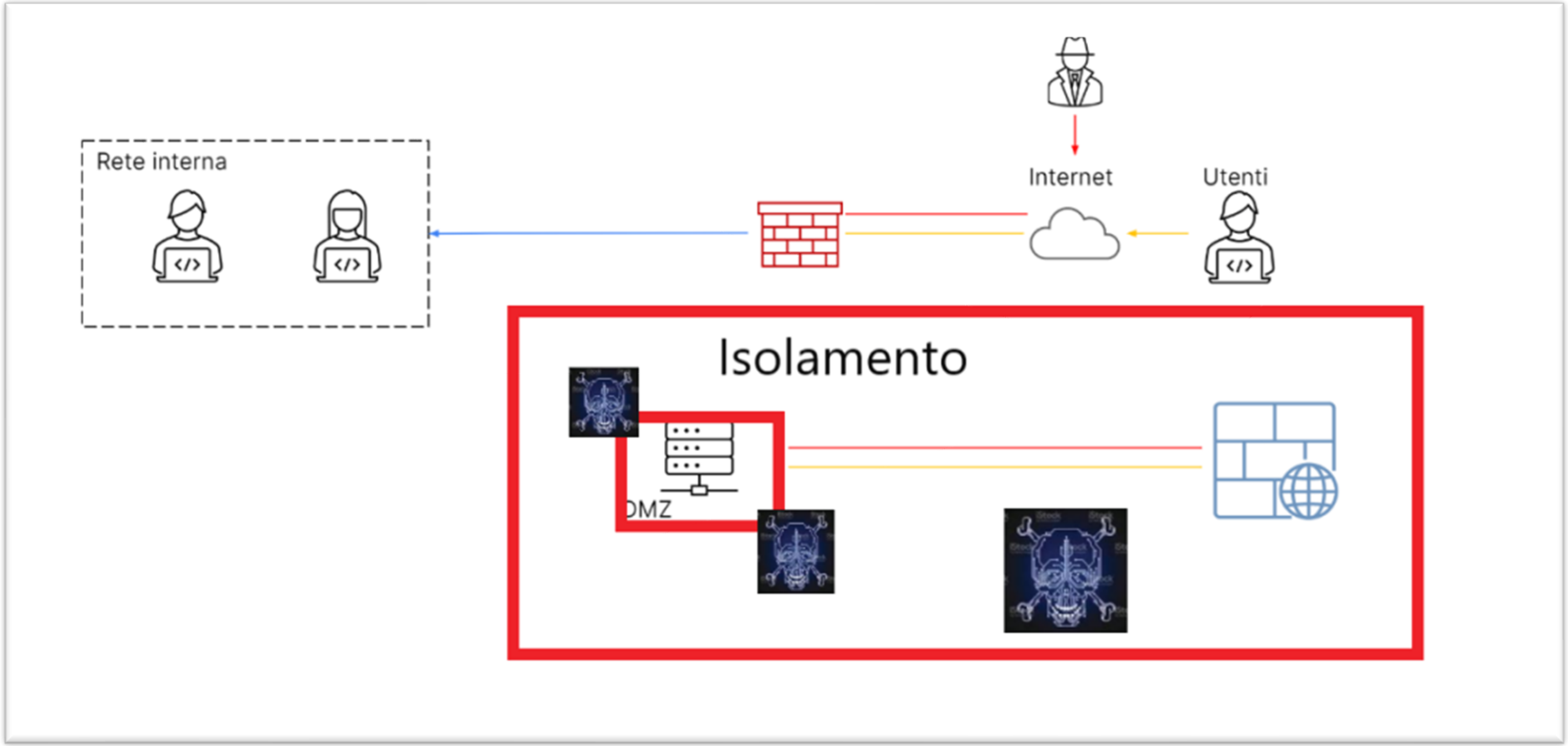
Nella terza parte dell'esercizio, un attaccante si è riuscito ad infiltrare nella rete, e dobbiamo isolarlo..



In questo modo possiamo isolare l'attaccante dal resto del sistema per impedirgli di accedere alla nostra rete interna

Esercizio 4, Soluzione completa

Unione delle soluzioni 1 e 3



Esercizio 5, Upgrade della Rete