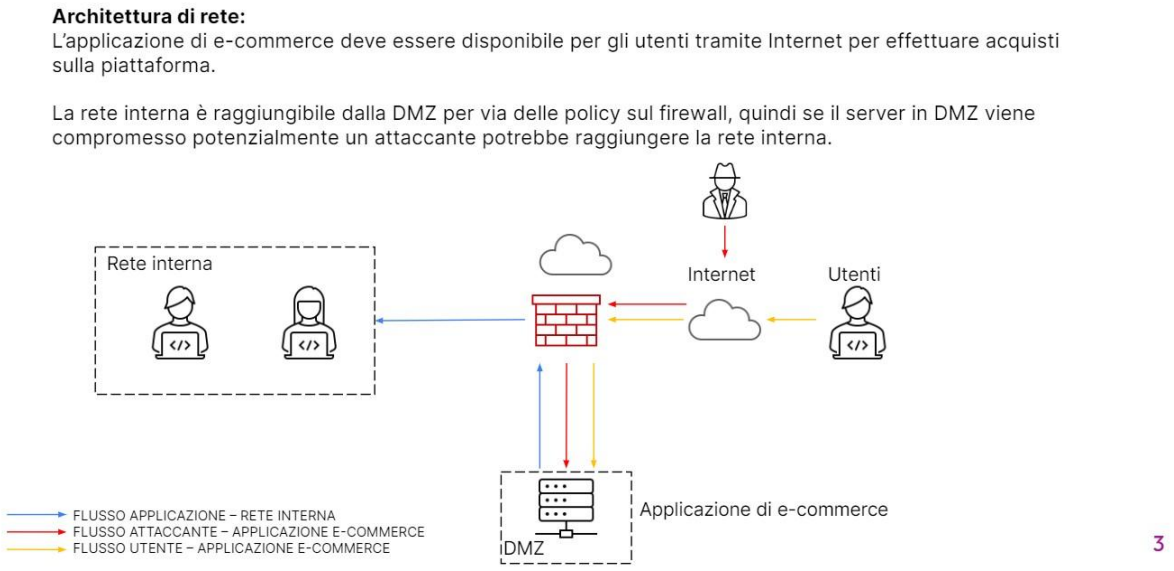
Rossella Amore
30/06/2023

Report - Incident Response

Nella traccia di oggi si chiede di risolvere ed effettuare azioni in un contesto di incidente di sicurezza.

In basso è riportata l'immagine originale dello stato iniziale dell'architettura di rete aziendale. Dallo schema si può intuire che il DMZ, accessibile sia da internet che da rete interna, possa diventare un ponte di passaggio per qualunque malintenzionato che riesca a trovare e sfruttare una sua vulnerabilità.
Non solo, un hacker potrebbe compromettere l'applicazione web per causare un disservizio o per ricavare dati sensibili.

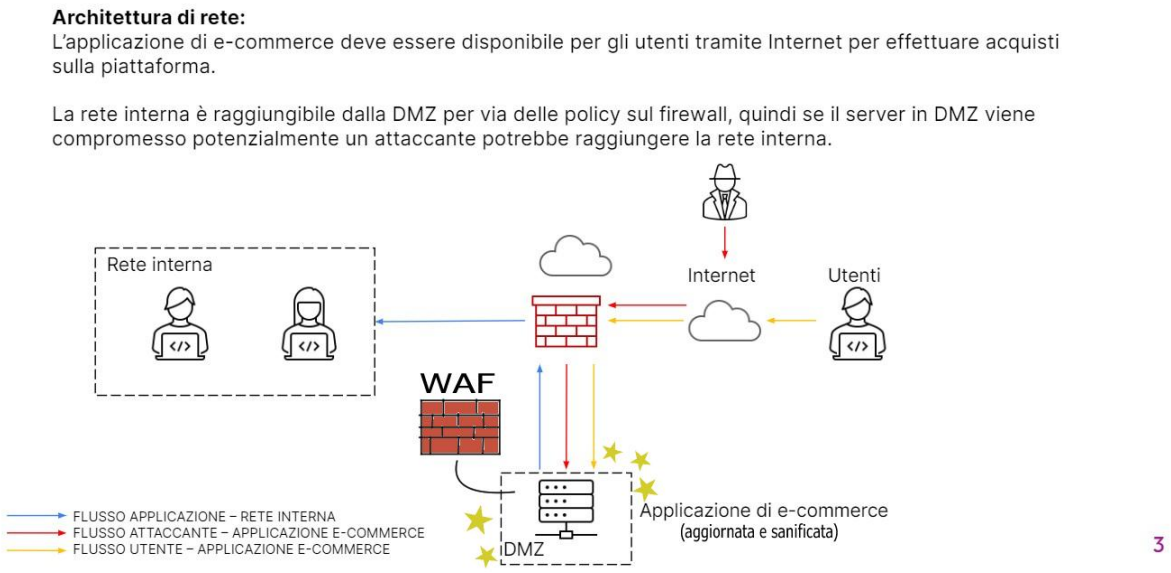


Una possibile vulnerabilità dell'applicazione web e-commerce potrebbe essere l'SQLi oppure un XSS stored o riflesso, che causerebbe un danno alla *riservatezza* dei dati e all'integrità del sito e degli account utenti.
Come possibili soluzioni abbiamo:

- aggiornamento del server con una configurazione ottimale e sanificata dell'input utente;

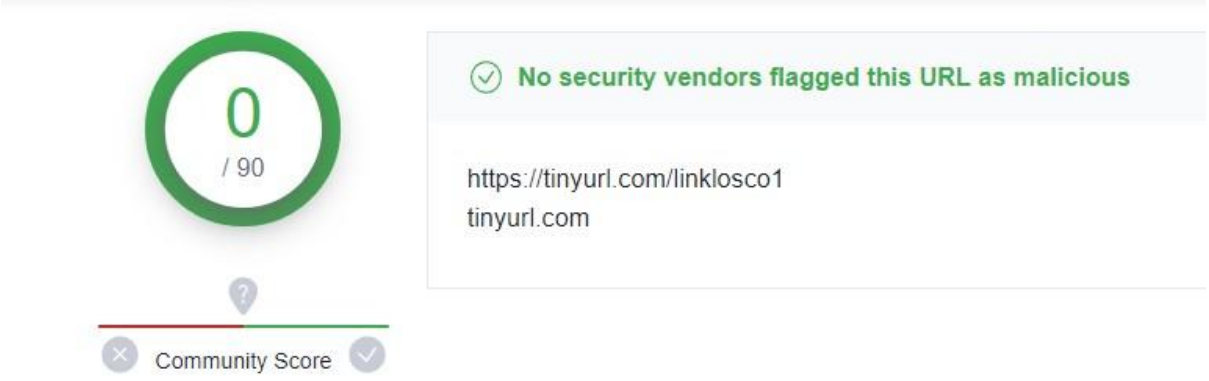
- per ulteriore sicurezza, usare un WAF.

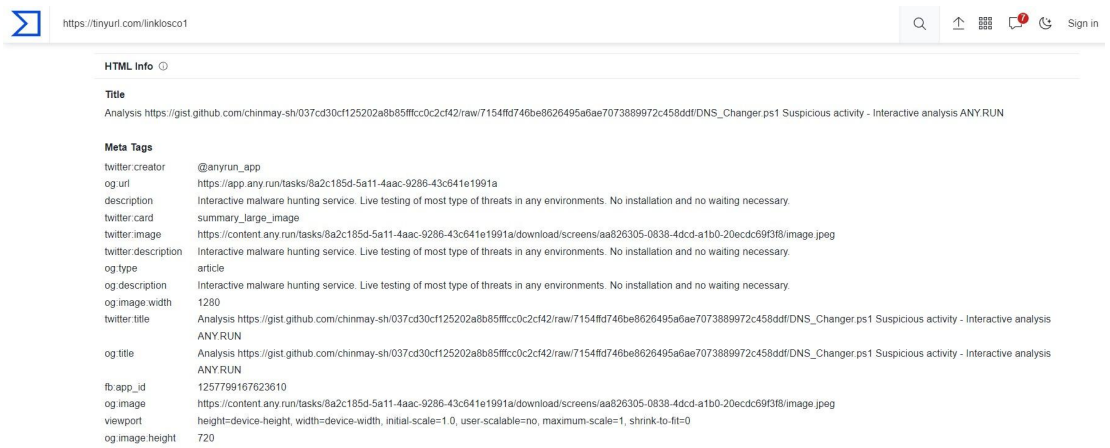
Qui in basso è mostrata l'immagine dell'architettura di rete con DMZ aggiornato e con WAF.



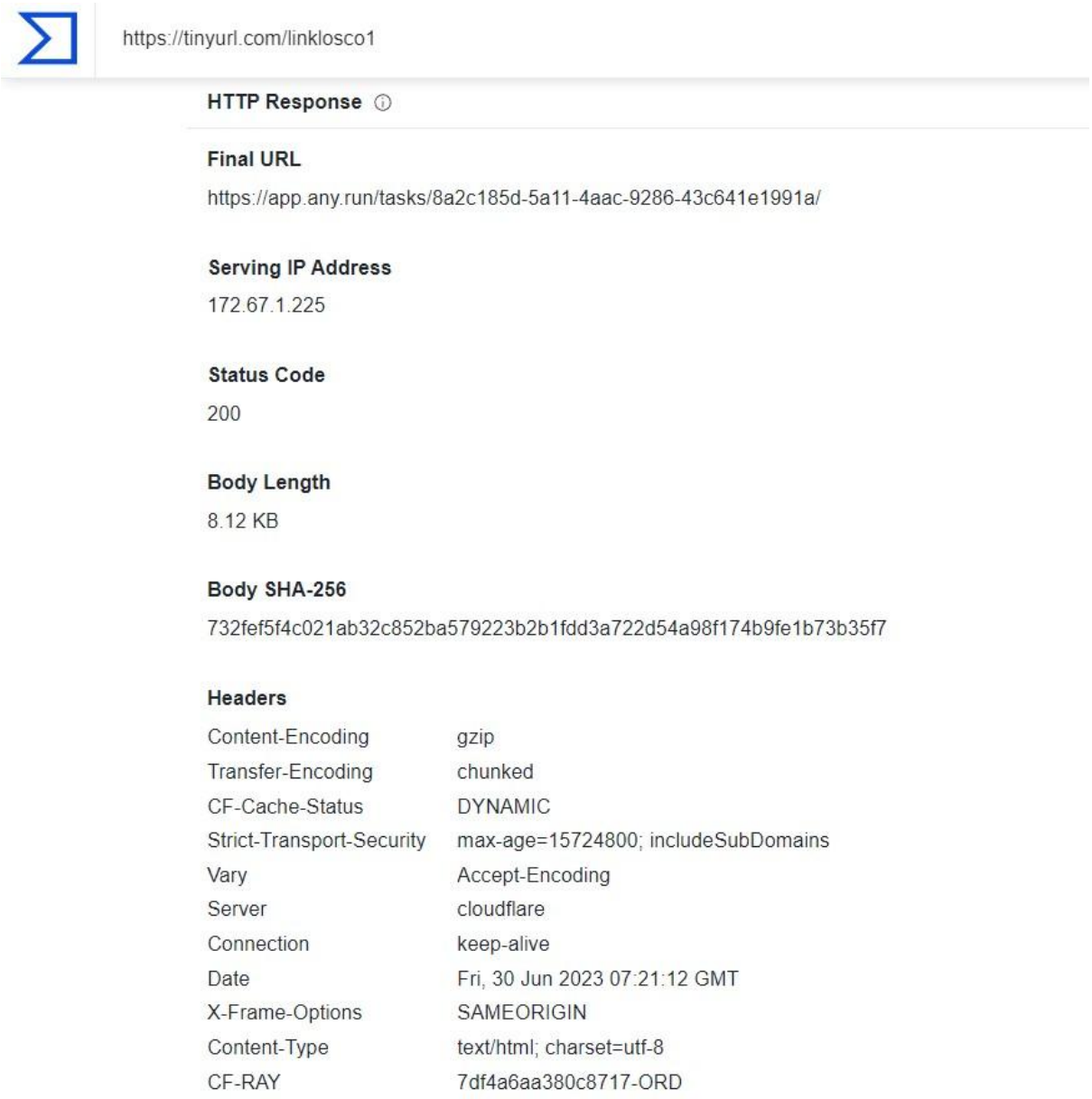
URL Analysis

Andiamo adesso ad analizzare due shortlink molto loschi e sospetti che ci sono stati inviati.
Per stare sicuri, utilizzo un'applicazione web per constatarne l'effettiva sicurezza prima di andarli ad aprire, onde evitare l'esecuzione di un programma malevolo. Partiamo con il primo link.

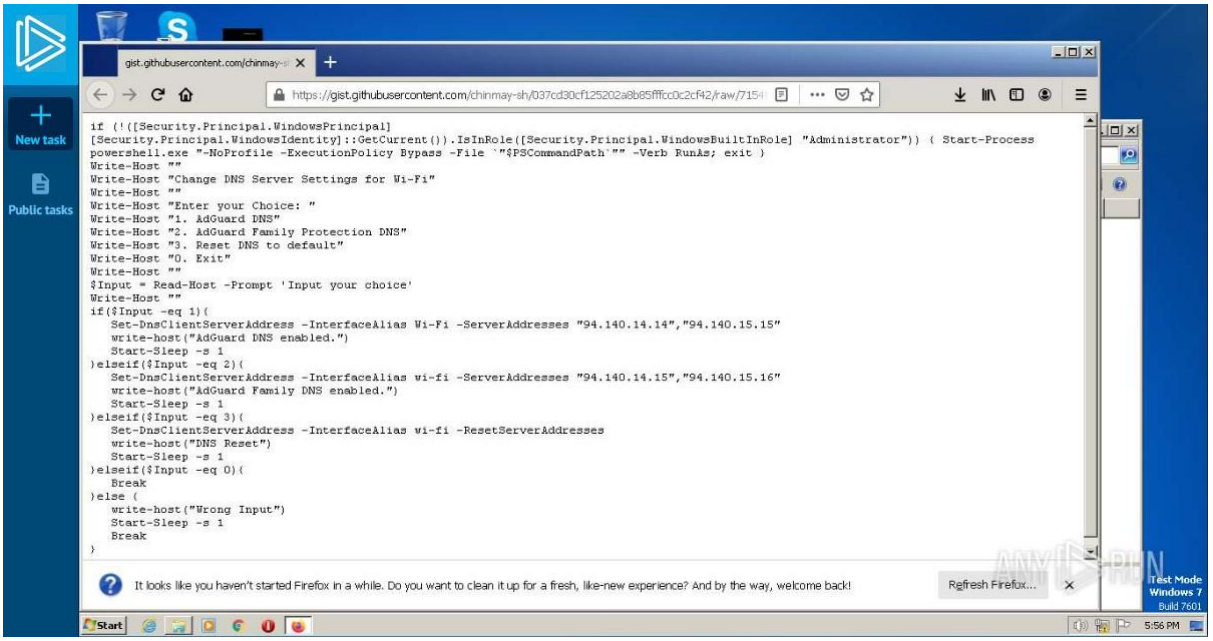




Questa prima analisi è stata eseguita con l'applicazione Web "VirusTotal", la quale mi ha restituito una dettagliata descrizione del contenuto del redirect, inclusa la risposta HTTP.
Il sito ci dice che il redirect non è malevolo e che rimanda al sito AnyRun, una famosa sandbox online per malware.



Abbastanza certi che il link possa essere aperto senza pericoli, procediamo a cliccarci sopra. Da previsione, il link apre una pagina AnyRun dove viene analizzato un'URL sospetta. Con ulteriore osservazione, scopriamo che è uno script scaricabile ed eseguibile per Powershell. E' ritenuto sospetto perché il codice, una volta scaricato, è eseguibile con permessi amministrativi di default, il che potrebbe comportare dei gravi danni qualora lo script fosse malevolo.



Behavior activities

Add for printing

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)

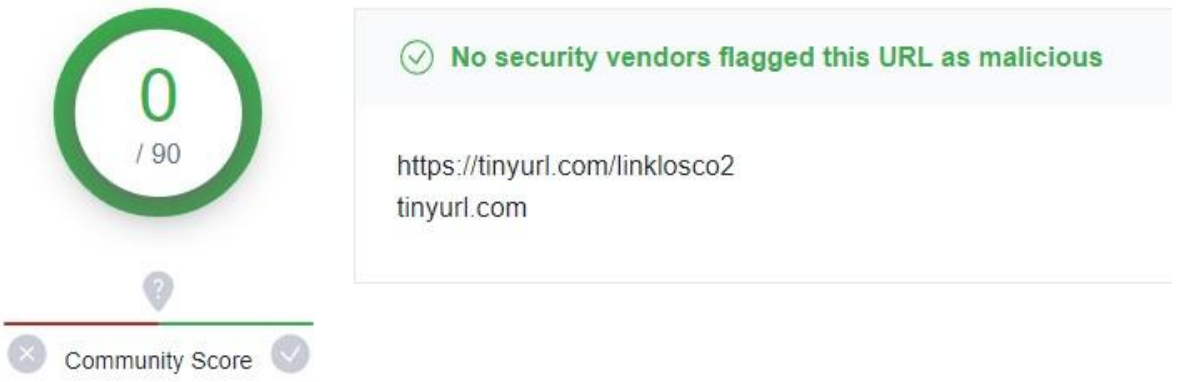
INFO

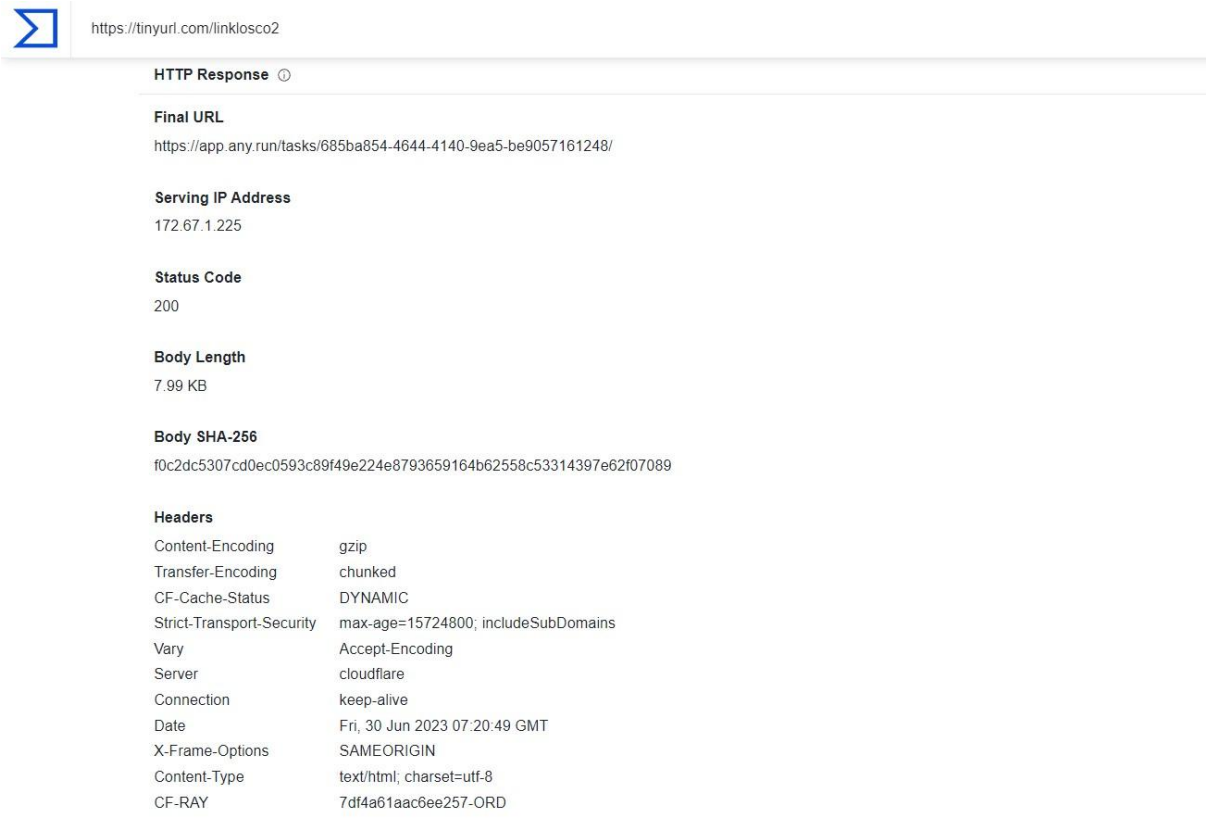
Application launched itself
- firefox.exe (PID: 2976)
- firefox.exe (PID: 3384)

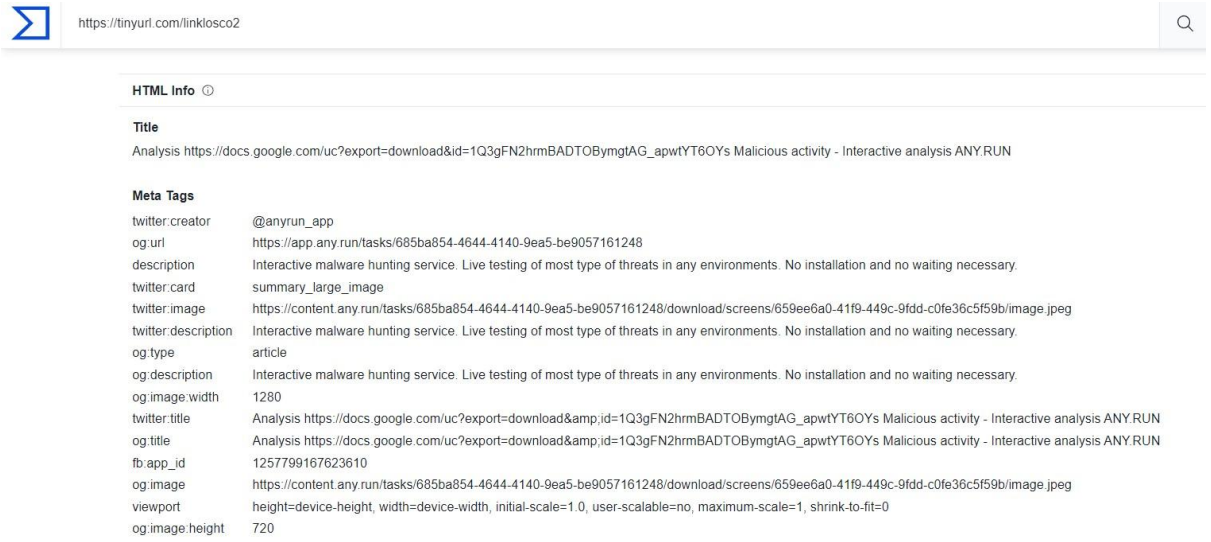
The process uses the downloaded file
- powershell.exe (PID: 2272)
- firefox.exe (PID: 3384)

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

Il secondo link, analizzato da VirusTotal, ci dice praticamente la stessa cosa del secondo: rimanda a una pagina di AnyRun e non contiene malware.



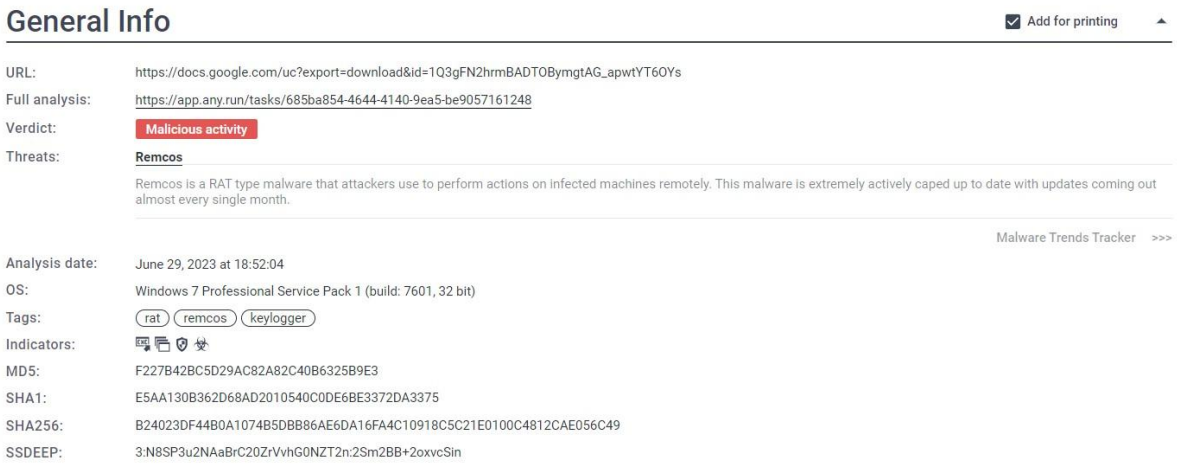




Andiamo quindi ad aprire la pagina.
Questa volta si analizza un malware dannoso. La sandbox ci informa che si tratta di un malware di tipo RAT (Remote Access Trojan).
L'utente, scaricando un programma camuffato da prodotto Microsoft, scarica sul dispositivo (oltre al programma legittimo) anche il malware composto da più elementi: *Autoruns.exe* che, quando eseguito, esegue in automatico *procexp.exe,* un fake "Esplora processi".
DOCX_SENTENCIA, invece, è un file camuffato da prodotto Adobe

estraibile e poi manualmente eseguibile che apre un compilatore di C# e il terminale cmd per eseguire comandi amministrativi. Esegue inoltre il file *csc.exe*, la vera e propria backdoor, che comincia a scrivere log di keylogging.

Con un po' di ricerche, si scopre che il RAT Remcos è un malware che riesce ad attaccare le versioni di Windows da XP in su, famoso per essere costantemente aggiornato e per essere molto sofisticato, riuscendo ad aggirare il controllo dell'account utente Windows UAC.



General Info

Add for printing

URL: https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADT0BymgtAG_apwtYT6OYs

Full analysis: https://app.any.run/tasks/685ba854-4644-4140-9ea5-be9057161248

Verdict: Malicious activity

Threats: Remcos

Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month.

Malware Trends Tracker >>>

Analysis date: June 29, 2023 at 18:52:04

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags: rat remcos keylogger

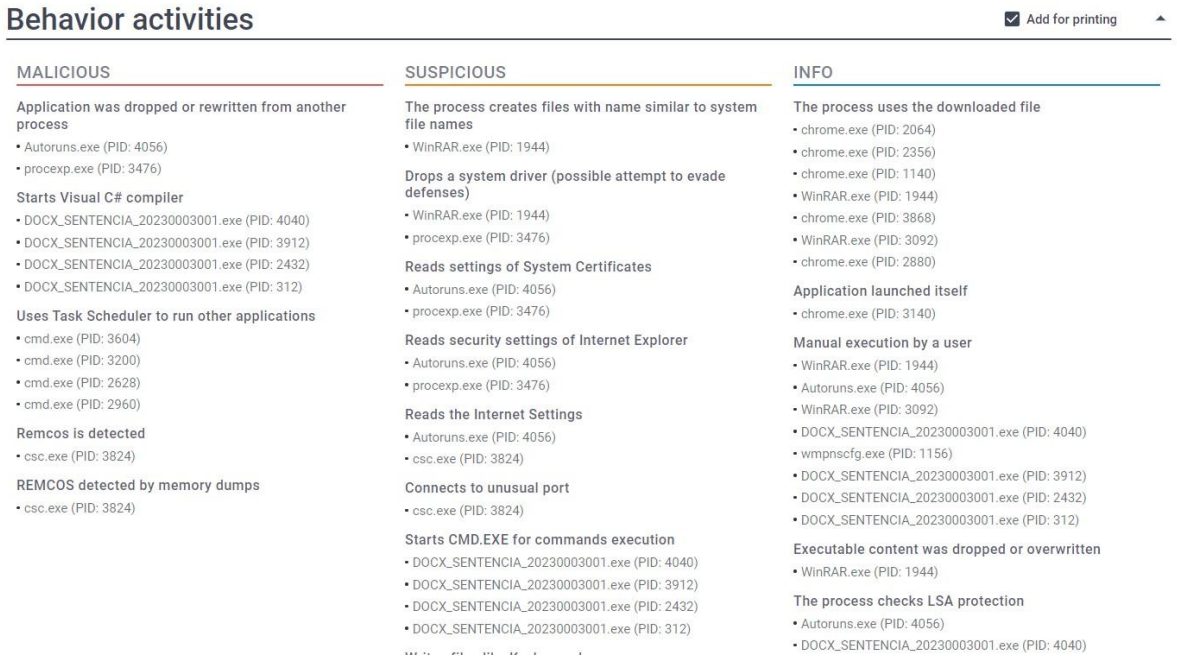
Indicators:

MD5: F227B42BC5D29AC82A82C40B6325B9E3

SHA1: E5AA130B362D68AD2010540C0DE6BE3372DA3375

SHA256: B24023DF44B0A1074B5DBB86AE6DA16FA4C10918C5C21E0100C4812CAE056C49

SSDEEP: 3:N8SP3u2NAaBrC20ZrVvhG0NZT2n:2Sm2BB+2oxvcSin



Behavior activities

Add for printing

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)

Starts CMD.EXE for commands execution
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

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)

Executable content was dropped or overwritten
- WinRAR.exe (PID: 1944)

The process checks LSA protection
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)

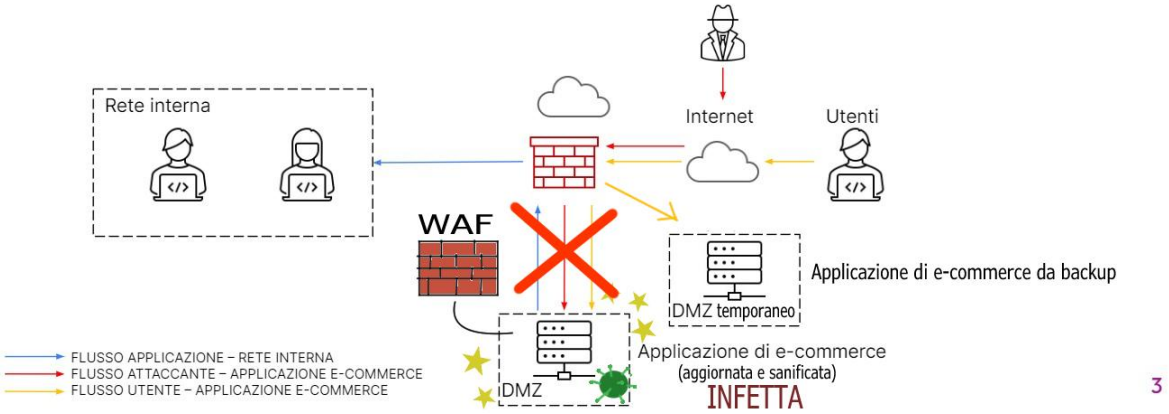
Response

Se l’applicazione viene infetta, bisogna agire in fretta per rimuovere il server infetto dalla rete interna e da internet in modo da evitare che il malware si infetti e che possa danneggiare l’esperienza degli utenti.

E’ necessario che il server venga isolato per poter sradicare il malware con scan e antivirus per poi essere sistemato o smaltito, quindi mancherebbe un servizio critico a tutti gli utenti, causando un grave danno economico all’azienda. Per rimediare, si potrebbe alzare un server temporaneo utilizzando i dati del backup (assicurandosi che non siano stati infettati) che funzioni come il principale e che sia collegato al firewall.

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.



Modifica dell’infrastruttura

Per evitare che l’azienda subisca tali danni in futuro, è opportuno aumentare la ridondanza dei server e la loro sicurezza per fare in modo che i servizi critici siano accessibili in qualsiasi momento.
Si dovrebbero implementare degli UPS (Uninterruptible Power Supply) per ogni server, fare backup frequenti, acquistare più server (fisici o cloud) e un hot site per eventuali disastri. I dipendenti andrebbero inoltre istruiti e sensibilizzati sulla sicurezza informatica per evitare che possano accidentalmente eseguire programmi malevoli o divulgare

informazioni confidenziali, e incoraggiati a usare password forti e a cambiarle ogni paio di mesi.

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.