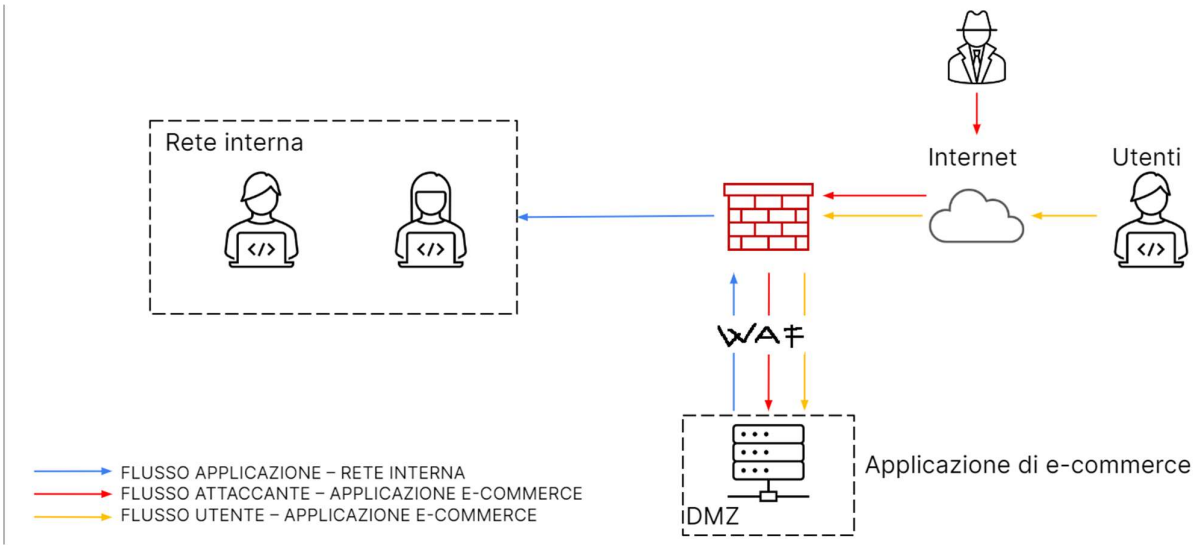
Esercizio Epicode 30/06/2023

Punto 1:

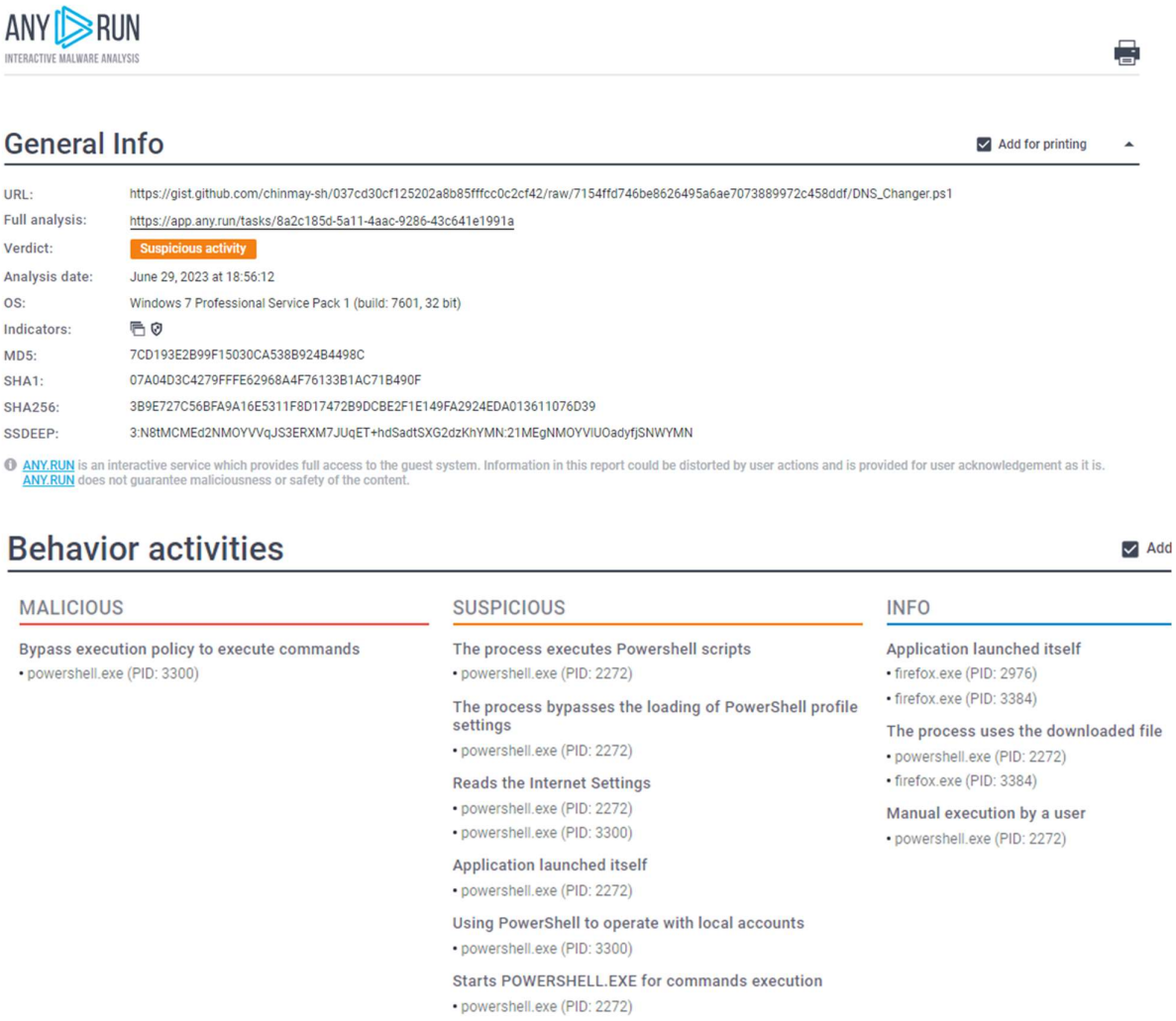
Come azione preventiva ad attacchi SQLi e XSS ho ritenuto necessario l'utilizzo di un Web Application Firewall (WAF) che consente di proteggere le applicazioni Web da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) a livello di applicazione. WAF consentirà di definire e gestire le regole per evitare minacce a Internet, tra cui indirizzi IP, intestazioni HTTP, corpo HTTP, stringhe URI, scripting tra siti (XSS), inserimento SQL e altre vulnerabilità. Il firewall dell'applicazione Web viene distribuito per proteggere le applicazioni Web e raccogliere i log di accesso per la conformità e l'analisi.



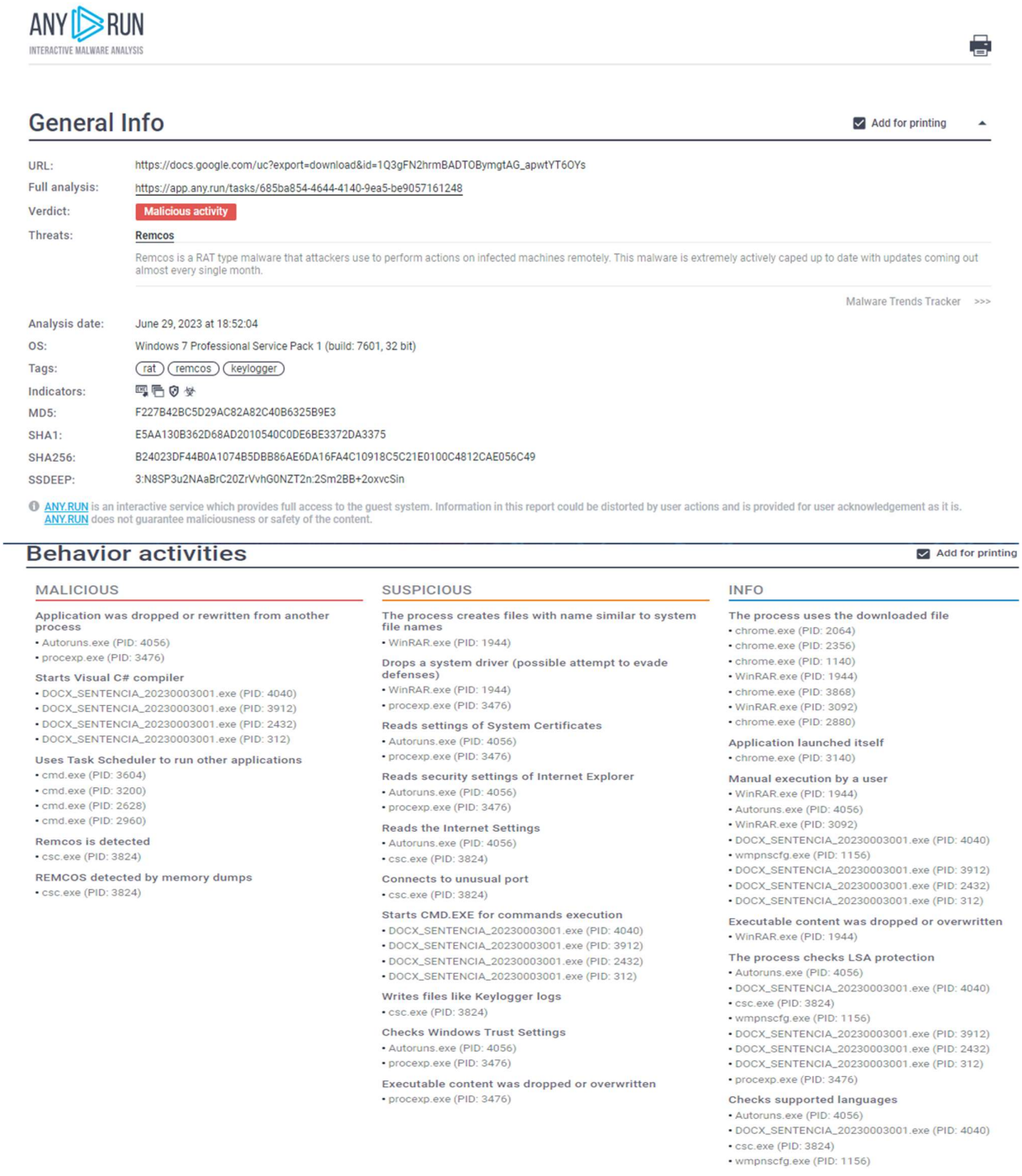
Punto 2:

Ho utilizzato **anyrun** per l'analisi di link.

1. https://tinyurl.com/linklosco1 si tratta di uno script per PowerShell che bypassa le policy di esecuzione al fine di leggere gli Internet Settings. Gli attaccanti possono abusare di interpreti di comandi e script per eseguire comandi, script o file binari. Queste interfacce e linguaggi forniscono modalità di interazione con i sistemi informatici e sono una caratteristica comune a molte piattaforme diverse. La maggior parte dei sistemi è dotata di un'interfaccia a riga di comando integrata e funzionalità di scripting; infatti, le installazioni di Windows includono Windows Command Shell e PowerShell. Gli avversari possono abusare di queste tecnologie in vari modi per iniettare codice malevole ed eseguire comandi arbitrari. Questa PowerShell serve a modificare i settings del server DNS per l'accesso al Wi-Fi. Si consiglia di non avviare applicazioni precedenti gli alert.



2. https://tinyurl.com/linklosco2 si tratta di un Remcos è un malware di tipo RAT (Remote Access Trojan) che gli aggressori utilizzano per eseguire azioni su macchine infette da remoto. Questo malware è aggiornato in modo estremamente attivo con aggiornamenti in uscita quasi ogni mese. Remcos (acronimo di Remote Control & Surveillance Software) è uno strumento commerciale di accesso remoto per controllare i computer da remoto. Remcos è pubblicizzato come software legittimo che può essere utilizzato per scopi di sorveglianza e test di penetrazione, ma è stato utilizzato in numerose campagne di hacking. Remcos, una volta installato, apre una backdoor sul computer, garantendo l'accesso completo all'utente remoto.



ANY.RUN
INTERACTIVE MALWARE ANALYSIS

General Info

Add for printing

URL: https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgtAG_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

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

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)

Writes files like Keylogger logs
- csc.exe (PID: 3824)

Checks Windows Trust Settings
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Executable content was dropped or overwritten
- procexp.exe (PID: 3476)

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)

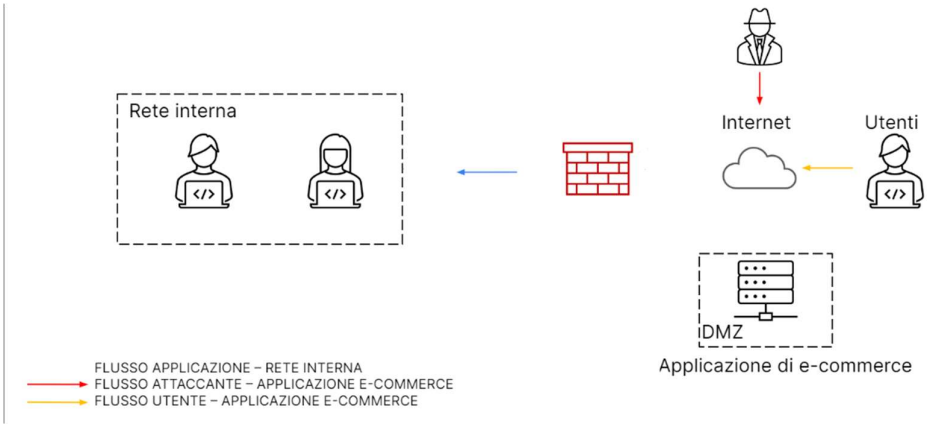
Executable content was dropped or overwritten
- WinRAR.exe (PID: 1944)

The process checks LSA protection
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)
- procexp.exe (PID: 3476)

Checks supported languages
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)

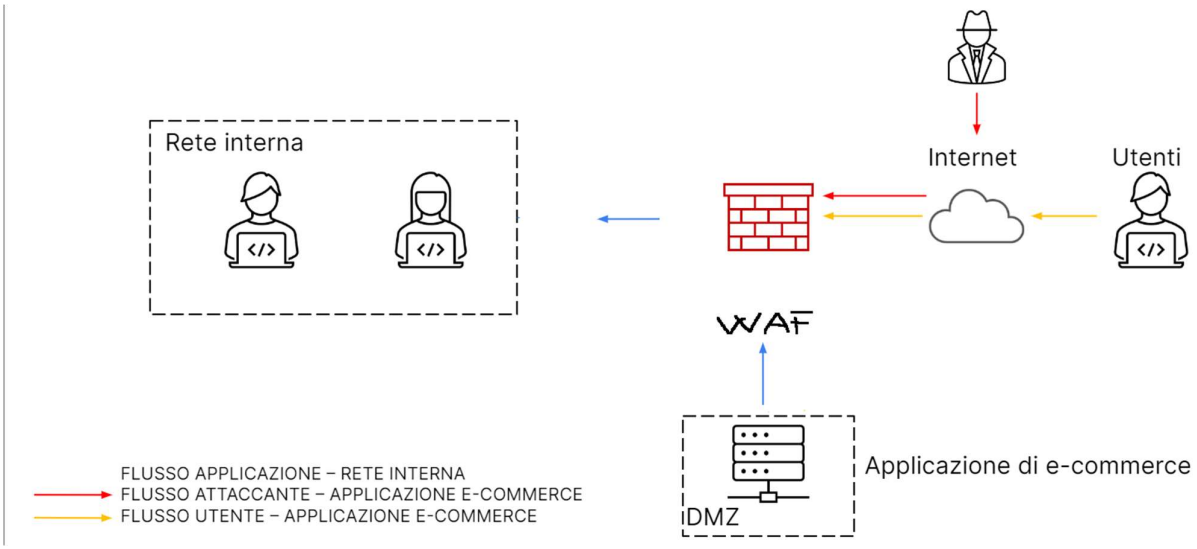
Punto 3:

L'applicazione web è stata infettata da un malware. È importante che il malware non si propaghi nella rete interna e che non divulghi informazioni sensibili verso Internet. Il server DMZ essendo stato compromesso, dà la possibilità all'attaccante di raggiungere la rete interna. Come response ho adottato la tecnica della rimozione, che consiste nella completa disconnessione sia dalla rete interna sia da Internet dell'applicazione web, così l'attaccante non avrà accesso né alla rete interna né alla macchina infettata.



Punto 4:

Ho unito i disegni dell'azione preventiva e della response.



Punto 5:

Integrazione altri elementi di sicurezza: ho deciso di optare per un doppio firewall con una DMZ. Il primo firewall consente solo il traffico esterno alla DMZ, mentre il secondo consente solo il traffico che va dalla DMZ alla rete interna. L'autore di un attacco dovrebbe compromettere entrambi i firewall per avere accesso alla LAN di un'organizzazione. Inoltre, ho ritenuto opportuno l'utilizzo della ridondanza includendo un'applicazione web aggiuntiva per permettere l'operatività del sistema anche a fronte della compromissione di una dei due. Infatti, in tal caso, la seconda applicazione web inizierebbe a funzionare rimanendo collegato alla rete interna permettendo l'accesso ai dipendenti.