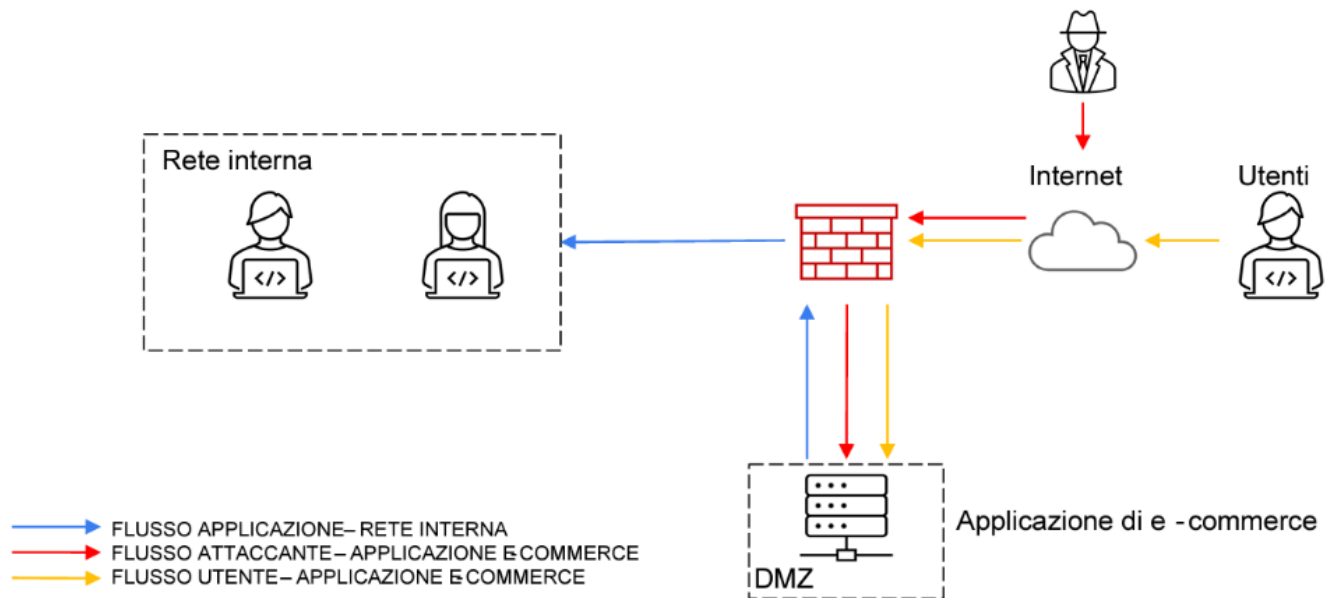


Ho un'architettura di rete dove gli Utenti provenienti da Internet possono accedere all'applicazione di e-commerce che si trova all'interno di una DMZ, mentre in una rete separata abbiamo la rete interna dell'azienda.

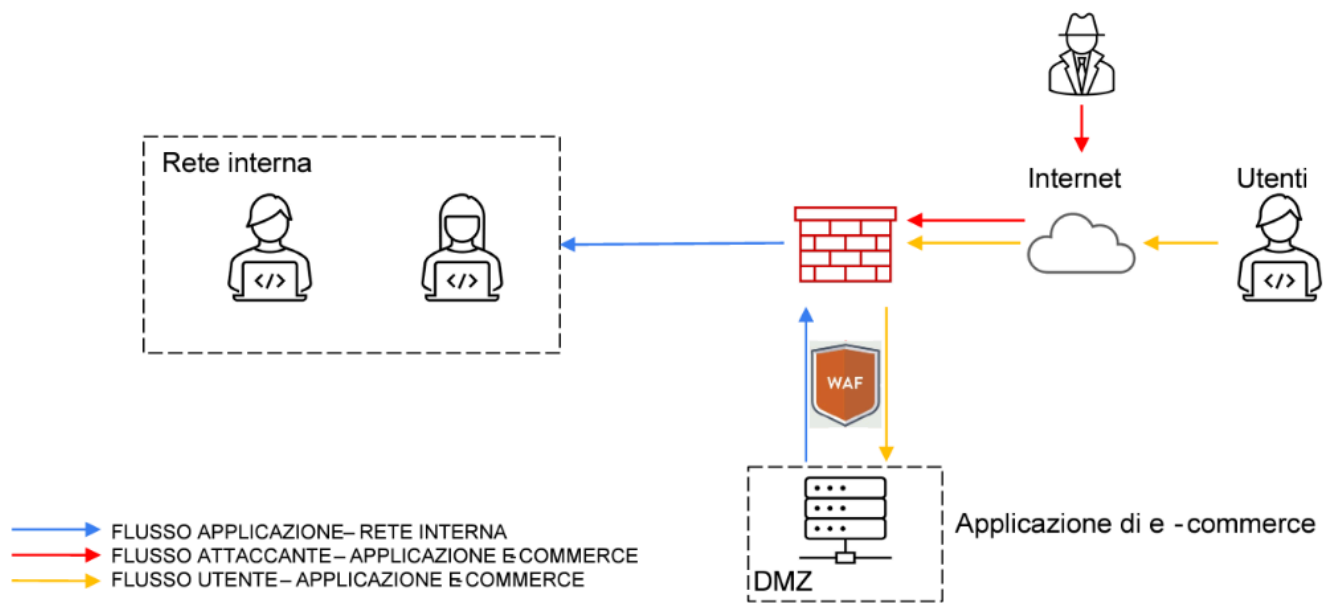
In caso di attacco se viene compromesso il server DMZ, l'attaccante può accedere, grazie ad i permessi sul firewall, alla rete interna dato che il server DMZ e la rete interna devono poter comunicare.



1. Azioni preventive: Per difendere il server DMZ da attacchi di tipo SQLi oppure XSS, posso preventivamente inserire un WAF tra la DMZ e il firewall.

Il WAF, o Web Application Firewall, è uno strumento di sicurezza informatica usato per proteggere le applicazioni web da minacce e attacchi, questo lo fa tramite:

- il filtraggio delle richieste HTTP
- il rilevamento e la protezione da attacchi SQL injection, questi attacchi sfruttano le vulnerabilità nelle applicazioni web manipolando o compromettendo il database SQL eseguendo comandi SQL non autorizzati.
- impedisce gli attacchi XSS (Cross-Site Scripting), esistono 3 tipi di questi attacchi, XSS Stored, Reflected e DOM-based, essi sfruttano le vulnerabilità nelle applicazioni web e con l'inserimento di script malevoli mettono a rischio la sicurezza e la privacy degli utenti che visitano le applicazioni web danneggiate da questi attacchi.
- gestisce e controlla l'accesso e le sessioni sull'applicazione web, registrando e monitorando i log.

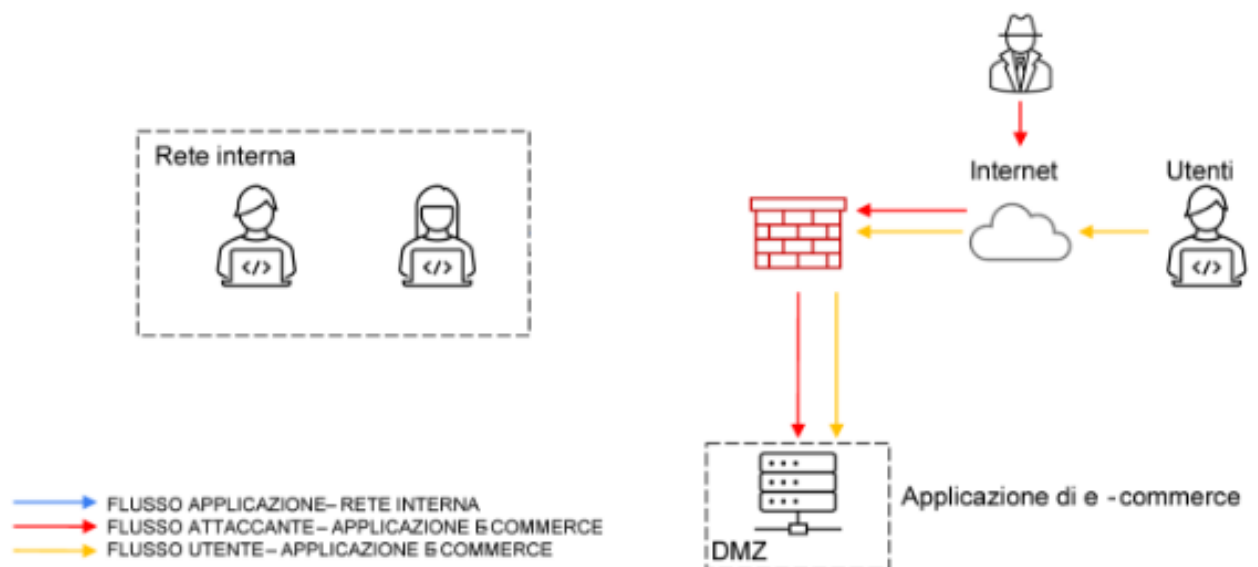


2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Sapendo che in media ogni minuto l'utente spende 1.500 € sulla piattaforma di e-commerce, il business perderà 15.000 €, mentre per prevenire questo tipo di problema possiamo fare diverse azioni:

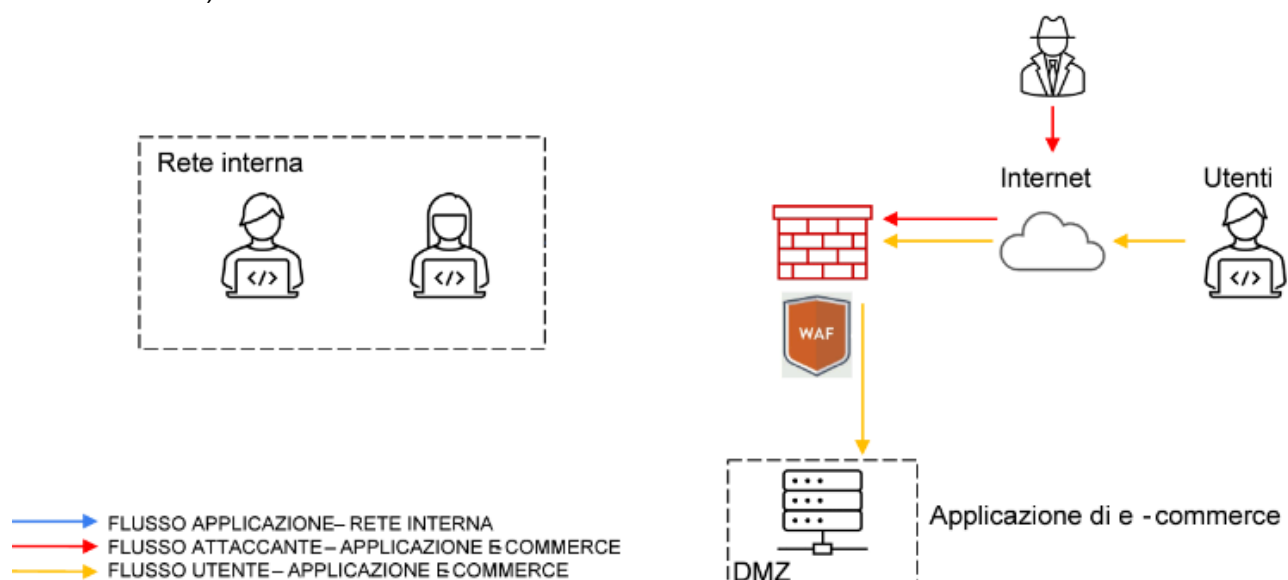
- la prima è una protezione DDoS che utilizza sistemi di sicurezza per rilevare e mitigare gli attacchi DDoS in tempo reale filtrando principalmente il traffico dannoso
- configurare una CDN (Content Delivery Network) che distribuisce il carico del traffico su server distribuiti geograficamente.
- implementare sistemi di bilanciamento del carico che distribuiscono le richieste degli utenti tra più server, migliorando la sicurezza e le prestazioni.
- implementare sistemi di monitoraggio per la rilevazione rapida di attacchi in corso

3. Response: l'applicazione Web viene infettata da un malware, l'interesse principale è quello di non far divulgare il malware sul resto della rete mentre non ci interessa che l'attaccante abbia l'accesso al server attaccato.

L'azione che si andrà a fare si chiama isolamento, quindi mettere in "quarantena" la parte di rete infetta levandoli il collegamento al resto della rete ma rimanendo l'accesso da internet.



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



5. **Modifica “più aggressiva” dell’infrastruttura:**

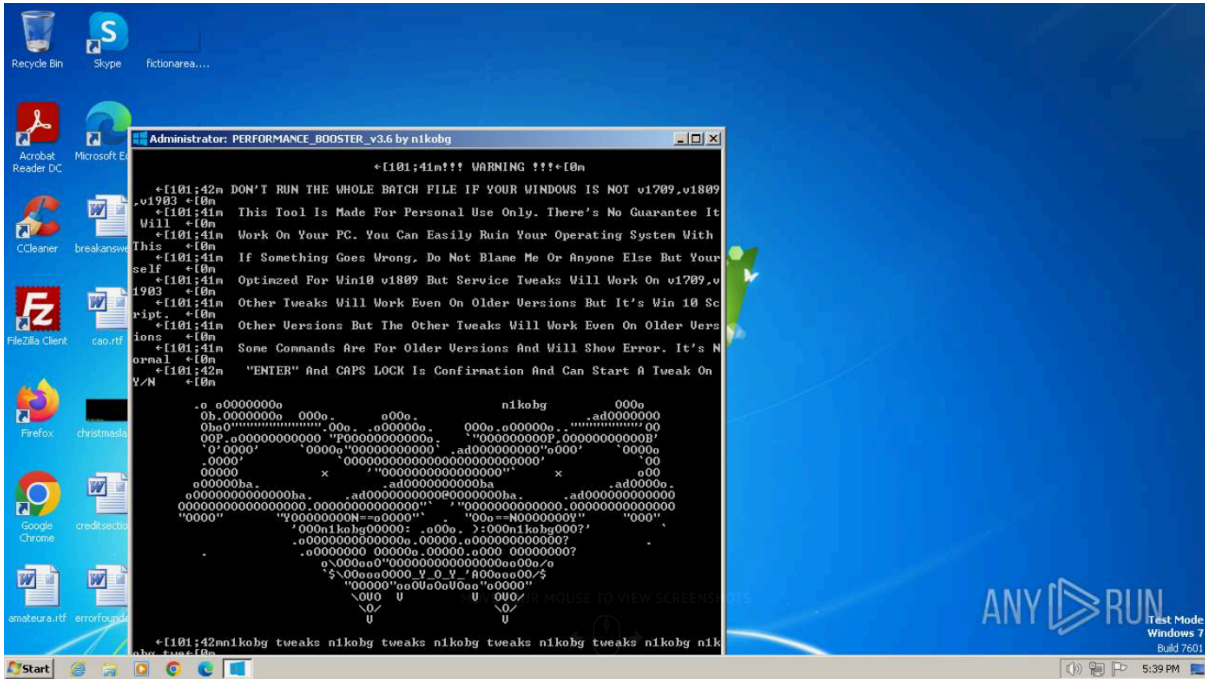
Nell’infrastruttura di rete con un budget di 8.000 € possiamo integrare eventuali sistemi di sicurezza del tipo:

- Subnetting per la divisione delle reti, tra interne e dmz.
- Sistema di Rilevamento delle Intrusioni (IDS) e Sistema di Prevenzione delle Intrusioni (IPS): Un IDS monitora il traffico di rete per rilevare comportamenti sospetti o attività anomale, mentre un IPS va oltre, bloccando automaticamente o rispondendo agli attacchi identificati.

Traccia Bonus

Traccia Bonus 1: <https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/>

Nella prima traccia bonus vediamo che l'utente scarica un programma chiamato PERFORMANCE_BOOSTER che sembra essere una semplice applicazione per dare un boost al computer, quando in realtà in background esegue azioni malevoli.



Questo programma una volta eseguito usa la powershell di windows per eseguire delle azioni malevoli, come per esempio l'esecuzione di comandi da remoto.

Techniques details

Get to know what this threat is about

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell)

Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from

- Using PowerShell to operate with local accounts (2)
3332 powershell.exe (2)
- Changes powershell execution policy (Unrestricted) (1)
668 cmd.exe (1)
- Starts POWERSHELL EXE for commands execution (1)
668 cmd.exe (1)

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Cmdline: POWERSHELL SET-EXECUTIONPOLICY UNRESTRICTED -FORCE

1 of 1

L'attaccante può modificare permessi di modifica a file e directory e creare un account sul computer attacco per rimanere connesso da remoto senza l'esecuzione di programmi, può infine sfruttare delle funzioni del sistema operativo che gli permette di nascondere importanti file di sistema e azioni eseguibili con permessi di amministratore.

Techniques details

×

● Warning (2)

Permissions required: Administrator

Data sources: Command: Command Execution, User Account: User Account Creation, Process: Process Creation

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system. Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

Local Account ▾

- Using PowerShell to operate with local accounts (2)
 - 3332 powershell.exe (2)

Techniques details

×

● Warning (1)

User Account: User Account Metadata, File: File Modification, Service: Service Creation

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.(Citation: Sofacy Komplex Trojan)(Citation: Cybereason OSX Pirrit)(Citation: MalwareBytes ADS July 2015)

Hidden Files and Directories ▾

- Uses ATTRIB.EXE to modify file attributes (1)
 - 668 cmd.exe (1)

Infine l'attaccante per ottenere maggiori informazioni riguardo il computer target può controllare i Windows Registry, che contengono un grande ammontare di informazioni riguardo il sistema operativo, i software installati e la sicurezza della macchina target.

Techniques details

Get to know what this threat is about

Warning (29) • Other (6)

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

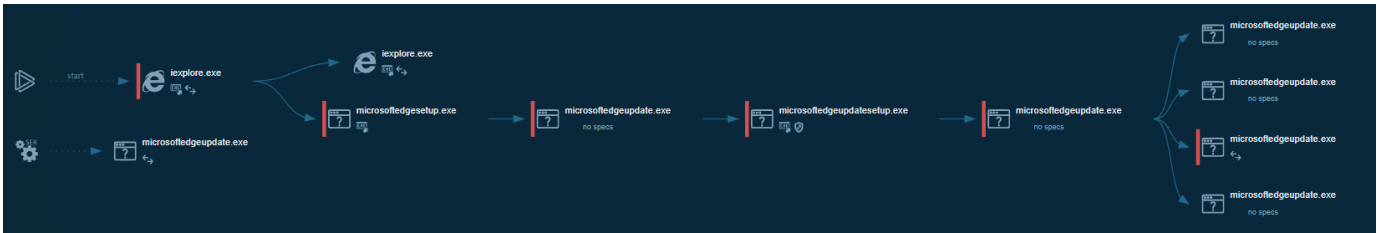
The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the Reg utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from Query Registry during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

- Reads Windows Product ID (1)
2824 regedit.exe (1)
- Searches for installed software (1)
2824 regedit.exe (1)
- Reads Microsoft Outlook installation path (1)
2824 regedit.exe (1)
- Reads the history of recent RDP connections (15)
2824 regedit.exe (15)

Questo software quindi abbiamo scoperto contenere un malware che permette all'attaccante di stabilire una connessione in remoto sulla macchina target, con la possibilità di eliminare le sue tracce e di ricavare tutte le informazioni che riesce a trovare sulla macchina permettendogli di aggirare i sistemi di sicurezza e di infettare completamente la macchina target. Per evitare questo tipo di software, per prima cosa bisogna vedere se quello che stiamo scaricando è un software di legittima provenienza e di avere un anti virus che ci ferma dall'installare contenuti malevoli che possono danneggiare il computer.


Traccia Bonus 2: <https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>

Nella seconda traccia possiamo analizzare che l'utente ha scaricato tramite un sito probabilmente malevolo, che può essere stato clonato. Quello che l'utente pensa di stare scaricando non è solo microsoft edge ma un trojan che si installa sul kernel, permettendo di fargli eseguire comandi malevoli.



Questo si può vedere dalle informazioni dei processi, per esempio nell’ultima parte.

Process information

PID	CMD	Path	Indicators	Parent process
1632	"C:\Program Files\Internet Explorer\iexplore.exe" "https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE"	C:\Program Files\Internet Explorer\iexplore.exe		explorer.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Internet Explorer	
Version:	11.00.9600.16428 (winblue_gdr.131013-1700)			
Modules				
Images				
c:\program files\internet explorer\iexplore.exe				
c:\windows\system32\ntdll.dll				
c:\windows\system32\kernel32.dll				
c:\windows\system32\kernelbase.dll				
c:\windows\system32\msvcrt.dll				
c:\windows\system32\api-ms-win-downlevel-advapi32-l1-1-0.dll				
c:\windows\system32\advapi32.dll				
c:\windows\system32\sechost.dll				
c:\windows\system32\rpcrt4.dll				
c:\windows\system32\iertutil.dll				

Questo si può prevenire istruendo il personale a verificare che il sito non sia clonato e con l’installazione di firewall o proxy per il filtraggio di dati malevoli.