team: iosint

IOSINT: Leading the way in cybersecurity, specializing in advanced threat detection and intelligent protection solutions.

info@iosint.org
+123 89283901

S9 - L5

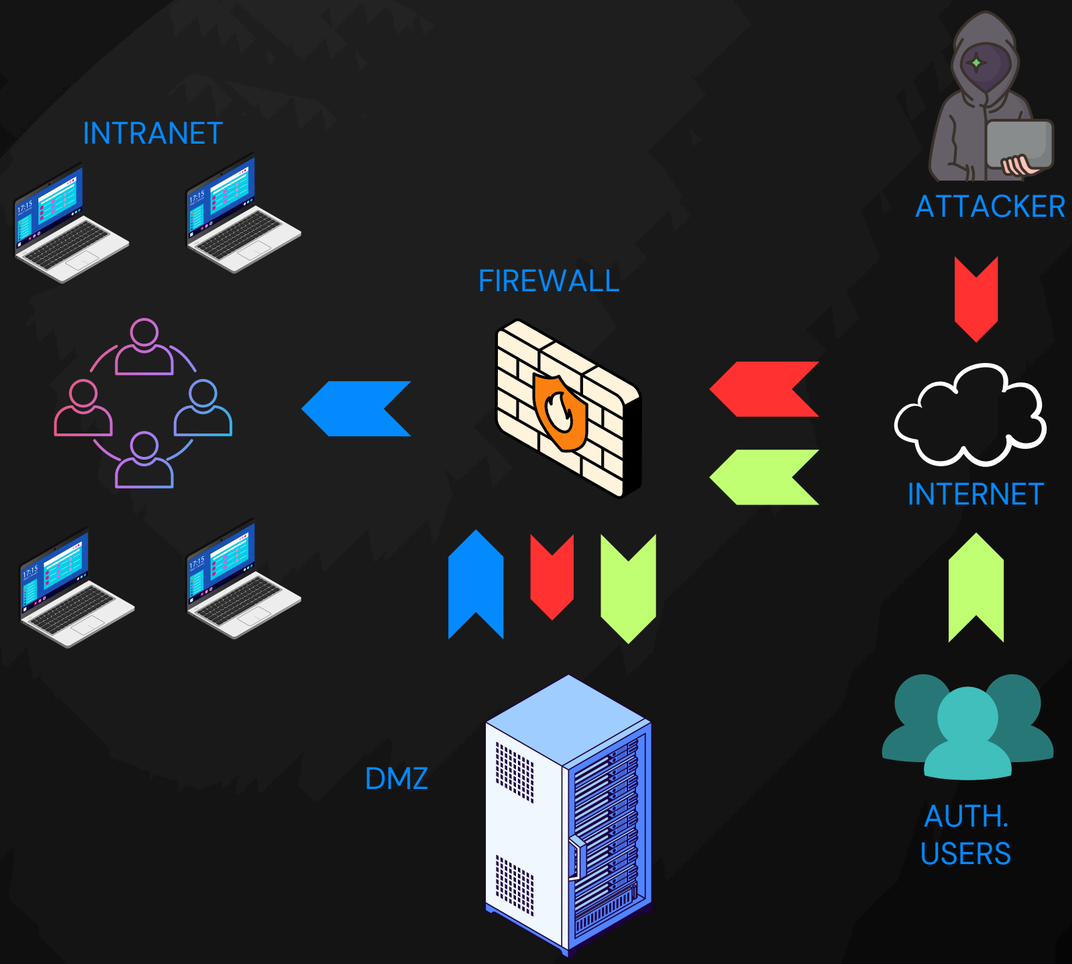
Date 07/06/2024

Report by:
Iosif Castrucci
Donato Tralli
Michael Andreoli
Luca Lenzi
Gianpaolo Miliccia Mendoza
Danilo Malagoli
Otman Hmich

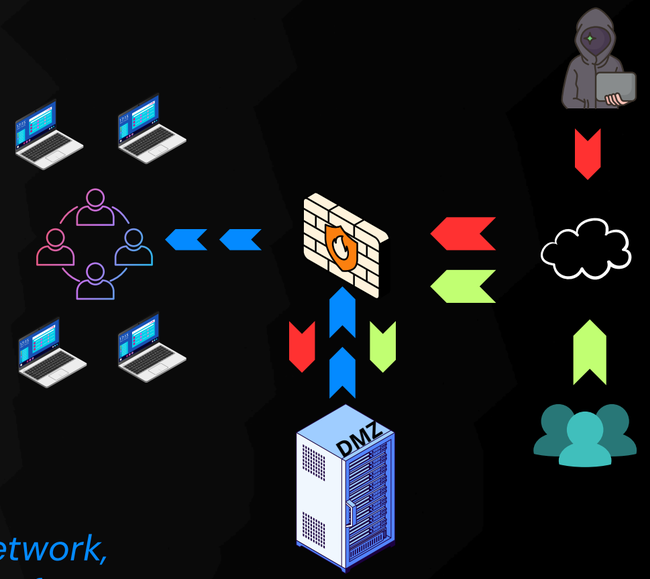
INDEX

INTRODUCTION

A company has contacted us for a consultation regarding recent issues with their corporate network. Specifically, we have been asked to examine the structure of their e-commerce website for potential XSS and SQLi vulnerabilities. Additionally, we will assess the financial damages resulting from potential service unavailability and check for the presence of malicious code on the hosting server. Finally, we will analyze the corporate network to propose an ideal solution to strengthen security.



VIRTUAL LAB



Reconstructing the initial situation before the assessment.
We will clarify some concepts related to the diagram shown in the figure:

FIREWALL: It is a (hardware and/or software) component used for the perimeter defense of a network, providing protection in terms of cybersecurity for the network itself and protecting hosts from malware or other dangers.

DMZ (Demilitarized Zone): It is a physical or logical subnetwork that contains and exposes services to an external network considered unsafe (such as the Internet). The purpose of a DMZ is to protect an organization's LAN.

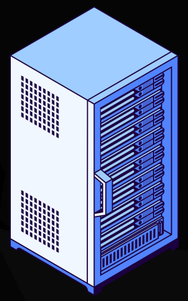
INTRANET: It is a private corporate network isolated from the external network (Internet) in terms of the services offered (e.g., via LAN), thus intended for internal use only.

OBJECTIVES

The company's e-commerce web application has XSS and SQLi vulnerabilities. By analyzing the provided company schema, we can deduce that the service is hosted within the server in the DMZ. The traffic to the server is thus monitored solely by the perimeter firewall.

The task requires us to:

Describe: Provide a detailed description of the identified vulnerabilities to clarify the potential issues.
Evaluate: Perform a risk assessment regarding the likelihood of an attack exploiting one of the described vulnerabilities.
Propose: Present a solution proposal, which may be implemented at the discretion of the designated company personnel.



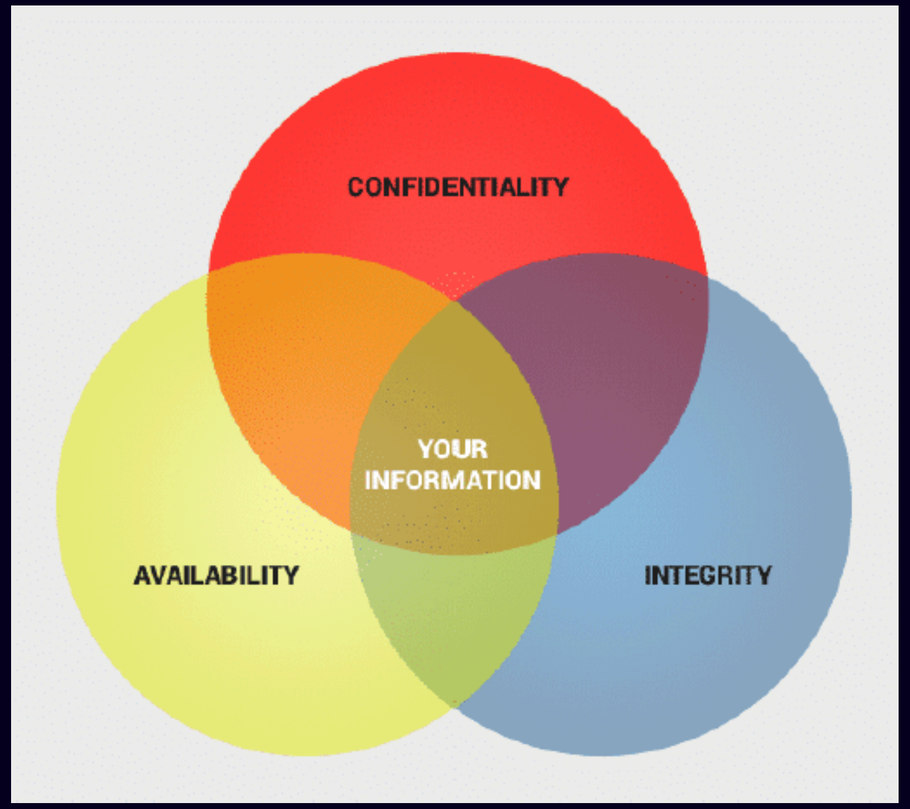
CIA

Here are some fundamental principles of cybersecurity.
Confidentiality: This ensures that data is accessible only to authorized users, safeguarding sensitive information from unauthorized access or disclosure.

Integrity: Data integrity ensures the accuracy and reliability of information. It guarantees that data remains unchanged and unaltered during storage, transmission, or processing, maintaining its reliability for both sender and receiver.

Availability: Availability ensures that data is consistently accessible to authorized users, even during emergencies or unforeseen circumstances. It ensures that critical information remains accessible when needed.

These principles form the CIA triad, a cornerstone of cybersecurity, emphasizing the importance of maintaining confidentiality, integrity, and availability of data.



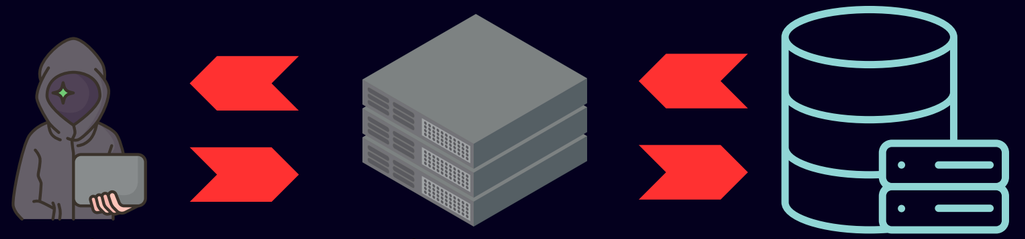
XSS (Cross-side scripting)

Let's delve into some key concepts that will aid our general analysis.
Cross-Site Scripting (XSS) is a cybersecurity vulnerability that affects dynamic websites with inadequate input control in forms.

Why is it crucial to protect against potential attacks exploiting this vulnerability?
XSS enables a malicious actor to insert or execute client-side code to carry out a diverse range of attacks, including:

Collection, manipulation, and redirection of sensitive information.
Viewing and modification of data on servers.
Alteration of the dynamic behavior of web pages, etc.

SQL Injection



Another common vulnerability that a poorly configured web app is often exposed to is SQL Injection.
SQL injection is a command injection technique used to attack applications that manage data through relational databases using SQL language.
The lack of user input control allows maliciously inserting SQL code strings that will be executed by the server application.
Why is it crucial to protect against potential attacks exploiting this vulnerability?
Through this mechanism, unauthorized users can execute SQL commands, even complex ones, enabling:

Data alteration (e.g., creating new users).
Complete download of database contents.
Unauthorized data reading from the database.

ERRORS

Logical Structural Errors
As discussed in the theoretical concepts, the company's web application is vulnerable to XSS and SQLi primarily due to excessive trust in user input.

01 Lack of Input Control

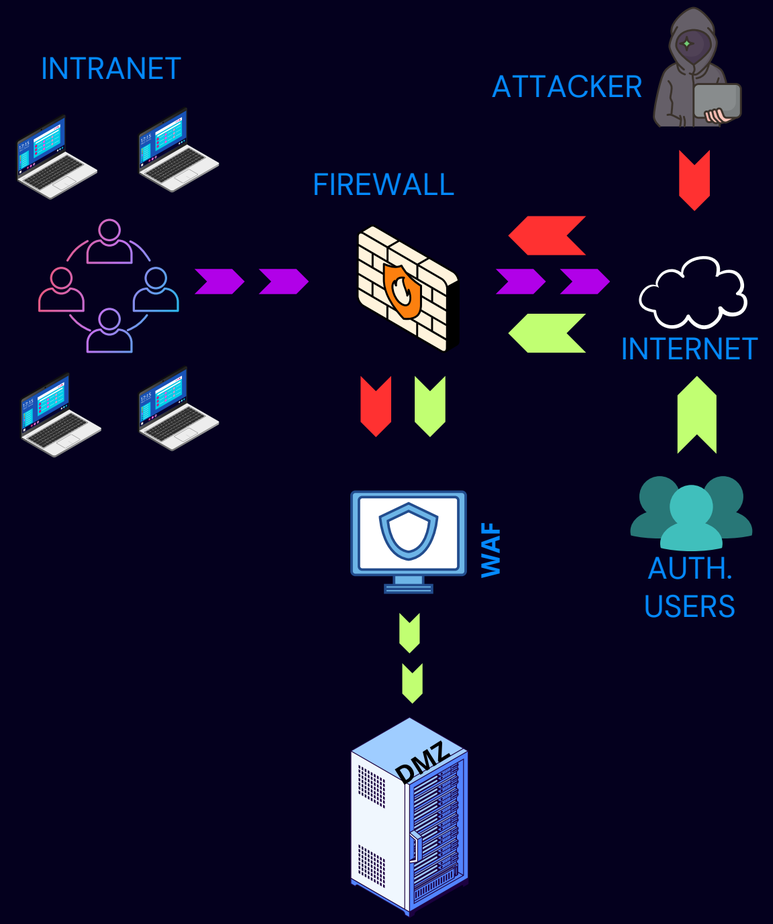
Theoretically, the DMZ should never solely provide outgoing traffic to another zone within the company's network. In our case, the outbound channel from the DMZ to the internal network, besides being excessive, allows potential attackers entry to the intranet.

The current network structure of the company is unable to adequately defend the web application due to the absence of intrusion prevention systems (IPS/IDS) and an additional WAF (Web Application Firewall).
Weak Structure 02
Evaluation Issues
Service Unavailability

The web application represents a core service of the company and, as such, must always be reachable, following the availability principle of the CIA. In the event of an attack, the site would become unavailable, contravening the previously described core security principle.

PROPOSED SOLUTION

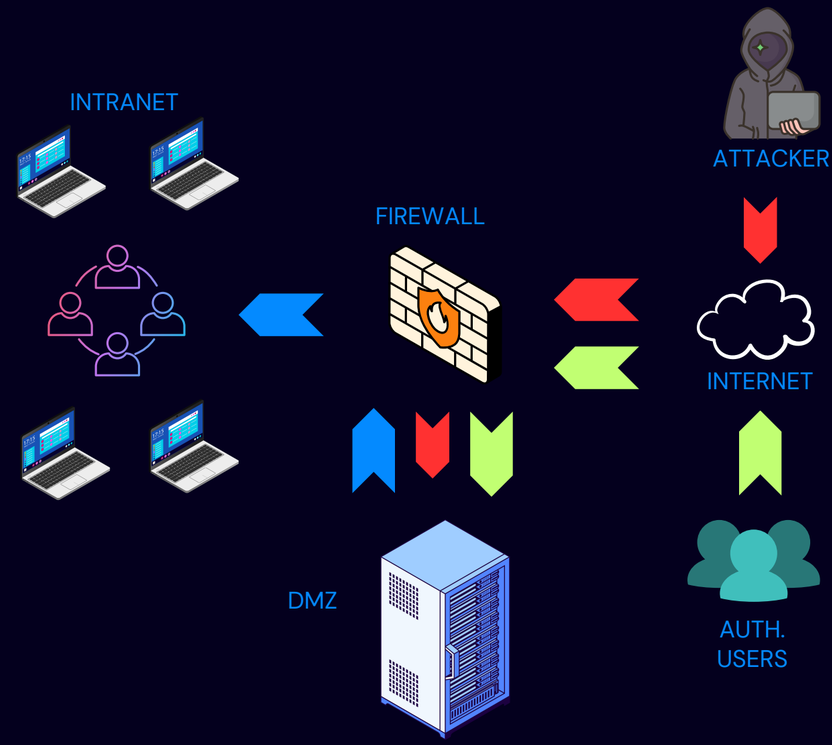
First and foremost, it is strongly recommended to implement more thorough user input controls:
adopt output encoding solutions capable of cleaning user input.
The implementation of input sanitization will prevent malicious users from exploiting
reflection points and/or injecting malicious SQL queries capable of deceiving databases.
Furthermore, the company is encouraged to procure a WAF, namely a web application firewall.
A WAF solution is designed to protect web apps by filtering, monitoring, and blocking
any incoming malicious HTTP traffic, while also preventing the unauthorized leakage of data from the application. Consequently, WAFs safeguard business-critical applications
and web servers from threats such as zero-day attacks, Distributed Denial-of-Service (DDoS) attacks,
SQL injection, and Cross-Site Scripting (XSS).
Additionally, the elimination of the flow from the DMZ to the internal network is requested for the reasons listed above.
One could consider allowing access to the DMZ from the internal network by connecting it to the internet; however, even though this solution is safer than the previous one, extremely strict firewall rules must be configured (access from the internet to the internal network is still PROHIBITED).



DDoS Attack Incident

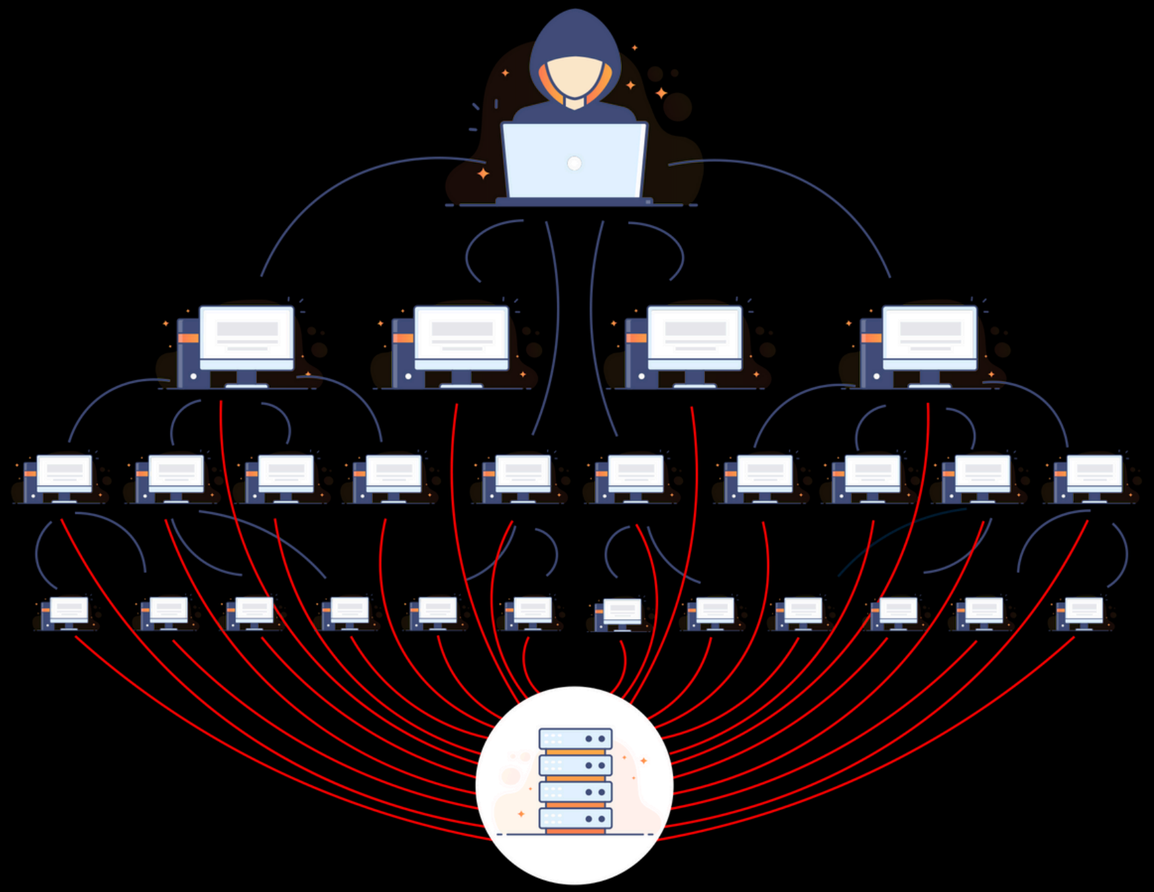
During the consultancy period, we received notification that the e-commerce Web App service (and its corresponding infrastructure) fell victim to a DDoS attack. Consequently, the client company tasked us with explaining the incident in detail, calculating the incurred damage, and suggesting any preventive actions to be taken.

We recall that the network diagram at the time of the attack was as follows:



WHAT IS DDOS?

Distributed Denial of Service (DDoS) attack is a specific type of attack within the Denial of Service (DoS) family, aiming to disrupt a service. Unlike traditional DoS attacks, DDoS involves multiple sources simultaneously targeting the victim. These parallel attack vectors often originate from a botnet, a network of previously compromised bots or zombies, controlled by a central command-and-control server. This server orchestrates and issues instructions to the bots to execute the attack.



THE DAMAGE SUFFERED

Therefore, let's conduct a quantitative analysis (with monetary assessment of the damage) following the incident.

EF
Exposure Factor

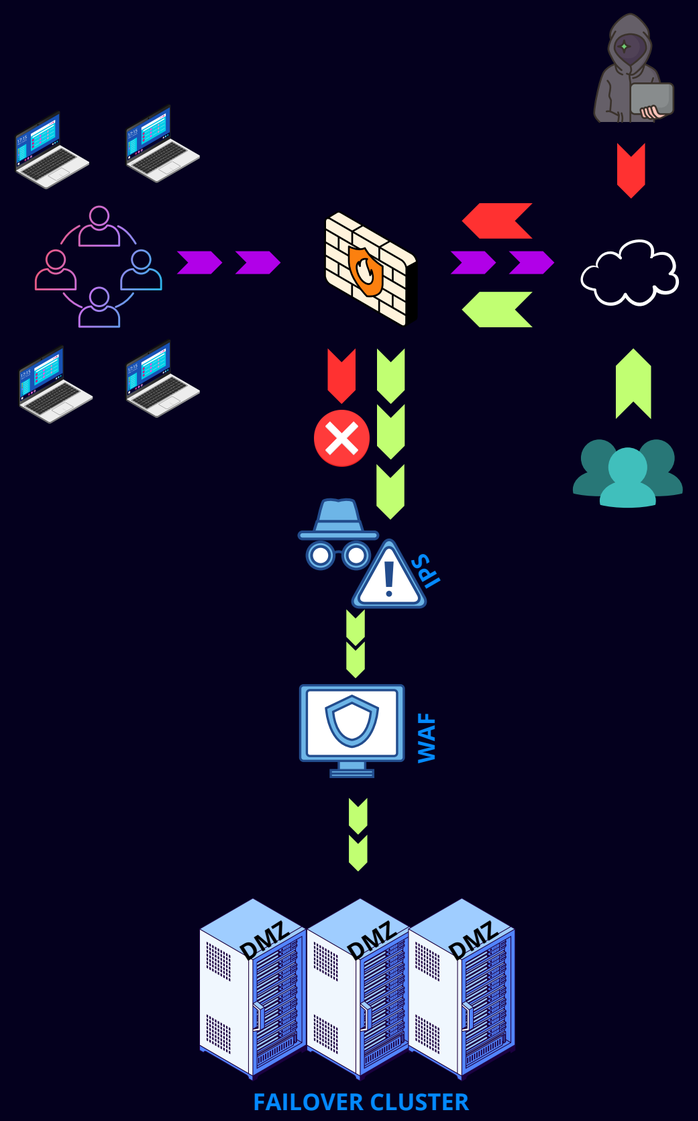
The first value to consider is the Exposure Factor: it represents the percentage of the service impacted by the event. In our case, the Web App was impacted in its entirety.
EF = 100%.

Asset Value

The second value we consider is the Asset Value: it indicates that the e-commerce service has a value of 1500 euros per minute. The time required to recover all functionalities (called RTO, Recovery Time Objective) was 10 minutes. Therefore, we can determine the asset value as:
AV = 15000€.

SLE
Single Loss Expectancy

The final monetary value that determines the damage suffered as a result of an incident is defined as Single Loss Expectancy, and is determined by the product of Exposure Factor and Asset Value.
SLE = EF x AV = 1500 x 10 = 15000€.

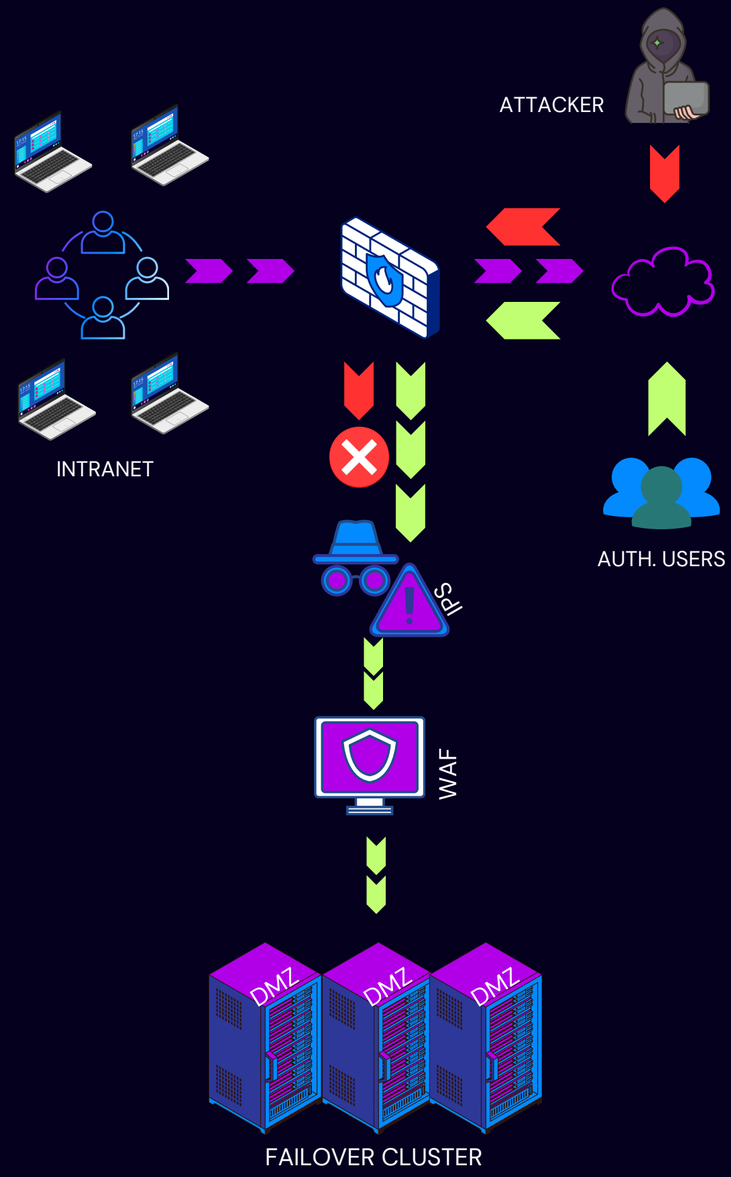


PROPOSED SOLUTIONS

Additionally, considering that a DDoS attack aims to render the service unavailable, we propose a solution to this further structural weakness. Following the CIA principles (particularly the availability principle mentioned earlier), the Web App should not remain offline except in extreme emergencies. Therefore, we suggest implementing a failover cluster in the DMZ. A failover is the process where a substitute node (in our case, a server) takes over a service when the primary node fails. A cluster refers to a set of identical physical servers dedicated to providing the same service. In our proposal, we depict three servers to enhance fault tolerance and ensure an active node even if one of the three servers in the cluster fails. Finally, for an additional layer of reinforcement, consider installing an hypervisor (such as Proxmox) on the servers. This allows virtualizing multiple virtual servers on the same machine, ensuring data synchronization and full node interfacing within the cluster.

PROPOSED SOLUTIONS

The cost of such a successful attack is extremely high, necessitating the adaptation of the network structure with precise security measures. Firstly, the company is advised to adhere to previously mentioned recommendations, such as implementing stricter firewall policies, isolating the intranet network, and introducing a WAF (Web Application Firewall). Additionally, the inclusion of an IPS (Intrusion Protection System) is recommended. An IPS is an active software component designed to enhance the cybersecurity of a system by detecting, recording, and attempting to flag and block malicious activities. It serves as an extension of IDS (Intrusion Detection System) as IPS can prevent and block identified intrusions. Specifically, an IPS can take actions like issuing alerts, removing malicious payloads, resetting connections, and/or blocking traffic from an attacking IP address. Following this implementation, it is advisable to introduce a company blacklist, a list where IP addresses blocked by the IPS are gradually added.



MALWARE RESPONSE

The company informs us that a malware has been detected on the hosting server. We are requested to describe the threat in detail, present a possible solution, and promptly intervene in isolating the infected machine. However, the company is not concerned with preventing the attacker from accessing the machine hosting the malware; their priority is to prevent the malicious code from spreading within the network. Additionally, we will proceed with proposing techniques for removing infected memories.

MALWARE

Malware, which stands for malicious software, encompasses any computer program designed to cause harm to an operating system. Consequently, it's conceivable that an individual with malicious intent exploited one of the previously examined vulnerabilities by injecting a malicious payload, thereby gaining unauthorized administrative access to the server running the Web App. Within an internet network, if a host becomes infected with malware, it should be promptly segregated from the remainder of the organization.

THEORETICAL CONCEPTS
IMPACT CONTAINMENT

To mitigate the impacts of a harmful event caused by a host infected with malware, the practice of dividing a network into multiple subnets through the use of subnetting and/or VLAN techniques is employed.

To safeguard the network from an infected machine, there are three methodologies:

Segmentation:

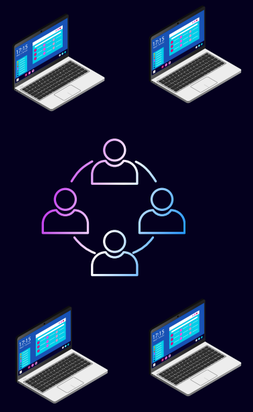
The network is divided, creating a quarantine subnet where the infected client is placed.
Isolation:

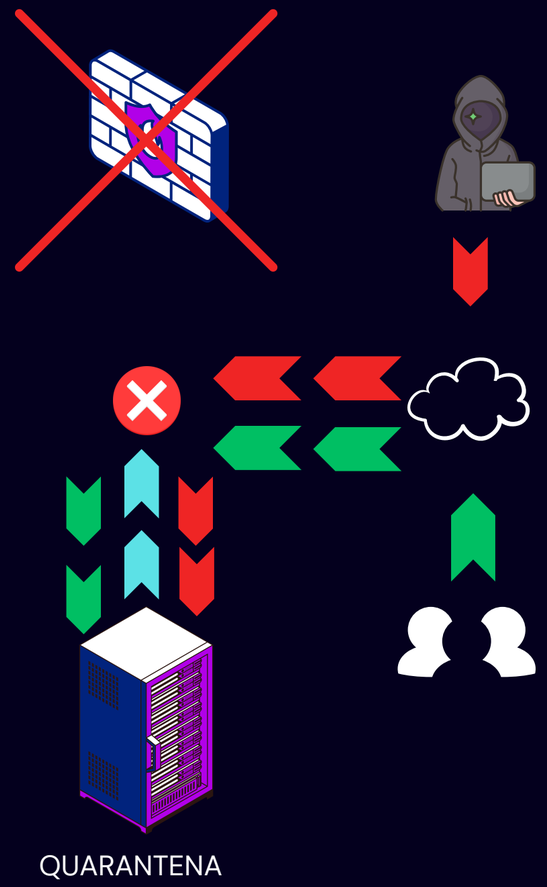
Similar to segmentation, but the new subnet will not pass through the firewall and will directly connect to the external network.
Removal:

The quarantine subnet, of which the infected host becomes a part, is disconnected from the Internet. This option is used when one wants to cut off the attacker's access to the victim machine. However, there will be a service interruption.

INCIDENT RESPONSE

Let's commence the operational phase of disaster recovery.
Among the techniques previously discussed, we've opted for isolation. This will allow the attacker to retain control over the victim machine but will prevent access to the intranet and thus other hosts on the network.
Firstly, we identify a new quarantine network to house the infected server.
Next, we eliminate the firewall: the primary reason this attack can be devastating lies in the link between the DMZ and the intranet, which, due to overly permissive firewall policies, left an open entry to the corporate network.
Therefore, we plan to review the entire firewall policy set later.
This ensures the protection of company data, yet the data of other users connected to the e-commerce service remain at risk. Without a partial disconnection from the internet (and thus session loss even for the malicious user), the actual extent of the damage caused cannot be estimated.
We plan to create an initial playbook (a descriptive document of the incident response procedure used) regarding these types of attacks.





FINAL MINIMAL SOLUTION

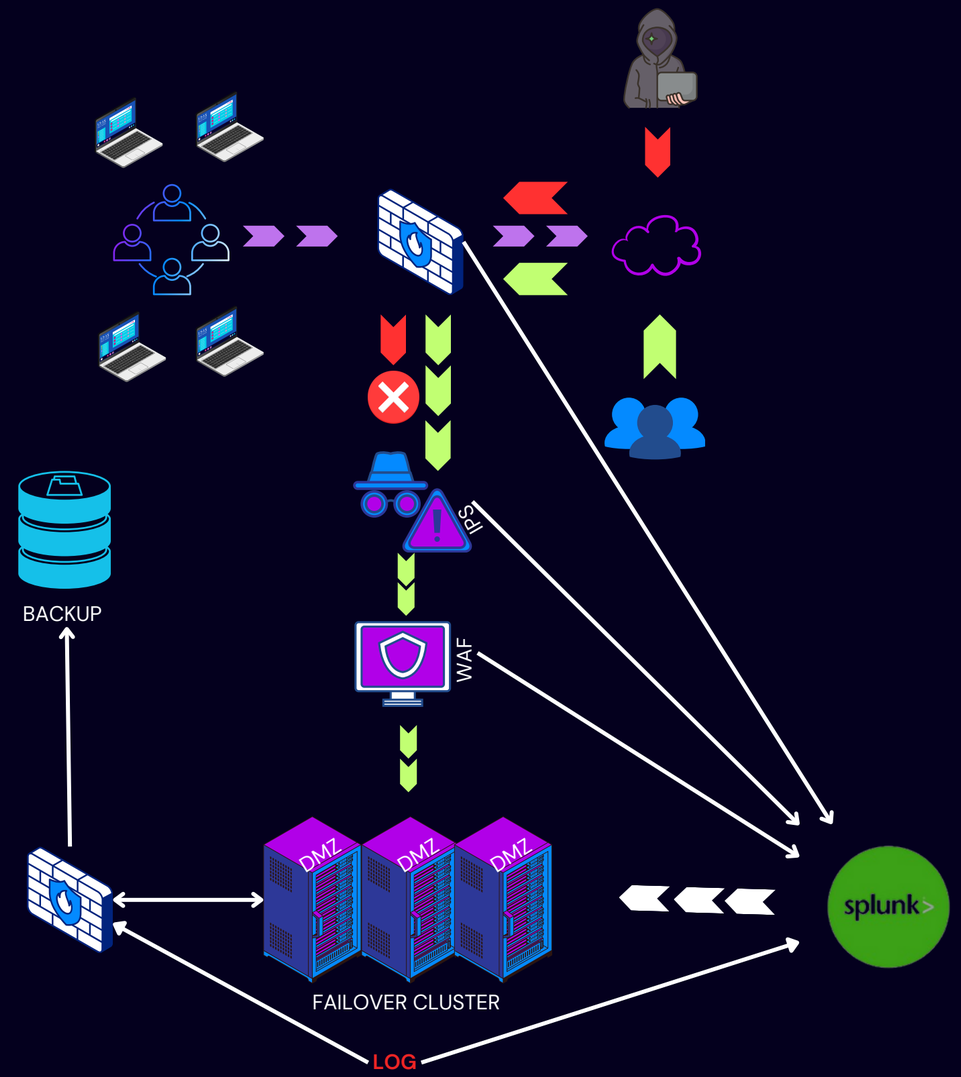
This is the proposed minimal network setup aimed at ensuring an acceptable level of security for the company system while also considering cost factors.

In addition to the previously justified implementations of WAF, IPS, more accurate firewall policies, and failover clusters in the DMZ, we have evaluated proposing two additional departments to enhance cyber attack mitigation and response efficiency and streamline system recovery times.

The first proposal involves introducing a dedicated server room for system data backup. We have observed that the response to the malware attack was particularly challenging due to the fear of losing important data.

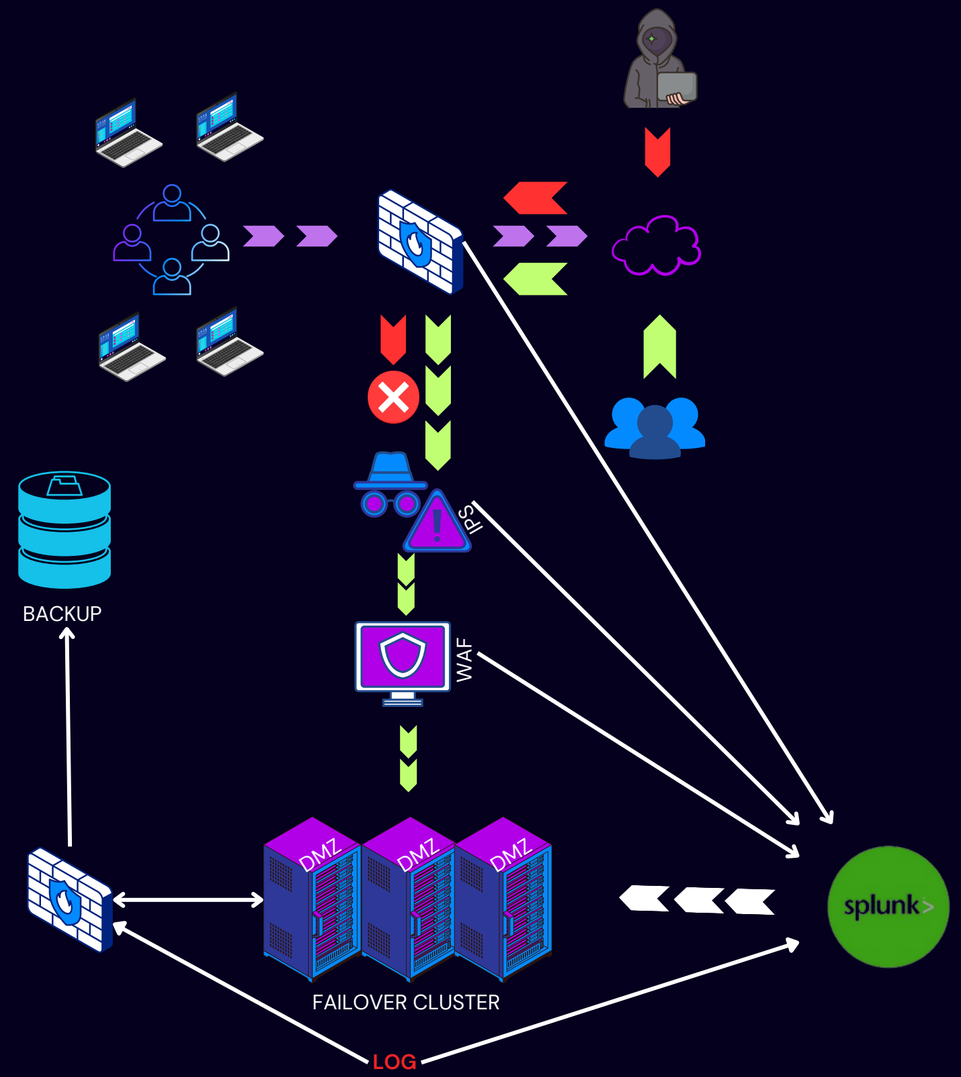
The solution entails an on-premise service (hosted on physical servers on-site), automated to perform an initial full backup (complete backup of the structure's data) and integrate it with a differential backup (adding missing data) on a weekly basis, away from service peak hours (to avoid slowing down usage).

The connection link between the DMZ and the dedicated backup server room must be protected by a firewall.



FINAL MINIMAL SOLUTION

A critical solution to implement promptly is the adoption of a SOAR (Security Orchestration Automation and Response) system. This automated system monitors real-time data flow across a network, collects endpoint logs, and configures alerts to signal potential threats instantaneously. Its primary function includes implementing workflows to automate response procedures to an attack, thus minimizing the time required to restore normalcy within the organization. Logs, detailing accesses to services or systems, are gathered through agents installed on endpoints and transmitted to the SOAR for analysis. The SOAR then decides, based on standard configurations, how to respond to a given event. It's also advisable to integrate the firewall, regulating the DMZ flow, with the SOAR to monitor the successful occurrence of weekly backups.



CONSIDERATIONS ON THE PROPOSAL

The network solution itself is optimal and aims to ensure peace of mind in delivering the e-commerce service. The internal network is also configured according to the required security standards and is not reachable by unauthorized external entities.

The costs of a solution like the one proposed are in line with the company's needs and, most importantly, cover what would be lost in terms of money by remaining exposed to attacks like those previously analyzed.

GENERAL CONSIDERATIONS

However, in the company's request for support, some fundamental aspects have not been taken into account.

First and foremost, we know that the most valuable asset for a company is its personnel. Therefore, the hiring of an IT team capable of performing routine tasks on the new installed devices (maintenance, updates) and on the services running in the DMZ should be strongly considered.

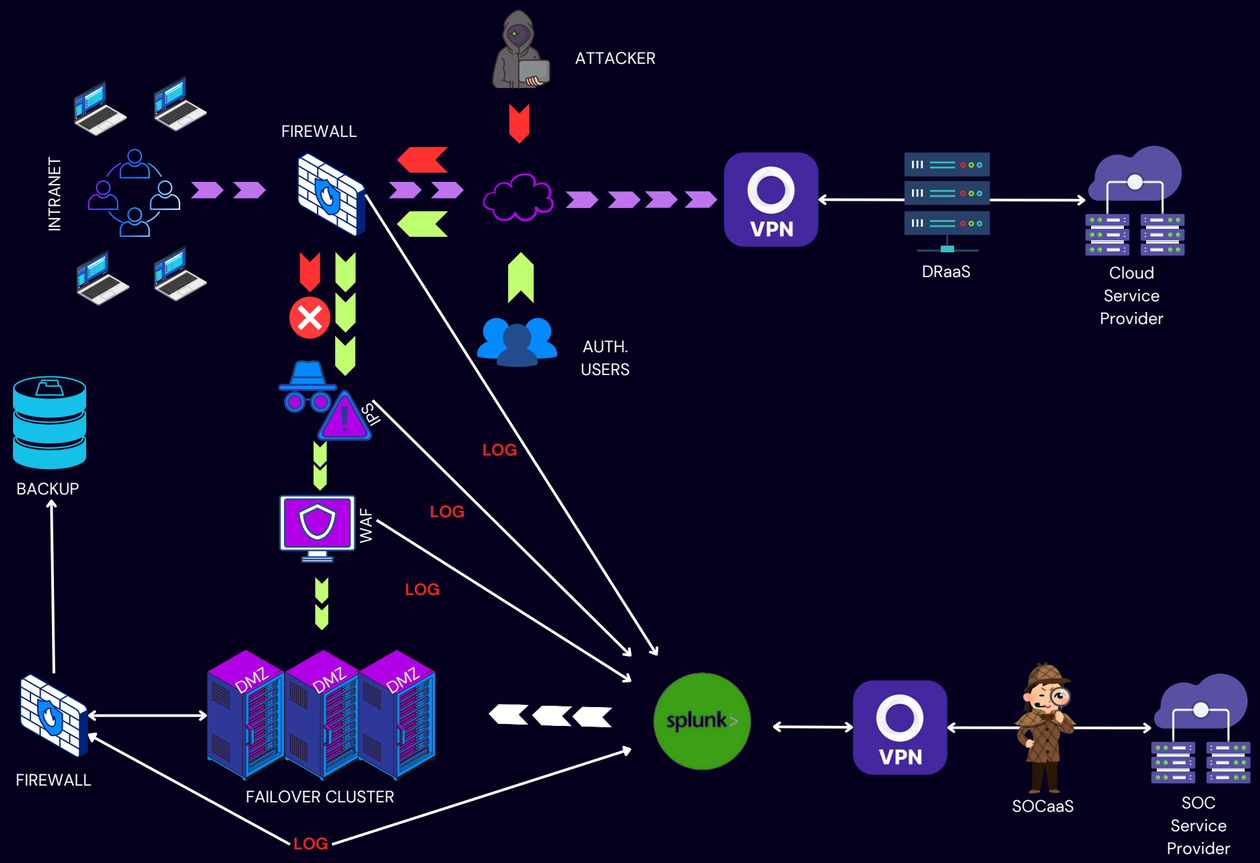
Furthermore, consulting with a physical security expert is essential to understand which physical access systems to configure in the envisioned new infrastructure

COMPLETE FINAL SOLUTION

The proposed final solution is much more comprehensive and also considers the possibility of outsourcing the management of SOAR (Security Orchestration Automation and Response) and backup services to external entities.

Premise:

In general, it is advisable to have an internal cybersecurity team or expert within the company. However, if the company operates in other sectors, it may still opt to outsource the management of certain services to a third-party firm. Nonetheless, drafting a BCP (Business Continuity Plan) by an internal team remains recommended to minimize impacts on the company's network. Additionally, it is pertinent to consider a significant statistic regarding cyberattacks: according to data from 2021, internal company employees are responsible for 84% of cybersecurity breaches. Strategies for addressing this additional threat will be explored subsequently.



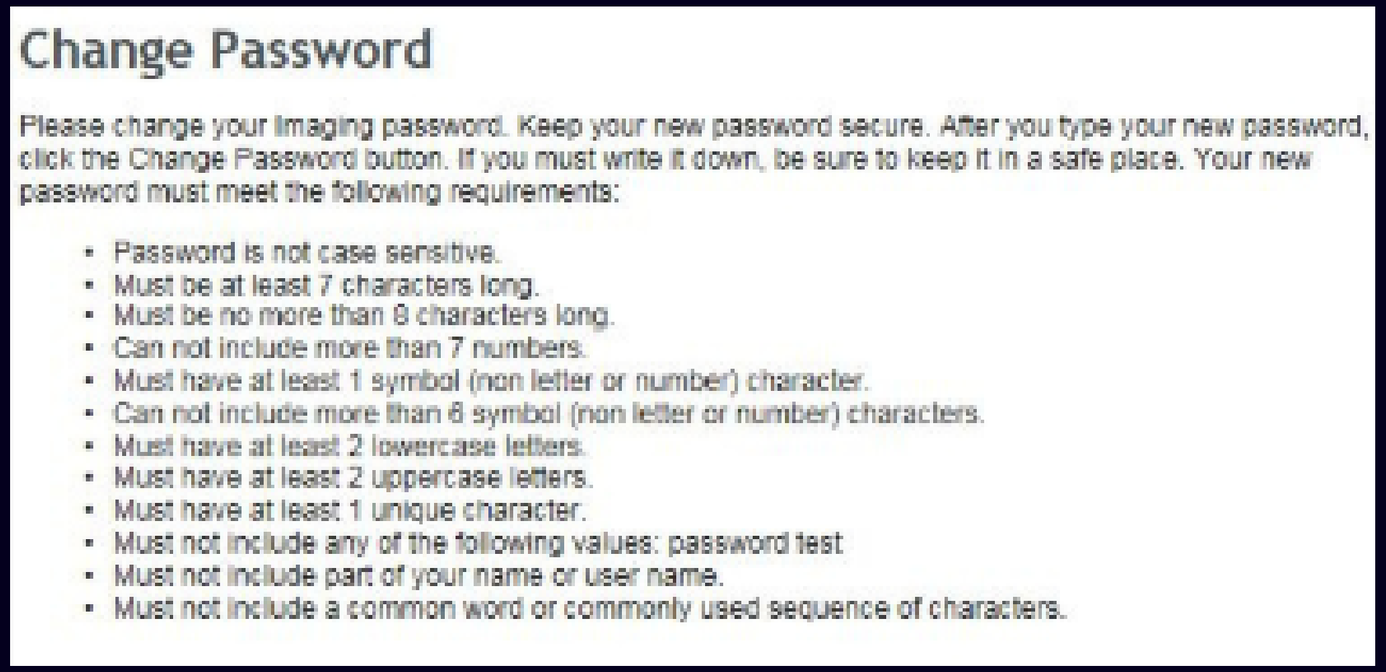
HONEYPOT

A honeypot is a hardware and/or software component that contains trap data intentionally placed in a traffic-free zone to deceive a malicious actor into believing they have accessed valuable data. In our case, it is positioned in a location isolated from the firewall but still leaving traffic open. The resource must remain reachable from any area of the network; this is indeed the primary security measure even towards internal employees. We will configure the firewall so that every time a user crosses that network segment, an alert is sent to the SOAR, which will automatically proceed to blacklist the user's IP, thus blocking them from continuing to explore the network.

AUTENTICATION

Let's then configure standardized accesses to the intranet. This will allow us to identify accesses from the intranet to other zones, although already highly restricted by the previously adopted policies. Additionally, it may be the responsibility of the cybersecurity department to assign secure credentials to each enabled user to prevent malicious actors from obtaining them.

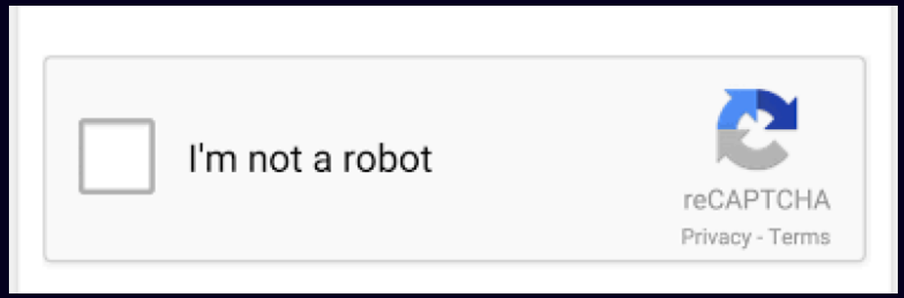
Moreover, we propose providing basic information on passwords for educational purposes to the staff.



CAPTCHA E BOT PROTECTION

Why Implement CAPTCHA Security on the Company's E-commerce Web App?
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a security measure known as Challenge/Response authentication. It protects users from spam and password decryption attempts by requiring them to pass a simple test proving they are human and not a computer attempting to breach a password-protected account.

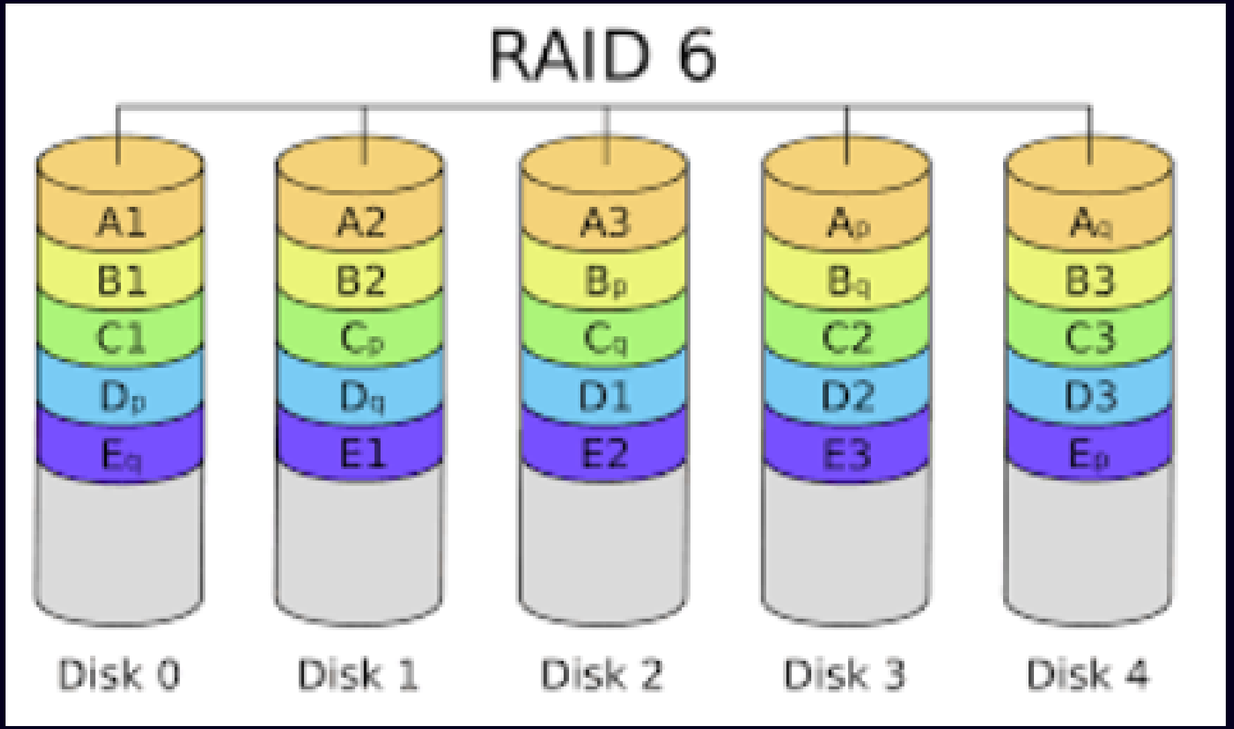
Implementing this security measure on the company's e-commerce web app serves a straightforward purpose: it renders a DDoS attack, such as the one previously experienced, ineffective since bots would fail to pass the test presented to them. Consequently, we preconfigure the network so that user addresses that fail the CAPTCHA for a certain number of attempts are automatically added to a blacklist by the SOAR after receiving the alert.



RAID 6

RAID stands for Redundant Array of Independent Disks, and as the name suggests, this technology is a combination of two or more disks working in parallel to provide a series of advantages. RAID 6, also known as dual parity RAID, is one of several RAID schemes that work by placing data across multiple disks and allowing input/output (I/O) operations to overlap evenly to improve performance and security.

For our backup service, we choose this solution because it can withstand up to 2 simultaneous failures.



DRAAS

Let's focus on the services that could potentially be outsourced to third parties.
The first one is undoubtedly DRaaS.
Disaster Recovery as a Service (DRaaS) involves replicating and hosting on physical or virtual servers by third parties to ensure failover in case of infrastructure damage.
It's provided by major Cloud Service Providers, who adhere to the 3-2-1 backup rule:
Three copies of your data: one in production and two backups.
Backups on two different mediums – such as network drives, external hard drives, and the cloud.
One of the backups is stored in a different physical location, or in the cloud.
In our case, the last point is already fulfilled thanks to the on-premise storage system located within the company.
This additional layer protects the company from both natural and man-made catastrophic events.
For data transportation, a VPN will be utilized, which is a virtual private network with encrypted tunnels, and the backup will be planned and synchronized with the physical one.

SOCAAS

SOCaaS, or Security Operations Center as a Service, reflects a service-based model that outsources parts of SOC functions to an external provider. A SOC (Security Operation Center) is a sub-department within the security department that provides services aimed at protecting computer systems. If the service is provided, some activities can be entrusted to the SOC service provider, such as:

Total management of the SOAR (Security Orchestration, Automation, and Response) platform.
Creation and management of effective intranet passwords.
Network attack mitigation.
Secure elimination and disposal of compromised disks using techniques like purge (overwriting and exposure to magnets) and destroy (overwriting and physical disintegration).
This solution is also more cost-effective compared to establishing an internal SOC within the company.

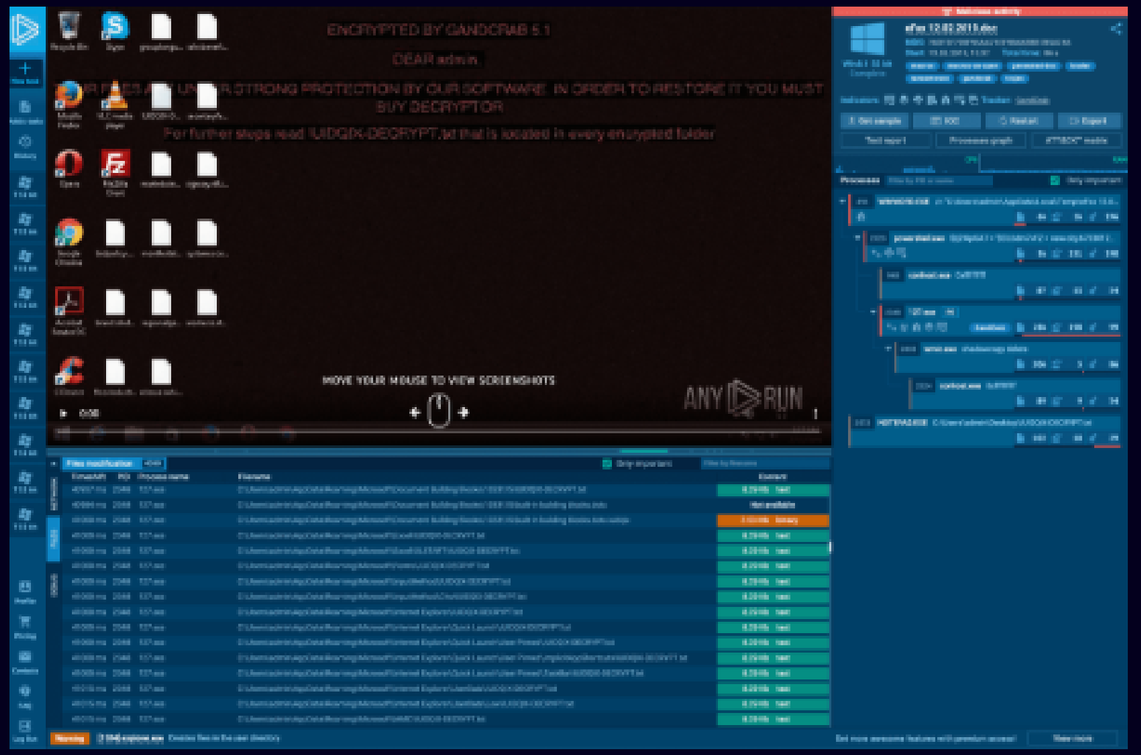
BONUS

We are requested to examine some reports uploaded to AnyRun and produce an explanatory report on the attack information, explaining to users and executives what type of attack it is and how to avoid these attacks in the future. You can consult the reports at the following links:

https://app.any.run/tasks/%20%20%208e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/%20
https:/app.any.run/tasks/%20%20%2060b9570f-175b-4b03-816ba38cc2b0255e/

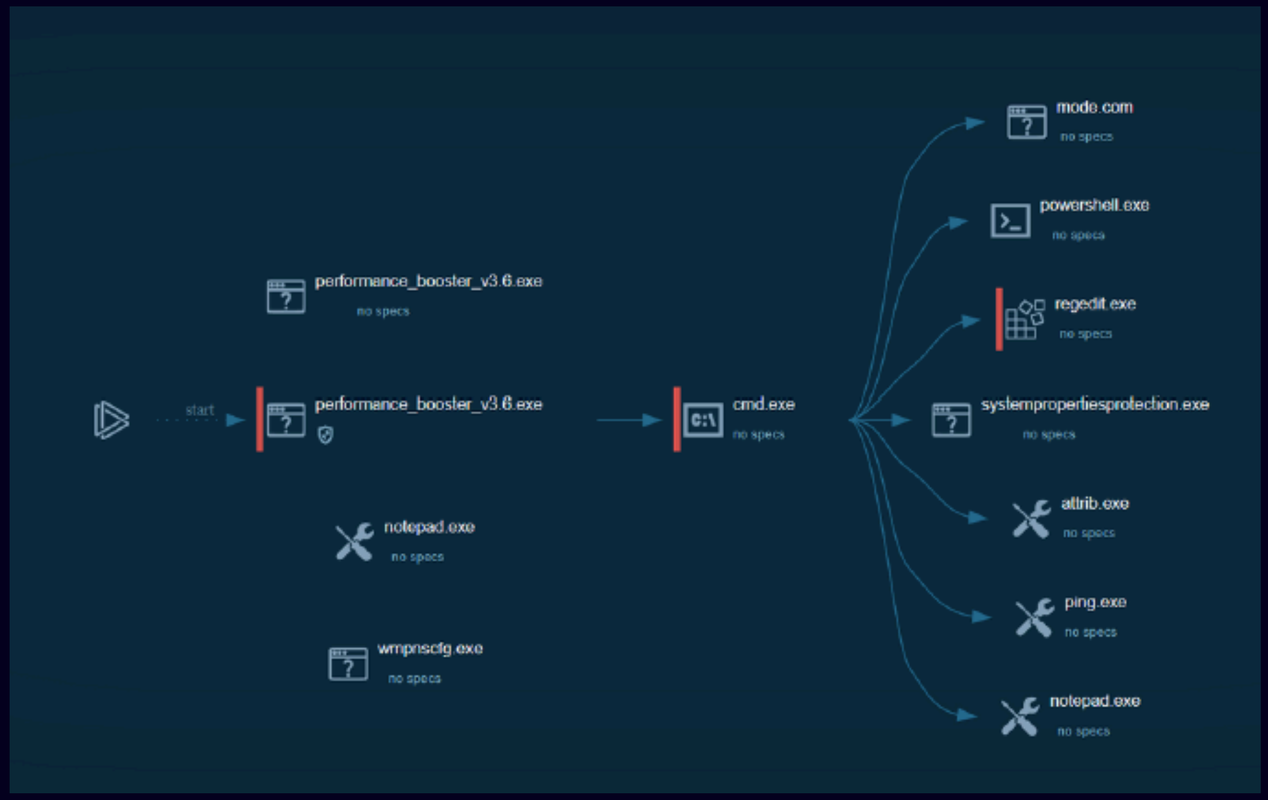
ANYRUN

ANY.RUN is a tool for real-time detection, monitoring, and investigation of computer threats. It is a sandbox, which is a sterile environment consisting of a virtual machine isolated from the rest of the computer, where potentially harmful software can be executed without risking damage to the computer or network. The virtual machine is created in the cloud, and within it, any file can be uploaded simply by selecting it from the user's terminal and uploading it to the VM. Once the execution is complete, the program details all the changes made to the virtual system, presenting them to the user.
Next to us, we see the graphical interface of the software.



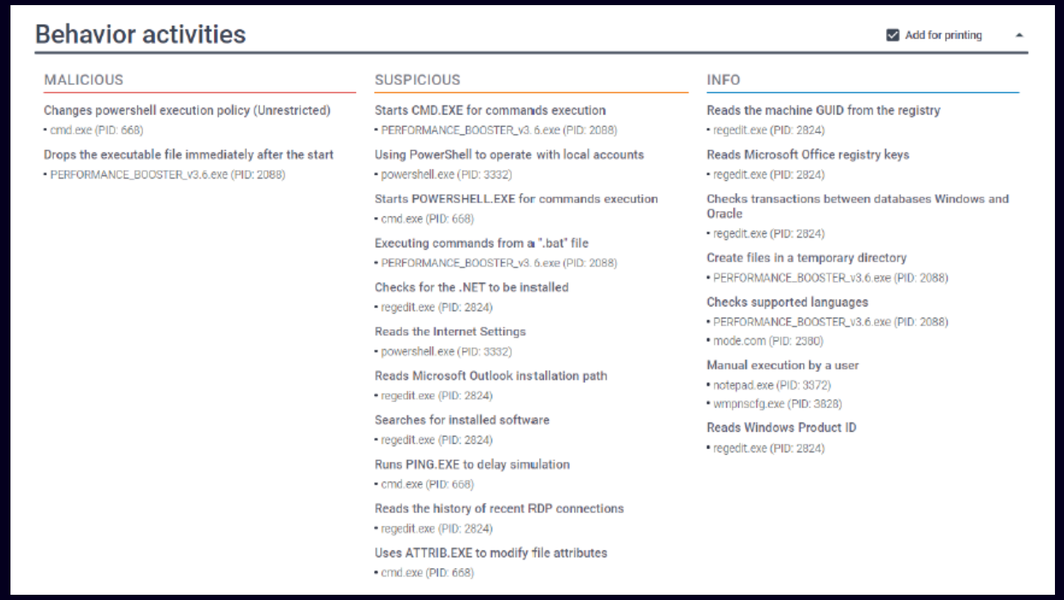
MALWARE 1

Let's open the ANY.RUN link that takes us to the report of the first threat.
The file under analysis is titled "PERFORMANCE_BOOSTER_v3.6.exe."
From initial analysis, one would think it's an executable file.
In the "Graph" section, we can consult the graph of the behaviors exhibited by the program during its execution.

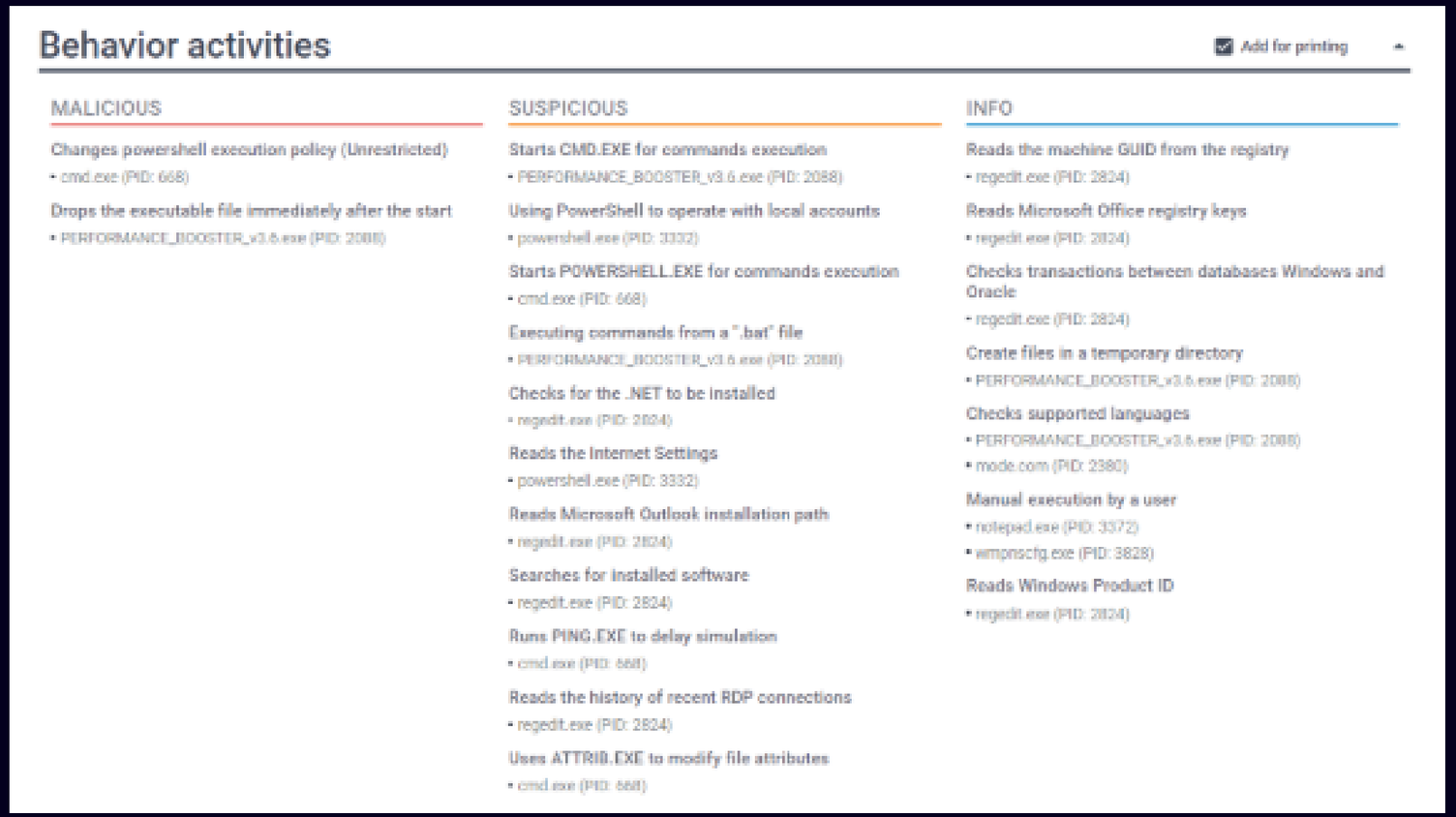


DESCRIPTION

Let's consult the report on the program's behavior detailed by ANY.RUN. We notice that 2 execution steps of the program are definitely malicious behaviors: after the start, indeed, the executable file is discarded, a symptom of intentions different from those declared, and after opening PowerShell (the Windows terminal), the file execution policy is changed, probably looking for one without restrictions (for example, "set-executionpolicy unrestricted").



Among the behaviors considered suspicious, we find some that confirm the maliciousness of the examined file. For example, the section "Reads Windows Product ID regedit.exe (PID: 2824)" indicates that the code attempted to retrieve the product key of the operating system. Similarly, in the case of "Reads the history of recent RDP connections regedit.exe (PID: 2824)," it can be understood that the file is seeking information on recent Remote Desktop Protocol (RDP) connections. Therefore, we can classify this file as a Trojan.



HOW TO DEFEND AGAINST TROJANS

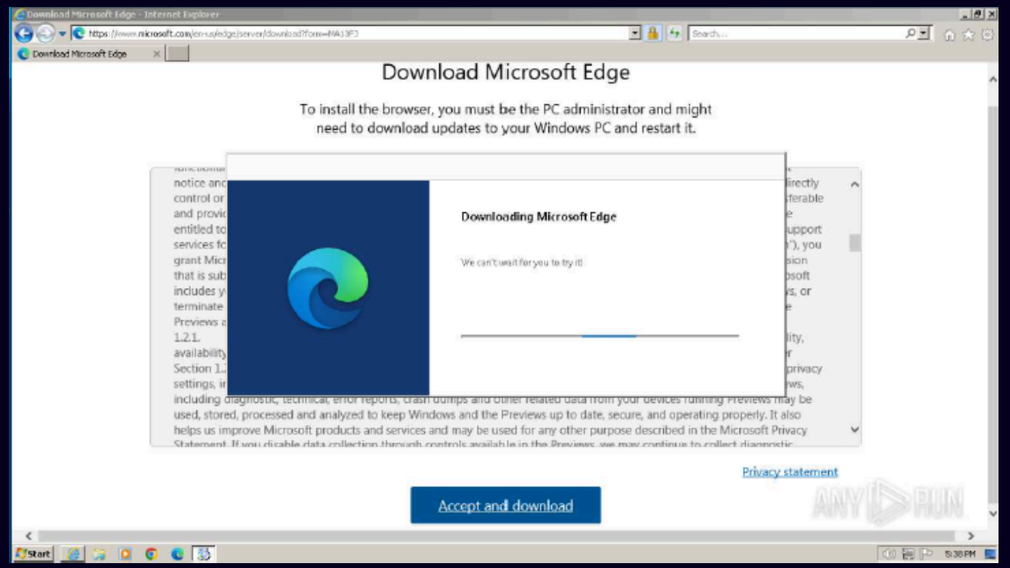
Below are some best practices useful for avoiding infection by a Trojan:

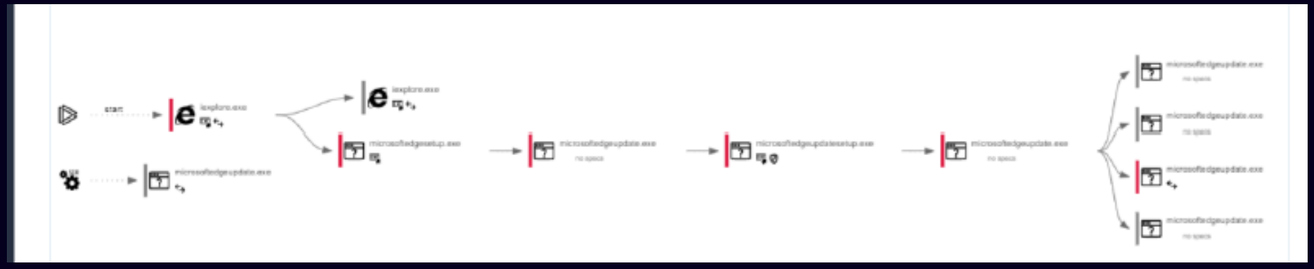
Install a reliable antivirus system.
Perform regular scans.
Update the operating system whenever updates are notified.
Also update installed software and applications.
Protect each account with complex and unique passwords, remembering to update them periodically.
Protect information using a firewall.
Regularly backup data.
Exercise extreme caution with email attachments.
In addition to good habits to follow, it is also important to know what actions not to take:

Do not browse unsafe websites (stick to sites with the HTTPS protocol).
Do not open links or download email attachments from unverified sources.
Do not download software or apps from unknown or unreliable manufacturers.
Do not click on pop-up windows inviting you to install free software.

MALWARE 2

Let's open the second report provided by ANY.RUN: from the screenshots, it might appear to be a simple update of the Windows Edge browser. However, the URL from which it originates does not seem to belong to an official Microsoft source. Let's examine the behavioral graph available in the report; we immediately realize that the file is malicious, as several actions are categorized as malicious or suspicious.
Upon further analysis, we can affirm that the malware is downloading harmful files from a remote server with the intent to disrupt the regular flow to the internet and slow down the system's functioning.





BEST PRACTICE CYBERSECURITY

For an organization, it's crucial to be aware of the best practices for handling critical situations in cybersecurity. The previously analyzed case is a typical example of inadequate staff training. Indeed, an employee downloading an obviously unreliable update can be extremely detrimental to the company itself. It's a good practice to distribute playbooks upstream of such incidents concerning the proper management of update installations to prevent the recurrence of such situations. Additionally, each machine should be equipped with antivirus software, aimed at preventing, detecting, and potentially neutralizing harmful code and malware for a computer. This would have allowed the threat to be identified before it could make changes to the machine and removed it easily.