ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable the European Industry to Overcome the Shortage of Cybersecurity Professionals,

No. 2020-1-RO01-KA202-079983

O3: Documental battery on cyber-attacks

Co-funded by the Erasmus+ Programme of the European Union

CONTENTS

INTRODUCTION

With the advent of IT and in the rise of the fourth industrial revolution, businesses are facing new challenges connected to cybersecurity and data protection. This is especially valid for production SMEs which often don't have the internal resources and capacity to effectively evaluate cybersecurity risks corresponding with newly implemented Industry 4.0-based technologies. At the same time, SMEs are more often becoming victims of various cybercrimes. According to the latest Verizon 2021 Data Breach Investigations Report *(Verizon, 2021)*, SMEs are victims of and are much more vulnerable to cyber-attacks compared to big enterprises as they lack resources, people, information and general capacity to avert the risks of a cyberattack.

Meanwhile, cyber threats have varying sources and are becoming increasingly sophisticated, for instance and if the teams have not experienced similar vulnerabilities and lack a clear guidance on how to respond to them, it may take days and even weeks to react properly, which can be fatal for some manufacturing processes. According to the 2021 SMB IT Security Report employees who don't follow guidelines are considered as the top barrier to cybersecurity and this tendency has worsened with the increase of remote work due the COVID-19 pandemic *(Untangle, 2021).* However, when there is a cybersecurity breach, it doesn't impact only people, it might as well cause financial losses, loss of customers' trust and damaged reputation *(Acronis, 2021).*

Taking into account the aforementioned, Encrypt 4.0 consortium has developed this document to serve as a know-how tool giving access to critical analysis of real cyber-attacks and lessons learnt as well as roadmaps on how to prevent, identify, tackle and recover from them.

The Encrypt 4.0 Documental battery on cyber-attacks is specifically tailored to the needs of EU manufacturing SMEs operating in the Industry 4.0 context and represents a compilation of case studies on cyber-attacks which is aimed at supporting SMEs in boosting their cybersecurity and preventing cyber-attacks.

STRUCTURE & METHODOLOGY

The Encrypt 4.0 Documental battery contains a total of **18 case studies**. Each of the ENCRYPT 4.0 partners has developed 3 real cyber-attack case studies based on desk research, personal experience and observations and in-depth interviews with CEOs, cybersecurity professionals, and IT specialists that cover various types of cyber-attacks and provide critical analysis of the reasons for the security breaches, how they were tackled and what the consequences were.

The ENCRYPT 4.0 consortium has built a specific model "PREVENT-IDENTIFY-RESPOND-RECOVER" (PIRR) based on the "Identify, Protect, Detect, Respond and Recover" model of the National Institute of Standards and Technology (NIST). The type of the cyber-attacks is based on the STRIDE model[1] as well as the MITRE ATT&CK framework. The PIRR model analysis contains 4 main categories/ sections based on the major steps for battling a cyber security issue as well as lessons learnt sections (see Fig. 1.).

Fig. 1. "Prevent – Identify – Respond – Recover" (PIRR) model categories

[1] You can read more about STRIDE model here:

- Benjamin, P., 2018. Demystifying STRIDE Threat Models [online]. DEV Community. Available at: https://dev.to/pbnj/demystifying-stride-threat-models-230m;

PREVENT

This section is focused on reducing the risk of exposure to cyber-attacks and preventive measures and for each case study includes the following:

- Specific security practices set in place that had proven effects in real cyber-attacks;
- Cyber security misconceptions: practices that each company applied and had zero or even negative impact in actual incidents.

IDENTIFY

The main aim of this section is to help SMEs distinguish between the different types of cyber attacks categorized using the STRIDE model and the MITRE ATT&CK frameworks. The STRIDE model represents a system-centric high-level threat model focused on identifying overall categories of attacks. It has the following 6 categories:

+Spoofing

+Tampering

+Repudiation

+Information disclosure

+Denial of service

+Elevation of privilege

For the purpose of the ENCRYPT 4.0 case studies STRIDE was used to identify the threats on higher level, whereas the MITRE ATT&CK framework was applied to specify the attacks in more detail. The ATT&CK framework intentionally takes an attacker's point of view to help organizations understand how adversaries approach, prepare for, and successfully execute attacks.

RESPOND

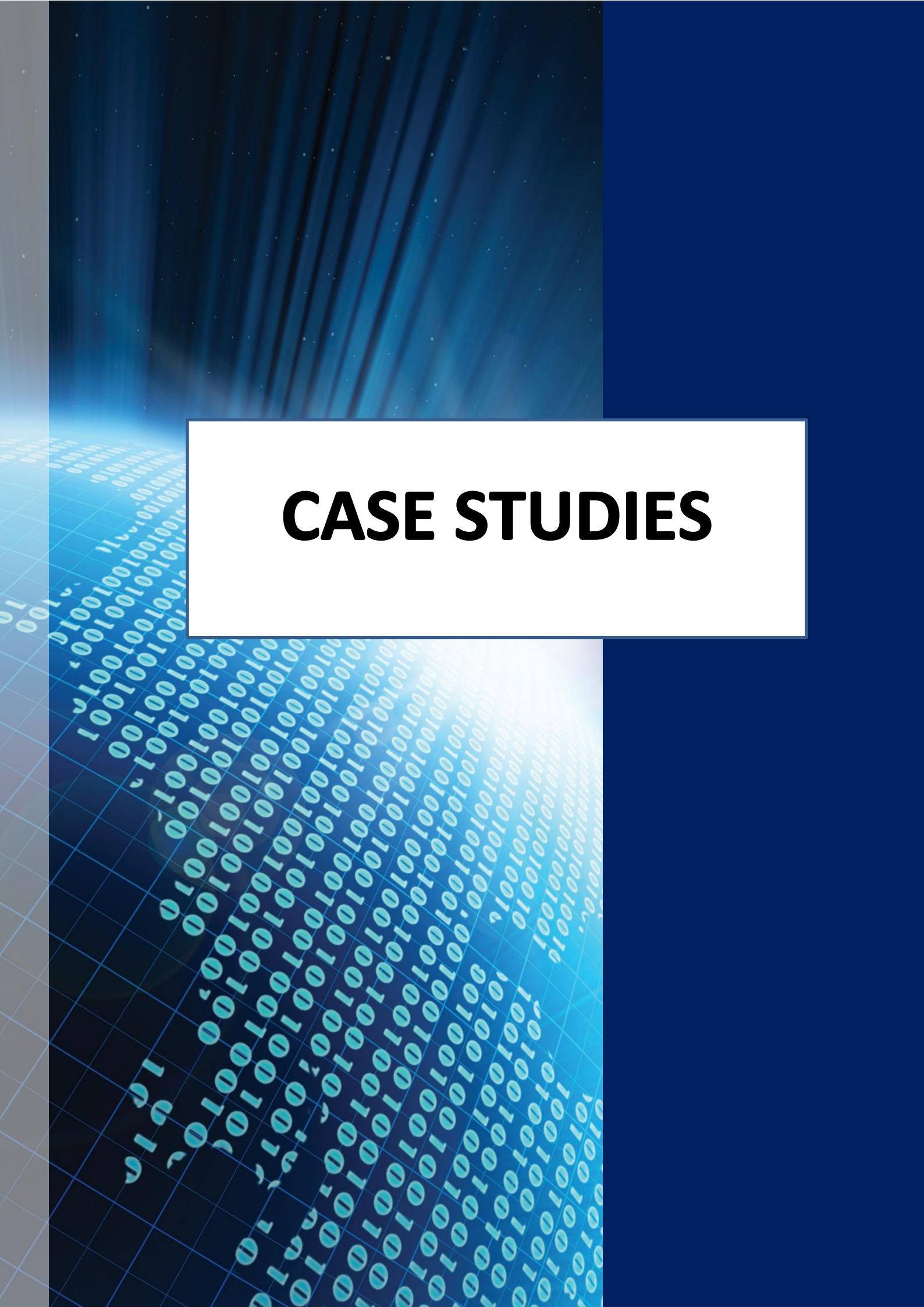
This section depicts the situations in which the threat is already present, providing analysis of real cyber-attacks and advice on how to react in similar cases after identifying them.

The cyber attacks within the case studies are outlined in the following format:

- WHO: the attacker
- WHOM: the target organisation
- WHY: the motives behind the attack (was it random or targeted)
- WHAT: the targeted property
- HOW: description of the attack and what were the techniques used.
- STRATEGY: how was the threat tackled and the measures that had zero or negative effect.

RECOVER

The section provides information on what were the consequences of the attack as well as analysis on how to perform a system recovery after some processes have been damaged and regain access to data that was lost, based on the real attack cases described in section RESPOND. The section follows the STRIDE & MITRE ATT&CK models outlining recovery practices based on each specified group of cyber threats presented in IDENTIFY section.


CASE STUDIES

CASE STUDY 1: THE REVERSE SHELL

THE TARGETED ORGANISATION

Innovalia Association is a private and independent technological centre that was created by Innovalia Group in order to articulate a critical mass capable of successfully achieving its long-term research ambitions and strategic objectives. Innovalia is an alliance for technology-based SMEs with headquarters in Spain. It has an international presence with offices in Basque Country, Madrid, Catalonia, Canary Islands, Europe, Asia, the Middle East, and Central and South America. Since its foundation, Innovalia Association has developed a special sensitivity for and awareness of the particular characteristics of technology-based SMEs. Today, it has become a leader in the R&D area by and for SMEs in Spain. It also offers solutions for facilitating international innovation processes aimed at SMEs. As a technological agent of the Basque Country Technology Network (Innobasque), Innovalia brings together the skills, laboratories and resources of the companies that founded the association.

"Command injection is a cyber attack wherein an attacker takes control of the host operating system by injecting code into a vulnerable application through a command. This code is executed regardless of any security mechanism and can be used to steal data, crash systems, damage databases, and even install malware that can be used later". (StackHawn, 2022)

HOW INFORMATION WAS ACQUIRED?

The information for this case study was gathered through in-depth interview with IT technician of the enterprise. During the interaction the interviewer posed initial questions, so that the respondent is encouraged to answer. The missing information was completed a posteriori with the data provided by the person interviewed.

PREVENT

The practice that Innovalia applied before the incident was the installation of a **firewall software**.

Specific security practices:

- ☑ **the awareness of employees about untrusted mails**. In this case, a hacker sent a seemingly legitimate email asking our employees to click a link in the mail to reset the access password, on the pretext that several unsuccessful login attempts had been registered.
- ☑ **the installation of internal firewalls** to reinforce their standard external firewall. When staff worked from home during the COVID-19 pandemic, they were required to install a firewall on their home network.

IDENTIFY

The type and nature of cyber-attack was: **Code injections into a vulnerability in the company's apache web server through remote command execution**. This type of attack can be described in detail according to the MITRE ATT&CK framework, as shown below.

- ☑ Reconnaissance: Active Scanning: Scanning IP Blocks and Vulnerability Scanning
- ☑ Initial Access: External Remote Services
- ☑ Execution: Command and Scripting Interpreter: Power Shell
- ☑ Privilege Escalation:
  - Process Injection: Dynamic-link Library Injection; Portable Executable Injection; Thread Execution Hijacking; Asynchronous Procedure Call; Thread Local Storage; Ptrace System Calls; Proc Memory; Extra Window Memory Injection;
  - Event Triggered Execution: Unix Shell Configuration Modification,
- ☑ Defence Evasion: Process and template Injection
- ☑ Exfiltration: Transfer Data to Cloud Account.
- ☑ Impact:
  - Data Manipulation: Stored, Transmitted and Runtime Data Manipulation
  - Service Stop
  - System Shutdowm/Reboot

RESPOND

- ☑ **WHO:** The attacker could not be precisely identified. Only the place of origin, China, was known.
- ☑ **WHOM:** Innovalia Association
- ☑ **WHY:** It was random
- ☑ **WHAT:** System of the organization Innovalia
- ☑ **HOW:** Process injection with remote command execution.
- ☑ **STRATEGY:** The threat was tacked with the firewall that the server had at that moment. Follow the steps described in the following section, on how to block IPs

RECOVER

The main consequences of the attack were:

- ☑ System compromise
- ☑ Research and Analysis
- ☑ Update of server version
- ☑ Change credentials

The **recovery strategy** was focused on blocking the IP through the firewall:

First of all, log in to the server on which you need to block the IP address. Then, click Start, type Windows Firewall with advanced security, and press Enter. In the left-hand pane, click Inbound Rules to show the currently configured rules in the middle pane.

In the right-hand pane, click Actions >New Rule: For Rule Type, select Custom and click Next; for Program, select All programs and click Next; for Protocol and Ports, select Any from the Protocol Type dropdown and click Next; and for Scope: under Which remote IP addresses does this rule apply to?, select the radial option: These IP addresses: Click Add.

Then, enter the IP address that you want to block from the server and click OK. You can also choose to block a range of IP addresses by selecting the This IP address range: radial option. After you finish adding the IP addresses, click Next. For Action, select Block the connection and click Next. For Profile, leave all options checked and click Next. For Name, give the rule a descriptive name, such as Blacklisted IPs. You can also enter an optional description of the rule. Click Finish. The newly created rule with the given name now displays in the middle Inbound Rules pane. To order the rules alphabetically by name, you can click on the Name column header. If you need to disable the rule, right-click on the rule in the list and click Disable Rule. If you need to modify the scope of IP addresses for the rule, right-click the rule in the list and click Properties. Then click the Scope tab, make necessary changes, and click Apply.

LESSONS LEARNT

We learned that it is better to have certain preventive and defensive measures, which are useful for this type of attacks, such as:

- ☑ To keep the server updated
- ☑ To add monitoring to the server machine
- ☑ To segment the network into VLANS, and
- ☑ To isolate machines that are exposed to the outdoors.

CASE STUDY 2: THE RECKLESSNESS OF AN EMPLOYEE

PREVENT

The organisation applied Intrusion Detection System (IDS), which monitors the CARSA's network for malicious activity or policy violations. CARSA applies firewall software to protect their network and system from unauthorized access.

Specific security practices set in place that had proven effects in other cyber-attacks are:

Validate and sanitize inputs: Scan for escape characters and other special symbols for the application language and operating system, such as comment marks, line termination characters and command delimiters. If the application only expects a limited set of values, accept only those values, for example by whitelisting or conditionally switching on them.

Avoid vulnerable evaluation constructs: we avoid using "eval()" and equivalent functions on raw user inputs. CARSA used dedicated language-specific features to safely process user-supplied arguments.

Lock down the interpreter: If you have control over the server configuration, it is better to limit interpreter functionality to the minimum required for the application to prevent escalation to system command injection. For example, if your PHP application doesn't use the system() function, you can disable that function in your php.ini file by specifying it in the disable_functions directive. Commonly disabled functions for PHP include: exec(), passthru(), shell_exec(), system(), proc_open(), popen(), curl_exec(), curl_multi_exec(), parse_ini_file(), and show_source().

Check our code: CARSA used static code checking tools to scan for vulnerabilities related to input validation and unsafe evaluation.

Scan the applications: the organization used a scanner to ensure that the applications are safe from various types of attacks. For example, CARSA has an Intrusion Detection System.

"In 2021, 83% of organizations reported experiencing phishing attacks. In 2022, an additional six billion attacks are expected to occur." (CyberTalk, 2022)

IDENTIFY

The cyber-attack occurred within CARSA, and the type of cyber-attack was '**phishing attack**'. The phishing attack is a type of social engineering attack often used to steal user data, including login credentials.

According to the STRIDE model, this type of attack has as „Threat" the elevation of privilege, because the property violated is the „authorization". In this type of cyber-attack, user allows someone to do something they are not authorized to do.

According to the MITRE ATT&CK framework, this attack is:

☑ Reconnaissance: Phishing for information: Spearphishing service, spearphishing attachment and spearphishing link.

☑ Initial Access: Phishing: Spearphishing Attachments, link or via Service.

☑ Execution: Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

☑ Discovery: the detection could be made through: Application Log (content), the file (file creation), or the network traffic (content or flow)

☑ Lateral Movement: Internal spearphishing

☑ Exfiltration: Social Engineering and Phishing Attacks; outbound mail, downloads to insecure devices, uploads to external services and insecure cloud behaviour

Impact: loss of sensitive data, reputation damage, client or customer churn, cost of downtime, etc.

RESPOND

WHO: The attacker was an unknown external person/organization, through a CARSA employee.

WHOM: The credentials for access to a payment (no public or open-source) software.

WHY: The theft of credentials as well as sensitive entity information.

WHAT: Data and passwords

HOW: An employee installed software that was not allowed by the company as defined in the company policy. This type of software wasn't allowed because of dubious reliability and security. (Generally, all software that is installed on employees' computers must be supervised by the entity's computer technical staff.) This software had a network "Trojan" horse. there are several ways in which a Trojan attacks a system, in this particular case, it was an "infostealer trojan", as it sounds, this Trojan is after data on your infected computer.

STRATEGY: The strategy followed was to trace the mac address to identify the infected machine and the employee responsible. Later, the software was removed as well as the virus.

RECOVER

IMPACT: theft of user credentials at the local level

RECOVERY STRATEGY:

☑ Through the MAC address we knew which employee was being attacked, without him even realizing it.

☑ software was uninstalled that should not have been installed

☑ an antivirus and antimalware programs were run on the specific machine.

☑ Changed compromised user credentials

BETTER STRATEGY: the entire computer could have been formatted because you can never be sure of its complete elimination.

LESSONS LEARNT

To increase employee accountability through:

- ☑ training with short lectures on the importance of not installing unannounced software and security confirmation from the technical support team and,
- ☑ remembering the company's security policies and common safety regulations in cybersecurity.
- ☑ To update the software of the company's machines (software: windows and antivirus programmes). To remind employees to run the anti-virus scan several times.

CASE STUDY 3: THE CREDIT CARD IN A SMES VIA WIFI NETWORK

THE TARGETED ORGANISATION

Bodegas Monje is located in an exceptional enclave of the island of Tenerife, in the place known as "La Hollera" in the municipality of El Sauzal overlooking the Teide. A long tradition of wine producers accompanies the Monje family since 1750. Oak barrels and modern maceration systems coexist to give red, white and rosé wines a special character and flavors, which are perfectly adapted to the best gastronomy of the Canary Islands. This winery also hosts cultural, gastronomic and leisure initiatives that expand the boundaries of wine and return it to the social environment from which it historically comes, a true commitment to wine tourism: Wine&Tours.

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was an in-depth interview.

PREVENT

The organisation did not apply any cybersecurity practice before this event. They only have a firewall in the Internet Service Provider (Router Movistar).

The specific security practices set in place in Bodegas Monje that had proven effects in the prevention of this kind of event were scheduled after the event. In particular, the actions taken were successful in preventing further attacks of a similar nature.

IDENTIFY

A customer of the establishment accessed the company to consume the manufactured products, and connected to the internet through the WIFI network. The cyber-attack was identified by the affected customer himself. This person detected movements in his bank accounts with online payments made with his credit card but not by him. All these movements were done just after he visited the company “Bodegas Monje”.
The customer alerted the bank to try to cancel those payments and block the card to prevent the cybercriminal from continuing to use it.
Afterwards, he notified the company “Bodegas Monje” as it was the last place where he actually used it.

RESPOND

WHO: a company's own customer who accessed the local network for illegal purposes.
WHOM: to another customer, through the company**.**
WHY: for stealing money
WHAT: to misappropriate bank details and make charges, benefiting from someone else's money
HOW: infiltration through the clients' Wifi network
STRATEGY: Redesign the network to separate the connection of customers visiting the business from the payment system and the company's internal network.

RECOVER

IMPACT:

- ☑ The credit card of a customer of the establishment compromised
- ☑ The customers' confidence in the company's security could be compromised and they would not be able to rely on making payments by this method so easily
- ☑ If more customers were be affected by this cyber-attack, it would impact directly in the company's reputation.

RECOVERY STRATEGY:

The strategy carried out by the owner of the company, from the moment he became aware of the incident, was to turn off the wifi and/or disconnect the guest network. Then, he contacted a cybersecurity company to solve it.

The new recovery strategy done by the cybersecurity team was to redesign the network to separate the customer network from the company's internal network where the most sensitive data (employees' and customers' own data, such as payment system data) is stored.

No money stolen could be recovered after the network was redesigned. The customer had to change the old credit card "stolen" by another new one. The person who carried out the cyberattack could not be identified. No legal actions could be taken.

There is a better strategy to be undertaken in this situation. Instead of disconnecting the company's wifi network, this could have been done in addition:

- ☑ To make a list of all compromised information, with all data contact of the possible customers that could be affected (by timeline – of who were in the enterprise at the same time that the affected customer).
- ☑ To inform other customers to be aware of any strange movements in their bank accounts made with online payments done with their credit card.
- ☑ To collect as much information as possible to not only be able to identify the culprit of the cyber-attack, but also to better warn customers who might also be affected.

To change passwords immediately to avoid a sudden shutdown of the company, because at that moment, the network was not split, it worked for customers and for employees at the same time.

LESSONS LEARNT

Among the lessons learned, the following stand out:

- ☑ that it is better to have the network segmented
- ☑ that zero-trust policies must be implemented
- ☑ that you don't need to be a big company to suffer a cyber-attack

that it is necessary to have up-to-date equipment and active cybersecurity systems (with a professional firewall, IPS, antivirus, etc.).

CASE STUDY 4: INFORMATION DISCLOSURE HANESBRANDS INC.

TARGETED ORGANISATION

Hanesbrands Inc. (HBI) is a multinational clothing company founded in 1901 and based in Winston-Salem, USA. They have over 250 outlets in 47 countries. Amongst the company's most famous brands are Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold, Celebrity, Maidenform, Zorba, etc. One of the competitive advantages of Hanesbrands is that 70% of the apparel they sell is manufactured in their own premises as well as in partner contractor's ones. In this way, the company manages to control the majority of the supply chain which also allows for establishing strong sustainability practices and contributes to its worldwide success. In 2021, HBI was named one of the World's Most Ethical Companies by Ethisphere and became a part of Barron's 100 Most Sustainable Companies three years in a roll. To ensure that the company is following a long-term policy of sustainability, it has set 2030 global sustainability goals (in line with United Nations' Sustainable Development Goals under three pillars: People, Planet and Product) and started a sustainability website.

In 2019 the company had revenue of $7.0 billion and around 61 000 employees. It is reported that HBI is spending over $100 000 for cyber security, mainly using Akamai products such as cloud services.

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was desk research, the specific information sources can be found in the References section of this document.

PREVENT

☑ **Practices that had zero effect:** Authentication on the website - In order to track his/her order of clothing, the user received a link to log in as a guest onto the website. The guest user had extensive rights to obtain information for the orders made by all other users just by altering the guest URL. Therefore, the database was compromised through the website since it did not ask for authentication and considered the guest user a valid user. The data visible for other clients consisted of names, last digits of their credit cards, address, phone number, etc.

"According to a new report by Blumira and IBM, the average breach lifecycle takes 287 days, with organizations taking 212 days to initially detect a breach and 75 days to contain it." (VentureBeat, 2022)

☑ **Practices that had proven effects in real cyber-attacks of this type:**

1. Discovery of data exposure (using external scanning systems).
2. Strong authentication (Single sign-on allowing a user to sign in in several different systems or different usernames/passwords for each system).
3. Prioritization of data access (e.g., HR may only need access to employee information and the accounting department may only need access to budget and tax data. Guest users should have minimal data access in principal).
4. Deployment of monitoring infrastructures and automated solutions that can quickly identify potential problems before they become emergencies, isolate infected databases, and flag to support and IT teams for next steps.

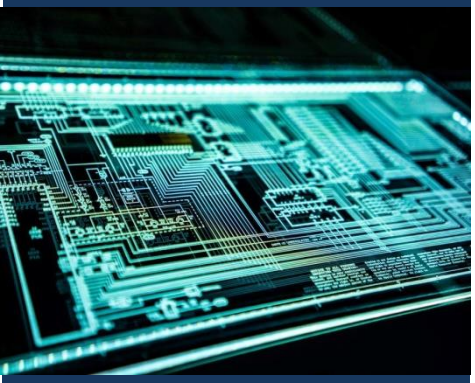
IDENTIFY

The attack against Hanesbrands Inc. was of **Information disclosure type**.

In the last week of June and the first of July 2015 Hanesbrands Inc. was a victim of cyber-attack. After the data was stolen the company got informed by the adversaries about the breach without giving a motive for their action. It is very probable that the company's weakness was discovered by scanning[1]. The hackers created "guest" check-out order on Hanesbrands website[2] (without even registering on the website). With the order link received the hackers managed to drain company's database that was responsible for holding data for all customers orders (orders that were

made on their website or through the phone) – as it turned out the "guest" check-out link was able to access every other order without authenticating. In a week's time adversaries managed to get information for over 900 000 customers. In order not to be detected hackers most probably used Port Knocking[3] in order to hide their activity. As per Hanesbrands, the adversaries used Screenshots[4] to extract the data, however it is very probable that they used more automated way – such as script that will parse the data directly[5].

The attack described by MITRE ATT&CK framework:
[1] Active Scanning: Vulnerability Scanning (T1592.002).
[2] Initial Access: Exploit Public-Facing Application (T1190).
[3] Persistence: Traffic Signalling: Port Knocking (T1205.001).
[4] Screen Capture (T1113).
[5] Automated Collection (T1119).



The attack was identified by the company after it was notified by the adversaries. Hanesbrands was not aware that this was happening until the hackers let them know.

RESPOND

On June 2015 Hanesbrands Inc. got informed by the adversaries about the breach. Through guest account on their website, the attackers managed to extract general user information for 900,000 customers. After being notified about the leak, Hanesbrands added authentication to their "customers' orders" database and removed the "guest check-out" option (even though they fixed it).

WHO: Unknown.

WHOM: Hanesbrands Inc.

WHY: It was a targeted attack to obtain information on customer database & clients' lists but no ransom was requested by the adversaries after all. They just informed Hanesbrands that they obtained the data.

WHAT: General customer information for 900,000 clients – names, addresses, customer's order status information, phone numbers and the last 4 digits of their Credit Card. But the customers' usernames or passwords were not disclosed. The hackers did not compromise the corporate systems of Hanesbrands.

HOW: Adversaries created an order via guest account check-out on Hanesbrands website. Posing as a "guest" that is checking an order (adversaries were not registered on the website) they managed to find a breach in Hanesbrands database by exploiting the link of the order. The hackers were able to access the clients' orders details and status, and

extract the data for about a week using the “exploit with check-out” option on the website.

STRATEGY: Once Hanesbrands was notified about the breach by the adversaries, they added authentication to their database to stop the Information disclosure hole. In addition, they repaired the “guest user” check-out through which the leak was managed. Hanesbrands notified their customers about the breach via e-mail and post. Since that accident, Hanesbrands are investing more and more in cyber security every year.

RECOVER

- ☑ **IMPACT:** The consequences were leaking general customers information. It is undisclosed of any lawsuits or other direct damage.
- ☑ **RECOVERY STRATEGY:** Hanesbrands informed their customers about the breach. Repaired the “guest user” link[1] in order not to have direct access to the database and overall disabling that as an option[2]. Offered customer service to answer if users have concerns. In addition performed security audit[3] and vulnerability scanning[4] to their existing systems and invested in cyber security trainings[5].

The mitigations described by MITRE ATT&CK framework:

[1] Software Configuration (M1054).
[2] Disable or Remove Feature or a Program (M1042).
[3] Audit (M1047).
[4] Vulnerability Scanning (M1016).
[5] Application Developer Guidance (M1013).

- ☑ **BETTER STRATEGY:** After repairing the “guest user” link through which a customer could review its purchase Hanesbrands are disabling that as an option. Instead they could have added a monitoring for suspicious activity and/or policies for reviewing only certain amount of purchases.

LESSONS LEARNT

Information disclosure attacks become very rare as many modern tools provide automatic cyber security in them and advice companies on what could be a potential leak. The attack on Hanesbrands shows that weak database auditing trail and lack of security expertise can be exploited rather easily. In a lot of cases databases get breached because of insufficient level of cyber security expertise and lack of relevant training/education of non-technical employees who as a result may break basic database security rules. IT personnel could also lack the required expertise to enforce security policies, conduct adequate incident report processes and actions.

Another point is that the database in Hanesbrand was vulnerable because of misconfiguration – databases usually become totally unprotected because of that. It is often forgotten that usually the adversaries are highly professional IT specialists, who surely know how to exploit such vulnerabilities. This can be countered by disabling of the default database accounts combined with trained and experienced IT personnel.

Hanesbrands had luck that only general information was leaked, as well that adversaries informed the company after extracting all the data they could. In addition to that Hanesbrands informed their

customers immediately for the breach which shows that the company wants to be upfront with its customers, and the issue is being taken seriously.

CASE STUDY 5: SPOOFING HUMANA

TARGETED ORGANISATION

Humana is a health insurance company headquartered in Louisville, Kentucky. Originally founded in 1961 as a nursing home operator, the company's main activity transitioned into owning and managing hospitals, then to health insurance plans in the 1980s. As of May 2015, Forbes estimated the company to be worth $26.7 billion. In 2020 Humana had revenue of $77.155 billion and around 48 000 employees. Monthly, Humana is spending over $100,000 on cyber security. Humana are using cyber security products like "Akamai" (cloud delivery platform) and "Prolexic (security solutions for protecting web sites, data centers, and enterprise IP applications from Distributed Denial of Service (DDoS) attacks)", "Proofpoint" (solution to protect your people and critical data from advanced email threats), "Alert Logic" (white-glove managed detection and response) programmes and others.

"Spoofing is an attack technique that relies on falsifying data on a network in a way that enables a malicious site or communication to masquerade as a trusted one.". (The Cyberwire Glossary, n.d.)

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was desk research, the specific information sources can be found in the References section of this document.

PREVENT

☑ **Practices that had zero effect:** Alerts for failed login attempts – Humana applied this practice before the incident. It was not effective as it took the organisation approximately one day to take measures in response to the numerous failed login attempts received.

☑ **Practices that had proven effects in real cyber-attacks:**

1. Account lockout after failed login attempt.
2. Blocking internet traffic from foreign countries with which the organization does not do business.
3. Forcing a password reset.

IDENTIFY

The attack against Humana was of **Spoofing type.**

On the 3rd of June 2018 Humana was a target of a sophisticated cyber spoofing attack that occurred on Humana.com. On the same day Humana

became aware of a significant increase of the login error attempts from foreign countries' IP addresses[1]. In order not to reveal their real location the adversaries used Multi-Hop Proxies[2]. The volume of the login attempts to Humana.com suggested that a large and broad-based attack was launched. The nature of the attack and observed behaviors indicated the attacker had a large database of user identities and corresponding passwords that were being inputted with the intention of identifying which might be valid on Humana.com by „brute force"[3]. The excessive number of login errors suggests that credential information didn't originate from Humana[4] (and most probably were bought from the „dark" web). On 4th of June Humana blocked the IPs. Based on these facts this can be described as identity spoofing attack. Adversaries collected data[5] for about 65 000 users that includes:

- ☑ Medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc.
- ☑ Spending account information such as health saving account spending and balance information.

After the incident Humana had taken additional measures as account lockout after failed login attempt, blocking internet traffic from foreign countries with which the organization does not do business and forcing a password reset.

The attack described by MITRE ATT&CK framework:
[1] Command and Scripting Interpreter: Network Device CLI (T1059.008).
[2] Proxy: Multi-hop Proxy (T1090.003).
[3] Brute Force: Credential Stuffing (T1110.004).
[4] Gather Victim Identity Information: Credentials (T1589.001).
[5] Automated Collection (T1119).
The attack was identified by alerts for multiple login attempts errors.

RESPOND

- ☑ **WHO:** Unknown
- ☑ **WHOM:** Humana
- ☑ **WHY:** Identity theft (to be probably sold to third parties)
- ☑ **WHAT:** Users sensitive information (medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc; spending account information such as health saving account spending and balance information)
- ☑ **HOW:** Adversaries collected large quantities of accounts and credentials. Then using multi-hop proxies brute forced login with the accounts they had. After successful login adversaries collected user data through small size data transfers.

☑ **STRATEGY:** Once Humana noticed the significant increase in the number of login attempts errors, their cyber-security operators blocked the foreign IP addresses from which the multiple login attempts were made. After that Humana forced password reset on all accounts known to be breached and even released a product - offering members an identity theft protection for one year.

RECOVER

☑ **IMPACT:** The consequence was the leaking of confidential information of users (medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc; spending account information such as health saving account spending and balance information). Many negligence lawsuits were filed towards Humana after that. There is no information if the lawsuits were won by the company which suggests that the results were probably negative.

☑ **RECOVERY STRATEGY:** Humana notified number of members to inform them about the data breach after a month had passed. They also took a number of steps to increase their cyber security including: 1) forcing a password reset[1]; 2) deploying new alerts for successful and failed logins[2] and 3) locked accounts that were connected to suspicious activity[3]. In addition, they deployed a series of technical controls to enhance web portal security (brute force attack block, SQL injection defence[4], installing an SSL security certificate[5], etc.). The company also blocked all foreign IP addresses that were not relevant to its operations[6].

The mitigations taken by Humana described by MITRE ATT&CK framework:

[1] Password Policies (M1027).
[2] Network Intrusion Prevention (M1031).
[3] Account Use Policies (M1036).
[4] Software Configuration (M1054).
[5] SSL/TLS Inspection (M1020).
[6] Filter Network Traffic (M1037).

☑ **BETTER STRATEGY:**

Humana could have notified users earlier. They also could have added additional security measures such as:

- Using authentication based on key exchange between the machines on an organization's network or multi-factor authentication for remote access;
- Using an access control list to deny private IP addresses on downstream interfaces;
- Implementing filtering of both inbound and outbound traffic;
- Configuring routers and switches - if possible - to reject packets originating from outside an organization's local network that claims to originate from within;
- Enabling encryption sessions on an organization's router so that trusted hosts outside its network can securely communicate with its local hosts.

LESSONS LEARNT

The lessons learnt could be identified as the necessity to put more focus on securing the personal data of users, organizing trainings of the staff in order to raise the awareness of cyber threats, to notify users of leak data because of the numerous negligence lawsuits towards Humana after the incident (Humana did not disclose any information that such attack has happened until a month later).

The effects of the attack were not only connected with expenses to deal with the attack and lawsuits but with the great damage to the reputation of Humana and its reliability. Since the firm is in the sphere of health insurance, it is crucial for it to have the highest security measures and trust of its clients as the data stored in its systems is very sensitive and confidential. That is why Humana was and remains a top target for cyber-attacks way before the one specified in this case and after as well. Considering this, the error in judgement of the severity of this attack could be regarded as surprising.

CASE STUDY 6: DENIAL OF SERVICE WILLIAM HILL

TARGETED ORGANISATION

William Hill is an online gambling company with headquarters in London, England - originally founded in 1934 by William Hill. The company changed hands many times – it was bought for a first time in 1971 by Sears Holdings. After being sold numerous times in April 2021 it was acquired by Ceasars Entertainment. In 2020 company had revenue of £1,324.3 million and 12000 employees (8000 in UK) in 2021.The company used to have more than 1400 betting shops but in 2019 it started closing more than 800 shops due to low profits but claiming they will keep its personnel intact.

Monthly, William Hill are spending over $100,000 for cyber security. The firm is using cyber security products like “Prolexic“ (security solutions for protecting web sites, data centers, and enterprise IP applications from Distributed Denial of Service (DDoS) attacks)”, “Proofpoint” (solution to protect your people and critical data from advanced email threats), “F5 BIG-IP Application Security Manager” (flexible web application firewall that secures web applications in traditional, virtual, and private cloud environments) , “Check Point” (protects its customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and advanced targeted threats), etc.

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was desk research, the specific information sources can be found in the References section of this document.

PREVENT

☑ **Practices that had zero effect:**

1. Anycast network diffusion – William Hill have such type of defence – which is useful to hold tremendous amounts of customers visiting its website or can dissolve huge amounts of unwanted network traffic (like the DDoS attack). That strategy typically works for most of the cases of DDoS attacks.

2. Simply increasing of network's bandwidth (how much traffic it can hold) didn't prove to be effective in this attack.

☑ **Practices that had proven effects in real cyber-attacks of this type:**

1. Implementing server-level DDoS protection – additional rules that help identifying and blocking malicious network traffic.
2. Adding 3rd party Anycast network diffusion – this can help companies tremendously increase their ability to take on much more network traffic or handle DDoS attacks.

IDENTIFY

The attack against William Hill was of **Denial of Service type.**

On 1st of November 2016 William Hill was a target of a high performance distributed denial of service attack[1]. Before the attack, the adversaries gathered information about William Hill's website network details[2]. After that the adversaries flooded William Hill's website with traffic so it couldn't function properly. The attack denied customers from placing bets on Tuesday evening's UEFA Champions League matches. The attack on William Hill was achieved with the help of a malware called „Mirai"[4], which creates a network of numerous computer systems which is known as „botnet"[3] to commence the DDoS attack through them.

"According to Cloudflare, in Q4, 2021 the manufacturing industry received the most application-layer DDoS attacks, recording a 641% increase quarter-on-quarter in the number of attacks.." (Cook, 2022)

The attack described by MITRE ATT&CK framework:
[1] Network Denial of Service: Direct Network Flood (T1498.001).
[2] Gather Victim Network Information: IP Addresses (T1590.005).
[3] Acquire Infrastructure: Botnet (T1583.005).
[4] Self-propagating worm virus that uses database of default credentials. With these credentials IoT devices (smart devices like fitness trackers, voice assistants, smarthome accessories etc.) are scanned and infected.

The attack was identified right after William Hill's website became unresponsive and stopped being accessible.

RESPOND

WHO: Unknown.
WHOM: William Hill.
WHY: Business feuds – it is very probable that company rival will make such actions especially in time of popular sports events like UEFA Champions League / Extortion – if William Hill do not manage to handle situation it is probable that ransom will be requested.
WHAT: William Hill's website was down for 24-hour outage, which caused losses for £4.4 million. It took days for William Hill to restore its website and systems fully.

HOW: On William Hill's website was conducted high performance Distributed Denial of Service attack with "botnet" network (multiple computers which were infected by malware virus and used to conduct such attack without their knowledge or consent) created by a malware called "Mirai".

STRATEGY: After noticing that their website is down William Hill IT specialists started filtering the incoming traffic. William Hill used Anycast network diffusion – sending network traffic scattering it over network of company's servers. That mitigation distributes the network traffic to the point where the traffic is absorbed by the company's network. This strategy usefulness depends on how big is the company's network and how big is the DDoS attack. In the case of William Hill – even with its top notch infrastructure and security were not enough to handle such an attack.

RECOVER

IMPACT: The DDoS attack against William Hill caused its site to remain down for over 24 hours in which customers couldn't bet on the UEFA's Champions League matches. That resulted in losses for over for £4.4 million in a single day. Luckily for William Hill only its website was targeted which kept its users sensitive data intact(which is a clue that adversaries wanted to deny users from visiting the website, and not to steal data). It took over 4 days working around the clock for William Hill IT specialists to revive their website and affected systems.

RECOVERY STRATEGY: In order to tackle the attack William Hill filtered the incoming network traffic[1]. Filtering network~~s~~ traffic – blocking the attack-only traffic and allowing legit one. Also started using 3rd party Anycast network diffusion vendors (companies that are offering such type of service – which dissolves the DDoS attack when scattering all the incoming traffic through its network).

BETTER STRATEGY:

☑ Host health-check, which will alert company's IT specialists when abnormal network usage is detected [2]. If detected in time, actions can be taken to help keeping website service available.

☑ "Blackhole routing" can be used. It is a technique which funnels both, the legitimate and the malicious traffic, to a null route and dropped out from the network. It is not an ideal solution as it makes the website inaccessible.

☑ Rate limiting. It limits the number of requests the server can receive – it alone can't stop the DDoS attack, but it is a useful tool in overall defence strategy.

The recovery strategy described by MITRE ATT&CK framework:

a. [1] Filter Network Traffic (M1037).

b. [2] Sensor Health: Host Status (DS0013).

LESSONS LEARNT

The attack against William Hill can show us that even a company with exceptional cyber security and one which is prepared to handle such attacks can suffer from them.

Even though its website was taken down by the DDoS attack (usually such attacks are just a smokescreen for the actual attack), company's top-level security was intact and functional, keeping customer's sensitive information secure. That showed their customers they are safe and kept company's credibility. Given that the adversaries did not further attempt to exploit William Hill's vulnerability, points that most probably the attack was done because of business rivalry (competitor company that wants to take advantage of the betting market) or an attempt for extortion (the company relies on its website, and keeping it down by adversaries generates losses).

With entering in the era of smart devices (IoT) when everything can be operated remotely (smart-home lights, vacuum cleaners, fridges, smart watches etc.), we also need to think about the security that needs to be applied. All of these smart devices have IP address, and can be hacked through the network – for obtaining information or "zombified" (your device is being controlled without you knowing and it start performing in a strange way) and used in DDoS attacks to flood a website.

CASE STUDY 7: COBALT STRIKE: THE USE OF RED TEAMING TOOLS BY CYBER CRIMINALS

TARGETED ORGANISATION

Cobalt Strike is a red teaming tool which was developed back in 2012. Its main purpose is to assist red teams to test and simulate cyber-attacks. As the tool has good capabilities to bypass security boundaries via evasions, attackers have hijacked some its versions to abuse it as a delivery tool for malicious payloads such as ransomware. This case study does not focus on a single organization as Cobalt Strike is used in the wild to perform in-mass attacks targeting various types of organisations such as manufactories, financial institutions, telecom companies, and more.

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was desk research, the specific information sources can be found in the References section of this document.

PREVENT

The detection and prevention of an attack which makes use of the red teaming tool Cobalt Strike involves a security chain throughout the complete infrastructure. This starts already with protection and monitoring software on the endpoint client and goes all the way up to the network level. Furthermore, active threat intelligence is also necessary to keep signature- based detection tools up to date.

This typically involves:

- ☑ Endpoint security (such as antivirus, host-based monitoring)
- ☑ Network security (such as firewall, proxy, signature/pattern detection in traffic)
- ☑ Email security
- ☑ Correct configured host/security policies

IDENTIFY

Cobalt Strike is a multi-functional commercial tool which fulfils different techniques of attacks. Considering the tool and its capabilities itself, it can be categorized as Information disclosure and Elevation of privilege. However, as it can also be used to further drop malicious payloads, especially as ransomware attacks were observed in combination with Cobalt Strike, the list can be extended with Tampering and Denial of service.

Considering all the features of the tool, it is a remote access tool with lateral movement capabilities. This leads to a huge list of attacks techniques used by Cobalt Strike, and therefore we will only cover some of them here.

- ☑ Abuse Elevation Control Mechanism (T1548)
  Once Cobalt Strike was executed on a system, it has the capabilities to perform various techniques used to gain higher permissions.
- ☑ BITS Jobs (T1197)
  BITS is a Windows tool which can be used by Cobalt Strike to download payloads
- ☑ Command and Scripting Interpreter (T1059)
  Cobalt Strike can use various tools to execute commands, code, and scripts. This includes PowerShell, Windows Command Shell, Visual Basic, Python and JavaScript.
- ☑ Exploitation for Privilege Escalation (T1068)
  To gain higher privileges, Cobalt Strike can exploit vulnerabilities within the operating system.

Input Capture (T1056)/Screen Capture (T1113)
Cobalt Strike can also act as a keylogger and collect screenshots from the infected system.

RESPOND

- ☑ **WHO:** Unknown
- ☑ **WHOM:** Multiple organizations around the globe
- ☑ **WHY:** Cobalt Strike was used in multiple campaigns focusing on different goals. On reason for the attack is to get access to the internal organization network for lateral movement. Another reason might be to cause damage to companies by attack the compromised network with e.g. a ransomware.
- ☑ **WHAT:** Mainly for remote access, network compromise and lateral movement.
- ☑ **HOW:** Cobalt Strike is a commercial red teaming tool used to simulate cyber attacks which were hijacked. The tool is used to gain the initial access to a company network as well as for further actions with the compromised network.
- ☑ **STRATEGY:** Depending on the attacked company, the information on how they identified and reacted on the attack is unknown.

RECOVER

- ☑ **IMPACT:** The attacker can gain full network access within the company. This can lead to information disclosure as well as further attacks which are delivered depending on the operator of the attack.
- ☑ **RECOVERY STRATEGY:** Depending on the attacked company, the information how their recovery strategy looked like is unknown.
- ☑ **BETTER STRATEGY:**
  - Keep antivirus systems up to date
  - Use Intrusion Detection and Intrusion Prevention Systems
  - Properly monitor systems for suspicious activities
  - Properly configure systems and disable not required services
  - Train awareness of employees
  - Use segmentation on a network level and limit the allowed communication to a required minimum

LESSONS LEARNT

Although it is necessary to build red teaming tools which can be used for attack simulation on a network to find possible vulnerable points one still has to keep in mind that such tool also can be compromised and used by an attacker.

CASE STUDY 8: ZERO-DAY ATTACK - HACKER GROUP HAFNIUM TARGETING EXCHANGE SERVERS

TARGETED ORGANISATION

Early 2021 researchers found multiple critical vulnerabilities in the Microsoft Exchange Server which led to massive exploitation around the world. The vulnerabilities were used in the wild by multiple criminal organisations, most notably the HAFNIUM group, before patches were provided by Microsoft. This made the attacks especially hard to respond and recover from.

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was desk research, the specific information sources can be found in the References section of this document.

PREVENT

Tens of thousands of companies were affected by this attack. Due to the general exposure of Microsoft Exchange Servers to the internet and the authentication bypass potential of the attack it was very hard to prevent in the first place. This further leads to the assumption that different security practices which apply for those companies had zero impact.

IDENTIFY

There are four different vulnerabilities which led to the described attacks. The vulnerabilities are **CVE-2021-26855, known as ”ProxyLogon”, CVE-2021-27065, CVE-2021-26857, and CVE-2021-26858**. The technique to exploit these vulnerabilities are described as **“Exploitation for Client Execution” (T1203)** under the MITRE ATT&CK framework.

CVE-2021-26855 is an authentication bypass using the internal proxy from the Exchange Server. With this an attacker can get privileged access to the Server itself. Combining it with another vulnerability like CVE-2021-27065, which allows writing arbitrary files onto the system, or CVE-2021-26857, to get SYSTEM access (T1078) via an insecure deserialization, creates an exploitation chain with no restrictions.

Attacks took place in the wild before Microsoft could release a patch for the vulnerabilities. According to numerous resources this timespan was around 58 days of zero-day exploitation. The first group which was associated with these vulnerabilities was HAFNIUM. Later multiple other groups started abusing these vulnerabilities. The capabilities of the attack allowed multiple

scenarios, reaching from data exfiltration (T1567) to ransomware deployment (T1486).
Following is a list of actions taken by the HAFNIUM group using this attack vector:

☑ T1589 – Collecting E-Mail addresses for users they intended to target
☑ T1071 – open source C2 framework (e.g., covenant)
☑ T1560 – 7-Zip, WinRAR to compress stolen files for extraction
☑ T1059 – Export mailbox data via PowerShell
☑ T1567 – Exfiltrate data via sharing sites, including MEGA
☑ T1105 – Downloading malware and tools onto compromised hosts (e.g., Nishang, PowerCat)
☑ T1003 – Credential Dumping of LSASS, and Active Directory databases (NTDS.DIT)
☑ T1505 – Deploying WebShells on compromised hosts (SIMPLESEESHARP, SPORTSBALL, etc.)

Identification of the attacks may take place due to log inspection on possible compromised machines. Microsoft released guidance on detecting every vulnerability according to their Indicator of Compromise.

RESPOND

WHO: HAFNIUM (likely state-sponsored group with links to China)
WHOM: Different companies around the globe, mainly US industry
WHY: Data Exfiltration and probably earn money via ransomware
WHAT: Company knowledge such as data, E-Mail addresses, mailboxes
HOW: Leveraging multiple vulnerabilities in Microsoft Exchange Server to allow unauthenticated remote code execution
STRATEGY: Scanning the IP range of the internet to collect IP-lists of Microsoft Exchange Servers. Exploiting the mentioned vulnerabilities to deploy web shells, or C2 beacons. Using this access allowed to compress and exfiltrate data via online sharing websites like MEGA. Occasionally deploying “DearCry” ransomware. This was possible due to the late availability of the patch and bad patch management of companies.

RECOVER

IMPACT: The consequences of this attack can be considered as information loss as both the exfiltration and ransomware fit into this category. Furthermore, if organizations have tried to pay the ransom to get their data back, they also ended up with a financial damage.

RECOVERY STRATEGY: Depending on the specific attack the recovery may differ. The recovery process from a ransomware may take a long time. All the infected systems must either be reinstalled or a backup needs to be reverted. If backups have been stored on an infected system, they

obviously can't be used for the recovery process. Recovery from data exfiltration is different. At first available patches should be applied and traces of web shells or C2 beacons should be removed. It is important to assess which, and how much data got stolen to measure the impact.

BETTER STRATEGY

- ☑ Keep antivirus systems up to date
- ☑ Use Intrusion Detection and Intrusion Prevention Systems
- ☑ Properly monitor systems for suspicious activities
- ☑ Properly configure systems and disable not required services
- ☑ Fast patch management to fix vulnerabilities as soon as possible
- ☑ Use segmentation on a network level and limit the allowed communication to a required minimum

LESSONS LEARNT

Zero-day exploitation with attack chains seem very intimidating. The key to tackling these challenges is a proper network segmentation and system monitoring to identify possible attacks in a timely manner. Network intrusion and prevention systems may also help detecting such attacks. What is also important is that patches for critical vulnerabilities must be applied as soon as possible to further remediate attack vectors.
As another lesson learnt I want to mention the security researchers from DevCore who first detected the vulnerabilities and helped with Microsoft in the patch process. This reinforces the importance of independent security research for the good cause.

CASE STUDY 9: WannaCry: WHEN A RANSOMWARE PARALYZES THE HEALTH SYSTEM

TARGETED ORGANISATION

Back in 2017 a new ransomware called **WannaCry (WannaCrypt)** which targets the Windows operating system infected thousands and thousands of clients around the globe. Rather than targeting a specific organisation the attack was widespread and affected lots of companies within different fields.

HOW INFORMATION WAS ACQUIRED?

The method applied to collect the information for this case study was desk research, the specific information sources can be found in the References section of this document.

PREVENT

Multiple companies were affected by this attack which leads to the assumption that different security practices which apply for those companies had zero impact.

IDENTIFY

WannaCry is a malicious application which is classified as **ransomware** as it encrypts user specific files on a targeted system. This leads to tampering of data and its destruction as the owner of the infected system is not able to decrypt the files. This subsequently ends in a denial of service attack due to the missing files and data.

One of the main characteristics of WannaCry is its technique used to automatically search for potential target systems which the ransomware then tries to infect as well. As this malware can infect other systems from an already infected one, it is also referred to as a worm. To achieve this goal, an exploit for software vulnerability in Microsoft Windows's SMB protocol called Eternal Blue is used which maps to MITRE ATT&CK ID T1210.

"The WannaCry outbreak, afflicted over 200,000 computers in over 150 countries. Costing the UK £92 million and running up global costs of up to a whopping £6 billion." (Acronis, 2020)

Before the malware can spread and infect other systems it first needs to search and find them. This is done via various techniques such as scanning for remote systems (T1018), enumerating active remote desktop session (T1563), scan for new attached drives on the infected system (T1120). Once a potential remote device or drive is found, WannaCry tries to copy itself to the target system and executes its malicious behaviour.

Before the ransomware starts its encryption, it performs changes on the infected system to disable recovery options, which is referred by T1490. Afterwards it searches for user specific files in various directories (T1083) and begins to encrypt each file found (T1486). For command and control server communication the Tor network is used (T1573/T1090).

For a behaviour-based identification of this attack, the following MITRE ATT&CK techniques can be used:

- ☑ T1210: Exploitation of Remote Services
- ☑ T1018: Remote System Discovery
- ☑ T1563: Remote Service Session Hijacking (.002 RDP Hijacking)
- ☑ T1120: Peripheral Device Discovery
- ☑ T1490: Inhibit System Recovery
- ☑ T1083: File and Directory Discovery
- ☑ T1486: Data Encrypted for Impact
- ☑ T1573: Encrypted Channel (.002 Asymmetric Cryptography)
- ☑ T1090: Proxy (.003 Multi-hop Proxy)

RESPOND

Back in 2017 a new ransomware called WannaCry (WannaCrypt) which targets the Windows operating system infected thousands and thousands of clients around the globe. Rather than targeting a specific organisation the attack was widespread. Large companies where some of them are

running their businesses worldwide such as car manufacturer were hit by the ransomware. However, also other organisation groups such as public transport, health services or telecommunication services were affected as well.

- ☑ **WHO:** Unknown
- ☑ **WHOM:** Different companies around the globe
- ☑ **WHY:** Reach high damage due to loss of data and probably earn money
- ☑ **WHAT:** Company knowledge such as data
- ☑ **HOW:** Infection of ransomware which was distributed via a vulnerability found in Microsoft Windows
- ☑ **STRATEGY:** The ransom note used by WannaCry appeared on the screen of systems which were infected. Antivirus systems and firewalls did spot the infection and spreading of the ransomware and therefore did not prevent the systems for further infections and damage.

RECOVER

IMPACT: The consequences of this attack can be considered as information loss as all the files which were encrypted by the ransomware are not readable anymore. Furthermore, if organizations have tried to pay the ransom to get their data back, they also ended up with a financial damage.

RECOVERY STRATEGY: The recovery process from a ransomware may take a long time. All the infected systems must either be reinstalled or a backup needs to be reverted. If backups have been stored on an infected system, they obviously can't be used for the recovery process.

BETTER STRATEGY

- ☑ Keep antivirus systems up to date
- ☑ Use Intrusion Detection and Intrusion Prevention Systems
- ☑ Properly monitor systems for suspicious activities
- ☑ Properly configure systems and disable not required services
- ☑ Fast patch management to fix vulnerabilities as soon as possible
- ☑ Train awareness of employees
- ☑ Use segmentation on a network level and limit the allowed communication to a required minimum

LESSONS LEARNT

Ransomware attacks are nowadays common and can hit all companies. It is highly recommended to follow known security practices to make the IT infrastructure as secure as possible to limit the damage of an attack to its minimum.

CASE STUDY 10: SPY ON SENSITIVE PRIVATE DATA

TARGETED ORGANISATION

In the autumn of 2020, at national level a new security alert was announced. It specified that many public and private entities have been severely affected, similarly as in other previous successive waves, by **malware attacks of the EMOTET type**, which led to numerous problems. EMOTET is a **malware** that infects computers running the Microsoft Windows operating system through infected malicious links or attachments (e.g. PDF, DOC, ZIP, etc.).

HOW INFORMATION WAS ACQUIRED?

The information needed to describe this cyber-attack was collected through an interview with IT technician of the company. The interaction was performed with the condition of keeping sensitive information anonymously. Even if the interviewee was willing to describe the incident, some information could not be obtained because the problem was delegated to a specialized company and had to be investigated separately.

PREVENT

Although awareness-raising campaigns have been carried out by specialized entities and organizations on the measures to be taken, many public and private organizations have been affected, according to existing reports.

In the case of the analysed company, from the perspective of cyber security, specific procedures and mechanisms operated, but these were not enough due to the low experience in the field of digital domain of some workers.

IDENTIFY

Emotet is a Trojan initially associated with banking fraud which, since 2017, has been limited to spam and secondary payload distribution. Currently can be identified numerous variants of Emotet and unfortunately this malware continues to evolve into new variants with more complex capabilities and evasion techniques.

Based on provided descriptions and supplemental from media reports, the following details were involved in the incidence:

- ☑ A socially engineered designed phishing email has been received with a Zipped archive attached and with the password included in the message.
- ☑ Malware was encrypted and password-protected in an archive file
- ☑ Evaded anti-malware solutions by using password-protected archives as attachments
- ☑ The Trojan loader contained benign code from a Microsoft DLL to evade antivirus solutions
- ☑ Thread hijacking to distribute malicious code using password-protected archives as attachments
- ☑ Compromised systems were leveraged to send malicious emails to other contacts
- ☑ E-mail systems shut down temporarily to stop further spread of Trojan
- ☑ Impacted internal networks

According to the MITRE ATT&CK framework, this incidence can be described as follows:

1. T1566.001 – Spearphishing Attachment
2. T1204.002 - User Execution: Malicious File
3. T1027 - Obfuscated Files or Information
4. T1036 – Masquerading
5. T1586.002 – Compromise Accounts: Email Accounts
6. T1586.002 – Compromise Accounts: Email Accounts
7. T1499 - Endpoint Denial of Service
8. T1498 - Network Denial of Service

"EMOTET was much more than just a malware. What made EMOTET so dangerous is that the malware was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomwares, onto a victim's computer." (EUROPOL, 2022)

RESPOND

WHO: The attacker could not be precisely identified. Only the place of origin, Vietnam, was known.
WHOM: not-specific targeted
WHY: Sensitive data gathering and ransomware payouts
WHAT: Company/users data
HOW: Spearphishing Attachment, script execution, process injection.
STRATEGY: The threat started on a computer without antivirus and has spread laterally. A cleaning process was performed by a specialised in IT&C company.

RECOVER

IMPACT: The main consequences of the attack were as following:

- ☑ Data loss
- ☑ Regular activity disruption
- ☑ System compromise
- ☑ Financial costs

RECOVERY STRATEGY: The recovery strategy was focused on cleaning and reinstalling the compromised computers, cleaning and/or reinitialising the compromise e-mail-boxes.

BETTER STRATEGY

- ☑ Install and keep an updated Antivirus/Antimalware
- ☑ Adopt a Network Intrusion Prevention
- ☑ Restrict Web-Based Content
- ☑ Assure the user awareness
- ☑ Better Password Policies
- ☑ Privileged Account Management
- ☑ Disable or Remove Feature or Program

- ☑ Execution Prevention
- ☑ Audit
- ☑ User Account Management
- ☑ Behavior Prevention on Endpoint
- ☑ Account Use Policies.

LESSONS LEARNT

Even if Emotet was taken down through an international concerted activity, it remains to be seen if this will have a long-standing impact.

If is to note that malwares use almost the same techniques to penetrate and spreading in the wild, so it is mandatory to be aware and careful as cyberattacks will continue to exist in the future. Measures such as considering communicating with the world using computer isolated from the network that hosts critical infrastructure, using of capable and updated security solutions, considering having latest updates are some that should be foreseen.

Phishing denotes an umbrella term for a social engineering type attacks that are carried out currently via emails or social networking applications.

CASE STUDY 11: ILICIT ACCESS GAIN TO CREDENTIALS

TARGETED ORGANISATION

As any modern company, in the case of described situation, electronic communications via the Internet with their customers and suppliers is the most preferred way. Within this type of communication one of the most used is the electronic e-mail. It allows asynchronously keeping contact with stakeholders managed in an efficient way by more than one person. The company found over half a century on the market has been strongly developed on digitalisation in every department, and in this context is included also the customers relation department. For related employees has been created an e-mail group for managing the online requests from dedicated computers protected by antivirus and spam filtering functionality on the email server.

HOW INFORMATION WAS ACQUIRED?

The information needed to describe this cyber-attack was collected through an interview with one of the IT technicians of the company. The interaction was performed with the condition of keeping sensitive information anonymously. Even if the interviewee was willing to describe the incident, some information could not be obtained because the problem was managed by a different team.

PREVENT

Although awareness-raising campaigns have been carried out by the National Directorate of Cyber Security on the measures to be taken, many publics, private organizations and individuals have been affected, according to existing reports.

The company enforced the usage of security tools and custom regulation on online working, but these were not enough due to the basic experience in the field of digital domain of some employees.

IDENTIFY

Phishing denotes an umbrella term for a **social engineering type attacks** that are carried out currently via emails or social networking applications. Usually, cybercriminals send out bulk unsolicited messages. They want to target as many people as possible, in order to catch some of them with their trick.

Cybercriminals try to exploit the trend of some sort of 'a great offers' or with some administrative instructions. Many of these types of messages seem to be legitimate as they use the same visual identity as well-known companies, online services or applications. Some examples include companies such as Google, Amazon, Microsoft, Yahoo, LinkedIn, etc. or popular banking services and applications such as that of managing web-based email.

Credibility is intended to be achieved by copying the colour scheme, style, logo and mottos of the copied identity. Typical attractive subject lines are used.

Based on the provided description and supplemental media reports, the following details were involved in the incidence:

- ☑ A socially engineered designed phishing email has been received that claimed the need to urgently change the access password to avoid the end of the service;
- ☑ Providing credentials to the illegitimate entity led to the access on the e-mail account and discontinuing the legitimate access by password change;
- ☑ The compromised account was used for unsolicited phishing messages sent to the existing contacts and other addresses owned by the attacker;
- ☑ Due to massive spam messages sent over the Internet the email service was blacklisted such that normal operation was disrupted;
- ☑ The e-mail system was suspended temporarily to stop further spamming;
- ☑ Online operations were impacted.

According to the MITRE ATT&CK framework, this incidence can be described as follows:

1. T1598.001 - Spearphishing Service
2. T1598.002 - Spearphishing Attachment
3. T1598.003 - Spearphishing Link

RESPOND

- ☑ **WHO:** The attacker could not be precisely identified, as from several countries origins have been logged. Possible VPN usage was involved.
- ☑ **WHOM:** not-specific targeted
- ☑ **WHY:** Sensitive data gathering and money extortion
- ☑ **WHAT:** Company/users data
- ☑ **HOW:** Phishing, credentials theft.
- ☑ **STRATEGY:** The threat started by opening an impersonated email, accessing spoofed links and submitting sensitive data. Resetting credentials and delisting from blacklisting services were carried out by the IT team.

RECOVER

IMPACT: The main consequences of the attack were as following:

- ☑ Credential loss
- ☑ Regular activity disruption
- ☑ System compromise.

RECOVERY STRATEGY: The recovery strategy was focused on resetting the credentials and cleaning the compromised email clients.

BETTER STRATEGY

- ☑ Install and keep an updated Antivirus/Antimalware/Email filtering system
- ☑ Adopt a Network Intrusion Prevention
- ☑ Restrict Web-Based Content
- ☑ Assure the user awareness
- ☑ Better Password Policies
- ☑ Privileged Account Management
- ☑ Audit
- ☑ User Account Management
- ☑ Behavior Prevention on Endpoint
- ☑ Account Use Policies.

LESSONS LEARNT

Even if phishing is not a new technique it remains one of the main ways in many cyber security attacks.

It is to note that malwares use almost this technique to penetrate and spreading in the wild, so it is mandatory be aware and careful as cyberattacks in this way will continue to exist. Measures such as considering using better updated protected email services, more awareness on accessing emails and proper analysing the legitimacy of the sender.

CASE STUDY 12: OUTDATED ONLINE EXPOSED APPS

TARGETED ORGANISATION

Nowadays many businesses have changed the way of providing their services by moving online. This is the case of the disused example, where at the desk provided financial type services started in 1998 have been migrated online for most than a decade. The new approach improved overall company activity and customers' satisfaction. However, these achievements were possible only after an important effort in developing the needed custom in-house developed software. This online application allowed customers and the employees to perform the needed operations. The provided platform developed in that time popular framework was maintained until the support was available before the release of the new major upgrade. In time the number of employees has been reduced due to the existing processes automation and market changes. Upgrade to the new distribution was delayed as major hardware and software were required.

HOW INFORMATION WAS ACQUIRED?

The information needed to describe this cyber-attack was collected through an interview with the CEO of the company. The interaction was performed with the condition of keeping sensitive information anonymously.

PREVENT

Although awareness-raising campaigns have been carried out by the National Directorate of Cyber Security on the measures to be taken, many publics or private organizations ignore or delays the decision and actions needed to update their information systems.

The company enforced the usage of known security solutions, firewalls, network segmentation, etc. but these were not enough as remained exposed vulnerability in one of the operated software modules.

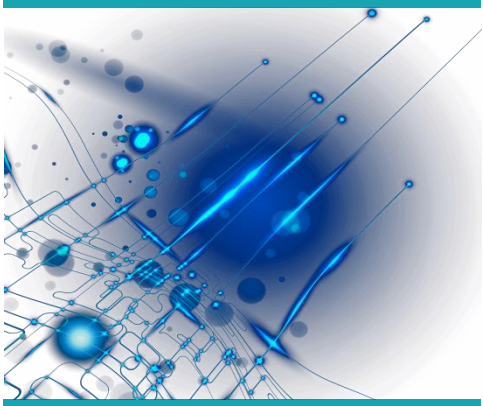
IDENTIFY

Stream injection attacks abuse the ability of an online web application to accept uploaded content such as different type of document or images files. Using remote file inclusion approach, an attacker can exploit the vulnerability in the server-side code into accepting a URL on another site as a valid input. This action is then used to execute malicious attacker's

code. Additionally local file inclusion can be used to get a web application to return the desired content from the local file system.

A popular example is met in case of PHP framework used by WordPress allowing the hacker to access its configuration file. This attack also may allow access to download any PHP source code files running the website, offering new possibilities for other security vulnerabilities. Recent PHP versions are protected from remote file inclusion by default, but if by mistake local file inclusion is exposed this type of attack is still possible.

Based on the provided description, supplemental technical reports, security and vulnerabilities bulletins, the following details were involved in the incident:



- ☑ By a brute force type attack, an account protected with a weak password is illegitimate accessed;
- ☑ The discovered credentials allow the data associated to the account to be changed;
- ☑ The compromised account allowed the stream injection vulnerability to be exposed and unwanted code execution on the server was used to remove the access history logs;
- ☑ Due to the uncontrolled server side code execution some modules of the app become unusable and conduct to the shutdown of the service so normal operation was disrupted;
- ☑ The system was disconnected from the Internet temporarily for further investigation related to the malfunction of the web application;
- ☑ Online operations were impacted.

According to the MITRE ATT&CK framework, this incidence can be described as follows:

1. T1110.001 - Password Guessing
2. T1078 - Valid accounts access
3. T1518 - Software Discovery
4. T1082 - System Information Discovery
5. T1007 - System Service Discovery
6. T0826 - Loss of Availability.

RESPOND

- ☑ **WHO:** The attacker could not be precisely identified.
- ☑ **WHOM:** not-specific targeted
- ☑ **WHY:** Sensitive data gathering and denial of service
- ☑ **WHAT:** Company/users data

- ☑ **HOW:** Brute force attack, credentials theft and code execution by stream injection.
- ☑ **STRATEGY:** The threat started by brute force attack that led to a weak credential discovery, exploiting vulnerability in a non-public accessible software module and then unauthorized code execution. Weak strategy of online access protection, outdated software module and unmaintained code are the main cause of the incidence.

RECOVER

IMPACT: The main consequences of the attack were as following:

- ☑ Credential loss
- ☑ System compromise
- ☑ Regular activity disruption.

RECOVERY STRATEGY: The recovery strategy was focused on major platform upgrade rewriting an important part of the code.

BETTER STRATEGY

- ☑ Install and keep an updated software
- ☑ Enforce strong passwords policy
- ☑ Account Use Policies
- ☑ Adopt two factor authentication mechanism
- ☑ Adopt a Network Intrusion Prevention
- ☑ Restrict remote access
- ☑ Assure the user awareness
- ☑ Implement a periodic security audit
- ☑ User Account Management
- ☑ Behavior Prevention on Endpoint.

LESSONS LEARNT

Even if outdated running software is known to be prone to security vulnerabilities it remains one of the main ways in many cyber security attacks.

Web applications being accessible world-wide are exposed to many vulnerabilities and as a consequence require a special attention from many perspectives.

Measures such as considering constant software updating, improvements and adoption of new techniques and solution for authentication mechanisms, adoption of a regular basis audit process are some of the common measures that can be considered.

CASE STUDY 13: THE RISKS OF AN ATTACK MADE BY A FORMER EMPLOYEE

TARGETED ORGANISATION

The organization where the cyber-attack occurred, acts on commercial follow-up, in an automotive branch, with approximately 2000 employees. Located in the state of Paraná and Santa Catarina in Brazil.

The cyber-attack targeted the area of information technology, due to the knowledge the hacker had from being an ex-employee of the organization, giving him the benefit of convincing the system.

HOW INFORMATION WAS ACQUIRED?

The information within this case study is based on a case study about the risks of a cyber-attack led by an ex-employee. The case study is done from the point of view of the organization that suffered the cyber-attack.

The general objective of this case study is to demonstrate the importance that companies must pay in relation to social engineering within their environments, in order to avoid invasions and/or frauds caused by the recklessness or unintentional assistance of employees as breaches for the hacker's job.

PREVENT

To prevent possible damage, the company already possessed an IT department that managed firewalls, information leakage tools and data encryption.

IDENTIFY

In this case study, the footprint started off with various visits to the association´s webpage, with the intent of understanding their dynamic, their businesses and especially their brands (considering the attacker directed the search for data that the hacker didn´t know yet). When the footprint started and the internal and specific information of the organization is on the attacker´s side, he moved on with doing connections to one of the stores in the chain to discover the names of managers and people who could have privileged access within the organization.

To do so, the attacker posed, via telephone, as a customer who had legal problems with the company. To resolve this problem, the company would have called the customer and asked him to talk to the manager of the store in question, given that he/she would be the person with the greatest

autonomy to answer for such a situation. Due to this interaction, it was easily achieved, the name of the manager, the location of where he/she worked and the telephone number.

After this phone call, attempts were made to contact the manager in the informed channels to check the information collected. Password reset was done when contacting with the information technology sector, posing as the employee himself, in order to get that mentioned sector to inform him of the user's access data.

Using a little persuasion, and the argument that data for the board depended on this access, finally the technician reset the password and informed the new password by telephone. More than that, it was possible to convince him to set up VPN access (technology for remote access to the company's environment) so that the hypothetical user could work from outside the office.

RESPOND

WHO: The attacker was an ex-employee;
WHOM: An organization that works on commercial follow-up, in the automotive branch;
WHY: The attack was targeted the organization with unknown motives;
WHAT: The property targeted was the information technology sector in order to collect inside information of the organization and personal data of the current employees;

HOW: The attack started with obtaining the name of the manager of one store, proceeded into contacting the information technology sector of the company and convinced them to reset the password. That way the ex-employee pretended to be the manager and had access to everything regarding inside information, personal data of employees and clients and whatever more the hacker wants.

RECOVER

The company started to train the collaborators to pay attention to the types of information that they usually pass on to third parties, especially if it is critical information. Never, under any circumstances, should an employee pass on information critical, such as passwords, over the phone. These must be provided to interested parties via safe methods, such as registered letters or through the responsible manager.

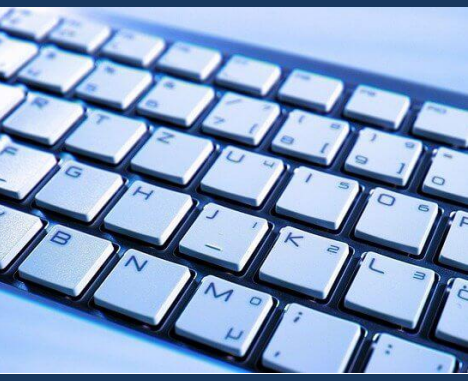
Also provide training to make employees aware of being careful with the information they share on the internet. Training focused on the risks that the information shared can bring to their occupation but also bring to personal life, such as kidnappings, life details and personal security.

This company is aware that needs to provide technical and physical conditions for the application of good security practices, but, above all, to

value and encourage the adoption of best practices and stricter security protocols by its employees, whether in a corporate or personal environment in order to control, in the best possible way, the weakest factor of information security: the human factor.

LESSONS LEARNT

The organization should establish the information in a simple pattern procedure that can frustrate the hacker. This procedure has 3 stages:

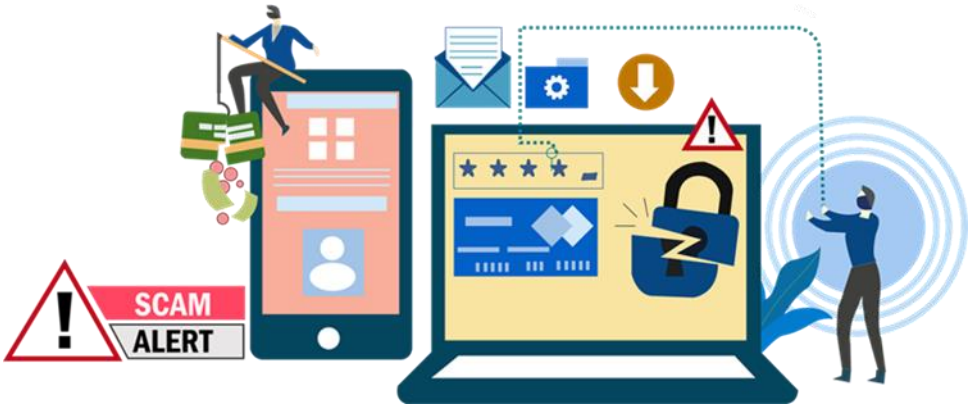


☑ **Public:** Information that could be given to anyone, for example, to commercial contacts and specific corporations, information between clients and the corporation´s business;

☑ **Private:** Information that cannot be given to any person and that only concerns the corporate environment. Are covered in this category information referring to internal procedures, corporate data administrative and strategic aspects of the company;

☑ **Confidential:** Information and data that should not be shared inside and outside of the company, such as employee registration data, compensation, results of sectors and strategic actions that only concern the direction or presidency.

Also, the organizations should have internal procedures to protect them from attacks of social engineering. Operators must be well trained on the processes they must follow and the actions they must take in situations where the company feels attacked, such as transferring the call to a person trained to handle this kind of situation. Simple actions can cause the attack to fail. Immediately it can be said that an initial checklist to confirm the data of the applicant would already make it difficult for the hacker to access. Bearing in mind that personal data is not something very difficult to obtain, the technicians could adopt a process of returning the contact to the registered telephone number of the employee, in order to confirm that it is in fact the employee in question.



CASE STUDY 14: CYBERATTACKS AS A NEW HOMELAND SECURITY CHALLENGE

TARGETED ORGANISATION

Portuguese government entities (especially the Ministry of Internal Administration), the Security Forces and large companies.

HOW INFORMATION WAS ACQUIRED?

The information for this case study was gathered through a desk research referring to a master's degree thesis, where the author applies a study and several exploratory interviews with specialists and people responsible for the national security forces, in order to conclude whether the hacktivist phenomenon poses a threat to the Portuguese security forces.

PREVENT

In order to prevent attacks, one of the steps the IT team responsible for cybersecurity in these organizations takes is to monitor social channels, for instance: IRC's (Internet Relay Chat), all kinds of chats, Facebooks, everything from which it's possible to get information on the internet, they also do a follow-up and try to see if there are any suspicious actions.

According to the "modus operandi", defined by the terms of the group Anonymous (Portugal), they initially advertise on social networks (IRC's and Facebooks), the actions they will take and that's when they start to communicate between them. Then they use private chat channels to communicate with each other, which led to the implementation of the SOC (Security Operations Centre) of MIA (Ministry of Internal Administration), to prepare for this type of attacks.

IDENTIFY

The consequences of these attacks varied, depending on the type of attack. Many dealt with a denial-of-service attack, (DOS, DDOS), which causes an exhausting of resources in terms of systems or communications. Also, they dealt with some types of attempted intrusion attacks such as SQL Injection and defacements. Fishing by email, it's also one of the most frequent attacks, leading sometimes to access to private information.

In November 2011, an attack was carried out on the website of the national union for the career of PSP Chiefs, with the disclosure of personal and confidential data (patents, telephone numbers and e-mail addresses) of 107 PSP personnel.

"DDoS attacks have been steadily increasing in frequency over the past few years. According to a report from Cloudflare, ransom DDoS attacks increased by almost a third between 2020 and 2021 and jumped by 75% in Q4 2021 compared to the previous three months.". (Cook, 2022)

RESPOND

An attack on the Public Security Police was assumed by the group LulzSec Portugal. The Portuguese Anonymous group has claimed several attacks on government websites and relevant institutions. Generally, the profile of the hacker is of someone young, of school age, at the secondary level (10th to 12th grade). There may be one or another situation in which they are already more adult people perhaps with less knowledge in the technological area but dissatisfied with society.

This type of attack is available to any citizen. It just takes the person searching on the internet for tools, methods, and groups and start participating. These groups of Anonymous people, at the time of the attacks, carried out workshops on how to do an attack, “abc” courses on how to understand the attack. They provide tools already developed and that anyone can access the site, it’s only necessary to insert the destination address and an application develops the attack.

Most of the attackers, that is, young people still in school, use tools that are used by many specialists, those specialists are people with a more advanced academic degree, and older, that use tools already developed for the purpose of cyber attacking. That is to say, on the internet, it is possible to search and obtain information to carry out the attack, how to do it and what kind of tools are used to help make the attack.

The attack made by LulzSec Portugal was justified on Twitter claiming that as a response to the action of agents provocateurs infiltrated a demonstration organized by them.

But most of the time these attacks happen because these people search for visibility or to jeopardize the organizations, as this often has to do with people's discontent in terms of the current context in which Portuguese citizens live, and people often demonstrate their displeasure in this way. Other times it is just a joke to the attackers, aged between 16 or 17 years, who do not have many concerns in social terms, it is often because friends do it, and to promote themselves within the group of friends, other times these are experiences that they do because it's the age of experimenting new things. Most of the time they don´t realize the impact that these attacks may have.

It all starts with a group of hackers that have the technical knowledge and develop tools to be used by groups of people who don´t have that same knowledge, which makes the process of hacking easy for anyone.

A characteristic of Portuguese groups is to attack unprotected websites and exploit vulnerabilities. They plan attacks on IRC's (Internet Relay Chat) and chatrooms, do not assume your identity and use nicknames. Portuguese hacktivists use the tools available online to carry out the attacks, that is, “they do not manufacture customized programs, but use those that are available on the network”. As for the people who take on the organization and leadership of this type of initiative, they are often people with little technical expertise, dedicating themselves to making announcements and disseminating the actions to be developed, and often “those who even have very specialized technical skills, they have no idea that they are the most competent and specialized in the group, they think that they are people who know little and that they are just helping others who know more”.

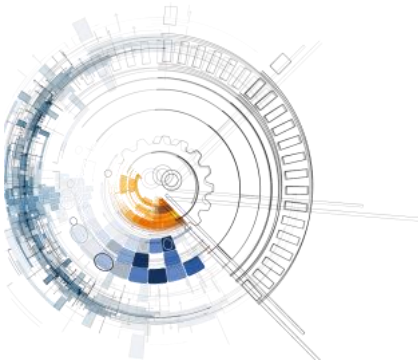
The Anonymous group uses conventional hacking methods such as Havij114 and SQL Injection, its main innovation being the creation of websites that carry out DoS attacks.

RECOVER

The possible consequences are the theft of information, the unavailability of the services and site defacements where are made changes in the information, as hackers sometimes remove information, they can also add it.

These attacks may jeopardize the trust placed by citizens in the institutions that are victims of these groups but also the identification of vulnerabilities and the influence of other people with certain ideals are situations that may happen.

These types of attacks evolve, and the techniques improve over time, and the organizations must adjust and evolve for the protection of its network. They were forced to stop accessing the network until the conditions were met to ensure that the security of internal information was maintained. And they've already done that, in total, for an hour at most. Occasionally, some services have been also inaccessible during the night.



CNCseg (National Centre of Cybersecurity) is being developed, which will have more to do with the issue of national defence, than there is the Cyber Defence Centre, which is in the competence of the Ministry of National Defence, whose main action is the attack on hackers who may be developing attacks, doing the detection and counterattack of these elements.

MIA will participate, at least in CNCseg, they are working together with the GNS, which is the entity that has this competence and will be one of the information inputs for this type of cybersecurity, the idea is for this centre to have the information on what is happening at a national level, the objective is to collect information both from the technological centres of Public Administration, banking, industry, the various areas of Portuguese society and, with that, have an idea of the impact and scope that may have a certain type of attack.

LESSONS LEARNT

Hacktivism is seen as a new challenge for institutions and, especially, in the case of Security Forces, a hacktivist attack can cause harmful consequences, which can even influence the performance of their missions, being therefore considered a real threat, in the sense that this is characterized by contradicting the organization's objectives, producing, as a rule, material and/or moral damages.

Hacktivist groups' ability to carry out an attack is usually low, as they use tools available on the network and are not very innovative in terms of hacking, taking advantage of exploiting existing vulnerabilities. Regarding the opportunity, anyone from a computer with access to the network and with some knowledge or willingness to learn from the information available on the network is capable of developing a cyberattack, and this fact becomes worrying for the security forces.

In terms of computer security, it is often said that there is no total safety and there are no 100% secure systems, so the government and Portugal are not an exception. What has been witnessed is the creation of a set of infrastructures that allow a security structure that can correspond and respond to this type of phenomenon: the recently created CNCseg, made by the PJ in order to fight against cybercrime. Educating people is certainly something that will challenge all to realize that we also use new technologies, internet platforms and other networks that have the power to change the safety of its citizens.

Consequences of a hacktivist attack on the national security forces:

- ☑ Direct: economic, social, political, and security consequences.
- ☑ Indirect: the feeling of security, social deregulation, and ultimately, the sovereignty of the country, institutions, and families.

CASE STUDY 15: THE "GOLDEN AGE" OF "RANSOMWARE". HOW TO PREVENT AND DEAL WITH A DATA HIJACK

"Ransomware will cost victims over $265 billion annually by 2031." (Cybersecurity Ventures).

TARGETED ORGANISATION

Most of Portuguese companies are in "generation 3" of cybersecurity and the attacks are in "generation 6". In this case study we learn about how to proceed to prevent ransomware attacks like the one faced by the IMPRESA group, more and more frequently.

IMPRESA is the largest Portuguese media group, operating in three business areas — print, digital and television.

HOW INFORMATION WAS ACQUIRED?

The information for this case study was acquired through a news article about the prevention of ransomwares, which includes the interview of Rui Duro, a cybersecurity expert.

PREVENT

The pandemic times facilitated the growth of this type of ransomware attack. On the one hand, working at home, which leads to the dispersion of systems and increases the risk. On the other hand, more and more applications are migrating systems to the "cloud".

"This has several associated risks", says Rui Duro. The systems are now "in another service provider" and it is necessary "to buy technology also for the cloud because it is not secure in itself". For the specialist, "this evolution to the

'cloud' was often faster than the evolution of knowledge of information technology employees".

On the other hand, many companies have been overtaken by the sophistication of the attacks. "We (IMPRESA group) are in generation 6 of attacks and most of the companies are still in generation 3, in a very early stage of protection given the evolution of attacks. The mentality has to change, there has to be a budget, and resources to adapt to this new reality", explains Rui Duro.

IDENTIFY

On the pages of the group websites, a message similar to the one SIC (Portuguese tv channel) received, appears: "The internal data of the systems was copied and deleted. 50 TB of data is in our hands. Contact us if you want the data back".

Rui Duro explains that "usually ransomware appears in companies through what we call the placement of an initial 'payload' within the company".

This happens in different ways, such as through a phishing attack on an element of the company. Other times, someone at the company inadvertently "downloads" the malware. There is still a third way, when actors have the purpose of attacking a specific company and are looking for vulnerabilities - this is a "target attack".

After the initial malware is inside the company, it downloads a second malware, which carries out the ransomware. It then begins to make a "scan", looking for servers and other systems. The goal is to make as much profit as possible - according to the expert, for criminals "there is no point in encrypting a computer or two, the idea is to encrypt as many computers as possible, and preferably the vital ones".

Hackers then install the malware on as many systems as possible, but it does not encrypt data right away. Usually, "it is left for several weeks, sometimes longer".

Those who attack know that one of the ways companies recover is through backups - so they expect there to be a backup, and as soon as it is restored, there is an infection again.

When encryption takes place, criminals then put pressure on companies, usually to ask for a cash ransom – usually in cryptocurrencies.

RESPOND

Two days after the hacking group "Lapsus$ Group" attacked Impresa group´s websites, the sites were still unavailable.

The Portuguese Judiciary Police confirmed that it was investigating the case, together with the National Cybersecurity Centre (CNCS), as the media group had already advanced.

This delay in resetting systems is common in attacks like this one. According to Rui Duro, responsible for Check Point Software in Portugal, "the time needed to deal with these attacks varies greatly. It depends a lot on the size of the company, the attack, the company's capacity in terms of information technologies (IT) and how prepared the company was to replace the systems. In a small company, it sometimes takes a day or two, if it is a large company, it can even take several weeks and sometimes it can involve redoing an entire infrastructure".

The ransomware attack has already become a real and proximate threat to companies all over the world - and Portugal is no exception. For the European Cybersecurity Agency (ENISA), the pandemic has brought with it a “golden age” for cybercriminals.

According to the agency, between April 2020 and July 2021, there was a 150% increase in recorded attacks.

In Portugal, there is still no official data on the last year, but in the annual internal security report, for 2020, ransomware is already identified as “the most common form of computer sabotage, having maintained high rates of cases and especially affecting institutions of the government and small and medium enterprises”.

According to this report, cyber-attacks doubled in Portugal from 2019 (754 incidents) to 2020 (1418 incidents). In the area of Information Security, where ransomware attacks are predominant, in 2020 there were about 10 times more incidents than in 2019. Rui Duro, head of Check Point Software in Portugal, explains that “90 to 95% of cases are not reported or known. Companies end up recovering through backups and do not report attacks”.

According to data from a study released by the company he directs, which creates technological security solutions for the world's largest companies, Portuguese organizations suffer an average of 947 malware attacks per week, a number higher than the global average of 870 attacks. About 90% of malicious files arrive via email.

Data from Check Point Software also shows that in December 2021, ransomware attacks reached more than 2.5% of Portuguese companies.

RECOVER

A ransomware is a form of malware (combination of the English words “malicious” and “software”) designed to encrypt servers and computer storage areas.

Usually, the “hackers” behind the attack display messages demanding payment of a sum to decrypt the system and return it to the owner. According to the cybersecurity expert, ransomware attacks are increasingly sophisticated, and pirates are increasingly being seen trying to “double or triple extortion”.

In double extortion, “during the period when the malware is waiting for backup, they copy significant data from databases, email servers, financial servers, try to search for sensitive data and export huge amounts of data. And they say it's not worth trying to recover the service with backups, because they have the data hostage”.

In the case of the triple extortion, with the sensitive data in their possession, the pirates threaten to target the company's customers and suppliers if the company does not pay the ransom.

LESSONS LEARNT

To prevent an attack it´s necessary to change mindsets and assume it will happen. For the cybersecurity expert, this is the most important thing. "I have more than 30 years in the market working in this area, I started when the attacks were a joke, compared to what they are today, but even today I see decision-makers thinking that it is not yet worrying, it is not relevant and that they

think that it won't happen to them. The first step is to change that mentality. It can happen to everyone, just a short time ago it happened to EDP. When it happens, I have to be prepared for it".

Take seriously the three pillars of cybersecurity: people, processes and technology

a) People

"Often, even companies that take cybersecurity seriously focus too much on technology as a way to protect themselves and forget that it is necessary to train people to behave safely", says the expert.

b) Processes

"It is important to have a process to recover from the disaster, to manage and qualify information, to have an effective backup process, to have information repositories. Many companies are not prepared, and the first hours are complete chaos, because they were not careful to prepare the process to recover", he reveals.

c) Technology

"Using technology suited to the reality we have today. Many companies buy technology and it's what I call buying a “false sense of security” - they buy technology, but it is no longer adequate for the reality we have today. the traditional firewall, instead of buying an advanced endpoint that avoids systems encryption, a simple endpoint is used, which detects some malware but does not prevent these encryptions".

The specialist recalls that, in these cases, "panic doesn't help at all". In these situations, it is necessary to inform the authorities and never pay the ransom, as this is the same as perpetuating the crime, telling criminals that it is worth it. One of the processes that companies must have in advance, for the specialist, is how to recover from such an attack, so that there can be that calm and for everyone to know their role in this process.

CASE STUDY 16: MALWARE/ KEYLOGGER

TARGETED ORGANISATION

A small family-owned manufacturing company made extensive use of online banking. The accounting employee logged in to the online banking system with a company and a user-specific ID and password. Two challenge questions had to be answered for transactions over €1,000.

The owner was notified that a payment transfer of €5,000 was initiated by an unknown source. They contacted the bank and identified that in just one-week cybercriminals had made ten transfers from the company bank accounts, totalling €10,000. How? One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account.

The attackers were able to install malware into the company's computers, using a keylogger to capture the banking credentials. A keylogger is a software that silently monitors computer keystrokes and sends the information to a cyber-criminal. They can then access banking and other financial services online, using valid account numbers and passwords.

HOW INFORMATION WAS ACQUIRED?

The information for this cyber-attack was collected through two interviews, one with the company's owner and one with a technician of the IT supporting company. Both of them were willing to describe and give details of the incident, but they asked to keep anonymous both companies because the information was too sensitive for them.

PREVENT

A keylogger is a software that silently monitors computer keystrokes and sends the information to a cyber-criminal.

In the analysed company, the cyber security procedures and mechanisms were identified as not satisfactory. Although the company's computers had antivirus software no one was updated. Furthermore, no awareness campaigns have been carried out and some employees seemed to have limited understanding of cyber risks.

IDENTIFY

Based on the provided information, the following details were collected about the incidence:

☑ A socially engineered designed phishing email has been received with a compressed zipped file attached as verification to a supplier order.
☑ Opening the file, the malware was installed on the computer
☑ A keylogger software was installed and silently monitors computer keystrokes and sends the information to a cyber-criminal.
☑ Then the cyber-criminal uses the captured credentials to access the bank account and made the transfer using valid account numbers and passwords.
☑ The incident was identified only when the cyber-criminal tries to make a transfer higher than €1000.

RESPOND

Not having a cybersecurity plan in place, the company's response to the attack was delayed.

WHO: The attacker could not be precisely identified. Only an email address was known and the possible origin.
WHOM: not-specific targeted
WHY: Sensitive data gathering and use those for stealing money
WHAT: Company bank account credentials
HOW: Keylogger, silently monitors computer keystrokes

STRATEGY: The threat started on a computer without antivirus. A cleaning process was performed by a company's ICT expert. The bank account shut down and credentials changed. The ICT company helped them to complete a full cybersecurity review of their systems and identify what the source of the incident was. They also recommend upgrades to their security software.

RECOVER

IMPACT: The company shut down their bank account and pursued legal action to recover its losses. The business recovered a small part of the losses. No money for time and legal fees were recovered.

RECOVERY: The recovery strategy was focused on shutting down the bank account to avoid any more losses. Other actions were, cleaning the compromised computer and the compromised electronic mailbox. Check all company's computers for any other attack.

STRATEGY: The company should implement various actions to prevent such incidents. Its strategy must concentrate on the following actions/steps:

- ☑ Implement security policies such as Change Password Policy and Account User Management Policy.
- ☑ Install and maintain an updated Antivirus/Antimalware software.
- ☑ Perform training programs to assure employees' awareness.
- ☑ Restrict Web-Based Content.
- ☑ Perform regular checks and audits.
- ☑ Execute Prevention and implementation of a risk management system.

LESSONS LEARNT

- ☑ Notifications - set up transaction alerts on all credit, debit cards and bank accounts.
- ☑ Access control. Restrict access to sensitive accounts to only those employees who need access; change passwords often.
- ☑ The company should evaluate their risk and evaluate cyber liability insurance options.
- ☑ Choose banks that offer multiple layers of authentication to access accounts and transactions.
- ☑ Create, maintain, and practice a cyber incident response plan that is rapidly implementable.
- ☑ Cybercriminals deliver and install malicious software via email. Train employees on email security.

CASE STUDY 17: A STOLEN COMPUTER CAUSES SERIOUS DATA BREACH

TARGETED ORGANISATION

A 10-person consulting company sent a small team to Hungary to complete a customer project. During their stay, the senior consultant left his work-issued laptop, which had access to sensitive customer information and bank details of the company, in a locked car while running a job. The car was broken into, and the laptop was stolen. Unfortunately, the data on the pc was unencrypted because the employee did not apply the company's policy to encrypt all sensitive data on his pc. The company was now afraid of a cyber-attack on its systems, bank accounts and customer data leakage.

Type of attack: Physical theft of an unencrypted pc. Encryption is the process of scrambling readable text so it can only be read by the person who has the decryption key. It creates an added layer of security for sensitive information.

HOW INFORMATION WAS ACQUIRED?

The information needed to describe the incident was collected through an interview with the senior consultant of the company and the IT technician of the ICT company that supports the consulting firm. The interaction was performed with the condition of keeping sensitive information anonymously. Even if the interviewee was willing to describe the incident, some encryption information could not be obtained and this is the reason that was asked from the supporting ICT company to enlighten the case.

PREVENT

Although the incident is not a clear cyber-attack incident, it is one serious and very common incident that causes a series of significant cyber-attacks.

In the case of the analysed company, from the perspective of cyber security, specific policies and mechanisms operated, but these were not implemented by some employees due to their low experience in the field of information and cyber security risks.

IDENTIFY

The employee immediately reported the theft to the police and his company. The bank also was informed to monitor account transactions. The company informed accordingly the ICT supporting company to disable the laptop's remote access and began monitoring activity. The laptop was equipped with security tools and password protection. Data stored on the hard drive was not encrypted – this included sensitive, customers' data and bank details of the company.

For a behaviour-based identification of this attack, the following MITRE ATT&CK techniques can be used:

- ☑ T1027 - Obfuscated Files or Information
- ☑ T1036 – Masquerading
- ☑ T1586.002 – Compromise Accounts: Email Accounts

RESPOND

Response: The company must follow state laws as they pertain to a data breach. The state laws and the EU regulations on GPDR are very strict with high-cost fines.

- ☑ **WHO:** The attacker could not be identified. Only the place of the incident was known.
- ☑ **WHOM:** not-specific targeted

- ☑ **WHY:** Sensitive data gathering and gaining money from the sale of the stolen equipment
- ☑ **WHAT:** Customers' sensitive data and company's bank details
- ☑ **HOW:** equipment loss, sensitive data leakage and bank account attack
- ☑ **STRATEGY:** The threat started on a computer without antivirus and has spread laterally. A cleaning process was performed by a specialised IT&C company.

RECOVER

IMPACT: The consulting company spent more than €20,000 on implementation, monitoring, and operational improvements. A data breach does impact a brand negatively and trust has to be rebuilt.

The main consequences of the attack were as follows:

- ☑ Data loss
- ☑ PC loss
- ☑ System compromise
- ☑ Financial costs

RECOVERY: The recovery strategy was focused on minimising the brand reputation and monitoring and controlling the company's internal systems and bank accounts. Preventively, all bank account credentials changed, and employee systems privileges were suspended and changed.

STRATEGY: The company should implement various actions to prevent such incidents. Its strategy must concentrate on

- ☑ Perform training programs to assure employees' awareness
- ☑ Perform regular checks and audits
- ☑ Execution Prevention and implementation of a risk management system

LESSONS LEARNT

- ☑ Companies must establish and train employees on secure handling of work-issued devices.
- ☑ Devices must be safely stored when not in the immediate presence of the employee.
- ☑ Companies must take steps to encrypt data wherever it is stored or transmitted.

- ☑ Employees should have a clear understanding of the importance of encryption and how to use it.
- ☑ Companies must understand and know their responsibilities under the data breach notification laws of the country in which they operate.
- ☑ A regular review of the company's security practices is imperative in modern organisations to prevent incidents, discover vulnerabilities, and reduce the impact of incidents.

CASE STUDY 18: DDOS ATTACK STOPS IMPORTANT SERVICES

TARGETED ORGANISATION

The targeted organisation was a hosting providing company. Attackers levelled a massive distributed denial-of-service attack against a specific website in mid-December 2021, topping a bandwidth of 1.5 gigabits-per-second and almost 100 million packets-per-second, the largest attack faced by a hosting company.

The company believes the attacker focused on the websites with online casino games, and the hosting provider was not the actual target. The DDOS attack causes the termination of the availability of the services of the customer for more than 12 hours.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

"There was a 57% increase in Mirai botnet variants identified in 2019. Mirai variants are typically used for brute force attacks on IoT devices. These attacks increased by 51%, while web exploits rose 87% in 2019.." (MCCART, 2022).

HOW INFORMATION WAS ACQUIRED?

The information needed to describe this cyber-attack was collected through two interviews (face-to-face meetings), one with the company's CEO and one with an IT engineer of the company. Both were willing to describe and give details of the incident, but they asked to keep anonymous both companies and their names because the information was too sensitive for them.

PREVENT

Although the hosting provider has several cyber security procedures and mechanisms, it seems that the attackers found a vulnerable point to explore.

The company's technician noticed that the website suddenly became slow, but they assume that it was a legitimate spike in traffic due holiday season. The attack was identified just after the website became unavailable and the customer complained.

IDENTIFY

The attackers used traffic from sources worldwide. It seems that the denial-of-service attack was created by a Mirai botnet. And because the Mirai botnet has a capability of sending around 600 megabits-per-second they used a second-level attack with a different Mirai botnet.

Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or "zombies". This network of bots, called a botnet, is often used to launch DDoS attacks.

The hosting provider used traffic analytics tools to identify the attack. The basic characteristic of the attack is the high volume coming from the same series of IP addresses. The engineers succeed to isolate those IPs and the website came back.
After that, they try to identify why the traffic analytics tool did not detect the attack from the first stages.

According to the MITRE ATT&CK framework, this incidence can be described as follows:

- ☑ T1499 - Endpoint Denial of Service
- ☑ T1498 - Network Denial of Service

RESPOND

- ☑ **WHO:** The attacker cannot be identified. The attack came from all over the world
- ☑ **WHOM:** The target was a specific website hosting online casino games.
- ☑ **WHY:** To interrupt its operation.
- ☑ **WHAT:** Company website.
- ☑ **HOW:** DDOS attack using Mirai botnets.
- ☑ **STRATEGY:** The attack started on a hosting provider sever to interrupt the operation of a specific website. The traffic analytic tool failed to alert for the possibility of a cyber-attack. The company increased the sensitivity of the alarms in the traffic analytics tool so they avoid similar incidents in the future.

RECOVER

IMPACT: The hosting provider had some extra significant costs to cover the attack and also, they had serious reputation damage. They had the extra labour cost to recover the website and the penalties on the SLA agreement with the customer. The total cost was estimated to be approximately €40,000.

RECOVERY: The recovery strategy was focused on isolating the attacking IPs to stop the attack and recover the operation of the website. Other actions were, to increase the alarms' sensitivity of the traffic analytic tool. Check all hosting servers and services for any other attacks or suspicious activities.

STRATEGY: The company should implement various actions to prevent such incidents. Its strategy must concentrate on

- ☑ Increase the sensitivity of the traffic analytic tool

- ☑ Install a second tool for extra security
- ☑ Perform training programs to assure employees' awareness
- ☑ Restrict some IP ranges
- ☑ Perform regular checks and audits
- ☑ Execution Prevention and implementation of a risk management system
- ☑ Certify their infrastructure and services on the ISO27001 and ISO22301.

LESSONS LEARNT

- ☑ Disruption comes in many forms. Disruptions or delays can come in many forms, especially for hosting providers. When an attack is identified, the appropriate response teams must dedicate resources to deal with it.
- ☑ Many cyberattacks are easily preventable. Sophisticated cyberattacks can cause a lot of damage, but many of them can be easily prevented with the right security in place. It is important to build a strong and proactive security management system to stop the attacks. Such a management system requires continuous maintenance, monitoring all systems and devices in the network, including updating the tech and applying security patches for known exploits.
- ☑ DDoS attacks should be taken seriously. Today's DoS and DDoS attacks are different seeing as they are more vicious, pointed, and capable.
- ☑ No time limit. Network layer attacks can last longer than 48 hours, while application-layer attacks can go on for days. Infiltration of systems and networks for spying—weeks and months.
- ☑ Cybersecurity should be a priority. Cybersecurity should be one of the highest priorities for all entities operating in today's landscape. These attacks have grown to be sophisticated, targeted, capable, and unregulated. All threats should be taken seriously, including DDoS attacks, which are growing more common.

CONCLUSION

Based on the diversified portfolio that is presented within the ENCRYPT 4.0 Documental battery on cyber-attacks, the following conclusions could be drawn:

- ☑ With the development of ICT and in the context of Industry 4.0, cybersecurity has growing importance and **companies lacking adequate cyber defence are putting their operations at serious risk.**
- ☑ **Employees play a key role in cyber-defence** therefore employees both within SMEs and big enterprises should receive at least basic training on how to protect company data and to work with sensitive information as more than many cyber-attacks happen due to lack of knowledge regarding these aspects, especially in the context of remote working during the COVID-19 pandemic.
- ☑ **SMEs disregarding of the sector they operate in, are becoming primary targets for hackers and organised cybercriminals** but at the same time only 1/3 of SMEs have a plan how to contain a potential cyber-attack, hence SMEs need to foresee cybersecurity as top priority in order to ensure their competitiveness in the long run.

REFERENCES

1. Acronis, 2020. The NHS cyber-attack. [Online] Acronis. Available at:https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/

2. Barber, B., 2016. William Hill apologise after website attack. [Online] Racing Post. Available at: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (Case study 6)

3. Blue goose, n.d. Information Security at William Hill. [Online] blue goose. Available at: https://bluegooseis.co.uk/work/william-hill (Case study 6)

4. Braue, D., 2022. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. [Online] 2022 Cybersecurity Ventures. Available at: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

5. Cook, S., 2022. 20+ DDoS attack statistics and facts for 2018-2022. [Online]. Comparitech. Available at:https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

6. Craver, R., 2015. Hanesbrands database hacked 900K phone, online customers affected. [e-journal] *Winston-Salem Journal.* Available at: https://journalnow.com/business/hanesbrands-database-hacked/article_543b338e-3664-11e5-b77e-c77df1e08b5c.html (Case study 4)

7. Cyber Startup Observatory. Available at: https://cyberstartupobservatory.com/ (Case study 4)

8. CyberNews, 2021. Thousands of Humana customers have their medical data leaked online by threat actors. [Online] 2022 Cybernews. Available at: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/ (Case study 5)

9. CyberTalks, 2022. Top 15 phishing attack statistics (and they might scare you) [Online]. CyberTalks. Available at: https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

10. Cyware , 2018. Humana websites hit by sophisticated spoofing attack from 'foreign countries'. [Online] Cyware. Available at: https://cyware.com/news/humana-websites-hit-by-sophisticated-spoofing-attack-from-foreign-countries-5ac77624 (Case study 5)

11. Dissent, 2018. Humana notifies members after credential stuffing attack on Humana.com and Go365.com. [online] 2009 – 2022, DataBreaches.net and DataBreaches LLC. Available at: https://www.databreaches.net/humana-notifies-members-after-credential-stuffing-attack-on-humana-com-and-go365-com/ (Case study 5)

12. EUROPOL, n.d. World's most dangerous malware EMOTET disrupted through global action. [Online] EUROPOL 2022. Available at: https://www.europol.europa.eu/media-

press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

13. Kolbasuk McGee, M., 2018. Humana Notifying Victims of 'Identity Spoofing' Attack. [online] *Data Breach Today*. Available at: https://www.databreachtoday.asia/humana-notifying-victims-identity-spoofing-attack-a-11153 (Case study 5)

14. McCart, C., 2022. 15+ Shocking botnet statistics. [Online] Comparitech. Available at:https://www.comparitech.com/blog/information-security/botnet-statistics/

15. Mimecast, 2022. Confronting the NEW WAVE OF CYBER ATTACKS: The State of Email security Report 2022. Mimecast. Available at: https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-2022.pdf

16. Moore, J., 2022. Top 10 List of Cybersecurity Facts for 2022. [Online] Elevity. Available at: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

17. Morran, Ch., 2015. Hanes Website Is The Latest, Oddest Victim Of Data Breach. Consumerist. Available at: https://consumerist.com/2015/07/30/hanes-website-is-the-latest-oddest-victim-of-data-breach/ (Case study 4)

18. StackHawk, 2022. What is Command Injection? [Online]. StackHawk, Available at: https://www.stackhawk.com/blog/what-is-command-injection/

19. The Cyber Wire, n.d. Definition of Spoofing. [Online]. The Cyber Wire. Available at: https://thecyberwire.com/glossary/spoofing

20. VentureBeat, 2022. Report: Average time to detect and contain a breach is 287 days. [Online] VentureBeat. Available at: https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/

21. Verizon, 2021. DBIR: 2021 Data Breach Investigation Report. Verizon, 2021. Available at: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

22. Wallarm, 2021. The Biggest Hacker Attacks on Gambling. 10. [Online] Wallarm. Available at: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (Case study 6)

ENCRYPT 4.0

Co-funded by the Erasmus+ Programme of the European Union

PROJECT PARTNERS

ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable The European Industry to Overcome the Shortage of Cybersecurity Professionals

The ENCRYPT4.0 Project (2020-1-RO01-KA202-079983) aims to enable manufacturing SMEs management to adopt a proactive approach towards cybersecurity by supporting them in the process of analyzing, identifying and tackling the cyber risks and threats applicable to their organization. By promoting interactive project-based learning with regards to boosting cyber-security skills and competences of SMEs' employees or/and cybersecurity professionals.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș - Romania

Project coordinator

European Center for Quality Ltd., Consulting company - Bulgaria

Instituto de Soldadura e Qualidade, Technological institution - Portugal

Avantalia, technology-based SME - Spain

FH Joanneum, University of Applied Sciencies - Austria

PCX Management, Computers & Information Systems Ltd. - Cyprus