Advanced Research on Information Systems Security, an International Journal

Detection and Handling of Threats in Pre-Established Networks Through a Junior Perspective in Internship Scenario.

Carlos Barros [a]*, Nuno Mateus-Coelho [b]

[a] *IPCA – Polytechnic of Cávado and Ave, Barcelos, 4750, Portugal*
[b] *IPGT – Polytechnic Institute of Management and Technology, 4450, Vila Nova de Gaia, Portugal*

[a]*Email: a17441@alunos.ipca.pt*

[b]*Email: nuno.coelho@isla.pt*

Abstract

In this paper there are two questions that we seek to answer, what are the tools used in the industry nowadays regarding its cybersecurity? How is cybersecurity being approached and dealt with by the companies and their greatest difficulties? Along the way it's observed how the entire interaction with clients is made as also how the investigation on possible threats is conducted and handled, passing through how to detect, analyse and interact with the client team in the mitigation of it, this taking into consideration their infrastructure and capabilities. This paper is taken from the point of view of a junior utilizing free tools to analyse threats and dealing with attempts of infiltrating the network utilizing social engineering tactics as well as more technical skills.

Keywords: cybersecurity; threats; infrastructure; free tools

* Corresponding author.

1. Introduction

With the increase in the number of attacks to computers and systems over the years it makes sense, more now than ever, for companies to dedicate part of their annual budget to security information technology, since the probability of suffering a data leak has increased so consistent. A report coordinated by the Ponemon 1 and IBM Security [1] states that in 2018 the probability of occurrence of a data leakage was estimated to be 27.9%, and in 2019 of 29.6%, which represents an increase of almost 2%. In order to have a clearer perception of the importance of this increase, we need to consider the year 2014, in which the probability was 22.6%, this means that there was a 7% increase in 6 years. Furthermore, it appears that the probability of the occurrence of a Data leakage has increased over the years. On average [1], the impact caused in costs in the first year of the incident is 67%, 22% in the second year and 11% in the years following. In 2020, the IBM study [1] reports that the overall average cost of a data breach was of 3.86 million dollars, of which 1.52 million dollars were due to the loss of customer trust. However, it is not just companies that are at risk of being attacked, as the ordinary citizen is also exposed [2], mainly with the increased use of IoT's, these present more and more complex risks as their use requires its constant maintenance and update as well as knowledge about its capabilities and methods of operation. Being presented then, by this growing increase in threats, it is necessary to create security mechanisms and methodologies so that they can be mitigated and that the threats that present themselves in today's critical environments are controlled.

2. Objectives

In this paper, it is intended that the following topics be addressed:

- Common practices used by companies to safeguard their data
- Infrastructure protection techniques
- Threat mitigation mechanisms
- Procedures in case of failure and exposure

3. Background

So, in order to start answering these questions and address the previous topics it was needed to join a company that would give support and for their expertise.

In the company where this research was done there are several teams responsible for virtually every area of cybersecurity, from the Malware team that analyses the workings of software caught in the wild, to more exciting areas as the Auditing team that deals with pen-testing and analyses of vulnerabilities and their exploitation in the client infrastructures. In this particular case, the research was made as a internship and was carried out in the Integrations team, for two reasons, first because it is the one that has the broader scope of tasks and responsibility and that perhaps reaches more areas and tools, secondly, because the team of integrations was looking for someone to be in direct relationship with a client on a daily basis in a permanent allocation regime, this client is one of the largest publishers in Portugal, so this turns this challenge even more attractive given the magnitude of the

infrastructure that supports this customer and the opportunity for personal growth. These two situations fit directly into the two areas in which the research was intended to fit.

4. Client

4.1. Client Service Background

This is not a new customer in the company and as such, there is already trust between the teams from both sides.

From the internship company, there is already an employee in placement who has been accompanying the client and acting as an intermediary between the two of them.

Thus, the service was transferred over a month, consisting of two phases, first, monitoring with the placement in order to understand the "uses and habits" of the customer, for example, what type of monitoring they usually receive, what formal nomenclature was used, with whom certain issues were discussed, the hierarchical stratification within the client, the peculiarities of the infrastructure and users, the problems being resolved, the recurrent problems waiting for a fix and the problems that could be seen in the future as well as more technical issues such as network diagrams and reporting models of the investigations made, as well as the work methods that were being used.

In the second phase, it was expected that the follow-up would have produced results and it became the intern's responsibility to perform these functions. These were monitored very closely, at least initially, by the placement that validated the investigations and their reports, the interactions with the customer were also oversighted in order to guarantee the continuity of the quality of service for the customer. Later on, the help of the previous placement started to show itself only as a last resort for solving doubts or problems and also for the persistence of knowledge of a situation that may or may not have been properly documented.

4.2. Client Infrastructure

Before the threat analysis can be carried out, they must first be recognized.

For this process to be carried out, a logging system that allows for an initial detection is needed, for which a Checkpoint firewall and a SmartConsole R80 system were used as its interface.

The firewall will block and authorize requests based on, certain predefined and custom, rules that are predefined and personalized, but which do not always manage to catalogue communications with 100% reliability. For further analysis, SmartConsole was used.

This is an "integrated security management solution, which includes policies, recording, monitoring, event correlation and reports" [3], it will allow for an analysis of user communications, thus enabling the validation of possible threats as for example the detection of anomalous behaviours that were not automatically detected by the behaviour detection mechanisms, as well as the categorization of malicious addresses in their proper categories.

4.3. Investigation

Has part of the normal day-to-day operations several reports were being produced and analysed.

These showed easily and readily a vast amount of information on the traffic that the infrastructure produced in the day prior, they contained a compilation of data into useful information as e most traffic which could indicate an anomaly as also the most visited which could demonstrate changes in patterns of use of the users, other several different stats were also showed like the most used type of traffic, HTTPS, HTTP, UDP, etc.

In order to continue the analysis, it is necessary to use all the tools available, and the most important tool will always be common and critical sense.

It can be considered, for example, that a website that allows you to download a network testing tool is not alarming for a user who is a systems administrator, however, for a Designer it will certainly raise doubts as this is not a behaviour considered normal or typical thus raising suspicions and alarms.

However, this sense of criticism is not enough, other analysis tools are needed to help separate malicious from trustworthy behaviours [4].

There are several companies on the Internet that offer paid and also free threat analysis services, both for websites and files, but… "if something is free, you're the product" [5], they collect the data that is freely given, such as a web address to validate the maliciousness or threat level. Thus, using user data, they build ever more accurate threat analysis models without needing to spend resources collecting information themselves. These free services were used as the basis for threat analysis.

Following, there is a small analysis of each of these services used, but in their entirety, they can be divided into two major categories, those that allow you to assess their maliciousness and those that allow you to test, and in some cases even interact with the test object, its behaviour with the user and also with the machine itself.

4.3.1. VirusTotal

This platform provides a URL, IP and file maliciousness reputation analysis. It serves as an aggregator of many other services as for example Fortinet, Armis, AlienVault, ESET, Kaspersky, Sophos, etc., all major players in the cybersecurity industry, which allows its users a very solid and concrete first analysis which often results in a simple consultation of this service to demonstrate with great certainty the level of maliciousness and threat of what is being validated.

4.3.2. Abuse IPDB

Here is another free tool for analysing maliciousness to a URL and IP's. This service is mostly supported by its community, instead of the VirusTotal platform that uses ratings from other companies in the cybersecurity area. The maliciousness ratings of this platform are based on the evaluation and categorization of threats by the platform's own users and collaborators which, although presenting some degree of risk in terms of the accuracy

of the ratings, as it depends on the reliability of their evaluation, presents the advantage of the numbers, if out of 100 people, only 1 of them introduces false or incongruous information, the platform reaches a very interesting level of reliability.

4.3.3. IBM X-Force Exchange

Like the previous ones, the IBM X-Force Exchange service is also a maliciousness analyser of addresses and IP's as well as files, however, it presents a monitoring of its maliciousness, its category and also the degree of risk over time. that allows us to assess persistence and their past behaviour.

Their assessments "come from internal infrastructures and databases, as well as open-source content and third-party partnerships to augment this information." [6].

4.3.4. Any Run

This is an interactive sandbox that presents the possibility of analysing a threat in an isolated environment, allowing the behaviour of these to be analysed without having to take the necessary precautions that it would have to be taken in case this was inside a live infrastructure. It also shows instantly without any input from the user all the connections and their maliciousness that are being made by the sandbox and our potential threat, giving us a quick summary of the connections that the threat does.

4.3.5. Joe Sandbox

Joe Sandbox [7] is considered by Splunk as "the industry's most advanced automated, in-depth malware analysis engine." [8]. It automatically performs a scan, of files or addresses, based on their reputation, maliciousness, and activities. In other words, it compares its behaviour with the Mittre Att&ck Matrix [9], a behaviour analysis platform, which provides indicators of possible attack vectors [10] that could be exploited,

It evaluates its reputation according to models of AI, analyses CPU usage, memory, accessed files and registers, network behaviour and others to present a analysis that shows which category, if any, the threat falls under, be it ransomware, phishing, spyware, etc.

4.4. Procedures

After the threat being analysed is considered malicious and it is concluded, therefore, that it is an offense, it is necessary to define what action should be taken in order to neutralize it. The time has come to get in touch with the customer's IT team.

This contact is made by email and following some specific rules in order to standardize the interaction with customers.

- The presentation of the investigation carried out is then made as follows:
- Threat presentation.
- Proof of communications.
- Details about the threat.
- Analysis of the threat and resources consulted.
- Assets affected.
- Conclusion with recommendations to be taken.

5. Notable Situations

During the internship, it was possible to verify a wide range of situations, from simple access to less secure and recommended websites to malicious software installed on the machines themselves and infiltration techniques such as SQL Injection and XSS.

One of the situations that generated some agitation was that of a possible direct attack on the infrastructure.

This situation was detected not by analysing the behaviour of users, but by analysing the behaviour of the network in terms of volume of communications. In this case communications with the signature Command Injection Over HTTP Payload were discovered.

This vulnerability consists in the exploitation of a misconfiguration, “sanitization” and/or treatment of user-supplied data in which the attacker is able to execute commands on the existing system on the server side, allowing the latter to control the system completely or partially, exfiltration of information, among others, was the one exploited. This attack had a somewhat common behaviour of the attackers, as a rule, companies, and their IT teams and/or cybersecurity teams suffer a decrease in responsiveness and visibility over their network when they go to their rest period at the end week, as they become less operational and possibly less responsive, this attacker took advantage of this period to attack and began his attempts to penetrate the network around midnight on Friday.

This situation lasted throughout the weekend and was only detected during the normal daily analysis carried out on Monday.

After the alert was given that something out of the ordinary was going on, the Audit team was activated, which is the one in charge of malware analysis, penetration tests, among others, to assess the situation. After analysis, they

came to the conclusion that the attacker was trying to infiltrate a variant of the Emotet malware, this one has a habit of occupying the most used malware tops in the customers' networks for ransomware around the world.

This situation was already relatively late in this internship and only after it was it known that although this attack was not successful, the customer would implement new technologies in order to create yet another barrier of entry to these threats.

6. Conclusion

During this internship, it was thus possible to find diverse information about the good and bad practices that populate the reality of companies that support the multitude of existing customers, not only in Portugal or in the physical world we live in but also in the virtual world that represents a new frontier in business development and interpersonal and commercial relationships.

This entire environment represents a new growth opportunity for companies in the virtual environment, but it does not present itself in a completely free of dangers and setbacks scenario. In this new challenge that we deal with, that goes by the name by Online Security, it is not easy to get a clear picture of what is an opportunity or if it is someone trying to take advantage of a given hard work, given company, or existing partners.

Thus today, there is a battle going on that is very similar to a castle siege of the Middle Ages. The closed and protected riches are coveted by an army of nameless shadows, who have no affiliations or causes other than their own gain and the destruction of what has been built by others, who try to find cracks in the walls to infiltrate and manage to control companies and/or stealing what is most valuable to them, which is the information that allows them to grow and function normally. It is therefore necessary that highly specialized teams, armed with techniques, equipment and products that fight these threats, are committed to the defense of companies and their employees [12].

These teams, unlike companies, face a different war, in this case we can consider that they are facing an arms race against all the opposing actors who, in this same theater, are trying to innovate and explore new angles of attack.

For some years now, attack methodologies have been expanding, these initially focused mainly on the attacker's technical capabilities, for the subversion of systems at will, through the attacker's intensive knowledge of the details of each platform, however nowadays we see that this methodology is no longer enough. Systems that previously had flaws to be corrected have already been fixed, and actors who were previously on the attackers' side now find themselves for various reasons switching positions to systems and infrastructure defenders and bring with them a lot of knowledge of how to defend them. So, we see an increase, not in attempts to corrupt systems, but in people. These more fragile and susceptible to attacks, as they are not governed by static content or inflexible programming, can be persuaded, coerced, or deceived into providing access to the target information that the attacker wants to access, using apparently normal email or browsing the Internet on a personal smartphone [13] for example.

Knowing this, at this stage it was possible to find cases that touched both methodologies, highly specialized cases were observed and directed to key systems in order to achieve a base of attack on the rest of the infrastructure as well as attempts to deceive employees into accepting to give access without knowing that Social Engineering techniques were being used. Different tools from various areas of cybersecurity were also addressed, from basic server configuration, vulnerability detection tools, traffic analysis, among others. We concluded that this internship was a success, having achieved all the proposed objectives and even culminating in a work proposal in this company.

References

[1] I. Security, "Cost of a Data Breach," 2020.

[2] N. Coelho, B. Fonseca e A. Castro, "Paranoid operative system methodology for anonymous & secure web browsing, doctoral project," in Atas da Conferência da Associação Portuguesa de Sistemas de Informação, Portugal, 2017.

[3] C. P. S. T. Ltd, "Check Point R80.10," [Online]. Available: https://www.checkpoint.com/downloads/products/r80.10-security-management-architecture-overview.pdf. [Accessed em 20 08 2021].

[4] M. M. Cruz-Cunha e N. R. Mateus-Coelho, Handbook of Research on Cyber Crime and Information Privacy, IGI Global, 2020.

[5] R. Serra, Realizador, Television Delivers People. [Movie]. USA: Richard Serra, 1973.

[6] I. XFE, "Perguntas mais frequentes," [Online]. Available: https://exchange.xforce.ibmcloud.com/faq. [Acedido em 16 09 2021].

[7] J. S. L. 2021, "Automated Malware Analysis - Joe Sandbox Cloud Basic," © Joe Security LLC 2021, [Online]. Available: https://www.joesandbox.com

[8] S. Bühlmann, "Joe Sandbox Add-on," 25 2 2021. [Online]. Available: https://splunkbase.splunk.com/app/4499/. [Accessed on 20 9 2021].

[9] T. M. Corporation, "General Information | MITRE ATT&CK," The MITRE Corporation, [Online]. Available: https://attack.mitre.org/resources/faq/.

[10] Y. Shin, K. Kim, J. J. Lee e K. Lee, "Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity," em 2021 World Automation Congress (WAC), Taipei, Taiwan, 2021.

[11] A. P. Bianzino, D. Pezzuolo e G. Mazzini, "Who is whois? An analysis of results consistence," em 2014 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2014.

[12] J. Acharya, A. Chuadhary, A. Chhabria e S. Jangale, "Detecting Malware, Malicious URLs and Virus Using Machine Learning and Signature Matching," in 2021 2nd International Conference for Emerging Technology (INCET), Belagavi, India, 2021.

[13] N. M. Coelho, M. Peixoto e M. M. Cruz-Cunha, "Prototype of a paranoid mobile operating system distribution," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019.