ANALYSIS OF THE 2019 RANSOMWARE ATTACK AT THE MAASTRICHT UNIVERSITY

Giulia Antonini – 0000965213
University of Bologna - International relations (9084)
Cybercrime and cybersecurity 2020/2021 – Prof. Giacomello, prof. Siroli

Table of contents

1. Introduction

According to the Exprivia observatory, between January and March 2020, there have been, in Italy only, 349 events including cyber-attacks, incidents and privacy violations, with a growth of 47% on the previous quarter and seven times more than in the first three months of 2020 (Exprivia, 2021). Among the techniques most exploited by cyber-criminals, phishing and social engineering continue to be the most popular with about 60% of cases (almost double compared to the last quarter of 2020), which particularly affects distracted users with little knowledge of how cybercriminals lure their preys using e-mails or social networks. This is followed by malware, which aims to steal sensitive information, mainly by spying on users' banking activities. On the third step of the podium there are the techniques with which the attackers exploit already known vulnerabilities. In general, there is an overall increase of 612% in attacks, incidents and privacy violations (Federprivacy, 2021)

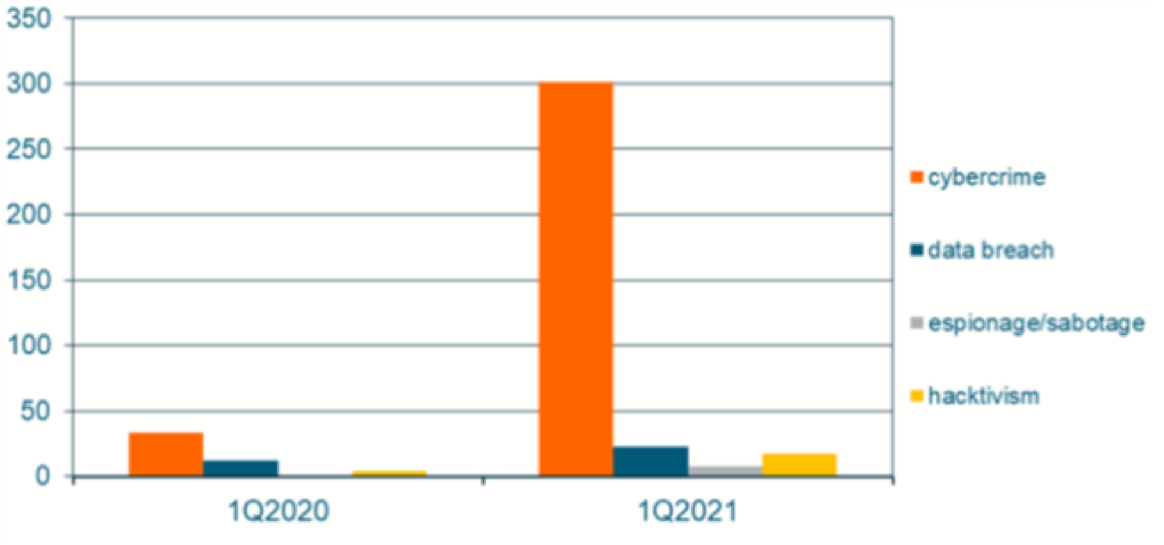


Figure 1 Image taken from "Threat Intelligence Report" (Exprivia, 2021)

Compared to 1Q2020, the growth of Phishing / Social Engineering attacks was over 1265% and those of Malware by 469.2%.

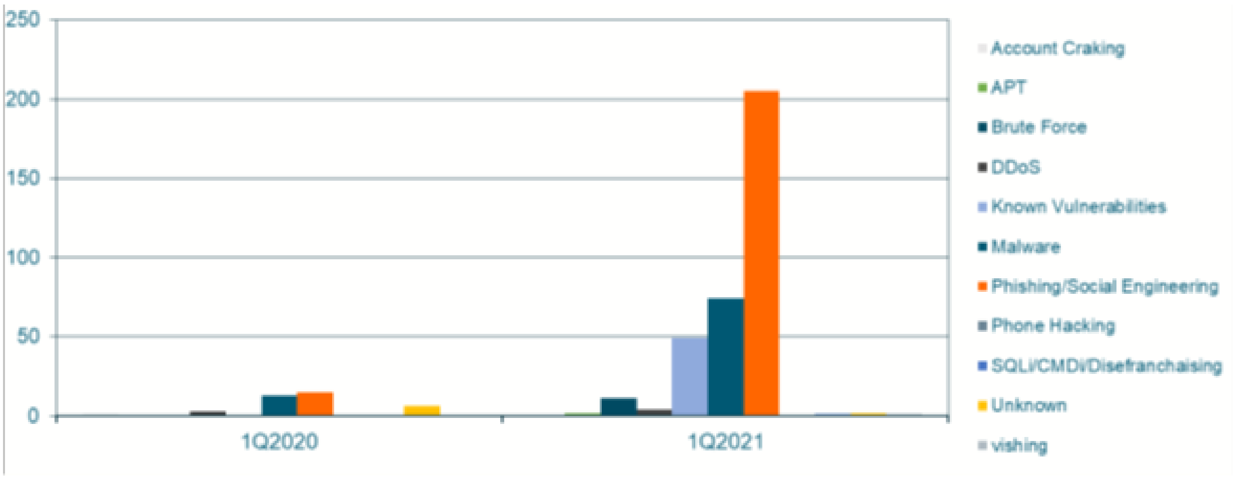


Figure 2 Image taken from "Threat Intelligence Report" (Exprivia, 2021)

The interest in the diffusion of ransomware is due not only to the high ransom required to obtain the decryption key of the encrypted data, but also to the ransom almost always required for not spreading the data exfiltrated, data that yield huge amounts of money on the black market and in the Dark Web. Among the most dangerous ransomware there are Ragnarok, LocktheSystem and JobCrypter, that in the first months of 2021 wreaked enormous damage in various sectors such as healthcare and business, even compromising private citizens.

This trend is also reflected in the number of attacks in all European states. However, it seems like there is an asymmetry between the relevance of this threat and the measures adopted by both the private and public sector to counter it. According to the Sophos annual report "The State of Ransomware 2021", around one third of the companies hit by a ransomware, decided to pay the ransom (Sophos, 2021). So, we can definitely claim that cyberattacks are becoming one of the biggest threats to our society, even though many of us are not prepared to fight it back.

One of the latest victims of a serious ransomware attack is the University of Maastricht, that in December 2019 had to pay 30 bitcoins, which at that moment equalled to 220,000 American dollars, to restore its database. I decided to analyse this case study because it highlights, first of all, which are the most common mistakes in the planning of a business recovery plan and, in general, in the prevention of cyberattacks, but also the fact that Universities have become one of the primary targets for cybercriminals.

In the first part of this paper, I will explore the context under which the attack has been carried out and I will explain some technical definitions. In the central part, I will provide a detailed analysis of how the attacked has been discovered and the mitigation process implemented by the CISO of the University and the cybersecurity agency FOX-IT. In this part I will also examine in detail all the steps that the criminal organization TA505 followed to enter into the University network and install the malware. In the third part I will try to recognize, *ex-post,* what the University should have done to avoid paying the ransom and try to draw a lesson. Finally, I will come to general conclusions about cybersecurity in universities.

2. Context

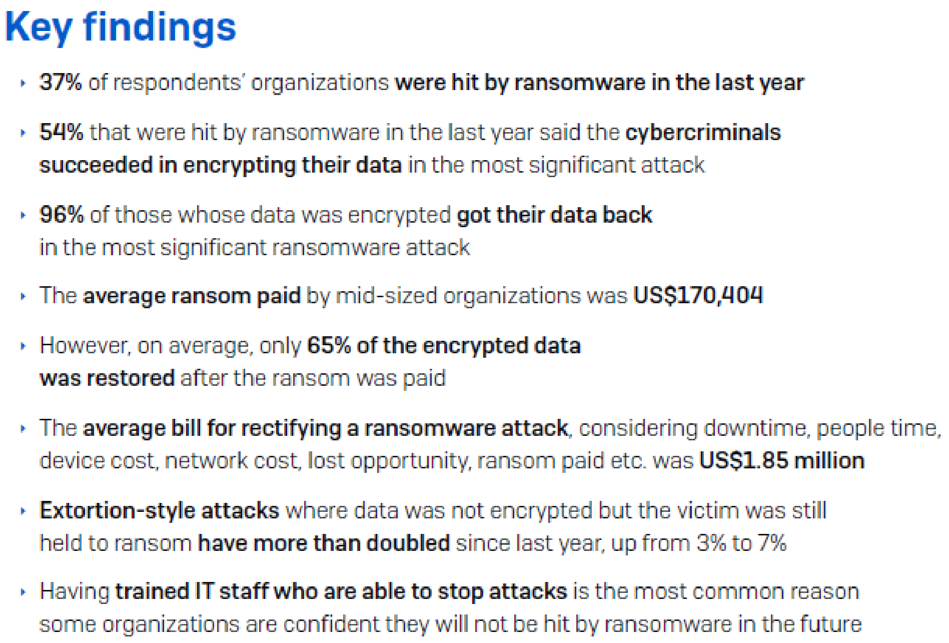
According to University officials, hackers infiltrated the University's systems via two phishing emails that were opened on two unified messaging systems on 15 and 16 October. Once the malware spread inside the University's computer system, blocking the e-mail boxes as well as the terminals, the hackers made their request which was examined by the top management of the University. It was confirmed that all DHCP servers, network drives, exchange servers, domain controllers were all encrypted and that the origin of the data breach was "Clop", a ransomware discovered in February 2019, which is a variant of the CryptoMix ransomware (Nexsys, 2021). The University leaders turned to the cybersecurity company Fox-IT, in order to analyse what happened and the investigation conducted led to the identification of the hackers, the Russian-speaking criminal group TA505. It was the vice president of the University, Nick Bos, who explained why it was decided to satisfy the requests of the hackers: *"The damage of that to the work of the students, scientists, staff, as well as the continuity of the institution, can scarcely be conceived".*

The main concern was that the attackers might be looking for scientific data, which Maastricht University processes in large quantities, but according to Gert van Doorn, a spokesman for the Dutch University, it appears that such data is safe: *"We no longer have access to the data. Our scientific data is, however, further protected in a different system. We are investigating whether hackers will be able to access it, but the expectation is that it will be very difficult for that to happen".*

2.1 What is a ransomware?

A ransomware is an extortion software that can lock down a device (or an entire network) and demand a ransom in exchange for release. In most cases, the genesis of ransomware infections is as follows: the malware enters the network and, depending on the type of ransomware, the entire operating system or individual files are encrypted. Finally, a ransom is demanded from the victims involved to have the encrypted files back. The first cases of ransomware occurred in Russia in 2005. Since then, this technique has spread around the world and continues to be successful in its various forms (Kaspersky, 2021).

The British security software and hardware company Sophos commissioned the independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries in January and February 2021. The following illustration summarizes the most interesting findings.



Key findings

- **37%** of respondents' organizations **were hit by ransomware in the last year**
- **54%** that were hit by ransomware in the last year said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- **96%** of those whose data was encrypted **got their data back** in the most significant ransomware attack
- The **average ransom paid** by mid-sized organizations was **US$170,404**
- However, on average, only **65% of the encrypted data was restored** after the ransom was paid
- The **average bill for rectifying a ransomware attack**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was **US$1.85 million**
- **Extortion-style attacks** where data was not encrypted but the victim was still held to ransom **have more than doubled** since last year, up from 3% to 7%
- Having **trained IT staff who are able to stop attacks** is the most common reason some organizations are confident they will not be hit by ransomware in the future

Figure 3 Image taken from Sophos annual report "The State of Ransomware" 2021 (Sophos, 2021)

Looking at the number of ransomware incidents by organization size, we see that larger organizations reported a greater prevalence of attacks, with 42% of the 1,001-5,000-employee group admitting to having been hit, compared with 33% of the smaller companies. In the following illustration, we can see the geographical diffusion of the attacks.

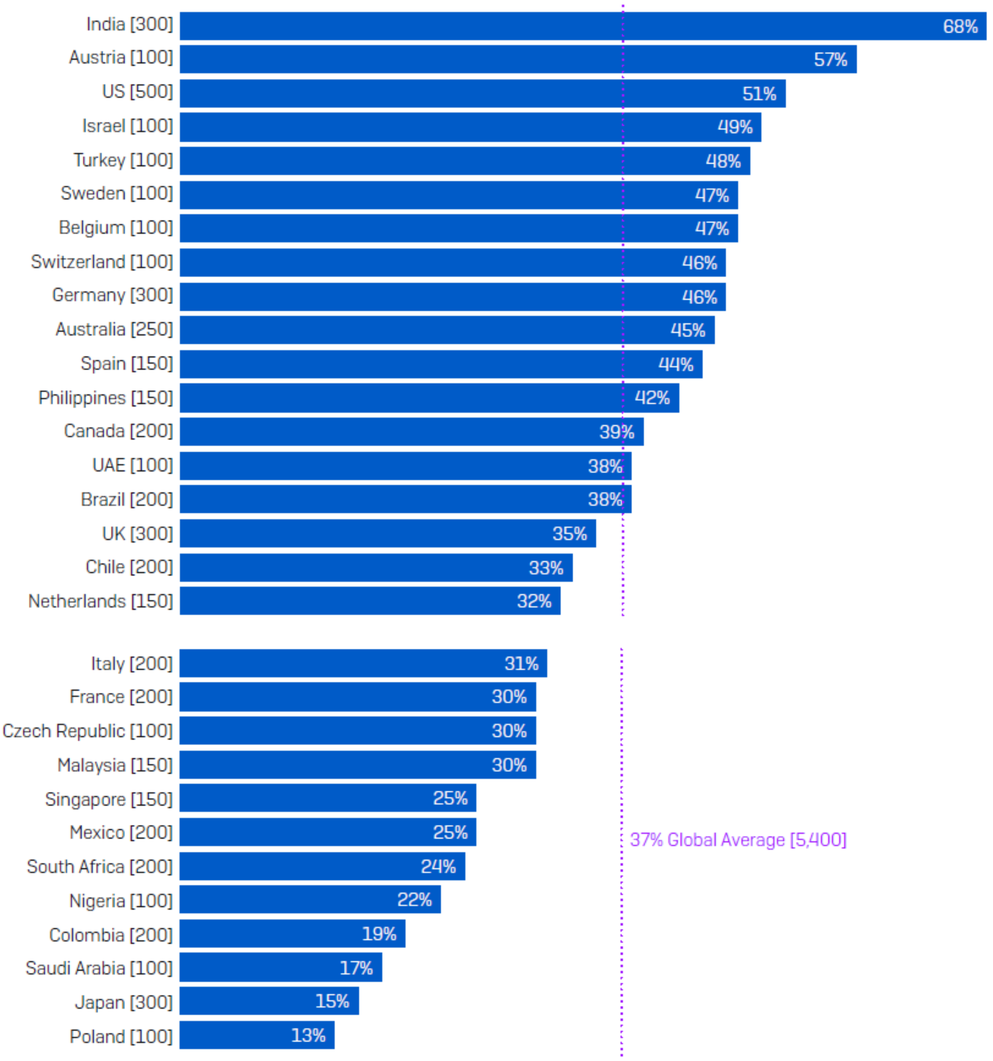


Figure 4 Image taken from Sophos annual report "The State of Ransomware" 2021 (Sophos, 2021)

Retail and education experienced the highest level of attacks, with 44% of respondents in these sectors reporting being hit.

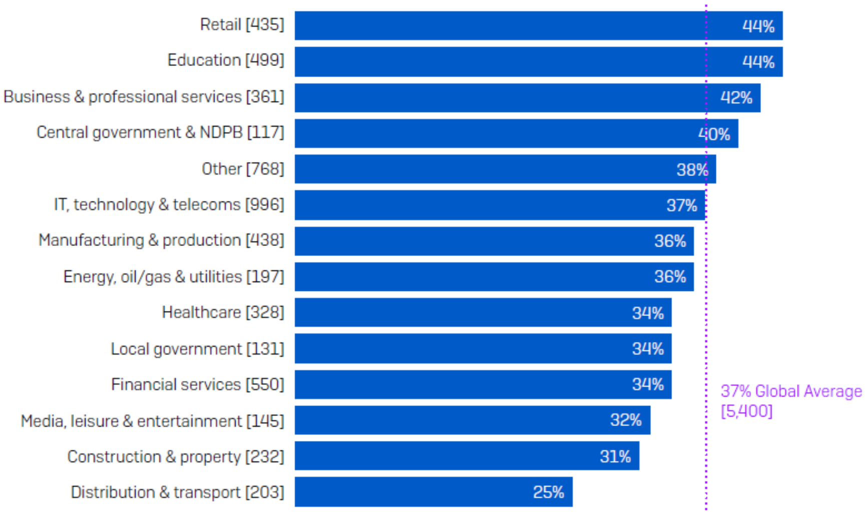
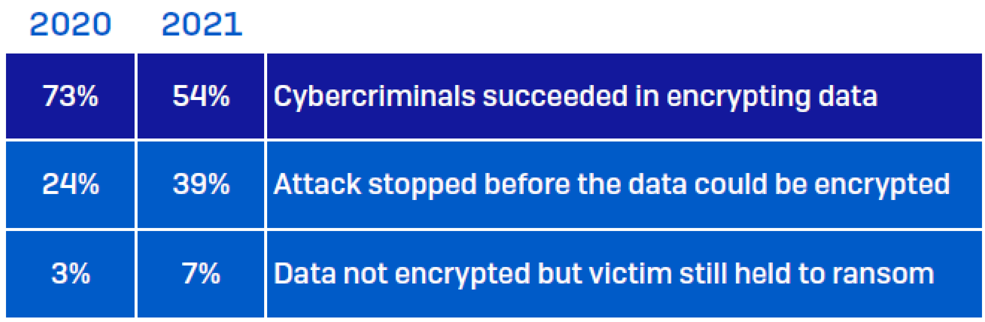


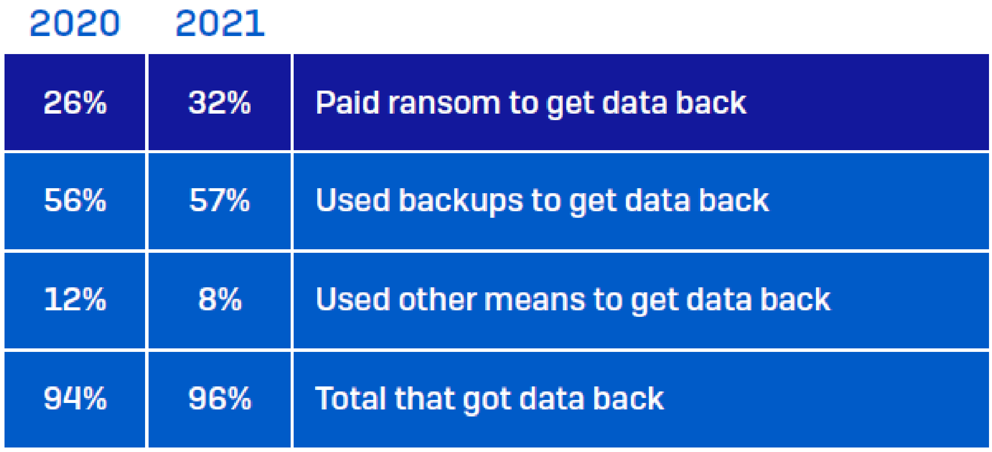
Figure 5 Image taken from Sophos annual report "The State of Ransomware" 2021 (Sophos, 2021)

Encryption is down. Extortion is up.



2020	2021	
73%	54%	Cybercriminals succeeded in encrypting data
24%	39%	Attack stopped before the data could be encrypted
3%	7%	Data not encrypted but victim still held to ransom

Figure 6 Image taken from Sophos annual report "The State of Ransomware" 2021 (Sophos, 2021)



2020	2021	
26%	32%	Paid ransom to get data back
56%	57%	Used backups to get data back
12%	8%	Used other means to get data back
94%	96%	Total that got data back

Figure 7 Image taken from Sophos annual report "The State of Ransomware" 2021 (Sophos, 2021)

However, the finding that I think is the most interesting is that, according to the Sophos study, in 54% of the cases, the cybercriminals succeeded in encrypting the data and that, on average, only 65% of the encrypted data was restored after paying the ransom (Sophos, 2021). In a following paragraph, I will argue why paying the ransom is not a good strategy.

2.2 Cybersecurity in Universities

In general, universities' IT systems are often characterized by a decentralized construction that attackers can easily exploit. For this reason, and others that I will later explain, the higher education sector is one of the most targeted by cyber-attacks in recent years. Therefore, all universities put a lot of emphasis and resources on cybersecurity and, just like companies, have a CISO with the responsibility of planning and implementing many cybersecurity measures.

Firstly, all universities implement some basic cyber hygiene measures that include patch management software, antivirus and firewall management. It is also really important for them to train staff and students on the basic rules of "on-line conduct", which includes how to spot a phishing email. Moreover, universities keep a firm hand on exactly who has access to the network and they validate all user credentials on a regular basis to tighten up security. As explained before, usually university networks tend to contain a crossover of smaller networks for each department. Even though this offers freedom for staff and students within these departments, it also presents a challenge when it comes to protecting data. For this reason, it is essential for them to update the network design frequently. Furthermore, due to the critical need for privacy, higher education institutions encrypt a large volume of traffic on their networks. Finally, since no system is ever entirely safe from hackers, all universities have a crisis management plan in place and a security team to help minimise any damage and disruption caused by a cyber-attack (Cahill, 2020).

Maastricht University is a Dutch public university founded in 1976, that has about 16,000 students, of which 47% are foreigners, making it one of the biggest universities in Europe. As other big universities, the University of Maastricht also has a very big and decentralized network. UM's IT infrastructure consists of a variety of servers and workstations, of which not all are directly under the mandate of the central IT management organization, the so-called ICT Service Centre (ICTS). In fact, there is also a part of the IT infrastructure that falls outside the mandate of ICTS, but it is still part of the central network. This part is managed in a decentralized manner by the relevant business units themselves. It differs per faculty, per server and per workstation whether they have access to the central Windows domain of UM (UNIMAAS). In addition to fixed workstations in the form of desktops and laptops, UM employees also make use of virtual workplaces when personal login details are logged in. The virtual workstations use Virtual Desktop Infrastructure (VDI) involving desktop virtualization in the data centre. This VDI environment is accessible via so-called thin clients and the local browsers. At the time of the attack the CISO of the University was Bart van den Heuvel (FOX-IT, 2020).

3. Analysis of the attack

On the 23rd of December, in the wake of Christmas Eve, Maastricht University found that almost all Windows systems were affected and e-mail services could no longer be used. On the same day, the University contacted Fox-IT, which provided support in the area of crisis management and mitigation. They also carried out a forensic investigation, mapping the circumstances of the attack and giving advice in the recovery process.

On 24th of December, UM put a protective "shell" around its entire network and, in order to work as safely as possible, it also took all other systems offline. A Crisis Management Team (CMT) was immediately set up, along with temporary “help desks” for students and employees. On the 2nd of January the University officials communicated in a public statement that all actions were aimed at getting education back to normal in time and to provide researchers with access to scientific data as quickly as possible (Maastricht University, 2020).

FOX-IT elaborated Project Fontana, a detailed document providing a technical analysis of the attack, as well as the factual representation of the findings and recommendations for the recovery and prevention. For the analysis in this paper, I will use the information provided by the document.

3.1 Discovery of the attack and measures taken

On December 24 the incident response experts of Fox-IT arrived on location at the Maastricht University and started assisting the Crisis Management Team (CMT) in setting up the crisis organization. Fox-IT emphasized that the timely involvement of a communication expert was a priority since the incident was already publicly known. For this reason, they advised that a communication team was to be created to handle the communication process. Moreover, the attention placed at transparency was also important because of the nature of a public organization such as that of the public Maastricht University. Actually, all the recovery process has been reported openly, transparently and in as much detail as possible via the daily updates on the University's website.

Fox-IT also advised that the business, as well as the IT and IT security part of the administration, participate in the daily crisis management team (CMT) consultation. This was for the purpose of determining the impact of decisions that had to be made. In the first days, the activities were divided into three tracks and three teams: organization, research and recovery. The University staff has mainly given substance to the organizational and recovery team while the research team consisted of a combination of Fox-IT experts and employees.

During the investigation, the experts secured log data from various systems in the network. They also registered metadata of all firewalls on the outside of the network connections in the so-called flow logging and secured other material that was relevant to the investigation, including mailboxes, database files and encrypted files. Additionally, to determine the initial scope of the investigation, Fox-IT made an inventory of the compromised systems and accounts. A system was considered compromised if manual attacker activity occurred, or if traces of malware were found. An account was considered compromised if the forensic traces investigation determined that it was used by the attackers. In total, Fox-IT discovered five accounts and 269 Windows systems compromised (of a total of 1,647 servers and 7,307workplaces). In addition to Windows systems, the University had Linux and OS systems within the infrastructure that were not affected by the attack.

By using network sensors, Fox-IT had the possibility for live detection and analysis of suspicious network traffic. Moreover, they used sensors that could catch all the metadata of the monitored network. At the first location, all incoming and outgoing internet traffic was monitored by two sensors. At the second location, a sensor monitored the internal network traffic within the UNIMAAS domain. Through network discovery at this level, it was possible to detect both an attackers' attempt to enter, as well as to detect lateral movement through the network.

In the first phase of the investigation, the University officials decided to give priority to the fast recovery of the business. For this reason, FOX-IT experts decided to secure research material during the forensic trace investigation. If this had not happened in time, valuable forensic evidence could have been lost. A software developed by Fox-IT was mainly used to secure forensic investigation material acquiring. It was able to copy the files that contained the most relevant forensic evidence from the Windows system and write them as a zip file on a device used solely for this research. Files were uploaded from this network location to Fox-IT's forensics lab for analysis. Disk images and log files were also collected due to the fact that the collection of such research material enabled the analysis of the historical activity and, thereby, to do a large-scale identification of the compromised systems. Analysing the data also helped to understand the path of the attackers and the scope of the attack.

For ensuring the business continuity, Fox-IT advised the setting up of a mitigation team, since the University established the goal of restarting the normal activities already at the beginning of January. Various activities fell within the range of the duties of the mitigation team, including the remotion of the malware, the identification and reinstallation of the critical system and the determination of the remedial measures. On December 24, the University closed the connections to and from the internet in order to prevent the attackers from accessing the network and to prevent the infected systems from communicating outwardly. In such a way, the isolation of the network has given the team the space to investigate what the scope of the incident was. However, for the recovery measures to be implemented it was necessary that a number of systems regained internet access. In order to do this, FOX-IT decided to give access again to certain systems, to both the internal network and the internet. FOX-IT also suggested some additional measures, including:

- The monitoring on the basis of firewall reports through e-mail notifications and the set-up of an escalation path for reporting incidents.
- The requirement of a password reset for all accounts within the UNIMAAS domain.
- The creation of a step-by-step plan to deal with systems infected by the attackers.
- The creation of a list of the so-called "crown jewels" of the organization in order to determine the priority of the remedial measures.
- The use of clean and "sanitized" systems.
- The monitoring through the network sensors, so that the network traffic can be checked and thus the integrity of the network safeguarded.

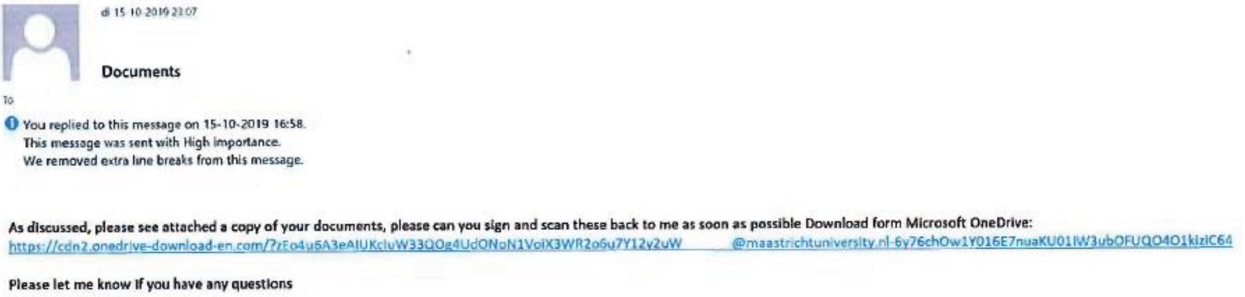
On 2 January it was announced that education could resume on 6 January and students and staff were required to change their password before that date. The emails not received were available again from 7 January (no email was lost) and from the same day, the network drives were again accessible via the wired networks (not via Wi-Fi). For the purpose of monitoring workplaces for suspect activities, the software Carbon Black was installed at all workplaces. The access for employees to the Virtual Private Network (VPN) was restored the 27th of January while the Student Desktop Anywhere (SDA) system for students to access UM services was already operational since the 6th of January. On Wednesday 5th of February, the University organized a symposium to communicate the lesson learnt from the attack.

Another essential part of the mitigation process was the communication with the attackers. Due to the fact that the mail servers had been affected, the communication took place via the personal email address of Bart van den Heuvel, the University CISO, which claimed that "*We communicated with them very regularly: on the one hand to gain time, on the other hand to make sure we were talking to the right party. For the latter reason, we also came up with both technical and financial control questions such as making a test payment*". He also claimed, in the week between the attack and the decision to pay the ransom that "*In 3 days, we managed to set up a new mail server. Its database was not encrypted. The archive system, on the other hand, was not usable: you can do without an archive for a few days, not for months. Our external partner Fox-IT managed to unlock one small file, but it had taken them a whole night to do so. We knew that we would lose a lot of valuable time if we chose this option. Making or having a "decryptor" yourself is, according to experts, either impossible or will take a very long time. The alternative was to rebuild all the infected systems and write off certain irrecoverable critical data. It would take many months for UM's* *education, research and business operations to even be partially up and running again*". (FOX-IT, 2020)

3.2 Technical analysis of the attack

Fox-IT has determined that the attackers initially gained access to the network of the University with two phishing e-mails that were opened on the 15th and 16th October 2019 on two workstations. The attackers compromised several servers and on the 21st of November, using a server with missing security updates, they managed to obtain full administrator rights within the infrastructure. Finally, on the 23rd of December 2019, they deployed the so-called Clop-ransomware on 267 Windows servers.

On October 15th of 2019, at 14:06:31 the following email was sent to an email account within the University domain with subject "Documents".



di 15-10-2019 23:07

Documents

To

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

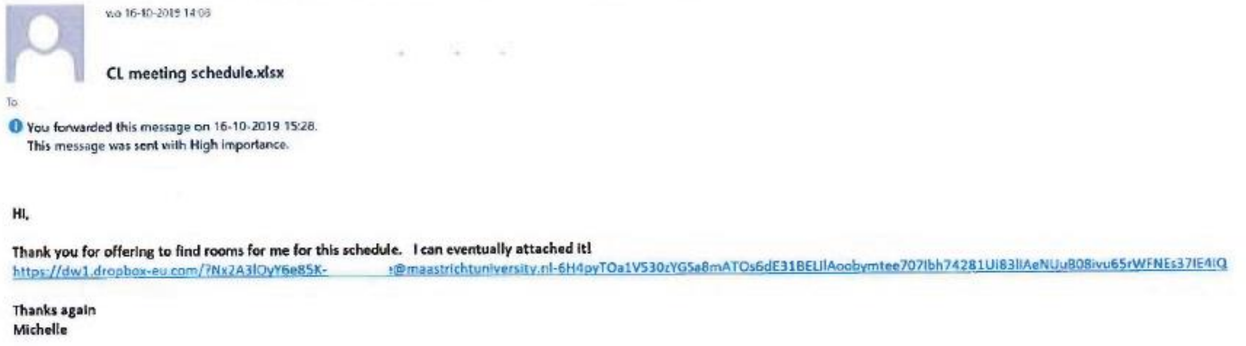
As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
https://cdn2.onedrive-download-en.com/?rEo4u6A3eAIUKcluW33QOg4UdONpN1VoiX3WR2o6u7Y12v2uW @maastrichtuniversity.nl-6y76chOw1Y016E7nuaKU01IW3ubOFUQO4O1kizIC64

Please let me know if you have any questions

Figure 8 Image taken from "Project Fontana" (FOX-IT, 2020)

The link in the phishing email led to an Excel document which contained a macro. This macro came from a remote server with the domain windows-en-us-update.com and IP address 185.225.17.99. When the employee opened the document, the SDBBot malware executed on the workstation.

On October 16 at 09:07:51 the following email was received by another account with the University domain with the subject CL meeting schedule.xls.



wo 16-10-2019 14:08

CL meeting schedule.xlsx

To

You forwarded this message on 16-10-2019 15:28.
This message was sent with High importance.

Hi,

Thank you for offering to find rooms for me for this schedule. I can eventually attached it!
https://dw1.dropbox-eu.com/?Nx2A3lQyY6e85K- @maastrichtuniversity.nl-6H4pyTOa1V530zYG5a8mATOs6dE31BELIlAoobymtee707lbh74281Ui83llAeNUuB08ivu65rWFNEs37IE4lQ

Thanks again
Michelle

Figure 9 Image taken from "Project Fontana" (FOX-IT, 2020)

The link in this phishing email redirected to a similar Excel document. Also in this case, the macro linked to the SDBBot malware from a remote server with domain name windows-afx-update.com and IP address 185.212.128.146. On both systems, the SDBBot malware then communicated every 15 minutes with an external server with the domain name drm-server13-login-microsoftonline.com and IP address195.123.242.250. Furthermore, the

SDBBot registered itself on the Windows system registry of both systems, so that the malware became active again even after the systems were restarted.

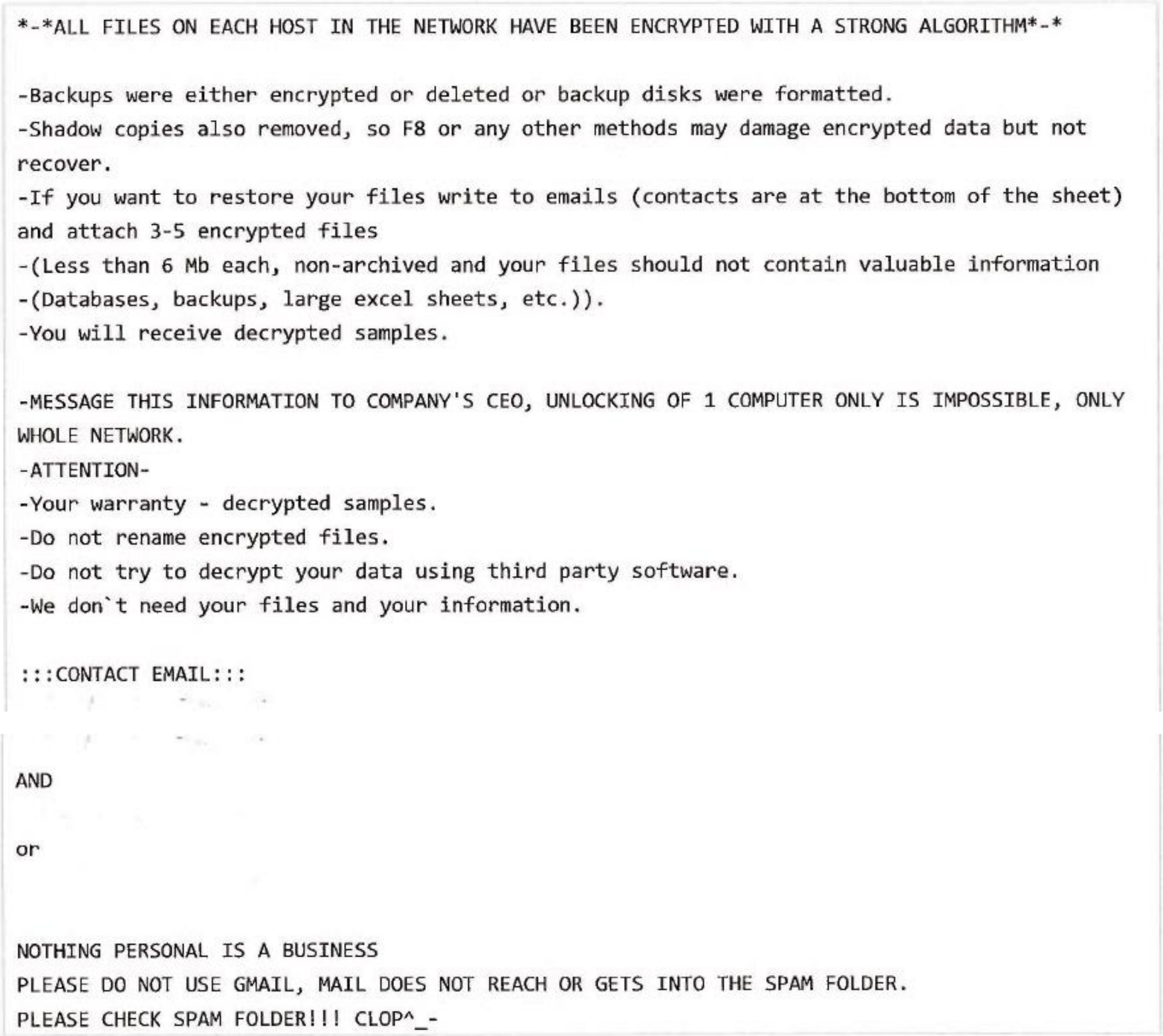
On October 16th the account started another type of malware via the SDBBot malware, namely Meterpreter3. This malware is primarily deployed by attackers to manually access victims' systems. This was, therefore, the first sign that the attackers had accessed manually the University network via the virtual desktop of the account that received the phishing mail. On October 17th the hackers had the first servers within the network compromised. Even though from the limited forensic traces on these two systems it is not clear how the attackers did it, it is in fact possible that the so-called EternalBlue exploit was used because both servers did not yet have the Microsoft MS17-0104 patch installed. The EternalBlue exploit allows an attackers to operate from another system in the network of the targeted system and run a malware with the local account. The Meterpreter malware was also launched on the server on October 20.

After the hackers have gained administrator rights on multiple servers within the network of the University, they relapsed to the two initially compromised workstations to further explore the network. On October 20th, on one of the two initially compromised accounts, the attackers used PowerSploit, which is a collection of PowerShell scripts that are usually used to test the security of a network. However, in this case these were used for malicious purposes. In fact, with this PowerShell scripts, the attackers scanned the internal network and tried to find as many vulnerabilities as possible. On October 24th they used PingCastle on a workstation. With PingCastle, the hackers could graphically visualize how the University's directory structure was configured, in order to find all the weaknesses.

On November 21st, after running the Meterpreter malware on another account, they succeeded in getting access to the Domain Controller, which has the highest privileges and full management rights within the University network. The attackers then used both CobaltStrike and Meterpreter to run the PingCastle software. FOX-IT also found traces of the software AdFind. With the access rights to the entire Windows domain of the University network, the attackers started the preparation for the final phase of the attack: the rollout of the ransomware.

To carry out this attack as controlled as possible, the hackers used a software with the file name sage.exe. This software supported the attackers in the rollout of the ransomware. On December 23rd this file, saga.exe, was executed on three servers (02, 04 and 17). On the server 04 the software was detected and removed by the McAfee antivirus. The attackers then used the local administrator account admin to remove the Mcafee antivirus software from the server, and then run sage.exe again. The hackers also removed the McAfee antivirus software from servers 02 and 17. FOX-IT experts found the saga.exe file on the C:\Users\Public\Music\folder of these three servers. Thanks to their Domain Administrator privileges, the attackers made the saga.exe file run on all Windows servers that were part of the UNIMAAS domain. They also used sage.exe to remove Windows Defender on all systems before starting the ransomware attack.

At around 18:52, on at least 267 servers, the ransomware had caused its damage by encrypting all the files. Affected systems include highly critical systems for the business operations of the University such as the Domain Controllers, exchange servers, file servers with research and operations data, and some of the backup servers. These backup servers may have contained copies of (or part of) the data encrypted on the other servers. The ransomware used by the hackers is the so-called Clop12 ransomware, which encrypts files using the RC4 encryption algorithm. The RC4 key is generated randomly for each file, and then all files are encrypted again with RSA-1024 bits key. Only the attackers have the corresponding secret key. As soon as the malware infiltrated the network, it quickly locked down the files from access with a “.Clop”. Each folder in which the ransomware had encrypted files also contained instructions addressed to the victim (FOX-IT, 2020). In the file called ClopReadMe.txt the following text was found:



```
*-*ALL FILES ON EACH HOST IN THE NETWORK HAVE BEEN ENCRYPTED WITH A STRONG ALGORITHM*-*

-Backups were either encrypted or deleted or backup disks were formatted.
-Shadow copies also removed, so F8 or any other methods may damage encrypted data but not
recover.
-If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 3-5 encrypted files
-(Less than 6 Mb each, non-archived and your files should not contain valuable information
-(Databases, backups, large excel sheets, etc.)).
-You will receive decrypted samples.

-MESSAGE THIS INFORMATION TO COMPANY'S CEO, UNLOCKING OF 1 COMPUTER ONLY IS IMPOSSIBLE, ONLY
WHOLE NETWORK.
-ATTENTION-
-Your warranty - decrypted samples.
-Do not rename encrypted files.
-Do not try to decrypt your data using third party software.
-We don`t need your files and your information.

:::CONTACT EMAIL:::


AND

or


NOTHING PERSONAL IS A BUSINESS
PLEASE DO NOT USE GMAIL, MAIL DOES NOT REACH OR GETS INTO THE SPAM FOLDER.
PLEASE CHECK SPAM FOLDER!!! CLOP^_-
```

Figure 10 Image taken from “Project Fontana” (FOX-IT, 2020)

3.3 Who is TA505?

The TA505 Hacker Group is a prolific cybercriminal group known for its attacks on multiple financial institutions and retail companies. This group has been known for infecting victims through phishing. Once a victim’s system is initially compromised, TA505 uses a wide variety of commercially available and custom remote access trojans for stealing sensitive financial data and, in some cases, deploying ransomware. Based upon their previous targeting trends, their motives are likely to be influenced by financial gain. These actors have recently been observed deploying FlawedGrace, FlawedAmmyy, Snatch, SDBbot, and ServHelper. One unique method employed by this group includes using various encodes to aid in detection evasion.

According to an analysis carried out by the Tailored Intelligence Team of Prevailion, the TA505 has committed different malicious activities around the globe, targeting in six continents and spread across a multitude of different sectors and countries (Prevailion, 2021).

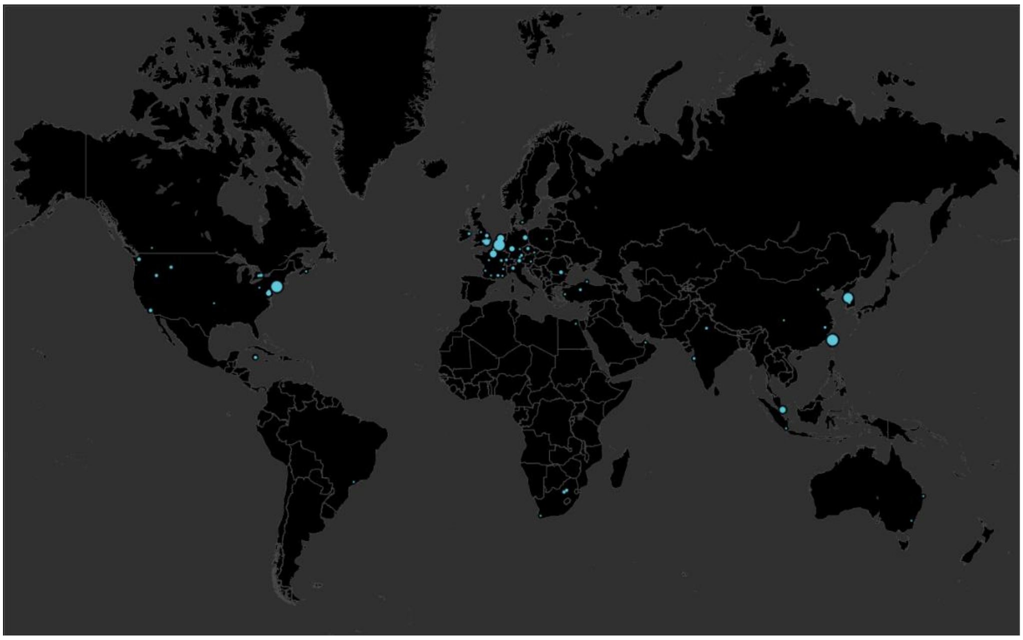


Figure 11 Image taken from "TA 505 Global Ransomware Criminlas" (Prevailion, 2021)

The most impacted geographic area was Europe and the two most infected verticals were education and finance. According to their study, infection within the education vertical, primarily universities, was most rampant. The following images illustrates their findings.

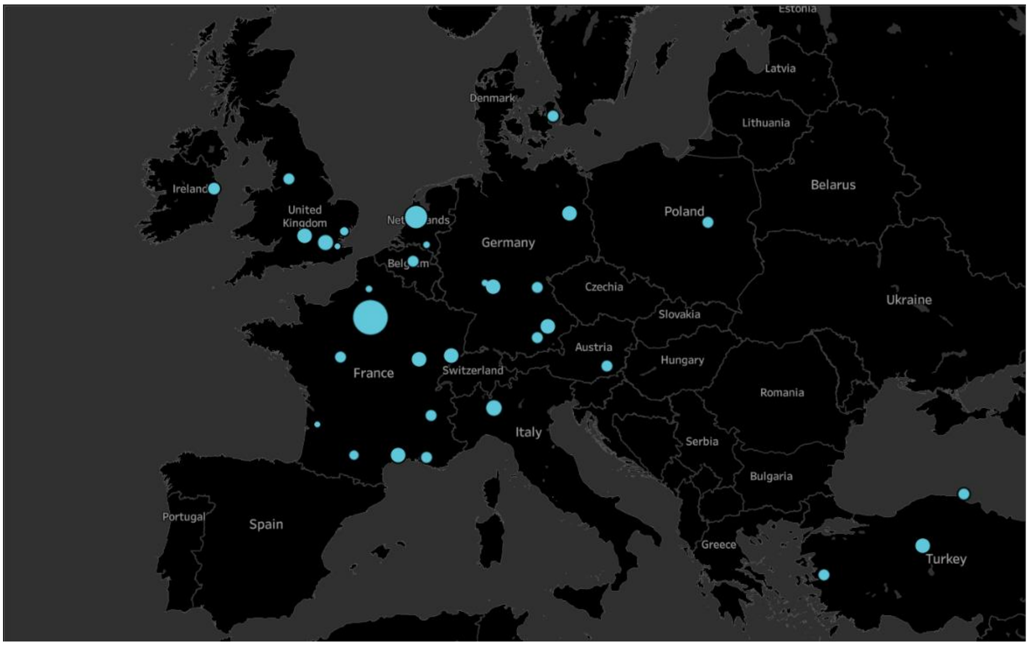


Figure 12 Image taken from "TA 505 Global Ransomware Criminlas" (Prevailion, 2021)

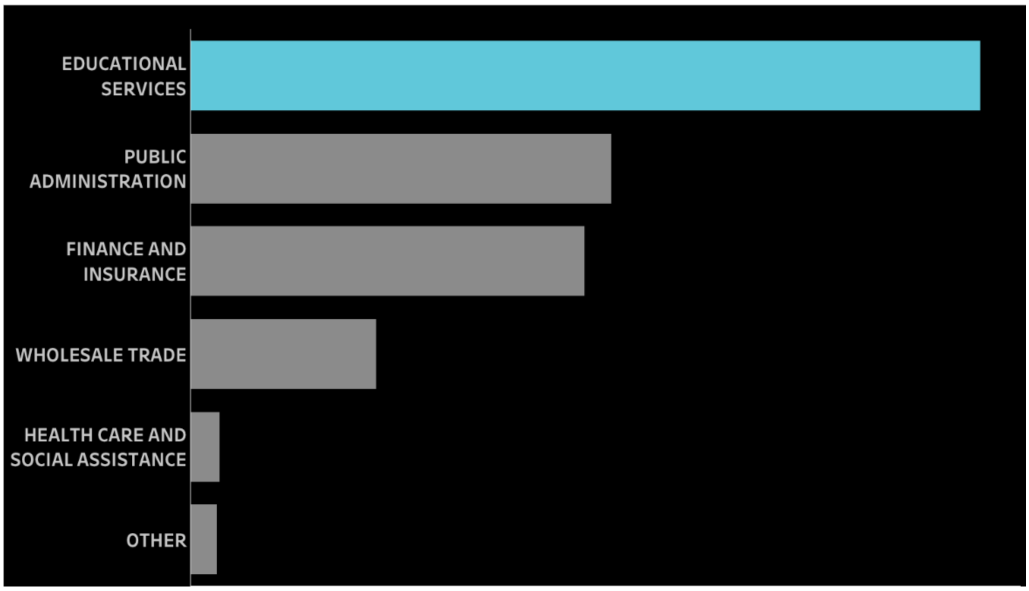


Figure 13 Image taken from "TA 505 Global Ransomware Criminlas" (Prevailion, 2021)

Universities are their primarily target probably because they lack sufficient security resources when compared to more hardened networks in the banking or insurance vertical, but also because they could be useful as a staging ground and may be employed by attackers to gain access to more hardened networks. In fact, during 2019 there have been many reports of universities threatened with ransomwares, just like the Maastricht University. According to the Preivailion study, the average cost of a data breach is approaching 3.9 million dollars. Even though these actors may not operate at the level of most APTs, they are still highly successful at compromising organizations because they have proven themselves capable of avoiding detection through various techniques such as signing binaries with legitimate certificates and obfuscating payloads with encoders (Prevailion, 2021).

The expert in cybersecurity, Marco Ramilli, analysed different attacks carried out by the TA505 group and he came up with some interesting insights on the group *modus operandi*. He discovered that the group, who was already known for having operated both the Dridex and Locky malware families, continues to make small changes to its operations. For example, they have used the new RAT dubbed SDBbot, such as in the attack at the Maastricht University. The security experts at Proofpoint observed the behaviour of this new bot and realized that it is a backdoor delivered via a new downloader dubbed Get2, that was written in C++ and used also to distribute other payloads, including FlawedGrace, FlawedAmmyy, and Snatch. According to Ramilli, TA505 group is expanding its operations, but it is still controlling an infrastructure involved in previous attacks across the years. In fact, they still leverage this infrastructure for "hit and run" operations or to test new attacks techniques and tools avoiding exposing their actual infrastructure. In his analysis he also discovered that another threat actor, likely financially motivated, is leveraging the same infrastructure used by TA505 and this makes the attribution of the attacks harder (Ramilli, 2019).

4. What went wrong

In this paragraph I will explain what the University of Maastricht should have done, or, in general, what universities should do, to avoid these types of attacks. I will include some personal considerations and recommendations that I have learned during the cybersecurity course and other workshops on cybersecurity, as well as the many points of the "lesson learned" document that the UM wrote as a response to the FOX-IT report.

4.1 What should the University have done?

The three "weak links" that the cybercriminals exploited for the attack and that the University should have put more attention to are: (a) the human training on cybersecurity; (b) the strength of the technical measures; (c) better back-up system (Maastricht University, 2020).

Humans are always the weakest link. Therefore, companies and organization that want to have a high level of security for their IT and OT systems, must invest in human training. According to the most recent research, 20% of users open phishing emails, especially distracted users and employees with little knowledge about security online. What went wrong in the case of the University of Maastricht was, not only the fact that two phishing emails were open on two workstations, but also the fact that, when the receipt of the phishing email was reported, it was ignored by the information security office. *"The user in question even reported the mail to the university's Service Desk afterwards. They turned out to be someone who was very 'internet savvy', but in these circumstances clicked on a fraudulent link anyway. I am convinced that it is impossible to completely prevent someone from clicking on a harmful link, but awareness remains crucial"*, said Bart van den Heuvel, the CISO of the University (Connect, 2021).

After the attack, the University officials recognized that what they needed was a better awareness for students and employees about social engineering, and also better handling of (report of) phishing emails. For this reason, they decided to invest on "awareness campaigns", with the aim of reducing the number of successful malicious attempts to attack. This campaign went beyond phishing and focused on basic cyber hygiene, like locking your screen when you are not using your laptop for a while. This will be repeated for students at the start of the new academic year in the beginning of September. The fruits of this awareness campaign are already showing, in fact UM's Service Desk has received 5 times more reports from users about phishing this year than last year.

On the basis of the report and recommendation made by the FOX-IT agency in their Project Fontana, the University of Maastricht recognized the technical measures that should have been implemented and committed itself in accomplish their implementation.

- Updating the software to close unsafe "loopholes": TA505 may have used EternalBlue to exploit a Microsoft vulnerability. In fact, the "patch" was not installed because the software was not updated to a new version. The update and, consequently, the installation of the patch, would have prevented the attack.
- Improving the segmentation of the Windows domain: before the attack, the domain administrator account with the associated rights was also used for management and maintenance work on regular servers. This made it easier for criminals to gain control of the domain via malware and thus perform malicious actions. The University, instead, should have monitored the use of domain administrator accounts more closely and restrict their use for maintenance of the domain and the domain controllers, so that

an administrator does not have automatic access to everything. Moreover, after the attack the University decided to put each of its servers behind its own firewall.

- Setting up a 24/7 monitoring system by the SIEM (Security Information and Event Management) as well as by the SOC (Security Operations Center)
- Configuration Management Data Base: the mapping of the “computer inventory” would have helped the informational security office and the FOX-IT expert to understand faster the scope of the attack and, therefore, put forward a faster mitigation process. “*We are going to improve our configuration management database (CMDB), so that we have a better overview of the systems that are part of our network. We also want to map in detail which processes are running on our servers and how those servers are connected to our more than 3,000 internal and external sources. This is quite a challenge: our central IT service alone manages 3,000 workstations. In addition, many systems are set up in a decentralised manner, and we do not have a good overview of these right now*” Bart van den Heuvel explained.

Nevertheless, what I think was the biggest mistake in the prevention of the attack is the weakness in the back-up storage system. The University of Maastricht finally decided to pay the ransom to get their data back not only because they did not have a back-up for all the work of students and researchers, but also because the cyber attackers were able to encrypt the online backups too from some critical systems. According to the Sophos report, in 2021 only 57% of companies that were hit by a ransomware got their data back through their back-ups, while 32% of them decided to pay the ransom to have the data decrypted. This means that the companies and organizations underestimate the need for an adequate back-up system that otherwise would have saved them a lot of time and money. So, the question becomes, how is a strong back-up system made?

Two types of back-up systems exist: storage (physical or virtual) and cloud. The physical storage back-up consists of scheduled copies of data and configurations of the server on a hardware that must be connected to the server only for the time needed for the copying process and it must be remoted (stored in a different place). The virtual storage back-up consists of scheduled copies of the snapshots on specific back-up software. The cloud back-up represents a more flexible and affordable choice, but also a more popular choice because it can be implemented over time. A good back-up system should consist of both a physical and virtual (or cloud) back-ups. Moreover, some requirements must be fulfilled. For the storage back-up:

- Never connect the storage to the LAN or create shared folders, otherwise the back-up too would be compromised in case of malicious attack.
- The folders must not be accessible for writing by any of the devices on the network and for copies it should be used a software that will authenticate itself correctly or use administrator protocols to perform synchronizations.

But also for the cloud back-up:

- The backups must be set hourly, daily, weekly or at customized times.
- Data must be stored with secure and exclusive access only to the Backup Account.
- It is essential to install a connection agent on the servers of whom we want to do a back-up and also a console for managing back-ups and reporting anomalies via email.
- Previous versions must be stored for at least 2 or 3 days (versioning).

The University of Maastricht officials claim that now they are using both an online and offline back-up system in order to avoid a similar failure in the future.

4.2 The payment of the ransom

After a careful analysis of the possibilities, on December 30th the University paid the ransom required to decrypt its files. The decision was a hard one to make but after a long deliberation they finally decided to pay the ransom in the interest of the academic community. "*The fact that the teaching and the exams in January were able to continue without too much hindrance and that there was little impact on scientific research, and that we were also able to pay wages for 4,500 employees on time, has strengthened our idea that we made the right decision*" said Nick Boss. After paying the ransom, the University received the key to unlock the system and, after a detailed analysis carried out by the FOX-IT experts, no evidence was found that the data was deleted, modified or made public.

The decision was made by the Board of Directors after evaluating the consequences of the extended downtime on servers at the University. The CEO of the cybersecurity awareness platform CybSafe, Oz Alashe, commented: "*In the ideal world, organizations should never respond to ransomware threats. This only serves to finance the actions of organized crime networks and rogue actors of the nation-state. But in this case, it seems that the university has been cornered. Rebuilding the entire IT infrastructure from scratch may have been more expensive than simply paying the ransom of 30 bitcoins* " (Marchetti, 2020)

A report made by the FBI estimated that the total amount of ransom payments was approaching $1 billion annually. The FBI's official statement on ransomware advises victims not to pay the ransom because there is no guarantee that the hackers will restore your information and, worse, it could put a target on your back if your business is seen as unprepared to handle cyber-attacks and willing to pay the ransom (Minahan, 2018). In fact, according to the Sophos report, only 65% of the encrypted data was restored after paying the ransom. Moreover, as already highlighted by Alashe, paying the ransom has the counterproductive effect of financing these new cybercriminal groups, for whom this type of activity is highly rewarding, since the average ransom paid, according to the Sophos report, is US$170,404 (Sophos, 2021).

However, the choice made by the University of Maastricht and, in general that of many companies, to pay the ransom is totally understandable, since the average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. is of US$1.85 million. So, what is the best option when hit by ransomware? This dilemma is ultimately a business decision: it depends on the specific nature of the company, the attack, and the risk and these are variables that change in every ease. The rule, as always, but especially when it comes to informational security, is better safe than sorry. In fact, the cost of implementing a good training campaign for employees and students and the cost of implementing a good double back-up system (online and offline), would have been much lower.

4.3 Why are universities under attack?

According to the SOPHOS annual report, Education (jointly with retail) is the sector that reported the highest percentage of organizations hit by ransomware last year (Sophos, 2021).

As a study made by the National Cyber Security Centre (NCSC) on UK universities' defences against cyberattacks showed, it can take hackers as little as two hours to bring a university network to its knees. Universities can provide cybercriminals with really worthy information including personal data (which in some cases may be phone numbers or donation history), financial systems and research networks. This is because universities have extensive databases on thousands of students and staff members, which include rich information that is very inviting to hackers, such as personal, financial, and research and development data. In fact, in addition to economic interests, the reasons why cyber-attacks are increasingly affecting educational institutions are to steal data or stop services. Moreover, advance research is carried out in universities, so stealing, manipulating or destroying this data can be another motivation for cybercriminals to hack universities' networks (Iurcu, 2020).

According to the NCSC, attacks on universities are often carried out with social engineering techniques and attempts to access networks to run ransomware and malware. At the end of the day, universities are vulnerable, as part of a sector that is constantly looking for the right balance between optimal digital security and providing an open and transparent environment for students and researchers. Therefore, it should be essential, among the many teachings, to lecture university's students on informational hygiene and how to be protected against cyber threats.

Italy is one of the countries most affected by cyber-attacks, especially when it comes to the educational sector. In 2019 there were several cyber-attacks, and among the universities involved were the University of Campania "Luigi Vanvitelli", the University of Siena, the University for foreigners "Dante Alighieri", the University of Venice, the University of Milan, the Polytechnic of Bari and the University of Salento. The attacks were launched by the Anonymous group who published more than 1700 pages containing personal data, identity cards, passports, telephone numbers and email addresses of students and professors (Iurcu, 2020).

5. Conclusion

To sum up, the Russian-speaking criminal group TA505 has gained access to the Maastricht University network via two phishing emails opened on two workstations. The phishing emails contained a link to an Excel document with a macro that installed malware on the two workstations. Using the malware infections on these two systems, the attackers first gained access to the University network and, from there, moved laterally through the network. According to the FOX-IT agency, the attack was possible due to a combination of inadequate responses to alarm signals and unsafe network and system configurations.

If we had to give feedback to the University response, it would not be a completely negative one. It has already been clarified that, before the attack, the University had not implemented the right measurers for the informational security of the IT system. Furthermore, the final decision of paying the ransom, with what TA505 will finance their next attack, could have been avoided with a better back-up system. Nevertheless, we need to recognize that the University did well on two sides.

On the one hand, even though the attack was strategically carried out during the Christmas Holidays, the University officials were able to call dozens, and later perhaps as many as two hundred UM employees, that did not spend the holidays undisturbed at home, but work at least part time for implementing the mitigation measures. According to what Bos declared during the symposium, they worked very long days and weeks without a whisper of a complaint and with an enormous loyalty to UM and its students and staff. The administrative tasks were also considerable.

On the other hand, we need to recognize to the University's officials their true commitment to transparency. All information around the attack was shared with the University community and, through daily updates on the UM website, users were able to follow the status of the incident. There has been also proactive communication to the press, but speculation and inaccurate reporting could not be avoided completely. On the 5th of February, they organized a symposium to share with the community the "lesson learned", during which they recognized the errors made and committed to the implementation of a number of cybersecurity measures for this type of incident to never happen again. Somewhat ironically, the launch by the University of a round-the-clock security operations centre on January 1st had been planned before the attack took place. However, as Bart van den Heuven declared, "*It shows what an incredibly difficult task it is to defend networks of this size against the kind of attackers Maastricht University had to deal with: mistakes are bound to be made and attackers will patiently spend months trying to exploit them*".

To conclude, in a world in which cybercrime is becoming increasingly professional and at a larger scale, "*a university must defend itself against this form of crime with limited resources and with an explicit preference for openness and accessibility*". "*It is important that we take cyber security to a higher level, as it is one of the greatest challenges in our society*" concluded Bart van den Heuvel.

6. Bibliography

Cahill, P. (2020, September 18). *5 ways universities and colleges can protect themselves from cyber attacks.* Retrieved from Fenews: https://www.fenews.co.uk/fevoices/55087-5-ways-universities-and-colleges-can-protect-themselves-from-cyber-attacks

Connect. (2021, November). *Case study: What Maastricht University (UM) learned from the ransomware attack* . Retrieved from Connect: https://connect.geant.org/2020/10/20/case-study-what-maastricht-university-um-learned-from-the-ransomware-attack-part-1

Exprivia. (2021). *Threat Intelligence Report.*

Federprivacy. (2021, May 17). *Cyber attacchi nel I° trimestre 2020 +612% rispetto allo scorso anno, ma in flessione quelli riusciti.* Retrieved from Federprivacy: https://www.federprivacy.org/informazione/societa/cyber-attacchi-nel-i-trimestre-2020-612-rispetto-allo-scorso-anno-ma-in-flessione-quelli-riusciti

FOX-IT. (2020). *Project Fontana.*

Iurcu, V. (2020, September 8). *Università sotto attacco: come e perché sono nel mirino degli hacker?* Retrieved from Avira: https://www.avira.com/it/blog/universita-sotto-attacco-come-e-perche-sono-nel-mirino-degli-hacker

Kaspersky. (2021). *Ransomware: definizione, prevenzione ed eliminazione.* Retrieved from Kaspersky: https://www.kaspersky.it/resource-center/threats/ransomware

Maastricht University. (2020). *Cyber attack* - *a summary.* Retrieved from Maastricht University: https://www.maastrichtuniversity.nl/cyberaanval-een-overzicht

Maastricht University. (2020). *Response of Maastricht University to FOX-IT report* .

Marchetti, D. (2020, February 8). *Attacco ransomware all'Università di Maastricht.* Retrieved from Criptovalute news: https://www.criptovalutenews.com/attacco-ransomware-alluniversita-di-maastricht/

Minahan, B. (2018, November 26). *The Dilemma: Should You Pay Ransomware or Not?* Retrieved from Anetworks : https://www.anetworks.com/should-you-pay-ransomware-or-not/

Nexsys. (2021). *Attacco ransomware università di Maastricht.* Retrieved from Nexsys: https://www.nexsys.it/blog/attacco-ransomware-universita-di-maastricht/

Prevailion. (2021). *TA 505 – Global Ransomware Criminals.* Retrieved from Prevailion: https://www.prevailion.com/ta-505-global-ransomware-criminals/

Ramilli, M. (2019, November 12). *TA-505 Cybercrime on System Integrator Companies.* Retrieved from Marco Ramilli Web Corner: https://marcoramilli.com/2019/11/12/ta-505-cybercrime-on-system-integrator-companies/

Sophos. (2021). *SOPHOS Annual Report "The State of Ransomware 2021"* .