Personal Development Portfolio

Javier Duran

Student Number: 3567885

Cybersecurity

Tutor: Qin Zhao

Table of Contents

Introduction

The Personal Development Portfolio (PDP) are all the activities that have helped me gain or improve certain skills during a certain project or time lapse. Through this PDP descriptions of assignments, skills learned and knowledge that assist with my personal and professional development.

My name is Javier Duran, I am an international student at Fontys University of Applied Sciences, in the Infrastructure Engineering BSc program. Very interested and motivated to keep learning about IT in general but more specifically cybersecurity. As risks keep in this area keep growing, I think it is very important to have a secure infrastructure to give companies the edge advantage. Globalization keeps expanding and most international communications are happening through the internet, therefore intelligence agencies and cybersecurity teams along organizations and governments should invest more in cyber security. In addition, I want to be part of people who will help build a smarter and better future through technology.

Purpose

The purpose of this assignment is to create Development Portfolio through which skills, techniques, knowledge, and topics learned during lectures will be laid out. In addition, the case studies will help us develop these knowledge and skills learned by putting them into practice. Most importantly, my personal development in professional skills such as teamwork, communication skills, and leadership will be evaluated. Different forms of evidence in the BoK will support all the above-mentioned characteristics. Critical reflection will be done on the work delivered. This facilitates the progress and gives an insight into my learning process.

Objectives

- Learn new technical and professional skills.
- Getting an insight into my learning process.
- Inform on the skills and knowledge learned during the semester.
- Reflecting on the assignments completed and explained in the BoK through the semester.
- Improve through self-evaluating what are my weak and strong areas and/or skills.

- Learn new technologies and constantly research about cybersecurity topics.

1. Ethical Hacker

1.1 How did you obtain the Body of Knowledge about the subject?

- To obtain the body of knowledge in this subject I completed several Capture the Flag challenges about different Ethical Hacking subjects such as File Inclusion, SQL injections, Cross-Site Scripting and other known OWASP vulnerabilities. In addition, I researched about vulnerabilities and security flaws in an IP Camera. Furthermore, a penetration test was done to a company.

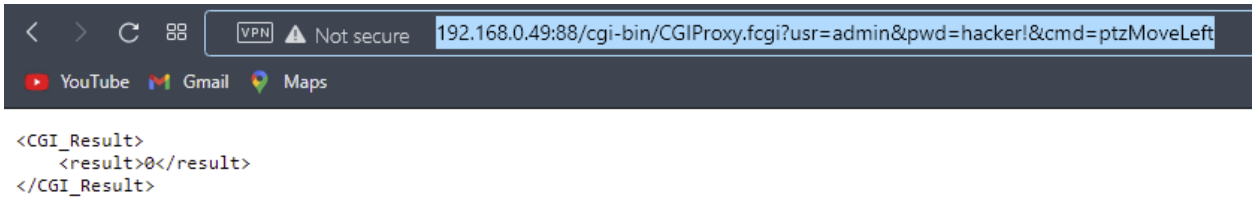


Figure 1.1.1

In Figure 1.1.1, it is possible to observe the response of the IP Camera after executing a XSS attack to move the camera remotely with authentication. The '0' result means the command was successfully executed.

1.2 How did you apply your skills into a practical situation?

- To apply the skills gained, along with a team, a penetration test was done to a cleaning services and products. Agreements were signed and the test was completed successfully as we found some vulnerabilities in the network and the web application. In addition, I participated in Cyber Apocalypse CTF competition, hosted by HackTheBox. In Figure 1.2.1, you can observe that during the pen-test I was able to find XSS vulnerability in the website, allowing me to execute commands from the application.

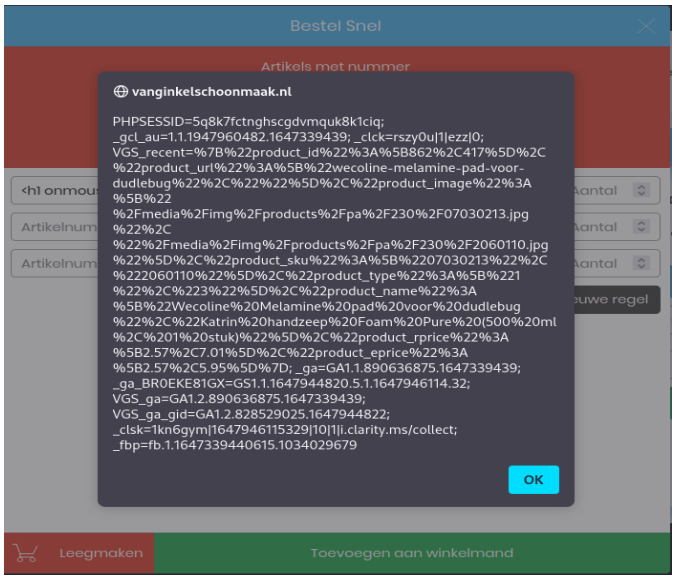


Figure 1.2.1

1.3 What have you learned considering this module?

- In this module I learned about the Cyber Kill Chain Framework, including the steps and the actions an attacker might produce on each step. In addition, I learned about different vulnerabilities and how I can search for them, especially web application vulnerabilities. Furthermore, I learned about certain laws and agreements and about the ethic regarding ethical hacking.

1.4 What are you proud of?

- I am proud of completing all the challenges given by our tutors regarding the ethical hacking. In addition, I am proud of completing different CTFs because I can notice that I have become more aware on possible security vulnerabilities on different subjects.

1.5 Which aspects do you want to develop further?

- I want to keep learning about web application vulnerabilities and how to patch them. In addition, I would like to improve my coding skills to produce better scripts and have a better understanding of how to write my own hacking scripts.

1.6 What will you do differently next time?

- What I would have done differently is to practice more, doing more CTFs to learn more about different techniques applied in each of the vulnerabilities and have a better understanding on how they work.

1.7 What grade would you give yourself on the corresponding outcomes?

- I would give myself an advance.

2. Risk Consultant

2.1 How did you obtain the Body of Knowledge about the subject?

- During the risk consultant section, I learned about the different security threats and threat actors that can target each entity. In addition, I learned how to complete a risk analysis and how to maintain business continuity from it. As a group, we assessed a company on their possible security risks, their possible actors, and possible mitigations to reduce the chance of a security incident. In Figure 2.1.1, the image shows the flow of how business continuity is applied.

Figure 2.1.1

2.2 How did you apply your skills into a practical situation?

- To apply this in a practical situation, I created a risk analysis table for the company previously pen-tested. The analysis was done after we identified, measured, and mitigated various risk exposures or security flaws facing the business or project. In addition, some possible mitigations were researched and shared to inform the company of their potential risks.

Threat	Impact	Impact level	Chance	Risk level	How & why	Conclusion
Ddos	Downtime, Reputation damage, Financial damage	3	3	High Risk	No DDoS protection thus easy target	Van Ginkel should get DDoS protection from a anti-DDoS provider and make sure to monitor traffic regularly for inconsistency's
Opportunists	Reputation damage, physical damage, Claims, environmental damage	4	3	Very Risk full Needs change!	Website is XSS and SQLi injectable	They should really look for more sanitized code and overall make sure that their website is protected against XSS and SQLi!
Malware	Reputation damage, physical damage, Claims, environmental damage, downtime, financial damage	4	2	High Risk	Anyone can fall for malware if not careful	They should in general be careful and always have either cloud or hard disk backup's in case of a hack. They should also keep customer credentials in a unreachable place
Phishing	Financial damage, reputational damage	2	1	Low Risk	Not really susceptible	Just watch out who mails and what they send you in links or attachments
Data breach (personal data)	Reputational damage, customer damage, claims human safety	3	2	Medium Risk	Possibility through XSS or SQLi	They should really protect their input bars better and make XSS and SQLi impossible on their website.
Stealing confidential business data	Reputation damage, Claims or Fines, financial damage	3	2	Medium Risk	Possibility through XSS or SQLi	They should really protect their input bars better and make XSS and SQLi impossible on their website.
Ransomware	Financial damage, Physical damage, Downtime, Incident handling costs, Environmental damage	5	2	Very Risk full Needs change!	Downloading wrong file can be disastrous	Ransomware is very popular these days, many company's experience them. Watch out what you download where you visit and for strange mails. Also keep software and os up-to-date
Advanced Persistent Threats	Reputation damage, Claims & Fines, financial damage	4	1	Low Risk	Not big enough to be attractive to for APT's	Since this is a costly undertaking and the company is so small this is unlikely but like with the other threats be careful on the internet

Figure 2.2.1

In Figure 2.2.1, we can observe the risk analysis table done by the team to inform the company about the risks and solutions.

2.3 What have you learned considering this module?

- In this module I learned about the different security threats such as malware, DDoS attacks, APTs, etc. In addition, I learned about the different threat actors and what security threat they might be threatening. With knowledge about the different security threats and actors, I also learned how to develop a risk analysis to enable a business to have business continuity.

2.4 What are you proud of?

- I am proud of completing all the tasks required in the Body of Knowledge. In addition, I am proud of understanding that Cyber Security also requires risks analysis to reduce the chance of security incidents. It is important to continuously look up for new possible threats or actors.

2.5 Which aspects do you want to develop further?

- I would like to improve in understanding the different types of threats and malware to know how they work, how they operate and spread. In addition, improve the mitigations given to the clients, to give more specific and effective solutions or preventions regarding the threats.

2.6 What will you do differently next time?

- Next time I would put more time analyzing the business and their possible threat actors, the threats that can be exploited, and suggest more specific solutions or prevention tools and practices for each of the threats mentioned in the analysis.

2.7 What grade would you give yourself on the corresponding outcomes?

- I would give myself a shown.

3. Security Engineer

3.1 How did you obtain the Body of Knowledge about the subject?

- In this chapter I learned about how to secure infrastructure or systems and grant end-users corresponding access to the system or infrastructure and the information in it. I learned why it is important to properly secure an infrastructure and follow the CIA Matrix. Furthermore, I learned about network segmentation, secure connections, and remote management. In Figure 3.1.1, you can see a solution that was delivered to a small

company web shop. It has high availability firewalls in the public LAN and proper network segmentation.

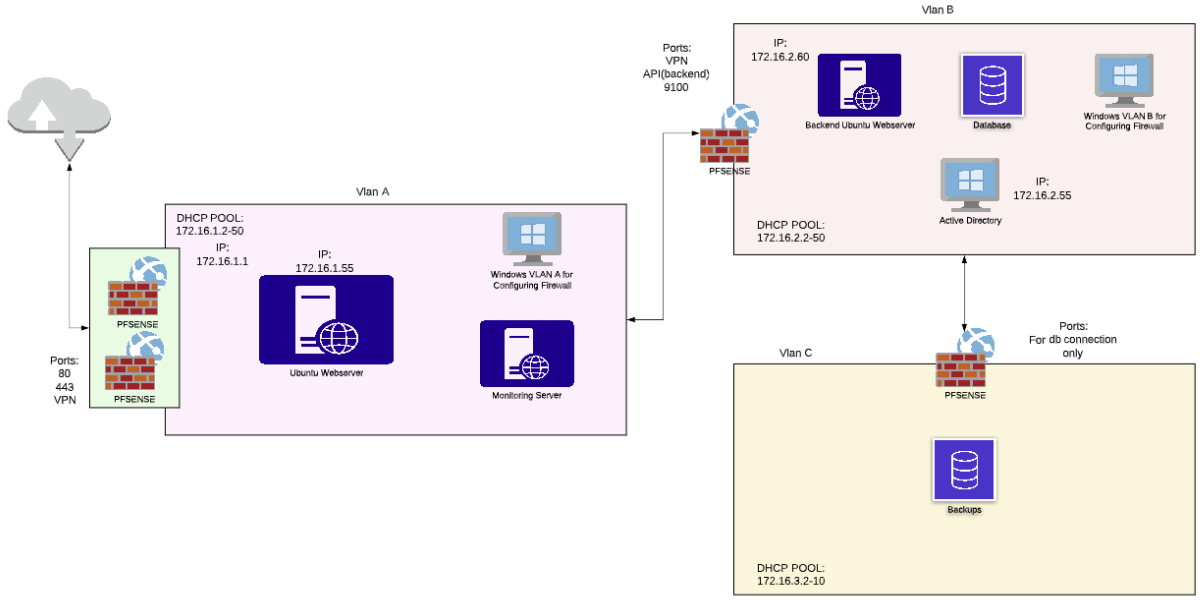


Figure 3.1.1

3.2 How did you apply your skills into a practical situation?

- As mentioned before, a solution was developed for a small company web shop. In this case, we secured the network using firewalls, VPN connections for remote management, only opened necessary ports, and put monitoring and IDS/IPS tools to continuously monitor our network. In addition, an Active Directory was set up, to provide user and group management and authentication when joining the network. In Figure 3.2.1, we can see the two different groups in the IT organizational group, one group has admin rights, and the other does not. In addition, users have password policies that require at least one capital letter and one number to reduce the chance of password guessing by attackers.

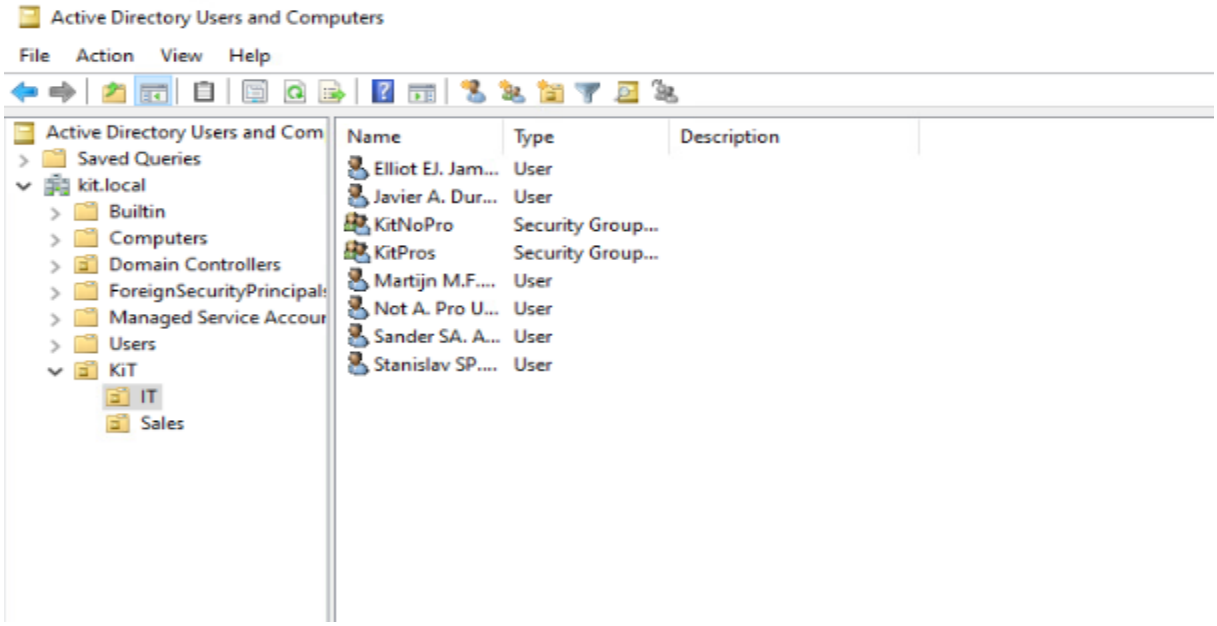


Figure 3.2.1

3.3 What have you learned considering this module?

- In this module, I learned about secure connections such as SSL and SSH, how to implement these services and how they work. Furthermore, I learned about secure remote management making use of VPN, made use of firewalls, and how to use Active Directory to harden the infrastructure by giving proper permissions and access.

3.4 What are you proud of?

- I am proud of developing a working secure solution that satisfies the needs of a small company web shop. In addition, I feel proud of the hard work I have put into the group project while developing the infrastructure. I am also proud of learning about the SSL certificates and why they are important, how to create them and how to secure HTTP connections.

3.5 Which aspects do you want to develop further?

- I would like to develop the practices of the CIA matrix to constantly keep improving tools and best practices such as:
  - Information security policies
  - Password strength

- Access controls
- Multi-factor authentication
- Antivirus software & firewalls
- Cryptography
- Legal liability
- Security awareness

In addition, I would like to learn more about network segmentation and how to properly secure every LAN.

3.6 What will you do differently next time?

- Something I would do differently next time is to spend more time learning about Active Directory and what are the different policies that can be set into place and learn about the complete functionality of Active Directory and what it is capable of.

3.7 What grade would you give yourself on the corresponding outcomes?

- I would give myself an advance.

4. Security Analyst

4.1 How did you obtain the Body of Knowledge about the subject?

- In the security analyst phase, I gained knowledge about what a security analyst does, monitoring tools and how alerts can prevent incidents, researching about CVEs on the system as shown in Figure 4.1.1., and about incident response. In addition, I learned about incident response and disaster recovery plans following the general steps of incident response procedure.

Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	LOW
User Interaction (UI):	NONE
Scope (S):	UNCHANGED
Confidentiality (C):	HIGH
Integrity (I):	HIGH
Availability (A):	HIGH

Figure 4.1.1

4.2 How did you apply your skills into a practical situation?

- To apply the skills learned in this phase, I implemented monitoring tools and alerts in the infrastructure of the secure solution. The implemented tools in the network for monitoring are Prometheus, Grafana, Node Exporter and Windows exporter to monitor individual computers and part of the network. In addition, Zeek was implemented to monitor the network traffic. Show in Figure 4.2.1 we can see Grafana monitoring dashboards and in Figure 4.2.2, Zeek connection logs.

Figure 4.2.1

```
root@student-virtual-machine:/opt/zeek/logs/current# ls
capture_loss.log  conn.log  dns.log  http.log  known_services.log  loaded_scripts.log  notice.log  ntp.log  packet_filter.log  stats.log  stderr.log  stdout.log  weird.log
root@student-virtual-machine:/opt/zeek/logs/current# tail -f conn.log
1654166860.538583       Cplrit3RooSqvgiHNg      172.16.1.18     50382   35.224.170.84   80      tcp     -       0.234268        0       148     SHR     T       F       0       ^hCadf  0       0       5
416     -
1654166851.370832       CfqA6M2cYnu6BskoK7      172.16.1.3      123     95.179.180.66   123     udp     ntp     0.003973        48      48      SF      T       F       0       Dd      1       76      1
76      -
1654166894.370711       CBJYQl2E7hli6xUROl      172.16.1.3      123     94.23.147.231   123     udp     ntp     0.011564        48      48      SF      T       F       0       Dd      1       76      1
76      -
1654166959.709269       C3xOpP2EpuaRu5VpSj      172.16.1.18     36718   185.199.109.133 443     tcp     -       -       -       OTH     T       F       0       C       0       0       0       0
-
1654166959.770383       CfDJMr3xZ25c61oZte      172.16.1.18     54166   34.120.177.193  443     tcp     -       -       -       OTH     T       F       0       C       0       0       0       0
-
1654166901.502882       CWNAQ5wnbgcEuWPo3       fe80::ffff:ffff:ffff:ffff       130     ff02::1 131     icmp    -       -       -       OTH     F       F       0       -       1       76      0
0       -
1654166901.519784       CGsAuv4jrua9uaOTRl      fe80::3a45:97a8:2585:64f        143     ff02::16        0       icmp    -       -       -       -       OTH     F       F       0       -       1       9
6       0       0       -
1654166901.698766       CHbael3VczpR3vulak      fe80::250:56ff:fe97:5bbf        143     ff02::16        0       icmp    -       -       -       -       OTH     F       F       0       -       1       1
16      0       0       -
1654166959.657309       CbTw3q2RZ5cYob01el      172.16.1.18     47116   172.16.1.2      53      udp     dns     0.030402        0       118     SHR     T       T       0       Cd      0       0       1
146     -
1654166959.657412       C2Z7yX1J88PZUrPhoh      172.16.1.18     50319   172.16.1.2      53      udp     dns     0.051300        0       166     SHR     T       T       0       Cd      0       0       1
194     -
1654166926.363335       CLObU73GOj87expnR7      172.16.1.3      123     185.80.247.36   123     udp     ntp     0.007686        48      48      SF      T       F       0       Dd      1       76      1
76      -
```

Figure 4.2.2

4.3 What have you learned considering this module?

- During this phase I have learned to install and configure different monitoring tools such as Zeek, Nagios, Prometheus and Grafana. I also learned the different steps to plan a security incident response. Furthermore, I learned how to prepare systems to reduce the chance of some threats and how to identify these threats.

4.4 What are you proud of?

- I am proud of learning how to properly install and configure different monitoring tools and how to identify the indicators of compromise that these tools will allow us to see. I am also proud of the personal specialization project in which I used different malware to learn how these malwares operate and what indicators can be seen from the monitoring tools and how to respond/prevent these threats.

4.5 Which aspects do you want to develop further?

- I would like to gain experience on how incident response teams operate and perform the different steps to recover operations for a business in a real-world scenario. In addition, I would like to learn more from different monitoring tools and their capabilities to know how to automate different alerts to keep the system constantly monitored.

4.6 What will you do differently next time?

- I would have tested different monitoring tools to see which performs the best and which are easy to configure and use. Furthermore, I would take more time to learn about incident response as it is very important to recover the operations of a business in case of a critical security incident.

4.7 What grade would you give yourself on the corresponding outcomes?

- I would give myself a shown.

Personal Specialization Project

Research Question

Main Question:

- What are the different types of malwares and how do they function/spread?

Sub-questions:

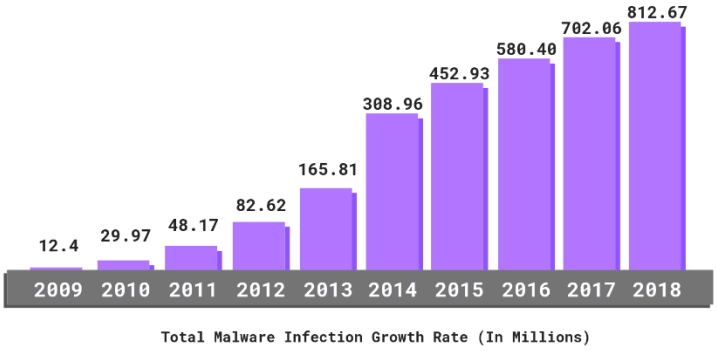
1. What are the indicators of compromise for each type of malware researched?
2. Which malwares are dangerous for a company, and which are dangerous for a casual user?
3. What are possible solutions against these threats?

Introduction

According to Security Magazine, Ransomware attacks rose by 92.7% in 2021 compared to 2020 levels, with 1,389 reported attacks in 2020 and 2,690 in 2021. This was a challenging year for cyber security professionals and IT experts, as they break down the record of most malwares' attacks in one single year. Professional analysts says that the number of cyber-attacks will increase during 2022 as the attackers are perfecting their techniques and finding more ways to get users data. The increasing started during the lockdown caused by the COVID-19.

The cost caused from these attacks also increased and the reports shows that in 2021 more than six billion of US dollar were lost. The main explanation of the lost is the fact that people had to work remotely and whenever a company faced a cyber-attack the time to respond and to find the origin of the attack was slower and more complicated.

The easiest way for an attacker to launch sophisticated assaults capable of bypassing even the strongest security systems is human errors, cyberattacks can come in various forms. Now a days the most common cyber-attacks are phishing, malwares and data breach. During this report we will focuses more on malwares, it is the most interesting attack, and it has a sophisticate elaboration. There are thousands and thousands of types of malwares, and we will present the five common categories that are trojans, ransomwares, worms, virus and key loggers.



Total Malware Infection Growth Rate (In Millions)

Goal

The goal for this research is to inform about the malware analysis done. This report will provide a breakdown on the functionality, risks, the process used by the malware to spread and some of the recommended solutions to prevent these malwares to infect your system. In addition, different types of known malware will be executed in an isolated network to be able to monitor how the malware behaves in a machine or network and what are the indicators of compromise in a machine for each malware. Furthermore, an analysis on how each malware can affect an enterprise or a casual user.

Objectives

- Research about different malware, what they do and how they function.
- Execute different malware in an isolated network to learn about their purpose.
- Record monitoring logs or charts to analyze the different behaviors of malware in a system and what are the indicators of compromise for each of the tested malware.
- Inform about the risks for a company for each malware.
- Inform about possible solutions to prevent or remove the malware from a system.

1. Testing Environment

Due to the nature of the research, an isolated testing environment was set up to be able to execute malware without spreading it into other networks or our own machines. In Figure 1.1 it is possible to observe a network diagram of the environment. The environment consists of two VLANs. In VLAN A, we will deploy a Linux machine that will act as the attacker, from where the malware will be sent to a machine that will be sitting in VLAN B. We will connect through SSH, to an Ubuntu machine in the same network as the "victim's" machine. From the Ubuntu machine we will attack the victim. In addition, we will have a monitoring server with Zeek, Prometheus, Grafana and Windows Exporter to analyze the behavior of each malware. In addition, we made sure the Linux based machines (Ubuntu and Monitoring Server) were updated with the latest version of the operating system to reduce the chance of the malware spreading to these machines.

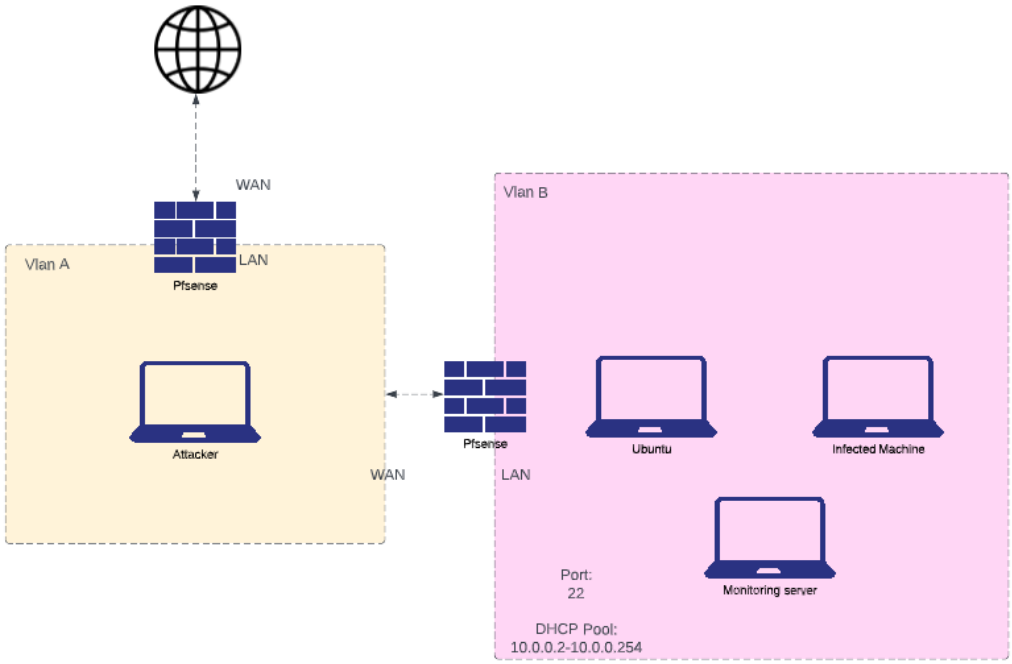
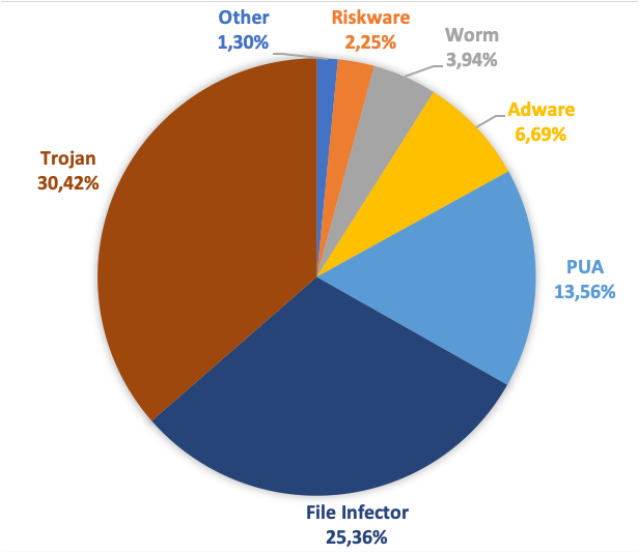


Figure 1.1

2. Malware

The term malware was created by the combination of the words malicious and software. Malware is the word used to define software or scripts that are specifically designed to cause damage to a computer, smartphones, networks and other electronic or programmable devices. There are many different types of malwares, which can cause different levels of damage to an enterprise or casual user. Depending on the malware executed, damage can be anything from hijacking a browser, degrading a device performance, encrypting and locking files, between many others. Based on how the malware infiltrated a computer or system, attack type, and damage levels, malware is broadly classified into 12 types, which are:

- Viruses
- Worms
- Trojans
- Spyware
- Ransomware
- Adware
- Rootkit
- Keylogger
- Browser Hijacker
- Botnet
- APTs
- Backdoors

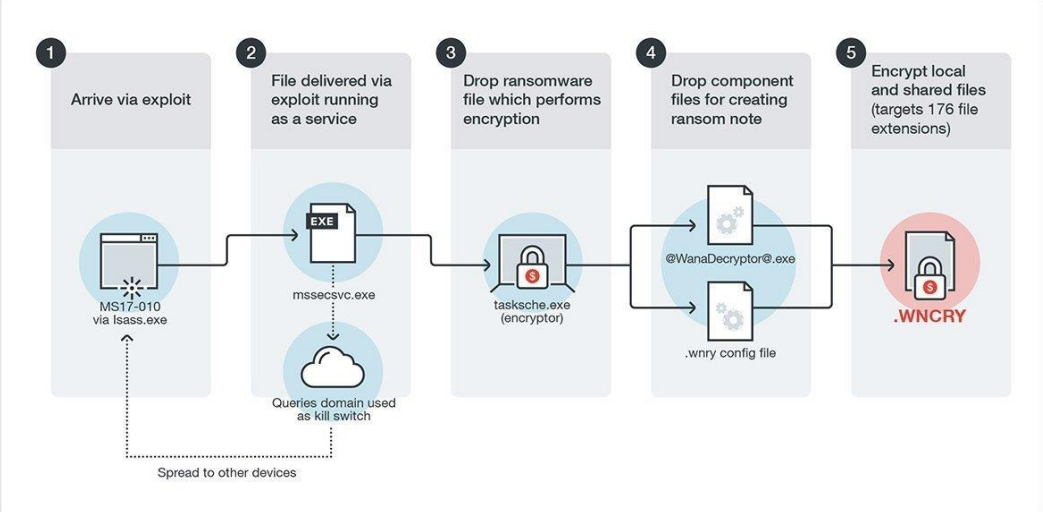


In general, a malware can infect a device in many different ways depending on the type of malware. Some of the most common ways malware can infect a computer or network are through free bundled software, phishing or spam emails, clicking on ad pop-ups, and through file sharing services.

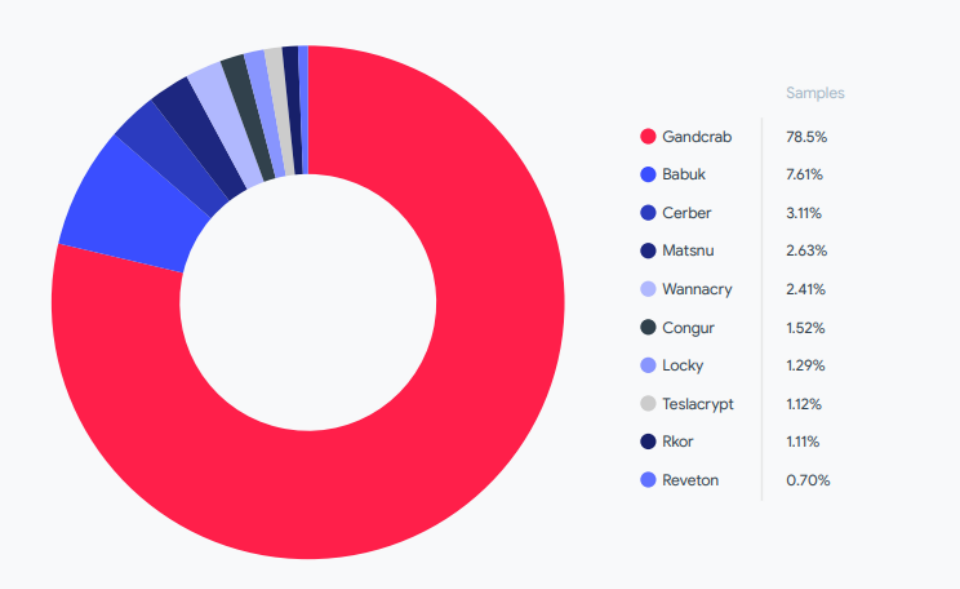
3. Ransomware

Ransomware malware encrypts an organization or user's critical data so that they cannot access files, databases or applications for a ransom. Ransomware is often designed to spread across a network and target database and file servers, and therefore quickly compromise the operations of an entire enterprise.

To understand more about this malware, WannaCry ransomware will be executed In a Windows Server abusing the Eternal Blue vulnerability in SMB shares. WannaCry ransomware is a ransomware worm that attacks Windows PCs. It is a form of ransomware that can spread from PC to PC across networks, looking for vulnerable devices, and then once on a computer it can encrypt critical files. Unlike phishing attacks, computer users don't have to click on a link or open an infected file. The WannaCry ransomware is executed with several components. A primary delivery program is executed. This payload contains other programs, including encryption and decryption software. Once WannaCry is on a computer system, it searches for dozens of specific file types and executes another payload to encrypt the files, which can only be decrypted using an externally delivered digital key.



This type of malware is extremely dangerous for businesses and casual users because all the information can be jeopardized. Historically, WannaCry is also one of the most popular ransomwares used. One report by MimeCast, noted a 53% increase in WannaCry ransomware in March 2021 compared to January of this year, while another stated that WannaCry was the top ransomware family used in the Americas in January with 1,240 detections.



3.1 Execution

To test how the ransomware worked and monitor it we executed WannaCry ransomware in a Windows 10 server machine. In Figures 3.1 and 3.2 the desktop of the machine is shown with some sample txt files and folders to see if they are encrypted by the ransomware. Once the files were created, we downloaded the ransomware software in the victim's machine to be then executed.

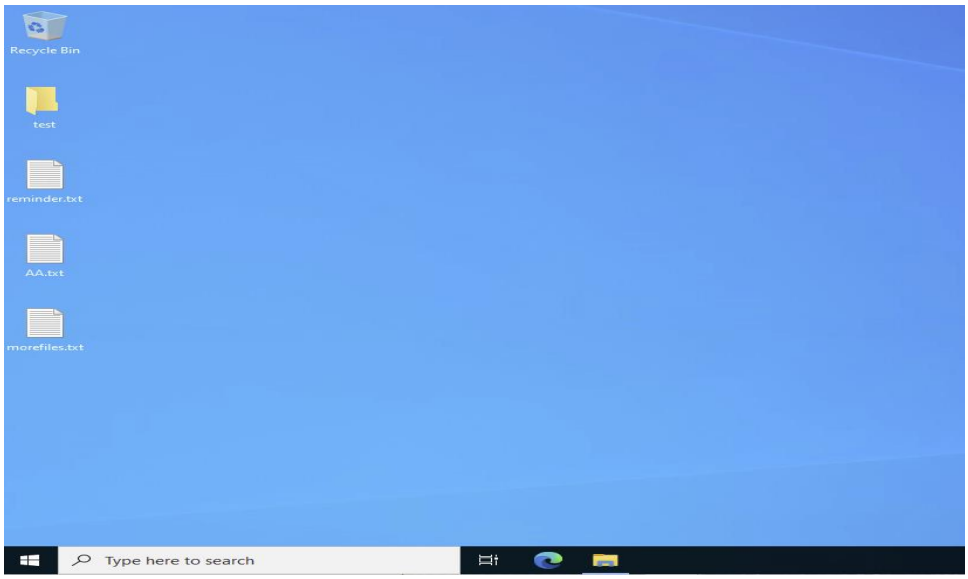


Figure 3.1

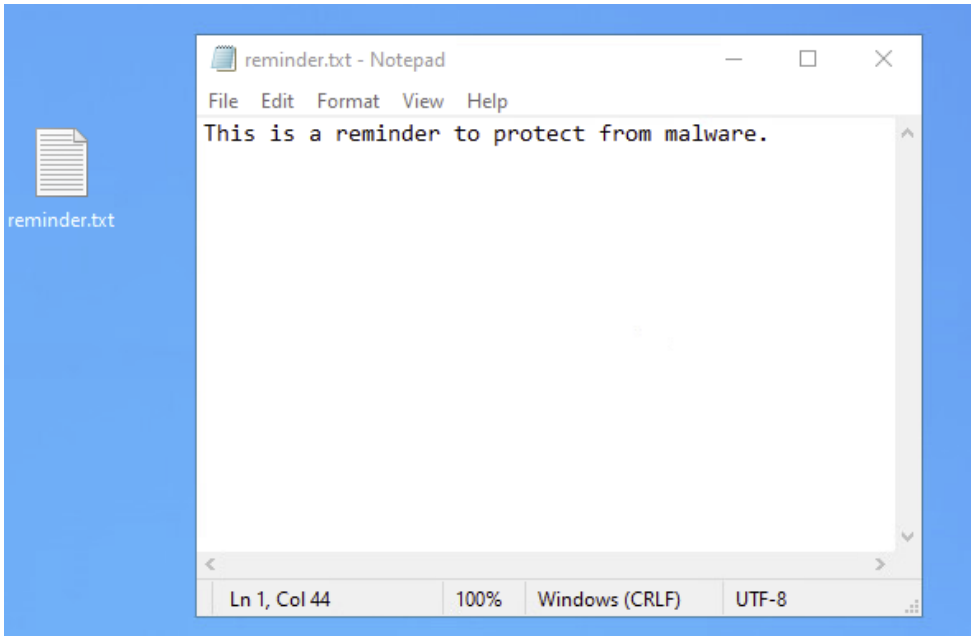


Figure 3.2

Once the ransomware was executed, it took only around 40 seconds until the desktop was as shown in Figure 3.3. All the files were encrypted like reminder.txt in the picture, and a ransomware payment application pop out.

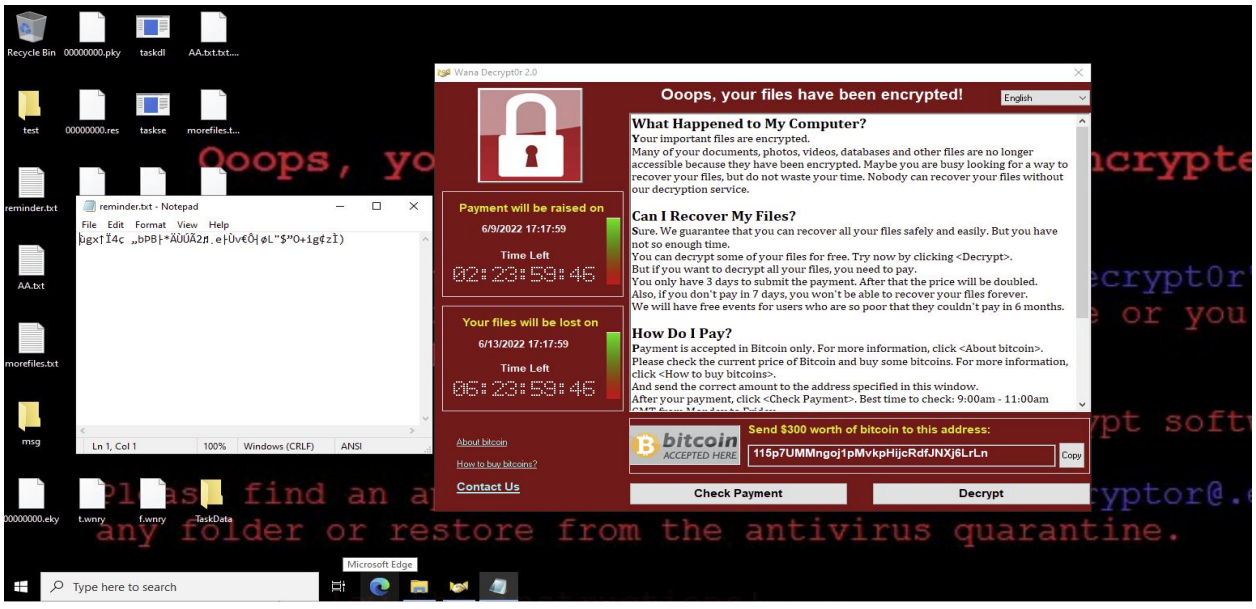


Figure 3.3

3.2 Monitoring

Using the monitoring tools installed we can observe some of the indicators of compromise that the ransomware showed in the attack. Some of the clearest indicators were the use of the CPU that escalated very quickly after it was in use. In addition, suddenly much information in the disk was read and then written as seen in Figure 3.4.

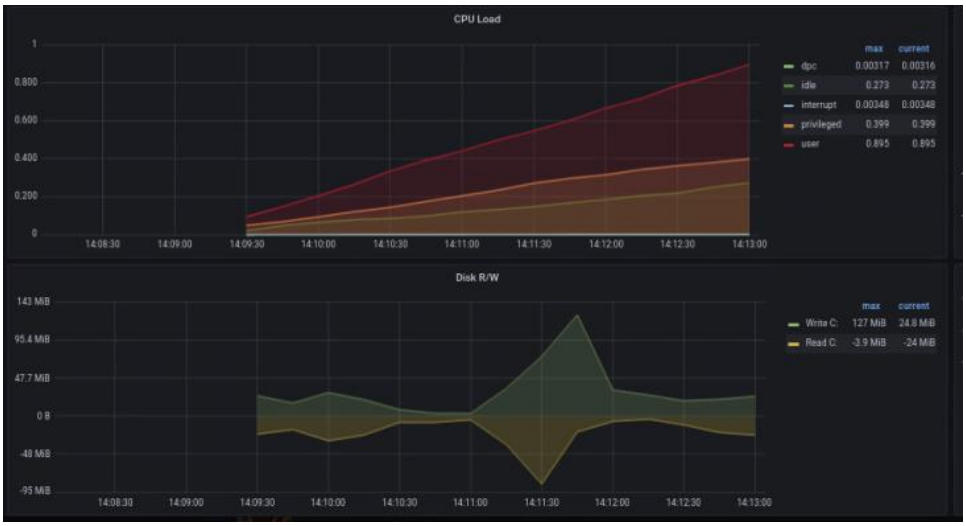


Figure 3.4

Since WannaCry ransomware is known to still be active and in use, some possible solutions and best practices to prevent a ransomware attack, more specifically threats similar to the WannCry ransomware malware:

- The ransomware exploits a vulnerability in SMB server. Patching is critical for defending against attacks that exploit security flaws. Disable the SMB protocol on systems that do not require it.
- Proactively monitor the network to reduce the risk of the malware from spreading.
- Filters to identify spam emails using tools to prevent email-based ransomware spread.
- Monitor the behavior of machines in the network to block unwanted modifcations or applications from executing in the machine.
- Network segmentation using proper security in all of the networks.
- Back up files offline regularly to help restore the computer in the event of an attack.
- Employee awareness on cybersecurity.

4. Worm

In simple words, a worm is a malware that uses computer networks and connections to spread. Once the worm is allocated in a computer, it will hunt for other connections or devices connected to the system and try to infect them too. Worms will likely spread through emails and through message and sharing services and usually do not need human activation after the system is infected. Some of the malicious actions the worm will perform after allocating in a computer system are:

- Drop other malware like spyware or ransomware
- Consume bandwidth
- Delete files
- Overload networks
- Steal data
- Open a backdoor
- Deplete hard drive space

To analyze the behavior of worm malware, the ILOVEYOU worm will be executed in a Windows Server. This worm self-replicates and sends copies of itself through a network without any action from a person. It started being sent as an email with a .vbs file that was masked as a .txt file titled "Loveletter". Once the malware was executed, it would steal passwords and overwrite almost all file types. In addition, it would also search on the Outlook contact list and send a copy to each of the members on the list, spreading even more. The ILOVEYOU worm infected tens of millions of computers globally, resulting in billions of dollars in damage when it was first spread. Many important entities were affected by the ILOVEYOU worm. Some of the most important entities affected were the Pentagon, CIA and the UK Parliament. Historically, the ILOVEYOU worm is known as the second worm to have more impact in the world. The worm is dangerous for both enterprises and casual users, because its techniques can be used to download or execute other malware which can put in risk entire systems.

4.1 Execution

To execute the malware, we downloaded the worm in the victim's machine. Once the worm was downloaded, a txt file named "Iloveyou.txt" was downloaded to the computer's desktop. When the file was opened the worm infected the rest of the machine and tried to infect other machines in the network. If an outlook account would have been linked to this machine, the worm would

look for the contact list of this account to replicate itself and send the malware file to its contacts, spreading even more. In Figures 4.1 and 4.2 we can see the before and after of the execution of the malware. The Iloeyou.txt is really a .vbs file, and converts the rest of the .txt files to .vbs files.

Figure 4.1

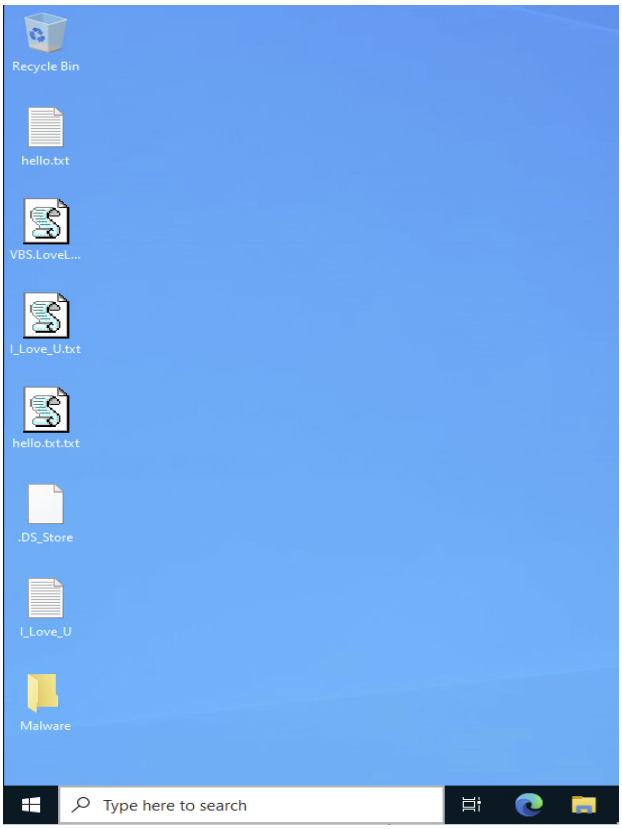


Figure 4.2

4.2 Monitoring

The clearest indicators that a machine has been infected with a worm were the network traffic coming out of the machine without the user trying connections to the other machines in the network. The traffic was monitored by Zeek, which can be seen in Figure 4.5 and by the traffic coming in and out of the machine recorded by Prometheus and Grafana in Figure 4.4. Other indicators were the CPU usage escalated every time a txt file was opened and converted to a .vbs file.

Figure 4.3

Figure 4.4

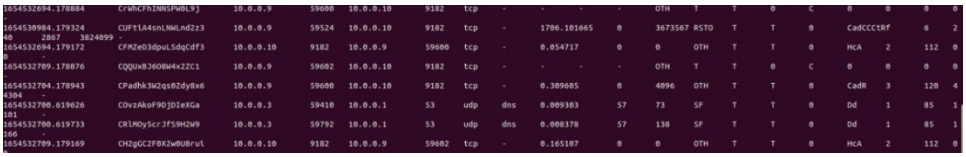


Figure 4.5

The ILOVEYOU worm is not active anymore, but other cybercriminals have used similar techniques that can harm a company; therefore, it is important to put in place prevention and detection measures against this and other worms. The following are prevention measures that will likely prevent worm attacks:

- Use a strong antivirus program that is able to perform live-scans, acts as a firewall, has automatic and regular updates, and has behavior-based detection. Furthermore, the antivirus should be able to remove software that is detected as malicious.
- Be cautious when opening email attachments. As a company add security measures to filter spam emails to reduce the risk of worm attacks.
- Do not click on pop-up ads when browsing the internet. Worms can inject adware into legitimate websites with hope that a user will open it and force the worm into the device.
- Use VPN when downloading from unknown sources or torrents.
- Update software and operating system regularly.
- Employee awareness on cybersecurity.

5. Key Logger

A key logger is a common cyber-attack that record the inputs of the victims' keyboards and store them in a text file. For example, if you log in to a website the attacker will get your username and password. This can be harmful for the user or a company. Key loggers are legitime, parents can use them to keep track of kids search, and companies can monitor their employees and keep an eye on their work. There are different types of keyloggers, the of this malware can be:

- Track activity like opening folders, documents, and applications
- Log clipboard text
- Record information that you cut and paste from other documents
- Take and record randomly timed screenshots
- Request the text value of certain on-screen controls

The keylogger we decided to use is RedRabbit, it is a PowerShell script that creates a file in a hidden folder from the victim machine, the attacker will name it as he wants to and whenever a key is pressed from the keyboard of the victim it will be recorded and copied to the file created by the attacker.

We will execute RedRabbit in the Victim machine and give a name to the file where all the keys will be saved, in this case we will put keylogger.txt.

5.1 Execution

To execute RedRabbit, we connected through SSH to the machine and downloaded the keylogger. Once the malware was downloaded, it was executed.

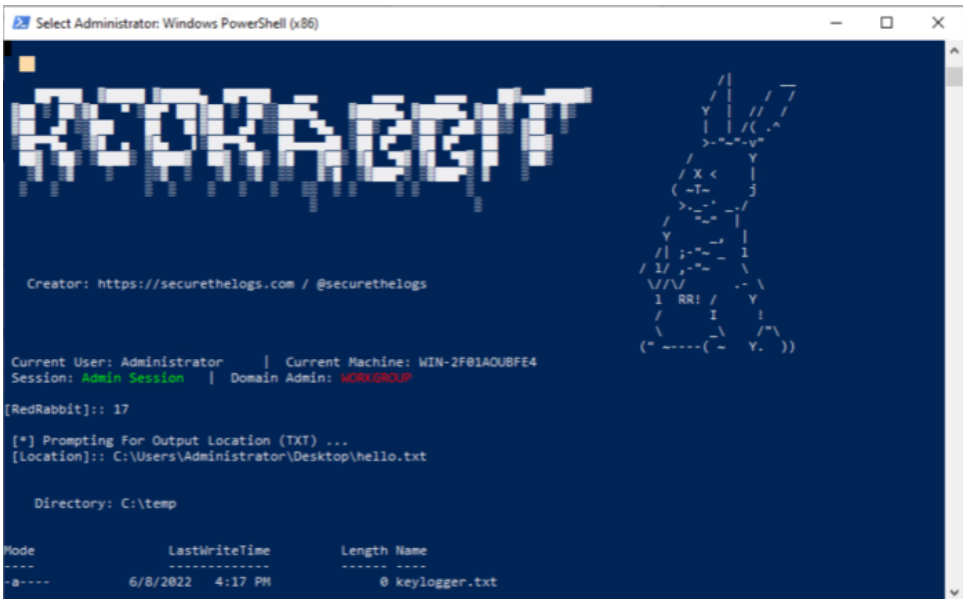


Figure 5.1

When the User types something in a text file or in another application all the keys will be visible in the Keylogger.txt file.

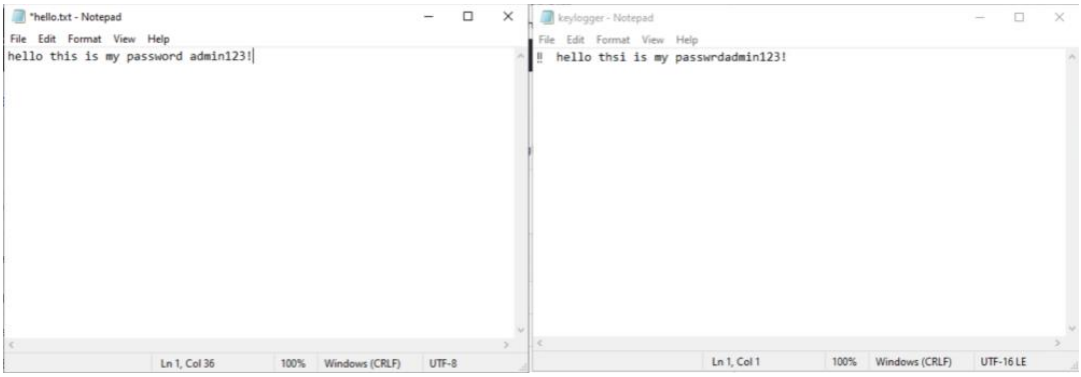


Figure 5.2

5.2 Monitoring

The only indicator of compromise received by Grafana was that there are files being written in the C drive whenever the user is typing something online or in another application. If the attacker is listening to the keylogger through network protocols such as HTTP or TCP connection, network traffic should also be detected.

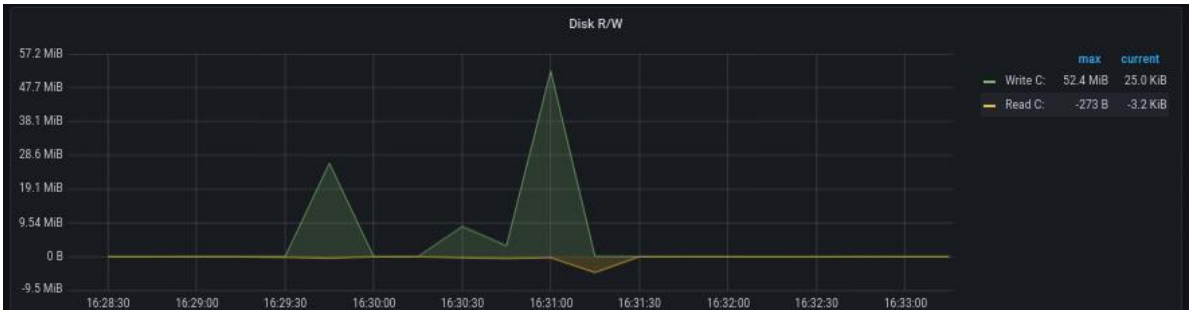


Figure 5.3

Keyloggers are highly active and are increasingly common type of malware. Some methods to prevent or stop keylogging attacks are:

- Use 2-Step verification to prevent an attacker from logging into your accounts if he/she has stolen any of your credentials.
- Installing software updates patches vulnerabilities on the computer and internet browser.
- Use password managers to decrease the need of typing important credentials.
- Use key encryption software to encrypt the keys you press on the keyboard to prevent keyloggers from capturing the exact keys.
- Avoid downloading software from untrusted sites.
- Use antivirus software to scan applications and files.
- Employee awareness on cybersecurity.

6. Virus

A virus is a malicious software or malware that causes damages to your data and spreads between computers. They are programmed to damage programs, delete files, or reformate the hard drive. Now a days there are hundreds of different types of viruses, it can be discoverable due to a slow or weird performance of the laptop. If the device is running slow, applications and internet speed are slow this mean that the machine is infected. Also, the fact of receiving pop-up windows and ads is a sign but usually from an adware. Viruses can damage your laptop in different ways.

The virus we will execute in the user machine will be YouAreAnIdiot, this virus is known to be annoying and difficult to terminate. When the virus is executed, the user device looks normal and do not present any anomaly however when the victim presses any application the device will start popping up different tabs with an image saying you are an idiot and with an annoying music

that will not stop until you turn off the machine. The big problem arrives when you restart the machine, and the virus will start again if you press another application. YouAreAnIdiot isn't harmful for your files or data, but it is irritating.

Here is the demo, this is the victim machine with only google installed and nothing else.

6.1 Execution

In this case, the file was only downloaded, but not executed. The virus, once allocated in the computer, will execute itself when the user opens their web browser (Google Chrome in this case).

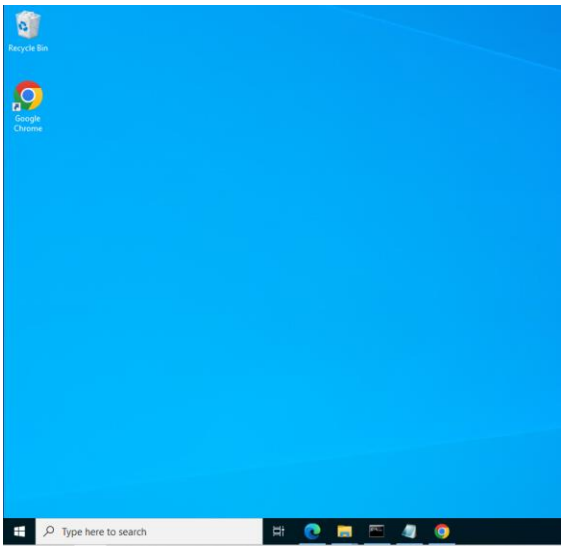


Figure 6.1

When the user opens the web browser application, windows start to pop up with a text "You are an idiot" and they can't be stopped, or another will appear.

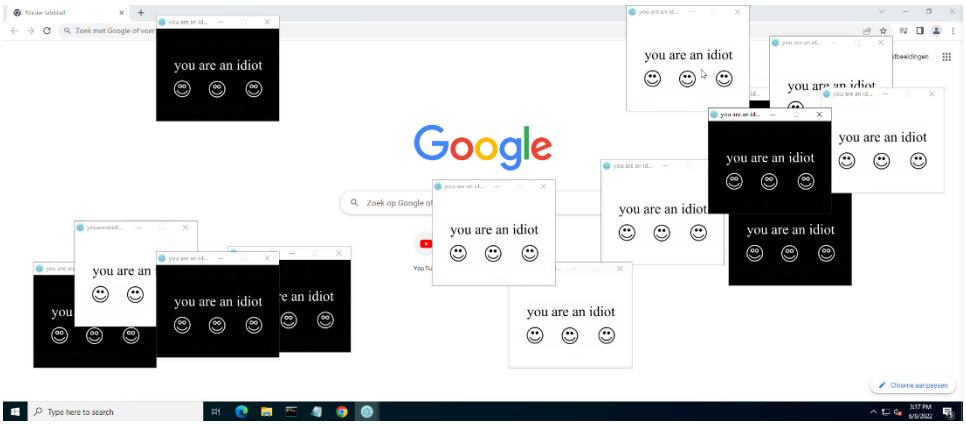


Figure 6.2

6.2 Monitoring

On the monitoring side we see that the CPU usage, processes, and user CPU increased enormously, when a tab appears different processes starts, and the CPU needs to use more power.

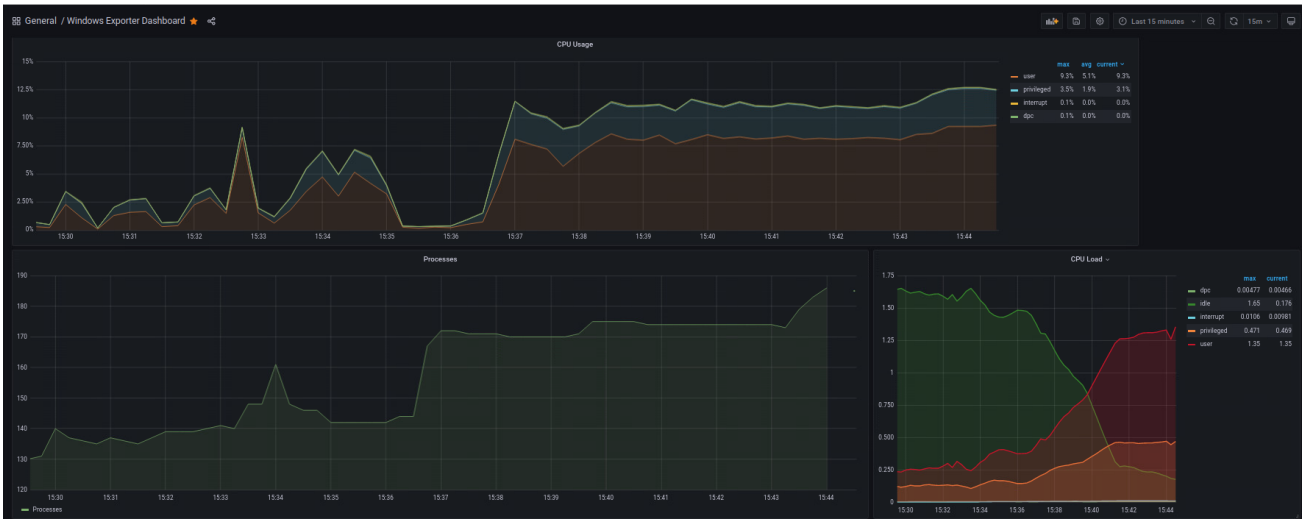


Figure 6.3

To avoid a similar situation, where your laptop loses power and execute strange actions, these are the solutions:

- Use a strong antivirus program that can perform live-scans, acts as a firewall, has automatic and regular updates, and has behavior-based detection. Furthermore, the antivirus should be able to remove software that is detected as malicious.

- Network segmentation to prevent spreading.
- Limit software installation options to reduce the risk of an employee to download malicious software.
- Employee awareness on cybersecurity.

7. Trojan

A trojan is another type of malware, it is the most popular "virus" in the society as everyone has heard the word trojan virus. This name comes from the Greek's mythology, due to the Trojan horse during the war between Greeks and the city of Troy. To end up the war the Greeks gave as a present a huge horse made by wood, after introducing it inside Troy, the horse was full of Greeks figthers, they all went out and conquer Troy. The trojan Virus is similar but with malicious code inside, for example, an user wants to download a game but doesn't have money to pay for it, the next step will be to search the game in none secured websites to find it for free. Once the game has being downloaded and the user starts it, the computer is infected and the trojan conquered the device. The main objective of a trojan is to camouflage from users and once it gets inside, they insert other types of malwares, malicious code or viruses in the device. They can be camouflaged in the form of regular software such as utilities, games and sometimes even antivirus programs.

We will use the 000 Trojan for this report and monitor all types of anomalies that goes on the machine. The 000 Trojan is a harmful malware that no one wants it inside their device. Once your machine is infected it will start downloading different types of files and programs with more malwares, it steals system and user data, it can also extract information from the browser and other application. This Trojan collects the following device data:

- GPU
- CPU
- Operating System
- RAM
- IP address/ geolocation
- Active processes

7.1 Execution

Once the Trojan was downloaded in the victim's machine, we proceeded to executing the malware. Once the Trojan starts to act, the machine will be restarted, and the user will notice that the username has changed to "UR NEXT" but the password is still the same.

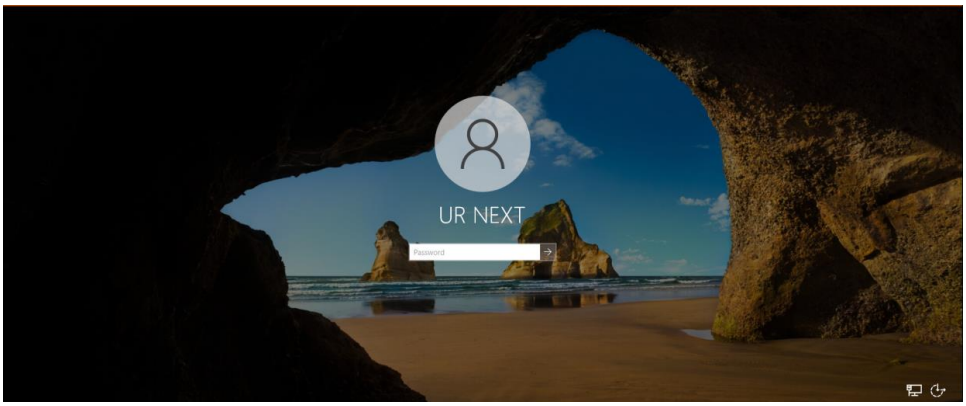


Figure 7.1

Once inside the machine, many processes start running and the whole desktop is full of text files, that can also be other applications, with "UR NEXT". Another anomaly is that the user is not able to open certain programs or applications. in this case we tried to open the task manager, but it was disabled by the malware.

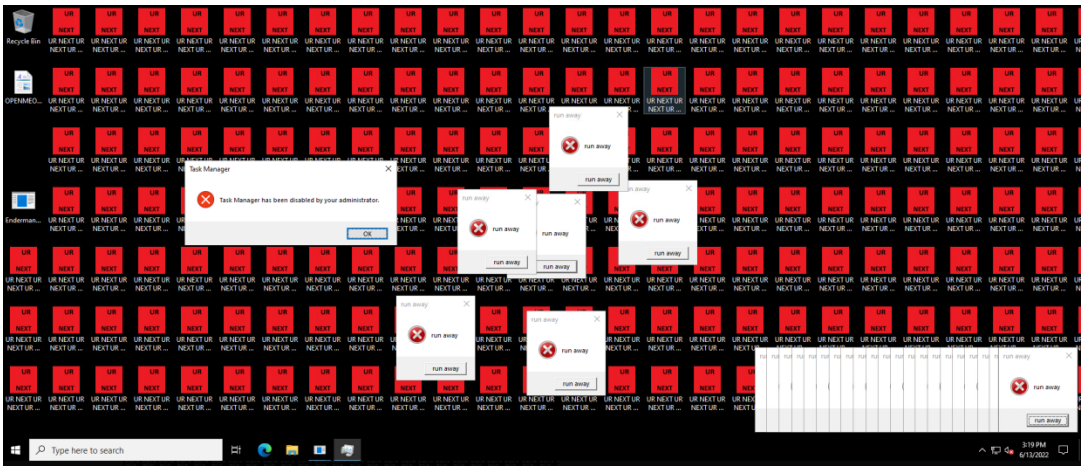


Figure 7.2

Finally, after two minutes of trying to delete the trojan, a video of a foggy and very sinister road appears on the screen, and it was not possible to escape it, making the computer completely useless until complete reset.

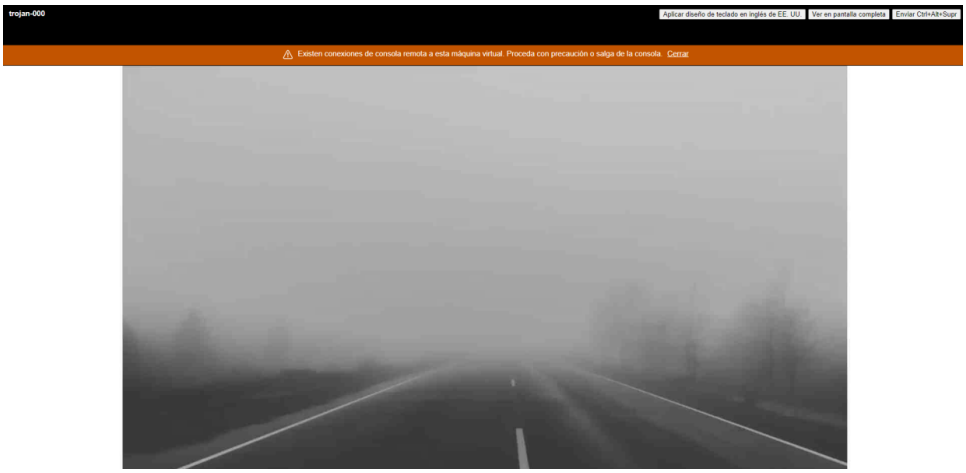


Figure 7.3

7.2 Monitoring

The monitoring tools showed that the CPU usage increased during the infection; we see in Figure 7.4, that the virus downloaded the video file. The processes also increased and because of this the CPU also increased, finally it wrote multiple files in the C drive.

Figure 7.4

The best way to protect against Trojan attacks is by practicing responsible online behavior, as well as implementing some basic preventive measures. Some best practices for preventing Trojan attacks are:

- Never click unsolicited links or download unexpected attachments.
- Use strong, unique passwords for all online accounts, as well as devices.
- Make use of spam filter to reduce the risk of phishing attacks.
- Back up files offline regularly to help restore the computer in the event of an attack.
- CrowdStrike Cybersecurity Company recommends a combination of methods to prevent and detect trojan malware. These methods include machine learning, exploit blocking, behavioral analysis, and block listing.

8. Conclusions

In conclusion, it was very interesting to analyze and learn how different malware behaves and how it can cause damage to certain individuals or entities. Analyzing the indicators of compromise that these malwares can show in monitoring tools to put alerts into place and prevent these malware attacks or at least reduce the chance of it spreading through a corporate network. In addition, knowing what tools and techniques can be used to reduce the impact of these attacks is very important for future security incidents that we can experience. Furthermore, it is important to be aware that these threats exist and can cause severe damage to a system, so we need to be alerted.