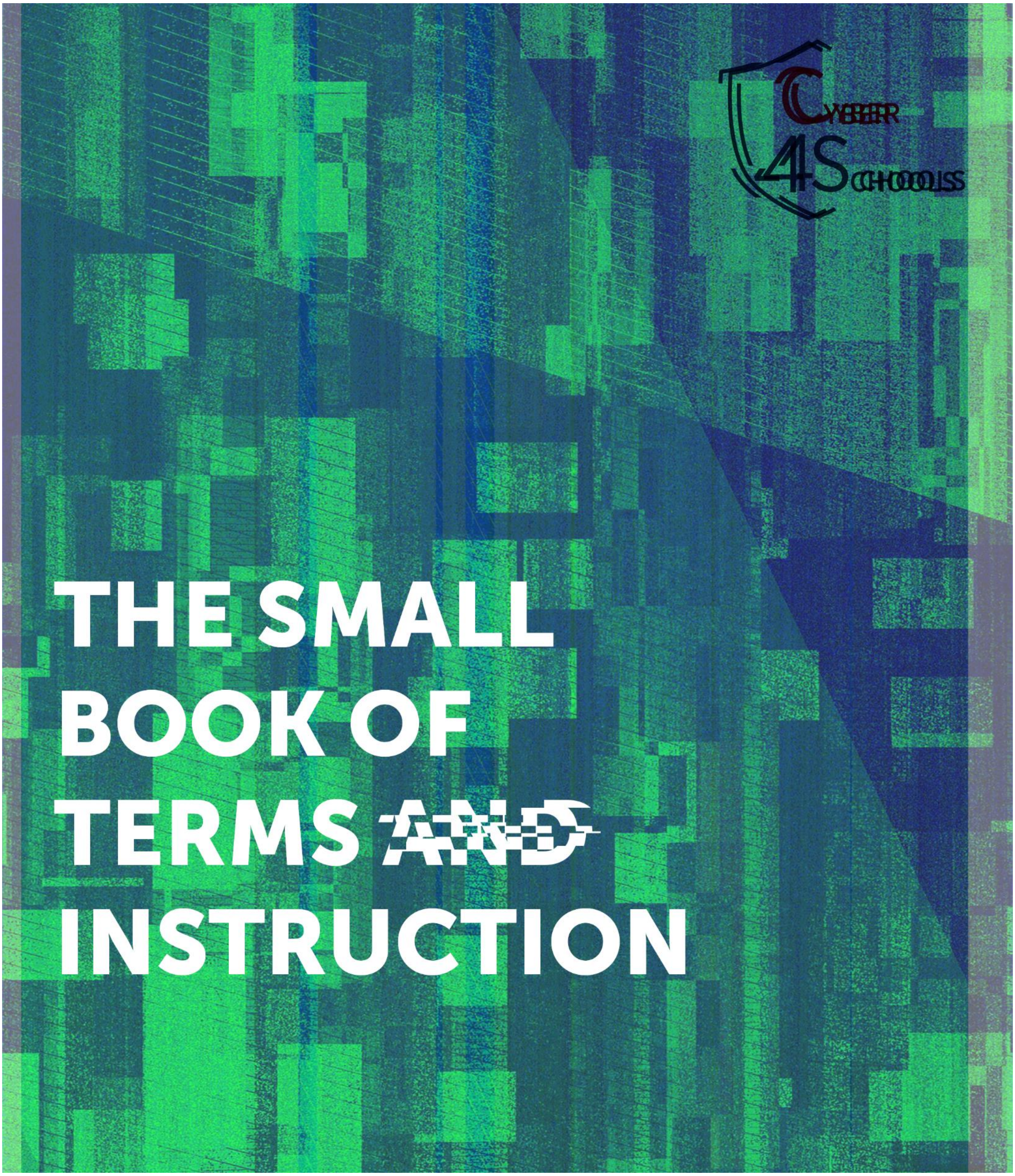


THE SMALL BOOK OF TERMS AND INSTRUCTION

Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Cyber
4Schools

WELCOME TO CYBER FOR SCHOOLS

This small cyber book will introduce you a wide range of security terms, commands and tools that will be needed for a successful game session!

And this is not even the coolest part!

Equivalents of attack and defence in security are the red team and blue team respectively. You will learn your duties and responsibilities as we dive on each of the episodes that you will play on the game. While the reds will use the Linux Terminal on their Virtual Machine to solve their tasks, which will mainly include simulation of hacker's malicious activities, the blues will use windows and will have to stay vigilant in order to detect and recognize malicious activity, links or attachments.

EPISODE 1: PHISHING

In this episode, Blues and Reds will be introduced to Phishing. Probably you have heard of this before! Hackers use multiple ways to trick people and then hack them. Sometimes they also use something called *social engineering*, which is a family of techniques that uses psychological manipulation to trick people into giving away secret or confidential information.
The most famous social engineering technique is *Phishing*, in which attackers send messages or emails to the victims, asking them for private information, or pushing them to click on links (websites), or sending them malicious files that at first glance might look normal.
In this episode, something like this might happen, so you need to stay really vigilant.

What phishing looks like:

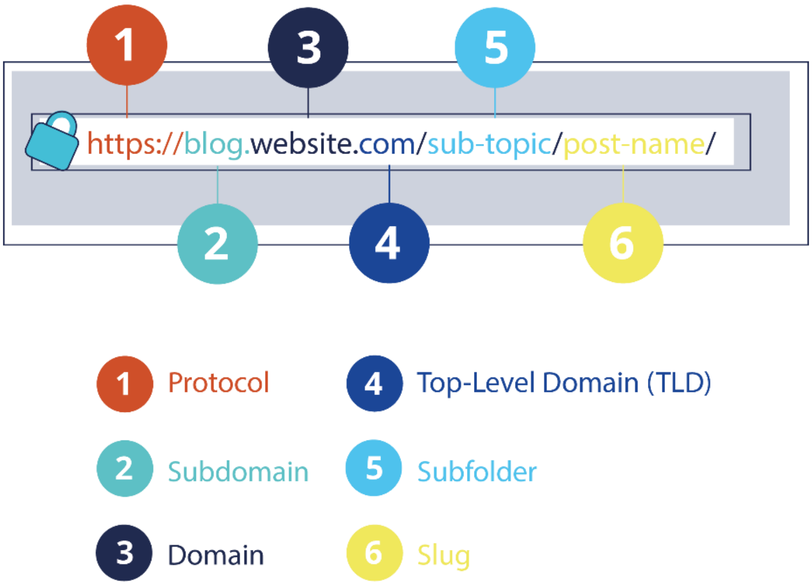
- Language: Sometimes it requires immediate action from you!
- Grammar: Look out for grammatical mistakes. Sometimes they have plenty!
- Pictures, Logos and Footers: All these might make you think the email is coming from a legitimate person. Do not be fooled!
- Attachments: You should know that the delivery of the malicious files is through this email, so it is highly possible that the file contains a malware!
- Links: Links included on the email could be quite dangerous. Are they safe? Be careful not to click them without making sure…

Some preventive measures you should keep in mind:

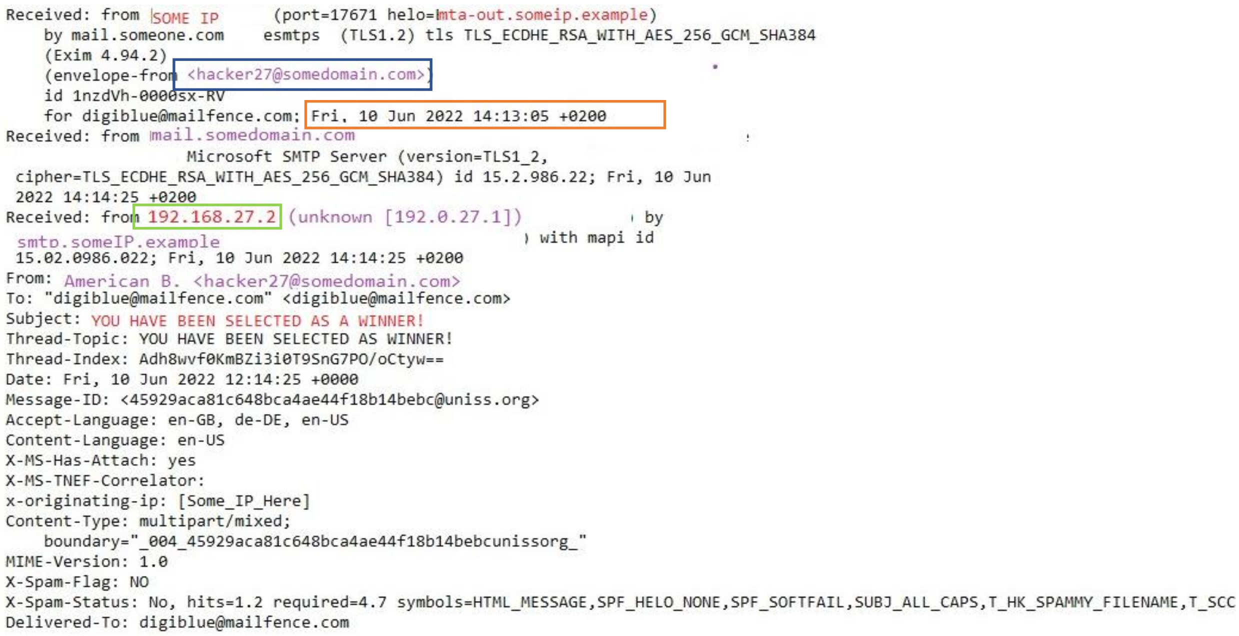
- Think: Was this email expected? Why is it this urgent?
- For attachments: Do not download anything without making sure what it is!
- For links: Use mouse hovering! Check the email source code to learn more about the email.

But, what is mouse hovering? How can I tell a website is safe at a first glance? What is the email source code?

Mouse Hovering is a simple technique you can do with your mouse by moving it to the link attached. If you are lucky enough, you will see the real website's name.
HTTP and HTTPS are the very first letters we see when we are browsing on the internet on the very top box. These two are both protocols used on the internet in order to transfer data. When a website is using HTTP, it is not secure! This means everything we type on the website such as username, passwords, emails, etc. can be easily captured by a malicious person.
HTTPS on the other hand is secure! Remember the **S** stands for SECURE! This means everything we type on a website will be difficult to understand for a malicious actor, as it will be *encrypted*, or changed from its original form when is being transferred.
The anatomy of a website:



Email source code investigation or just investigating the **header of an email**, sometimes can help us to determine the legitimacy of an email. Below is an example of an email source code, which format is quite different from what we have seen. However, we can get a lot of information from it! Let's see what is important! You teacher will guide you how to go there from the mail service you are using!



```
Received: from SOME IP      (port=17671 helo=mta-out.someip.example)
    by mail.someone.com    esmtps  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    (Exim 4.94.2)
    (envelope-from <hacker27@somedomain.com>)
    id 1nzdVh-0000sx-RV
    for digiblue@mailfence.com; Fri, 10 Jun 2022 14:13:05 +0200
Received: from mail.somedomain.com
                  Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.986.22; Fri, 10 Jun
 2022 14:14:25 +0200
Received: from 192.168.27.2 (unknown [192.0.27.1])              by
 smtp.someIP.example                                          ) with mapi id
 15.02.0986.022; Fri, 10 Jun 2022 14:14:25 +0200
From: American B. <hacker27@somedomain.com>
To: "digiblue@mailfence.com" <digiblue@mailfence.com>
Subject: YOU HAVE BEEN SELECTED AS A WINNER!
Thread-Topic: YOU HAVE BEEN SELECTED AS WINNER!
Thread-Index: Adh8wvf0KmBZi3i0T9SnG7PO/oCtyw==
Date: Fri, 10 Jun 2022 12:14:25 +0000
Message-ID: <45929aca81c648bca4ae44f18b14bebc@uniss.org>
Accept-Language: en-GB, de-DE, en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-originating-ip: [Some_IP_Here]
Content-Type: multipart/mixed;
    boundary="_004_45929aca81c648bca4ae44f18b14bebcunissorg_"
MIME-Version: 1.0
X-Spam-Flag: NO
X-Spam-Status: No, hits=1.2 required=4.7 symbols=HTML_MESSAGE,SPF_HELO_NONE,SPF_SOFTFAIL,SUBJ_ALL_CAPS,T_HK_SPAMMY_FILENAME,T_SCC
Delivered-To: digiblue@mailfence.com
```

You see, there are three **Received chains**. Think of these as the places or servers the email has hopped in order to get to you.

The last **Received** is more important as it shows the internet protocol or *IP* of the sender.

Other information you can get: the exact time and date, the real email address of the sender, the subject, the real domain where the email is coming from, etc. can all be identified.

Did you know:

- Microsoft is the most impersonated brand globally when it comes to phishing attempts! People fall for it!
- The most common data types that are stolen from phishing emails are: Credentials (usernames and passwords), personal data (phone numbers and email addresses), medical data and banking data (credit card information).
- Brazil is the country with the highest number of phishing emails at the moment!

INFORMATION FOR THE BLUES:

- You should stay vigilant and pay attention to all the up-mentioned information
- You will be using Windows to solve this first episode as well as the others
- You will be provided extra tools on Windows in order to check out the malicious link; check them out and paste the link there without clicking

INFORMATION FOR THE REDS:

- In order to create a phishing email, you should also take notice of the above
- You should try hard to mimic a real person or appear legitimate!
- You will be using Linux terminal, which is a place to help you easy operate into the system, or do whatever activity you want just by writing some easy commands
- In order to ease the creation of a malicious website which will be placed on your phishing email, below you can find a table of commands to use in terminal (to have your own fun time!) or Aliases (or simple commands we created for you) to make the process easier
- The commands below can be used for any of the episodes, while aliases are unique for each of the episodes!

Aliases, commands and tools for Reds

Check "Tools and their Details" folder inside the Episode1 folder on Desktop, to learn more about the adjusted tools you will use.

create_bad_link – This will redirect you to a "portal" where you can create your own malicious link, where you have to follow steps on the screen based on your preferences
where_is_data – This command will send allow you to see in which file the data is saved and how it is named. Note: This command views the filename but the content you have to check yourself!
prepare_bad_email – This will redirect you to a portal where you can step-by-step prepare a phishing email, which you will test yourself.

whoami – Ask the terminal this and you will get your username
cd – It stands for "Change Directory" and with this command you can switch from one folder to another.
ls – This command will list you all the files inside one directory or folder
mkdir – This command is used to create a new directory or folder
mv – This command is used for moving and renaming files or folders inside a directory
pwd – This stands for "Print Current Directory" and you will get the location or the folder you are in; you can be in Desktop, or inside any folder
nano – Nano is a text editor tool you can use to view the content of a file from the terminal
date – It displays the system's date and time
cp – A command to copy files
sudo – Using this before every command, will let you execute anything as an administrator! Be ready to type the VM-s password a lot…

EPISODE 2: MALWARE (Spear phishing)

In addition to the malicious links, there are also malicious attachments that if downloaded, can harm our computer. These malicious softwares are called **malware** and depending on their type, they can affect our computer in different ways, such as infect, steal the data inside, encrypt the data (or make it inaccessible/unreadable), or conduct any other behaviour that the attacker wants.

RANSOMWARE:

In this episode, you will have a closer look at the malware called **Ransomware**. The behaviour of the ransomware looks like this: After installed on the computer, it will search for specific files and make them inaccessible from you (or else *encrypt* them), until you pay a certain amount of money (or *ransom*) that the attacker has demanded from you. Usually, there is always a message on your screen informing you that your files have been encrypted, and you need to pay money to get the key from the attacker in order to decrypt them, or else get them back. This is called a *ransom note*. Your files are held for ransom (the amount to be paid), and that's where the name of the malware is derived from.

But first, let's talk a bit about encryption. Encryption allows the data to be hidden or not readable from humans, and it is done with a secret code or a key. When the ransomware locks our files, the files are said to be *encrypted*. The opposite process is called decryption, and it is the process of changing the encrypted information back to *plaintext*, or else readable text, with the use of a secret key. This key can be the same as the encryption key (called symmetric encryption), or different from it (called asymmetric encryption).
Below is a schema of "Hello" message that is first in plaintext, encrypted in the second block so you can only see symbols, and decrypted in the third block where you can again read it!

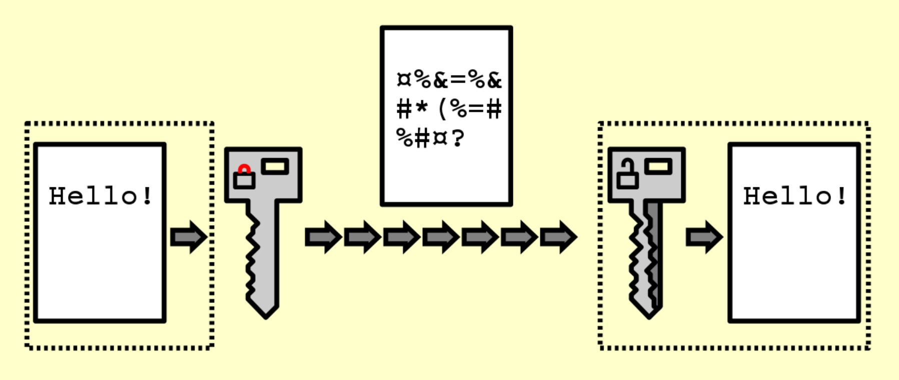
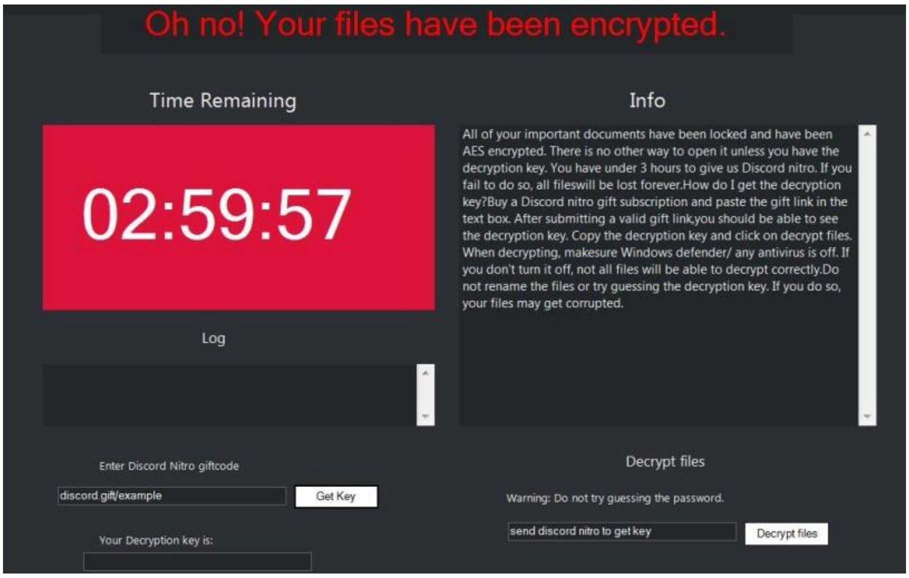


Figure 1: Encryption/Decryption, Source: https://en.wikipedia.org/wiki/Encryption

How does a ransomware note look like after files get encrypted? On the left is an example of it!



Oh no! Your files have been encrypted.

Time Remaining

02:59:57

Info

All of your important documents have been locked and have been AES encrypted. There is no other way to open it unless you have the decryption key. You have under 3 hours to give us Discord nitro. If you fail to do so, all fileswill be lost forever.How do I get the decryption key?Buy a Discord nitro gift subscription and paste the gift link in the text box. After submitting a valid gift link,you should be able to see the decryption key. Copy the decryption key and click on decrypt files. When decrypting, makesure Windows defender/ any antivirus is off. If you don't turn it off, not all files will be able to decrypt correctly.Do not rename the files or try guessing the decryption key. If you do so, your files may get corrupted.

Log

Enter Discord Nitro giftcode

discord.gift/example

Your Decryption key is:

Decrypt files

Warning: Do not try guessing the password.

send discord nitro to get key

Figure 2: Nitro Ransomware note, Source: https://i0.wp.com/howtofix.guide/wp-content/uploads/2021/04/givemenitro-ransom-note.jpg?resize=810%2C560&ssl=1

OTHER MALWARE:

Below is a table of other types of most common dangerous malwares that exists:

Ransomware: Malware designed to block the access to a system (through the encryption of the data) until a certain amount of money is paid. Examples: NotPetya, SamSam, Maze, WannaCry, Locky, GrandCrab, etc.	Trojans: Maliciously designed malware that gets access to a system by appearing as harmless. Fun Fact: The name is derived from the infamous Trojan Horse from Ancient Greece that led to the fall of Troy.
Worms: A standalone malware that replicates itself in order to spread to other computers by using different means. Fun Fact: The first computer worm was devised to be an Anti-Virus software.	Logic Bomb: A malicious piece of code inserted into a software which sets off harmful actions if certain condition are met. Fun Fact: Viruses and Worms may contain Logic Bombs in order to spread unnoticed.
Spyware: Malware designed to gather your personal computer data and forward it to a third-party without consent. Fun Fact: Data compromised include Login Credentials, PINs, Credit Card details, Browsing Habits, etc.	Backdoor: A means to access the computer system or encrypted data that bypasses the security mechanisms. Fun Fact: The infamous SolarWinds attack was assisted by a backdoor installed on the code of the company's software. It remained undetected for a long time.

OBFUSCATION:

Obfuscation is a technique commonly used by hackers in order to create or alter data to make it difficult to read or interpret. This way, they will hide the behaviour patterns of the malware as well as bypass the detection (usually by the AntiVirus).

BASE64:

While there are many obfuscation techniques, you will hand on practice the **base64 encoding**. This simple malware obfuscation technique converts or alters the desired scripts into strings, only using 64 characters. This is where the name is derived as well. The opposite action is called **decoding**.
These characters include: A-Z, a-z, 0-9, +, /, =.
[Full list: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=]

Encoding and encryption, from a broader view, seem to do the same thing. However, there are major differences between the two. These are shown in the table below:

Encryption	**Encoding**
Transforms, or alters data into another format to keep it a secret from others. This secret (encrypted data) can only be reversed or decrypted possessing specific knowledge, such as the key for decryption. Only specific people could perform this. It is used to maintain data confidentiality.	Transforming or altering the data into another format, so it can be transmitted safely, without any danger of being manipulated. It uses a scheme that is publicly available, so decoding the encoded data is easily done. It is used for maintaining data usability.

Did you know:

- The first ever ransomware is called AIDS Trojan or PC Cyborg Trojan created by a biology professor called Joseph Popp.
- Phishing is one of the most common ways for the Ransomware to reach your computer.
- 95% of the Ransomware files are executables suitable to run only on Windows.

INFORMATION FOR THE BLUES:

- You will also be provided a decryptor at your hands.
- Be careful! You should first examine it and eventually perform decoding.
- Will you be able to get your files back?

INFORMATION FOR THE REDS:

- You will still behave like the bad guys and play with a malware script!
- You will be able to edit and customize it as you wish, and test it on your system.
- You will perform encoding to ensure you remain undetectable.

Useful commands and tools for Blues

Cmd – Command line interface for Windows, where you can run multiple commands or else interact with your computer directly using these commands. Refer to the folders inside the episode on how to use and access it.
Notepad++ - Text editor tool to assist you in viewing text files.
DROID – A tool for the filetype identification. Refer to the folders inside the episode on how to use it.

Certutil base64– A cmd command to perform encoding and decoding.
Example of its use: certutil -encode my_data.txt encoded_data.txt
Example explained: certutil (name of the tool initiated) -encode (action to perform) my_data.txt (file where data I want to encode is saved) encoded_data.txt (new file where data inside is encoded)

Base64decode.org – Online tool to assist you with the decoding of the encoded file/text.
Base64ecode.org - Online tool to assist you with the encoding of the decoded file/text.

Aliases, commands and tools for Reds

edit_script = You can freely edit parts of the script that will encrypt the files
run_malware = Will run the malware and then you will see its consequences.
run_decryptor= Will run the decryption script, so you can possibly read your files again.

base64 – A terminal command to perform encoding and decoding.
Example of its use*: base64 simple_text.txt -w 0 > encoded.txt*
Example explained*: base64 (name of command initiated) simple_text.txt (the file I want to encode) -w 0 (this option will save the outputted encoded text into one line only, so wrapping is 0) > (arrow indicating that the output will be saved somewhere with a specific name) encoded.txt (this is the name of the file I chose for the encoded output that will come from the execution of the command)*

Base64decode.org – Online tool to assist you with the decoding of the encoded file/text.
Base64ecode.org - Online tool to assist you with the encoding of the decoded file/text.