Activity 1 - Security History

1. Research and read texts about at least 10 different viruses. Choose one of them and raise intel about it: how much money loss did it cause, if its creator was arrested, and more;

   The virus that I particularly found most interesting was code red, it is stated to be able to run entirely into the machine's memory, leaving no traces of it on the hard disk. Another factor that has caught my attention was its capability of using its infected machines to DDOS attack many different websites, the white house included. If this wasn't already enough, it'd also exhibit "Hacked by Chinese" on its infected pages' bodies. It spread itself into 300 thousand machines within 24 hours, and it is esteemed to have caused a two-billion of dollars worth of loss.

2. Research about Petya and WannaCry ransomware;

   WannaCry was a cryptography ransomware, it'd invade a computer, cryptograph its important files (which made them inaccessible) and ask for a bitcoin price in exchange for the file's access. This ransomware took vantage of a hack called EternalBlue to spread itself. At the beginning of the contamination Microsoft had already released a Windows update to prevent EternalBlue, but due to the users' lack of update checks, many people and organizations were victims of this virus. It is esteemed that the one contained 230 thousand computers and made a four-billion-dollars loss around the world.

   Petya was a block-type ransomware, it worked by cryptographing Windows' master file table, without it, the computer wouldn't be able to find any file or even initialize, which made the entire machine unusable, this situation could only be solved through a bitcoin payment. The virus has affected countries from all over the world but caused some serious damage in Ukraine. Petya took benefit from the same EternalBlue vulnerability that made the WannaCry crisis possible sometime before, and its success only emphasizes that even after the problems its predecessor caused, computer users still hadn't learned about the importance of keeping their operational systems updated, what would've prevented the virus.

3. Research about botnets: the biggest one, its purpose, how much money loss it caused, and more;

   A botnet is a practice when a hacker invades and takes control over several different machines with the main purpose of articulating this infected computer network to apply grand-scale attacks like DDOS or spam. This hacking method makes it harder to find the culprit because every single machine has its IP address, hiding the criminal's presence. The biggest botnet ever recorded was

Storm, which infected around 1.000.000 and 50.000.000 machines, it was utilized for spam, DDOS, e-mail address harvesting, and SMTP retransmissions. Due to its massive size, it was able to leave a whole country without Internet connection and make more calculations per second than some supercomputers at its time (2007).

4. Research about government virus attacks with Stuxnet or other malware that a country's government used to attack another federation;

   Stuxnet is known as the first government-orchestrated cyberattack intended to harm another. The attack, initiated at president Bush's mandate, was intensified by Obama's management and tried to sabotage Iran's uranium enrichment plants. Due to a code failure, the virus escaped Iran's plants and fell into the Internet, to be posteriorly analyzed by security specialists from all around the globe.

   In addition to it, in 2020, companies like Microsoft, Malwarebytes, and even USA's justice department were affected by a hacker attack that took advantage of the network-monitoring software Orion, from the company Solarwinds. It is estimated that this attack was financed by the Russian government.

5. Research about Brazil's most significant data breaches: how much data was compromised, who was responsible for the violation, and more:

   In 2020 last months, a failure at the e-SUS system exposed data from 243 million Brazilians. It is the most significant data breach ever recorded in Brazil. The failure was caused by a login and password insertion at the Brazilian ministry of health website code. The number of compromised registers is bigger than the actual country population (212 million) because information about deceased people was also exposed. Among the leaked information there is CPF, full name, address, and phone number. Such data could come from any Brazilian, alive or dead, that has already been signed up at SUS, or any health insurance.

Sources:

1. Exercise 1;
   1.1. 11 vírus famosos que marcaram a história dos computadores | Avast;
   1.2. Um breve histórico dos vírus de computador e qual será seu futuro.

2. Exercise 2;
   2.1. Ransomware WannaCry: tudo o que você precisa saber;
   2.2. Surto do ransomware Petya em 2017 — Seu guia rápido de segurança | AVG.

3. Exercise 3;
    3.1. O que é botnet? - Definição;
    3.2. Os 12 piores botnets da história - Danysoft.

4. Exercise 4;
    4.1. Governo americano criou o vírus Stuxnet para atacar o Irã | VEJA;
    4.2. DefesaNet - Cyberwar - STUXNET - Obama ordenou os ataques ao Irã;
    4.3. SolarWinds: ataque foi o “maior e mais sofisticado” que o mundo já viu.

5. Exercise 5:
    5.1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal | Tecnologia | G1;
    5.2. Vazamento no e-SUS expõe dados de 243 milhões de pessoas | Minuto da Segurança da Informação.