Group 2 Malicious Software - T97, CC 111
Belisario, Alyxa Janine
Chavez, Czarina Amor
Jalacdon, Sinead Alriz
Paypa, Ivor
Tion, Issyd Kate

I love you virus 2000

There was a time in the early 2000's when people were ignorant and cybersecurity was not strong enough to protect people's technological safety, a malicious software has spread worldwide called the I love you virus. This virus is considered a malicious software that appeared on May 4, 2000, released by two Filipino college students. It quickly spread and was discovered via email, taking advantage of people's curiosity and duping them into opening an attachment included in a message. It spread worldwide. The malware worm lasted a week but brought fear to everyone, including those people who owned big companies. The I Love You virus has been stopped, but it left a scar and a lesson for everyone, until this day.

The I love you virus was made by two college students, mainly, It was Onel De Guzman who made the plan and had his classmate help him in executing the program. It all started when he proposed a thesis regarding a malware that could steal people's passwords in the neighborhood, but then it was rejected, causing him to drop out of college and start the program on his own. Who could've thought that a mere college student can execute such a plan?

After leaving school, de Guzman planned to continue with his goal of using the script he had created to steal internet passwords from the people in his neighborhood. Out of curiosity, he removed the restrictions on spread and location while tinkering with it one night. As a test, he sent it to one person in Singapore he had met in a chat room before heading out with friends. When he returned, international news outlets were discussing a global manhunt for the hacker who had crippled global infrastructure with malware, for which the naïve online world was not yet ready.

The perpetrator was eventually caught when the Philippine National Bureau of Investigation received a tip that the hacker had attached a signature and email to his script, which they eventually tracked back to his family's home. The virus had infected around 45 million Windows computers, and ultimately infected around 10% of the world's internet-connected computers before being mitigated, a process that cost billions of dollars in addition to the repairs and lost productivity. The malware damaged an estimated amount of 15 billion dollars worldwide, causing chaos to the international community.

When the said virus spread, the United States Congress launched investigative hearings after major corporations, as well as government institutions, were crippled: the Pentagon, as well as the British Parliament and MI6, shut down their own email systems out of fear that the hacker was attempting to steal critical information from their servers. Fear of the same occurrence happening again, the Philippines have established a law banning the creation of malware and hacking after the perpetrator had been caught. To prevent it from happening, different kinds of software have been made, such as antivirus, in order to improve social security. With this, it can identify malicious software before entering your device. This is also where social security has become much more powerful than before.

Some local and international crimes that have been happening lately relating to the mentioned malware is the Email Spoofing and Phishing, The virus used email spoofing to trick users into opening a malicious attachment. This technique is commonly used in various forms of phishing attacks to steal personal information or install malware, and because of this, large shows and companies have been hacked and have their private information displayed publicly.

Overall, the ILOVEYOU virus is a stark reminder of the power that malicious code can wield and its potential to wreak havoc. It was one of the first computer viruses to spread rapidly through email attachments, leading to significant financial losses and downtime for businesses worldwide. In our opinion, to prevent such attacks in the future, we should enhance online users' education and awareness regarding some threats in the technology world, as well as enhancing technological defense such as threat detection that can identify unusual patterns in your computer. Also, keep in mind that not all attachments and links provided to your computer and accounts are safe. May this I Love You virus occurrence become a lesson for those who lack security and are easily lured to open such malicious attachments.

References:

https://www.computermuseumofamerica.org/2023/02/07/i-love-you-virus/
https://www.goldskysecurity.com/the-history-and-impact-of-the-iloveyou-virus/
https://www.techtarget.com/searchsecurity/definition/ILOVEYOU-virus