**Malicious Software**

Members:
Abecia, John Paul
Barsana, Justine
Cantiver, Miershan
Familar, Jyms Carl
Palmares, Melvis Alfonse

## ILOVEYOU

The event focused on the ILOVEYOU worm, also known as the Love Bug or Love letter, which was created by Filipino Onel De Guzman, a 24-year-old computer science student at AMA Computer College and resident of Manila, Philippines. De Guzman had just dropped out of college after his professors rejected his undergraduate thesis paper, on the possibility of using malware to steal internet passwords from people in the neighborhoods nearby. He wanted everyone to have internet access, which he believed to be necessary in order to access the sum of humanity's knowledge and improve one's quality of life; he even called it a human right. It was clear that de Guzman had been experimenting with a functional version of such a program for some time. When his professors rejected the thesis for being unethical and likely illegal, de Guzman left, calling the professors close-minded. The ILOVEYOU virus comes in an email with "ILOVEYOU" in the subject line and contains an attachment that, when opened, results in the message being re-sent to everyone in the recipient's Microsoft Outlook address book. Perhaps more seriously, it results in the loss of every JPEG, MP3 and certain other files on all recipients' hard disks. Although commonly referred to as a computer virus, ILOVEYOU is actually a worm. While a virus is malicious code that replicates itself following human intervention, a worm is a type of malware that can replicate itself and spread from system to system without human interaction or intervention. It doesn't even need to attach itself to software. ILOVEYOU works via email, specifically via a malicious email attachment. When the affected user opens the attachment, their action instantly downloads the worm into their system without their knowledge and starts spreading it across the network. The email consisted of the subject line "ILOVEYOU" and a simple message: "kindly check the attached LOVELETTER coming from me." When a recipient opened their email, the virus sent copies of itself to everyone in their address book. On May 5, 2000, the ILOVEYOU worm began to spread, and at the time, Windows platforms, which are the primary computers, were widely affected by the worm as Windows hid the latter file, VBS, a form of interpreted file by default since it is an extension for a file type that Windows recognizes, leading users that are unaware to believe it was a normal text file, which is not.

The ILOVEYOU virus first emerged in the Philippines in May 5, 2000. It quickly spread via email attachments, infecting millions of devices worldwide. It was eventually contained after a few weeks, but the harm had already been done. The virus caused considerable financial losses and downtime for organizations, as well as disruptions to internet services in a number of countries. The ILOVEYOU virus is no longer active. It only lasted for 10 days but was able to have a total of 45+ million users.

The attacker, Onel de Guzman was the only one involved in its creation. 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 answer is yes and no. Yes, the Philippines National Bureau of Investigation appeared at de Guzman's doorstep and were able to put Onel de Guzman to a trial, but there were no laws in the Philippines prohibiting the development of malware at the time, the Philippine Congress passed Republic Act No. 8792, also known as the E-Commerce Law, in July 2000 to discourage future iterations of such activity. However, the Philippines' Constitution prohibits ex post facto laws, so de Guzman could not be prosecuted.

Government institutions like the United States Congress who launched investigative hearings after major corporations as well as other US 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. Then the 45 million users who were infected by its worldwide.

Significant new crimes have emerged since the year 2000, most notably the ILoveYou worm, which damaged major websites and cost over $11 billion. Denial-of-service assaults have also resulted in losses of $1.2 billion. These cases highlight the increasing prevalence of cybercrime, which includes hacking, malware distribution, and electronic theft. The originator of the ILoveYou worm was not found guilty, a sign of the legal systems' inability to keep up. Academics argue over whether the current legal frameworks are adequate or whether traditional laws should be rethought for the digital age.

The United States Congress launched investigative hearings. 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. Soon, the Philippines National Bureau of Investigation appeared at de Guzman's doorstep. They had 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. De Guzman's mother, fearing prison time for her son, hid his computer, but the police found floppy disks Guzman had hidden in his room which contained copies of the worm, confirming that it was his creation. De Guzman later confirmed that he had written the script in court. However, the police needed to prove that de Guzman had intended to cause the mayhem and destruction that had resulted from his test, and all they were able to get out of him was that "it was possible" that he had released the virus accidentally. The ensuing trial found that he had broken no law, as he did not steal physical property nor did he violate the only computer-related crime on the books, which was credit card fraud. The Philippines, like much of the developing world, had barely considered the possibility of a person committing crimes using nothing but a computer and an internet connection. Soon after, the Philippines passed a law banning creation of malware and hacking, but it was too late to try de Guzman. De Guzman's worm, barely more than an experiment that rapidly spiraled out of control, shocked global leaders and tech companies into doing something about cybersecurity, a task that was often seen as a waste of time and money. The United States Senate hearing on the Love Bug described it as "the equivalent of a nuclear bomb going off in cyberspace" and they repeated what the financial services industry had told them: if the bug had written over spreadsheets instead of just text and images, the financial services industry would have essentially collapsed overnight. They also discussed newer worms that used exploits in different email systems that automatically opened links embedded in emails, which meant that even without the user clicking on an attachment the worm could overtake their computer immediately after the email was received. They discussed how the

Department of Defense had been completely unprepared for the worm, and that hundreds of employees opened the attachment. In general, they found that even the United States wasn't ready for a new age of malware and hacking, and that the developing world was entirely unprotected. It filled the world with such a fear of the potential that hacking could have in the future that corporations, nations, and users around the globe began learning ways to protect themselves from hacking attempts. It was made clear that just because this time it was a student in the Philippines testing his code, next time it could be something far more malicious.

More than two decades ago, computer users were terrified that a destructive and undetected virus called CIH might be present in the memory of their computers and become active on April 26 and delete programs in hard drives, flash the BIOS, and brick the motherboard. The date was chosen as it is the anniversary of the Chernobyl nuclear meltdown. Back then, IT support staff informed users not to open their PCs on that date so that it would not be activated. All the leading antivirus companies at the time developed fixes for that virus, and it was estimated that the virus caused damage equivalent to $250 million to $1 billion. Not long after that, an email arrived at users' mailboxes with the subject "ILOVEYOU" and containing a Visual Basic Script attachment. This email used social engineering to trick users into opening the attachment. When opened, it exploited a Microsoft Outlook vulnerability, changed the file name extensions, and spread via email using the infected computer contacts. The ILOVEYOU worm infected 50 million computing systems with some impact on many government bodies, intelligence agencies, and military institutions.

The other local or international crimes related to the crime discussed were other forms of Ransomware, worms, and viruses. All of which are examples of malware that is intended to cause harm to people. Malware variations numbering in the millions, with billions of dollars in harm have been found. The Morris worm, the ILOVEYOU virus, and the WannaCry ransomware are a few notable instances. The Sasser and Netsky worms have caused losses of approximately $31 billion, making them extremely harmful. Malware has also been employed by governments for political espionage. Security software and an awareness of harmful online conduct are necessary for effective prevention. To battle malware that is getting more and more complex, ongoing innovation is needed.

In our opinion, from the information that have gathered, we had learned that this attack was only made possible because no-one was aware that they could do it. Other factors include the Complacency of Cybersecurity of the time which was largely ignored and not funded. Onel de Gozman first presented the idea of his creation at his college and his college rejected it for distaste of its purpose. With his thesis paper not accepted, Onel de Gozman dropped out of college. This was a mistake since we might have learned it in full detail and might be able to create the necessary countermeasures and in the real time events, the ILOLVEYOU virus and worm changed Cybersecurity forever since it was easily able to spread itself into different Government intelligence agencies worldwide and caused much panic in people, organizations and governments. It finally convinced the funding of Cybersecurity so that incidents like this won't easily occur in the future. So instead of rejecting those people, we should embrace them, hire them and work together with them so that we may together forge a path forward on a much safer internet Environment in the future.

**References**


Awati, R. (n.d.). ILOVEYOU virus. TechTarget. https://www.techtarget.com/searchsecurity/definition/ILOVEYOU-virus#:~:text=In%20fact%2C%20this%20is%20exactly,about%20%2410%20billion%20in%20damages.

Awati, R. (n.d.). The history and impact of the ILOVEYOU virus. Gold Sky Security. https://www.goldskysecurity.com/the-history-and-impact-of-the-iloveyou-virus/#:~:text=Although%20the%20ILOVEYOU%20virus%20is,to%20protect%20yourself%20from%20them.

ILOVEYOU virus. (2024, August 22). In *Wikipedia, The Free Encyclopedia*. https://en.m.wikipedia.org/wiki/ILOVEYOU

Kumar, K. N. (2001). Cybercrime and the law. *University of Pennsylvania Law Review, 149*(4), 1003-1114.

MacDonald, C., Agarwal, A., Ngo, F. T., & Govindu, R. (2020). Dangers associated with malicious software. In *International cybercrime and cyberdeviance: A Palgrave handbook* (pp. 793-813). Palgrave Macmillan.

Schmidt, B. (2023, February 7). I Love You virus. Computer Museum of America. https://www.computermuseumofamerica.org/2023/02/07/i-love-you-virus/#:~:text=In%20May%20of%202000%2C%20a,the%20world%20thought%20about%20cybersecurity.

The history and impact of the ILOVEYOU virus. (n.d.). Gold Sky Security. https://www.goldskysecurity.com/the-history-and-impact-of-the-iloveyou-virus/#:~:text=Although%20the%20ILOVEYOU%20virus%20is,to%20protect%20yourself%20from%20them.

Viegas, V., & Kuyucu, O. (2022). The cybersecurity challenge. In *IT security controls: A guide to corporate standards and frameworks* (pp. 1-16).