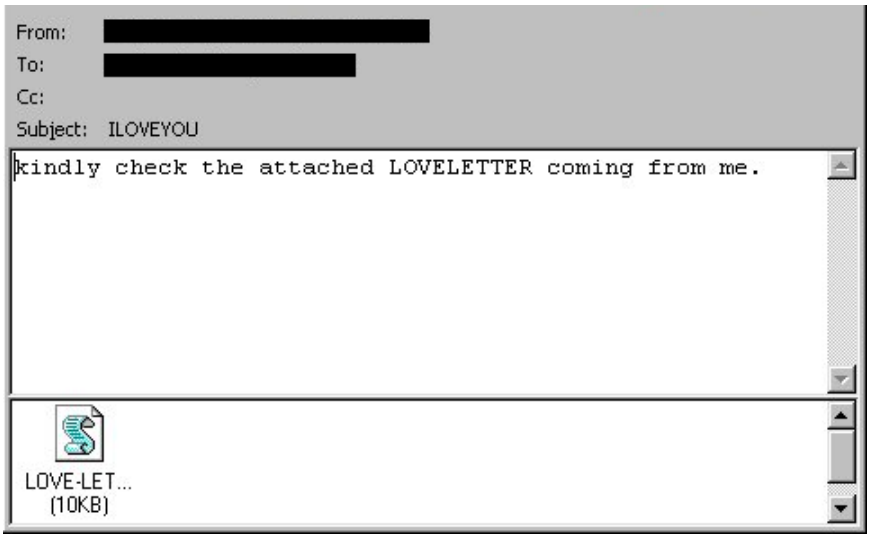
Helana Solomon
CS338
Computer Security Project
09/12/25

Is This a Worm or a Love Confession Disguised as a Worm?

Investigating the ILOVEYOU worm

Introduction ♥

Imagine waking up one morning and checking your email to see you received a message from your friend saying 'ILOVEYOU.' You look at the email confused because you recognize the email address, a close friend of yours who you are often in contact with, but you rarely send emails to each other. You open the email to see the message "kindly check the attached LOVELETTER coming from me." You're a little confused but also curious to why your friend sent you this message so you click on the file, nothing really happens. You're a little bit confused… but end up moving the email in the trash and soon forget about it. But little did you know clicking on that file led to a reaction that not only affected your computer but others you've emailed before.

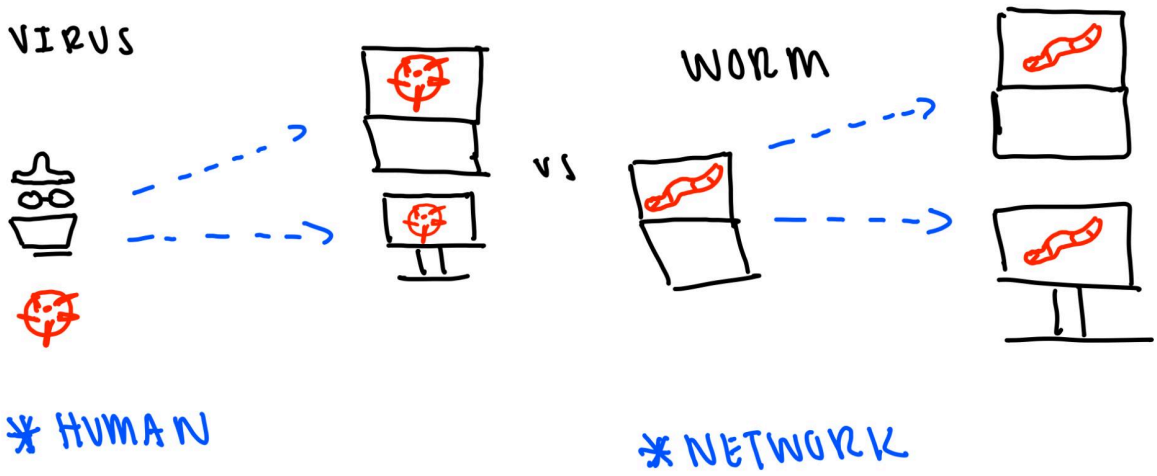


This image is from wikipedia and shows what the content of an email with the ILOVEYOU virus looks like.

What is the ILOVEYOU worm? ♥

ILOVEYOU is a computer worm, also known as the lovebug, that affected 45 million computers worldwide in 24 hours. Within this timespan, 10 percent of computers connected to the internet were affecting thousands of companies worldwide. The ILOVEYOU worm is mainly referred to as a worm but also contains components of a virus. A computer virus is a type of malware that is designed to attach itself to a legitimate file or program so it can spread from one system to another. A virus cannot spread itself and needs the user to run the infected file. The ILOVEYOU worm needs someone to run a file to actually execute the malicious attack. A

computer worm is similar but different. It is a type of malware that spreads across computers and networks without needing a host file or user interaction; It replicates itself. The ILOVEYOU worm replicates itself once the user runs the file. The commands executed in the file execute the main malicious attack that occured: sending emails to everyone in the victim's contact list.



Visualization of the difference between a virus and worm. This image was drawn by me but I used an image from Avast that also has the same features as reference.

This worm was created on May 4th 2000 by Onel de Guzman, a 24 year old student at AMA Computer College. Guzman lived in the Philippines where the internet usage was not free. Guzman specifically developed this worm so he could access the internet for free by stealing passwords. In the Philippines, they used dial-up internet which consists of connecting to the internet using a telephone line. Guzman did not have the money to pay for this service, so he wanted to develop a way to steal other people's passwords for their accounts so he could use their accounts to access the internet. He believed there would be no harm done for those who have their passwords stolen, and he would benefit from it because it allowed him to use the internet for free. He never anticipated that the worm he created would cause worldwide damage.

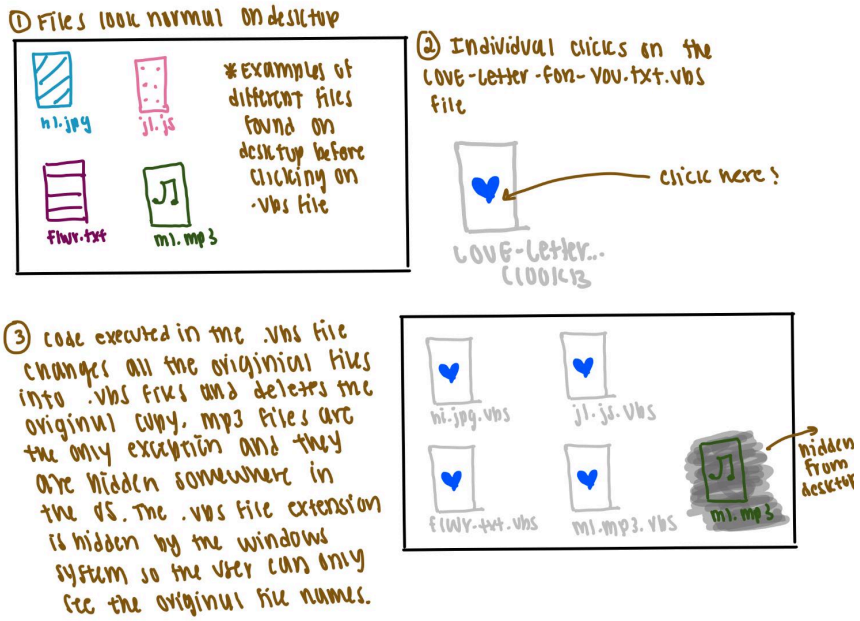
Guzman actually never received a sentence for the damage he caused. During this time, in the early 2000s, the Philippines did not have any laws that addressed how hackers should be charged for their offenses. The ILOVEYOU worm was the attack that brought this to the attention of the Philippines government so that future cases could be successfully brought to trial. The government worked towards creating a law and eventually in 2012 passed the Cybercrime prevention act of 2012 which helps address the legal issues that concern cyber crimes in the Philippines.

How Does the ILOVEYOU worm work? ♥

The way this virus works is fascinating! Individuals receive an email in their inbox from someone in their contacts: could be a friend, co-worker, or someone you often receive emails

from. The subject of the email states “ILOVEYOU,” with a message that says “kindly check the attached love letter coming from me” with an attached file named “LOVE-LETTER-FOR-YOU.TXT”. Unfortunately, many people, out of their own curiosity, clicked on this txt file without knowing it was not a txt file, it was actually a .vbs file with malicious intent inside. It was an intentional misdirect that wouldn’t have been caught unless you looked at the file extension, which the typical individual would not have known that this file type was incorrect or even recognized it. Windows hides file extensions so the victim should have checked the extension before opening the file. Because the act of sending and receiving emails wasn’t new, many people trusted the messages they sent and received. This attack specifically targeted that trust in ways that led to irreversible damage. Unless the individual has experience with phishing emails, then they could have avoided spreading the worm, but the majority of the population (at that time) did not.

Once the first person who received the email from Guzman opened it, the ILOVEYOU worm spread like wildfire. The issue with the ILOVEYOU worm began when one person ran (opened/executed the attached file). If anyone who received the email did not run the attached file, instead, they deleted the email, then their system was never affected. But, when the file is executed it attempts to do five main tasks: generate copies of itself within the computer system, send copies of itself (the email) by taking all the people in the affected user’s address book. Then it attempts to send the same email to the current users’ contact list. Furthermore, it attempts to infect the internet relay chat program so that the next time a user starts chatting on the internet, the worm can spread to everyone who connects to the chat server. Finally, it also searches for pictures , videos, and music files (jpg, png, mp3 etc..) and overwrites them to a .vbs file but keeps the name and extension file to disguise the change. This is so that it can be executed in different contexts. Most of the old files were permanently deleted and could never be recovered. Only mp3 files were hidden and could be found only if you were able to figure out their location.

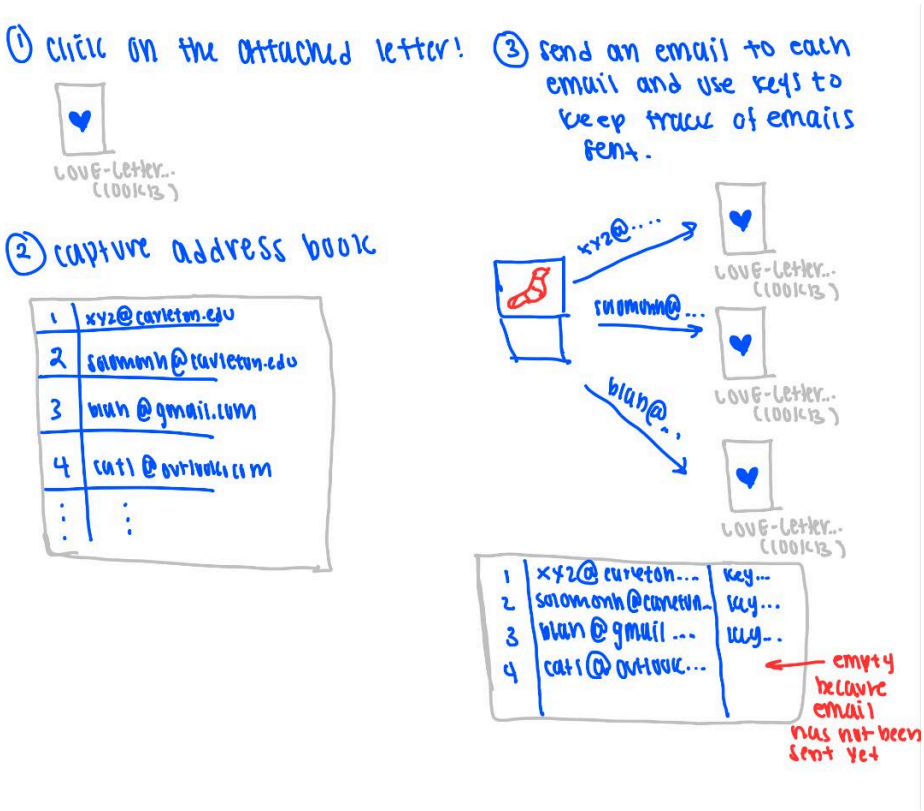


Visualization of how the worm replicates itself into existing files and then deletes old files.

Visual Basic Script and Emails

To provide some context, a .vbs file, also known as a Visual Basic Script file, a deprecated script as of October 2023, is a programming language for scripting on Microsoft Windows using Component Object Model. It was popular with system administrators and used for managing computers and automating many aspects of computer environments (Wikimedia, ILOVEYOU). The only computers that were affected by this attack were Windows users because Visual Basic Script only runs on Windows. Before its deprecation, visual basic script was installed by default in Windows. Linux and Mac systems were not affected by VBScript because it relies on a windows based interpreter to run the file. So during this attack, if a Linux or Mac user opened the file, it would not execute properly.

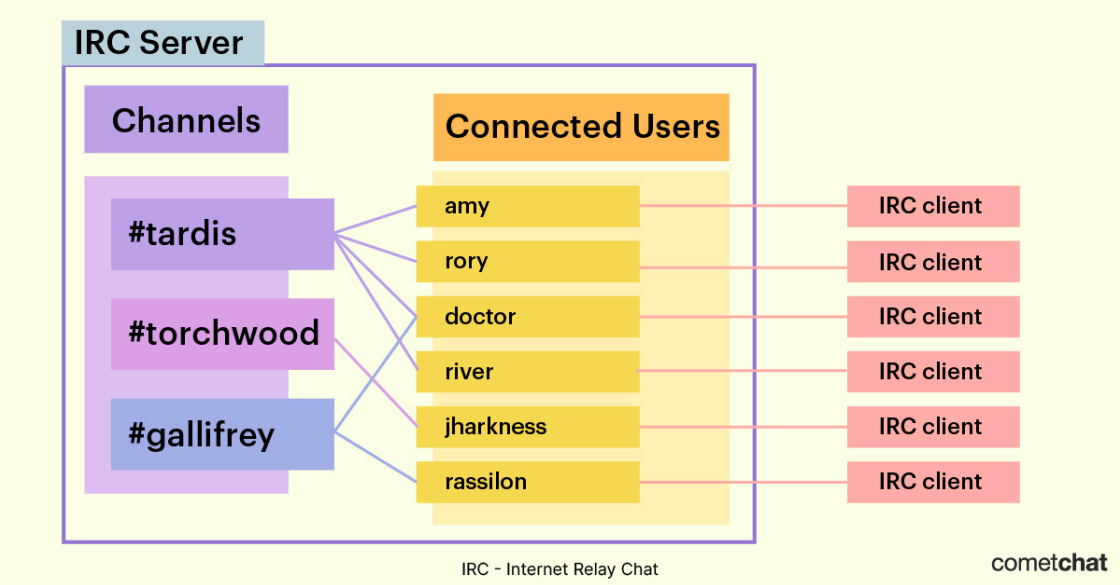
Unfortunately, Microsoft Outlook heavily relied on VisualBasicScript due to its easy use and the overall functionality of Outlook. Because of this, once the .vbs file was run, the user's address book was directly accessed and emails were sent. The address book is a list of email addresses. To make sure the worm was not sent multiple times to one person, the worm sets up a register key for each email in the address book and will update the key once an email has been sent to the individual.



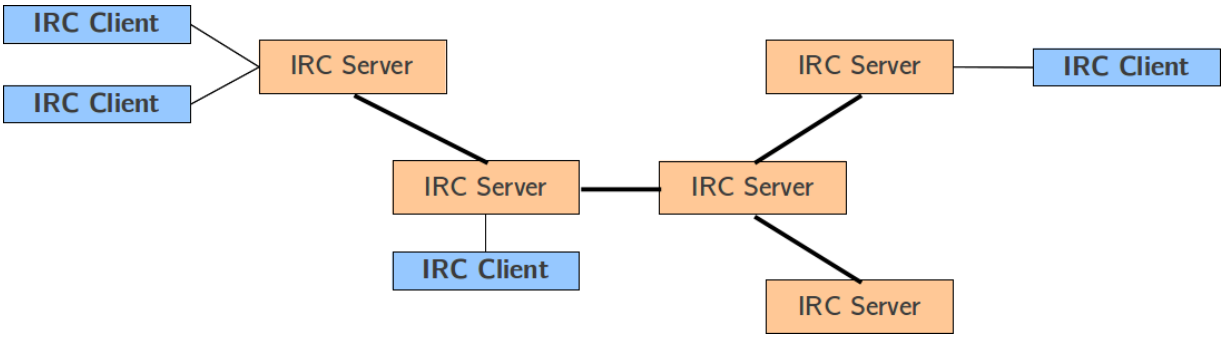
Visualization of the process of how the worm sends emails.

Internet Relay Chat

The worm's functionality was not limited to sending love messages to all recipients. In addition, it was also capable of spreading via an IRC messenger. An IRC messenger is an internet relay chat, a text based chat system for instant messaging. It was designed for group communication in discussion forms called channels. But, you could send messages one-on-one via private messages (Wikimedia, IRC). The internet relay chat is implemented as an application layer protocol to facilitate the communication. With IRC, users connect with the client program (which can be a web application, desktop program, or some larger program) to an IRC server which is usually part of a larger network that allows users to communicate with each other.



This is an example of IRC made by U-ChicagoXProjects but replicated by cometchat.



This from U-ChicagoXProjects and also shows at a larger scale a multi-server IRC architecture.

Permanent Exposure

Finally, once a user opens the file, the worm actually copies itself into the relevant directories associated with the rebooting of the computer. The worm makes 3 copies of itself on the host machine and 2 of the 3 act as legitimate Windows library files MSKernel32.vbs and Win32Dll.vbs. The third copy stays in the original form of LOVE-LETTER-FOR-YOU.txt.vbs. The MSKernel32 file is a dynamic link library which is found in the windows kernel module. It mainly handles memory management, information and configuration, input/output operations, thread synchronization and other tasks. It can be found in the root folder (Bishop, M). When this file is missing or corrupted, you may have issues with accessing your system data. The Win32Dll.vbs file can be found in the systemfolder. The worm made sure to make these copies so that it would make sure that the worm restarts every time the machine was restarted or reset.

Password Stealing

One of the main original purposes and functionalities of the ILOVEYOU virus was stealing passwords. To do this, the worm sets up a tempfolder with a win-bugsfix.exe file inside. Then, they attempt to set the Internet home page for Internet Explorer to download the trojan horse win-bugsfix.exe upon opening the browser. If it downloads successfully, then once the computer is rebooted the trojan is set up successfully. The trojan horse used by the worm was written by Guzman which emailed cached dial-up passwords so he could use them to access the internet.

How did this impact Society? ♥

Originally starting in Manila, Philippines, the worm spread across multiple countries. First, moving to Hong Kong, then to Europe and then finally to the United States. The estimated cost was about $5.5-8.7 billion in worldwide damages and it was estimated to cost the use 10-15 billion to remove. Within ten days of the attack, over fifty million people reported to be affected by the attack. In the United States, the worm affected most of the federal government agencies. Unfortunately, the Veterans Health Administration received 7,000,000 ILOVEYOU emails during the outbreak. In the UK, the British parliament, Belgium's banking system and many companies in European countries like Denmark, Italy, Germany (and more) were all affected.

The ILOVEWORM worm caused significant damage to society. This was the first worm to ever reach widespread media coverage and it was the most expensive because of the worldwide impact. Most of the damage was estimated for the lab was for the labor cost of the removal of the virus. It took multiple days for infected companies and organizations to recover from the virus; Even then, some of the damaged and overwritten files were recovered but many were lost.

The ability of the worm to get access to the address book and send emails to everyone is the critical piece of this attack. Because individuals can send each other emails across personal emails and professional emails. Doing so, establishes a connection between personal and work emails. So, once a personal email is infected by this worm, it can send an email to a business email which causes the chain reaction of sending emails to people within the company and other organizations as well. Because of this, many organizations were affected. Only a few people from each organization had to access the attached file to generate millions of more messages that overwrite millions of files on thousands of computers.

The Bigger Picture + Lessons Learned ♥

In today's age, the ILOVEYOU worm is considered a social engineering attack, specifically a phishing attack. Guzman found a way to trick people into questioning why they were receiving an email from someone they knew, specifically, why were they confessing their love to them. This human nature (our curiosity), was manipulated to persuade individuals to quickly open the attached file in the email without a second thought. The lack of critical thinking came from two components - because of our curiosity and because this email was sent from a

trust sender. But, the person who received the email was not at fault, it is difficult not to say that people in the early 2000s were a bit naive but this was the time when these types of worms and viruses began to rise. But even today, many people still fall victim to phishing emails. While some are more obvious attacks, others can be disguised in ways that are specific to the individual and their interest, where they may be completely out of sight and don't ever figure out that it is a malicious attack.

It is extremely important to always stay cautious when responding to emails. Phishing is still very prevalent in society today, especially at school. It is very important to keep a critical eye on anything that is very important to you. The ILOVEYOU worm was just one eye-opening attack, but even at Carleton College there have been many simulations of attacks and potential effects that it is hard to control and predict the damage some could cause. But, practicing the open mindset and continuously staying aware when reading through emails can significantly reduce the chance of being attacked!

My Thoughts and Overall Reflection ♥

I enjoyed researching this topic. Although it was very difficult to find more technical details about the different components of this worm, it was fun to learn about the worm and the lasting effects. It would have been if I could have implemented a visual/interactive representation of the project which I think I may do in my free time, but it may be somewhat difficult to actually replicate this worm in a safe (virtual) environment.

Through this research, I discovered Professor Matt Bishop, who wrote a paper on the analysis of the ILOVEYOU worm. As I was looking for it, I found his presentation which included a lot of the technical background behind the worm. I couldn't ever get access to his actual article but his slides presentation was really informative but also included a lot of technical jargon. But one quote that stood out to me was "the ILOVEYU worm can do only what you can. You could, by hand, do everything the worm does. So, how can security mechanisms determine that you're not doing it? That the worm is doing these things without your knowledge and permission? The inability to answer this question clearly, simply, and correctly every time is a reason the Trojan horse problem is a major computer security problem." This stood out to me the most because I didn't even think about what the worm could really do that a human could do. It makes sense because the functionality exists so humans can change file extensions, get the address book associated with your email address, etc.. but the fact that it can be so easily replicated with no system that regulates some software file before actually executing the file is very interesting. At the very least, the outlook application should have a system in place to verify you want to send an email, or get access to all the emails before doing it.

References:

1 mesleki ingilizce - technical English II prof. dr. Nizamettin Aydin. (n.d.-a). https://www3.yildiz.edu.tr/~naydin/MI2/lectures/PDF/MI2_02.pdf

A&E Television Networks. (2025, May 27). *"iloveyou": How the infamous Computer Worm wreaked havoc*. History.com. https://www.history.com/articles/i-love-you-computer-worm

Bishop, M. (n.d.). The iloveyou worm - nob.cs.ucdavis.edu! https://nob.cs.ucdavis.edu/classes/ecs153-2011-02/handouts/iloveyou-s.pdf

For release on delivery expected at 10 a.m. Thursday, May 18, 2000. (n.d.-b). https://www.gao.gov/assets/t-aimd-00-181.pdf

GeeksforGeeks. (2025, July 15). *Difference between worms and virus*. https://www.geeksforgeeks.org/computer-networks/difference-between-worms-and-virus/

Iloveyou virus attacks computers: Research starters: EBSCO research. EBSCO. (n.d.). https://www.ebsco.com/research-starters/computer-science/iloveyou-virus-attacks-computers

Internet relay chat¶. Internet Relay Chat - The UChicago χ-Projects. (n.d.). http://chi.cs.uchicago.edu/chirc/irc.html

IRC VS XMPP: Comparing instant messaging protocol. CometChat. (n.d.). https://www.cometchat.com/blog/irc-vs-xmpp-instant-messaging-protocol-comparison

Latto, N. (2025, September 16). Worm vs. virus: What's the difference and does it matter? https://www.avast.com/c-worm-vs-virus

Root, E., Buxton, D., Kaminsky, S., Lazaricheva, A., & Team, K. (n.d.). *Iloveyou: The virus that loved everyone*. Daily English Global blogkasperskycom. https://www.kaspersky.com/blog/cybersecurity-history-iloveyou/45001/

Wikimedia Foundation. (2025a, November 8). *IRC*. Wikipedia. https://en.wikipedia.org/wiki/IRC

Wikimedia Foundation. (2025b, November 9). *Iloveyou*. Wikipedia. https://en.wikipedia.org/wiki/ILOVEYOU

https://www.youtube.com/watch?v=ZqkFfF5kAvw