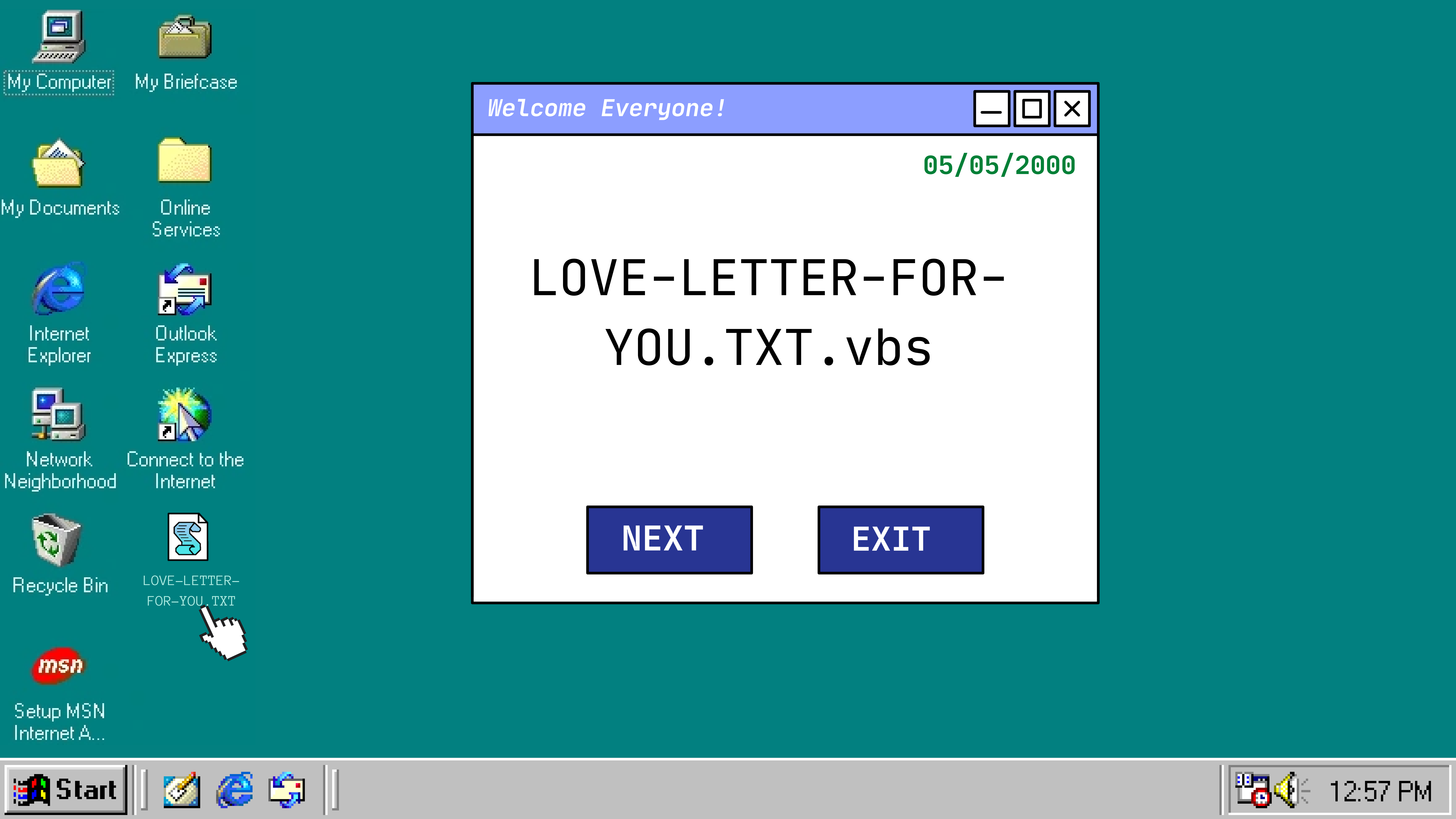
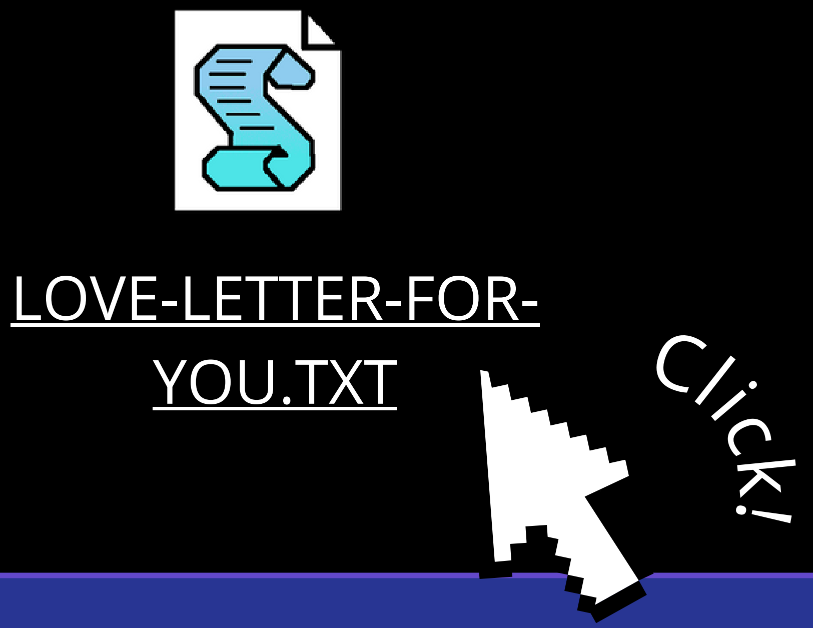


Welcome Everyone!

05/05/2000

LOVE-LETTER-FOR-YOU.TXT.vbs



What Will Happen Next?

Let's See-->

Here's what will happen to your system

After you click on the .vbs file obviously

Internal Working--^

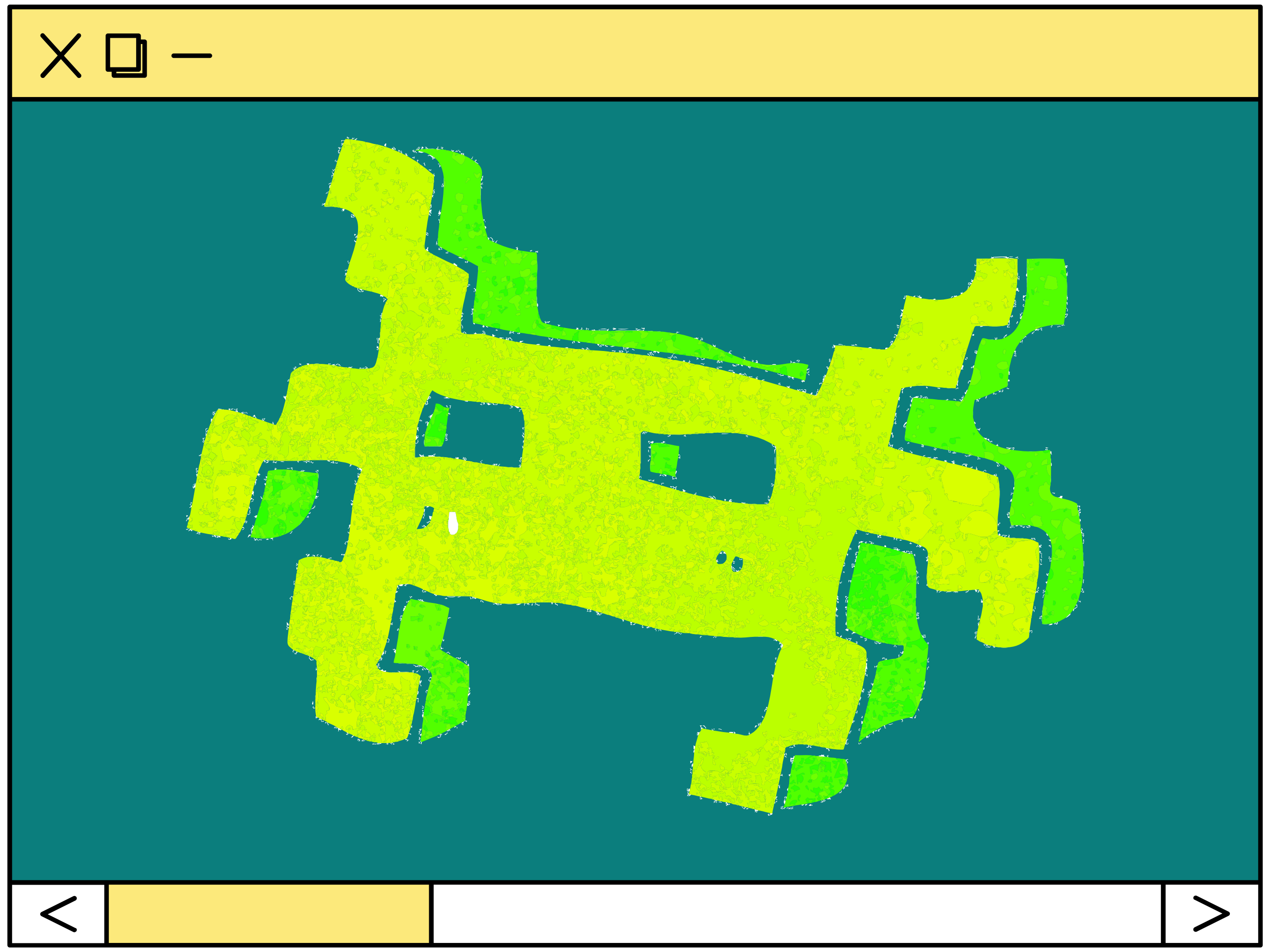
Opening the assumed txt file (attachment) activates the worm

The worm inflicts damage on the local machine, overwriting random types of files (including Office files, image files, and audio files; however after overwriting MP3 files the virus hides the file)

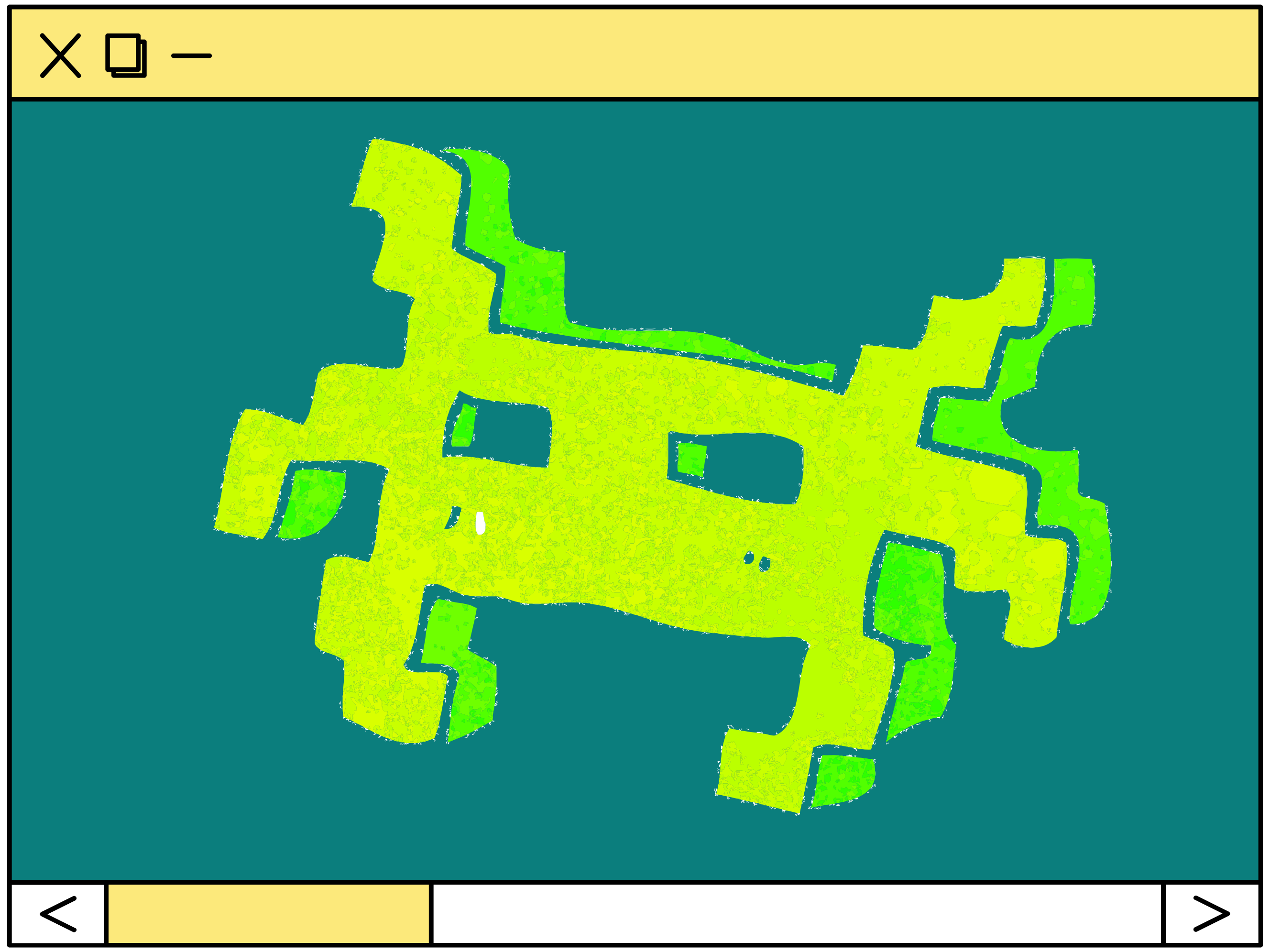
It sends a copy of itself to all email addresses in the Windows Address Book used by Microsoft Outlook for its replication and spread on other machines.

SO HOW ITS WORKING?

ILOVEYOU relied on the scripting engine system setting (which runs scripting language files such as .vbs files) being enabled, and took advantage of a feature in Windows that hid file extensions by default (New feature being added since Windows 2000), which malware authors would use as an exploit. Windows would parse file names from right to left, stopping at the first period character, showing only those elements to the left of this. The attachment, which had two periods, could thus display the inner fake "TXT" file extension.



SO HOW ITS WORKING? CONTD..



True text files are considered to be innocuous as they are incapable of running executable code. The worm used social engineering to entice users to open the attachment (out of actual desire to connect or simple curiosity) to ensure continued propagation. Systemic weaknesses in the design of Microsoft Outlook and Microsoft Windows were exploited to allow malicious code capable of gaining complete access to the operating system, secondary storage, and system and user data in, simply through unwitting users clicking on an icon.

IMPACT

The worm originated in the Pandacan neighborhood of Manila in the Philippines on May 4, 2000, moving first to Hong Kong, then to Europe, and finally the United States. The outbreak was later estimated to have caused US$5.5–8.7 billion in damages worldwide, and estimated to cost US$10–15 billion to remove the worm.

Within ten days, over fifty million infections had been reported, and it is estimated that 10% of Internet-connected computers in the world had been affected.

Damage cited was mostly the time and effort spent getting rid of the infection and recovering files from backups.
To protect themselves, most large corporations decided to completely shut down their mail systems.

At that time, it was one of the world's most destructive computer related disasters ever happened. This incident not only destroyed the data but also the mental health of many people.

WHO DID ALL THESE?

ONEL DE GUZMAN

Just Like us college fellows, A guy whose name was Onel De Guzman, a college student in Manila, Philippines, who was 24 years old at the time did all this just out of curiosity. De Guzman, who was poor and struggling to pay for Internet access at that time, created the computer worm intending to steal other users' passwords, which he could use to log in to their Internet accounts without needing to pay for the service. He justified his actions on his belief that Internet access is a human right, and that he was not actually stealing.

LIVE DEMONSTRATION TIME!