“ILOVEYOU” WORM OVERVIEW

A brief overview of the ILOVEYOU Worm

Jordan Patterson

2024

ILOVEYOU Worm Overview

Jordan Patterson 2024

Date introduced: May 4, 2000

Characteristics: The ILOVEYOU Worm was a Visual Basic script. The Script was named with a double file extension to trick users into believing it was harmless, for example, the name could be ILOVEYOU.txt.vbs. Since most people leave their computers default settings intact, which is to hide file extensions, the script would often be perceived as a text file at first glance, since the .vbs files extension would be hidden. Once the script was executed, it had the ability to overwrite or delete important system files and personal documents. It could also attempt to download other malicious files from the internet.

Propagation: The ILOVEYOU Worms main method of transmission was via email. The recipient would receive an email with the subject “ILOVEYOU” and a message promising love and companionship if they opened the attached file. The recipient was social engineered into wanting to open the file. The Worm would then send copies of itself to all contacts in the victims Microsoft Outlook address book. It did this by using its own SMTP engine, allowing it to send emails without the need for a mail client.

Impact: Millions of users were infected with this worm, resulting in major disruptions to email systems and financial losses for businesses.

Remediation The worm was cleaned up by antivirus companies who quickly updated their software to be able to detect and remove the worm.

Dependencies:

Email Systems: The ILOVEYOU Worm depends on emails systems to propagate.

Social Engineering: The Worm uses social engineering tactics to convince people to execute the file.

Microsoft Windows OS and Outlook: The Worm exploits vulnerabilities in Windows and Outlook

File execution and scripting: The Worm relies on windows ability to execute .vbs scripts.

Double file extension: The worm depends on the user not noticing its true file extension.

Adress book access: The Worm relies on the contacts of the users address book to propagate itself further.

Lack of Users Awareness: In the year 2000, home computing was still being widely adopted and concepts like phishing scams, social engineering, and cybersecurity awareness were not widely known.