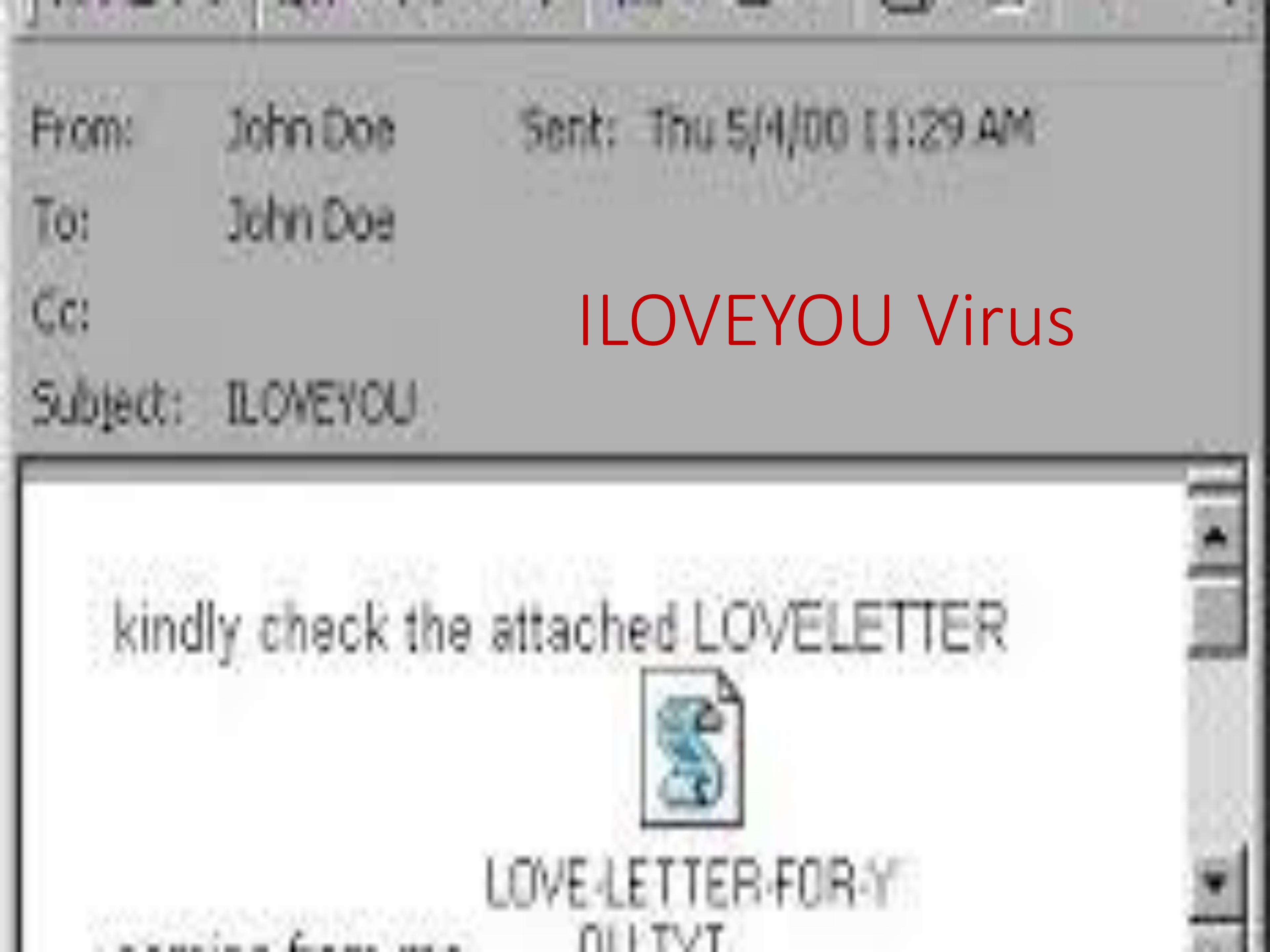
ILOVEYOU Virus



From: John Doe Sent: Thu 5/4/00 11:29 AM

To: John Doe

Cc:

Subject: ILOVEYOU

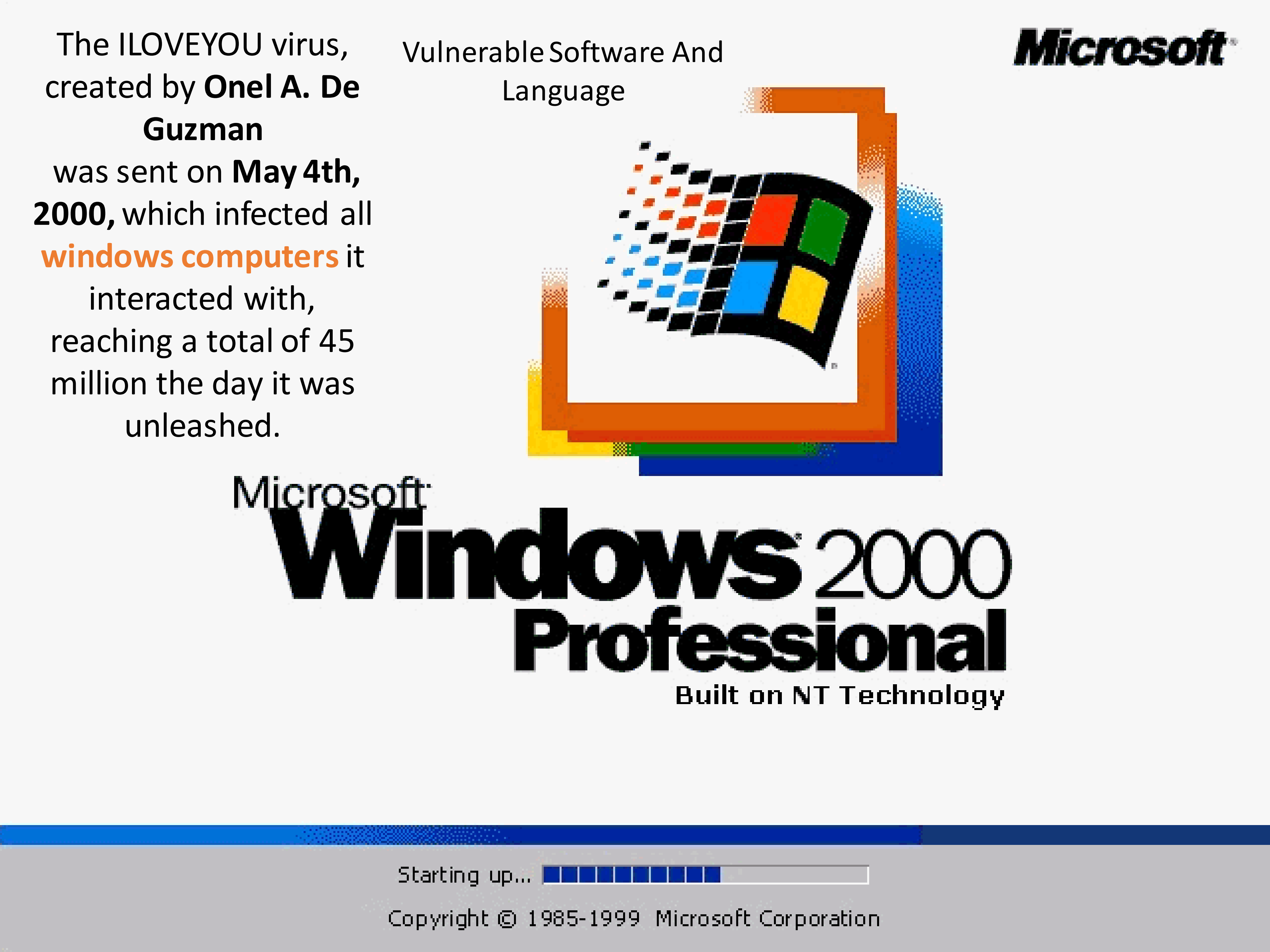
kindly check the attached LOVELETTER

LOVE-LETTER-FOR-YOU.TXT

coming from me

Vulnerable Software And Language

The ILOVEYOU virus, created by **Onel A. De Guzman** was sent on **May 4th, 2000,** which infected all **windows computers** it interacted with, reaching a total of 45 million the day it was unleashed.



Microsoft

Microsoft Windows 2000 Professional

Built on NT Technology

Starting up...

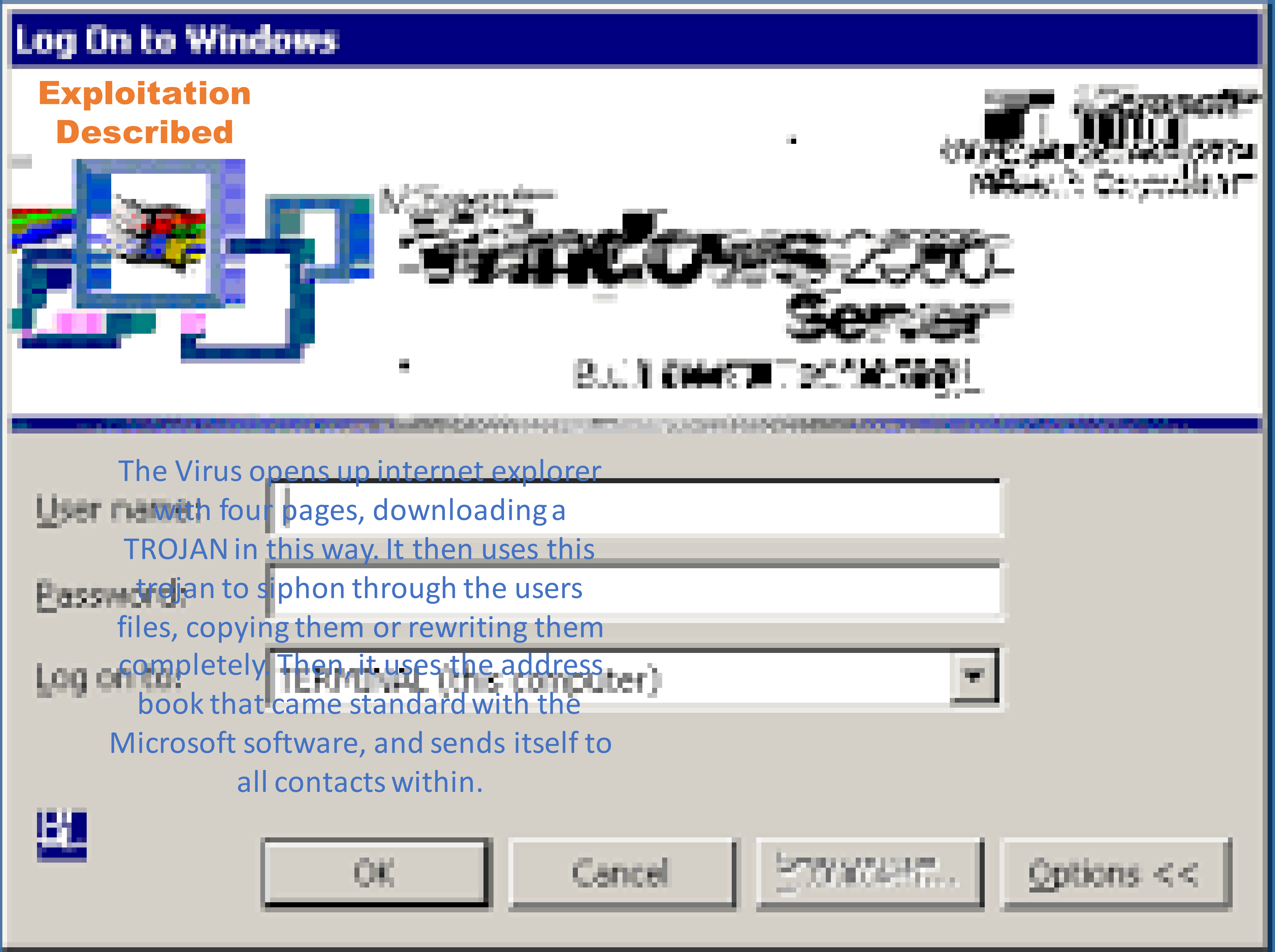
Copyright © 1985-1999 Microsoft Corporation

The mailing system within Microsoft 2000 was what allowed the virus to spread so quickly, as it appeared to be "safe", since the message was coming from a known acquaintance or family member, when in actuality, they simply just allowed the ILOVEYOU virus to come in and wipe away their files. This system allowed for millions of messages to be generated and sent by only a few unknowing users.

This was how the virus affected over 40 million on its first day of infecting, and with how one click on opening the file spread the virus into the computer entirely, using HTML mainly to infect the computer it was currently on. It's easy to see how it was so capable of entering these computers through the use of the program.

Vulnerability Described

Exploitation Described



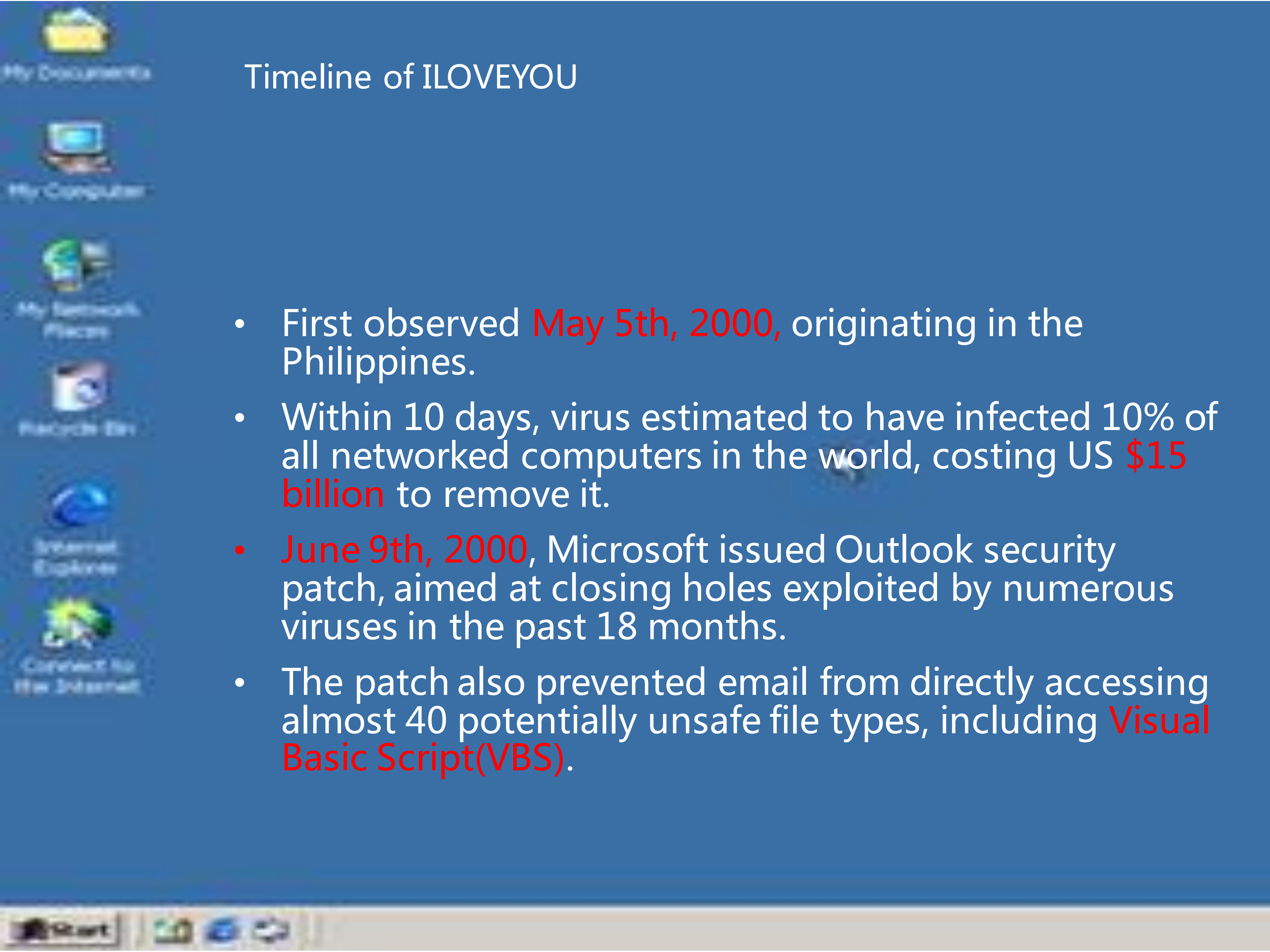
Log On to Windows

User name:

Password:

Log on to: TERMINAL (this computer)

The Virus opens up internet explorer with four pages, downloading a TROJAN in this way. It then uses this trojan to siphon through the users files, copying them or rewriting them completely. Then, it uses the address book that came standard with the Microsoft software, and sends itself to all contacts within.

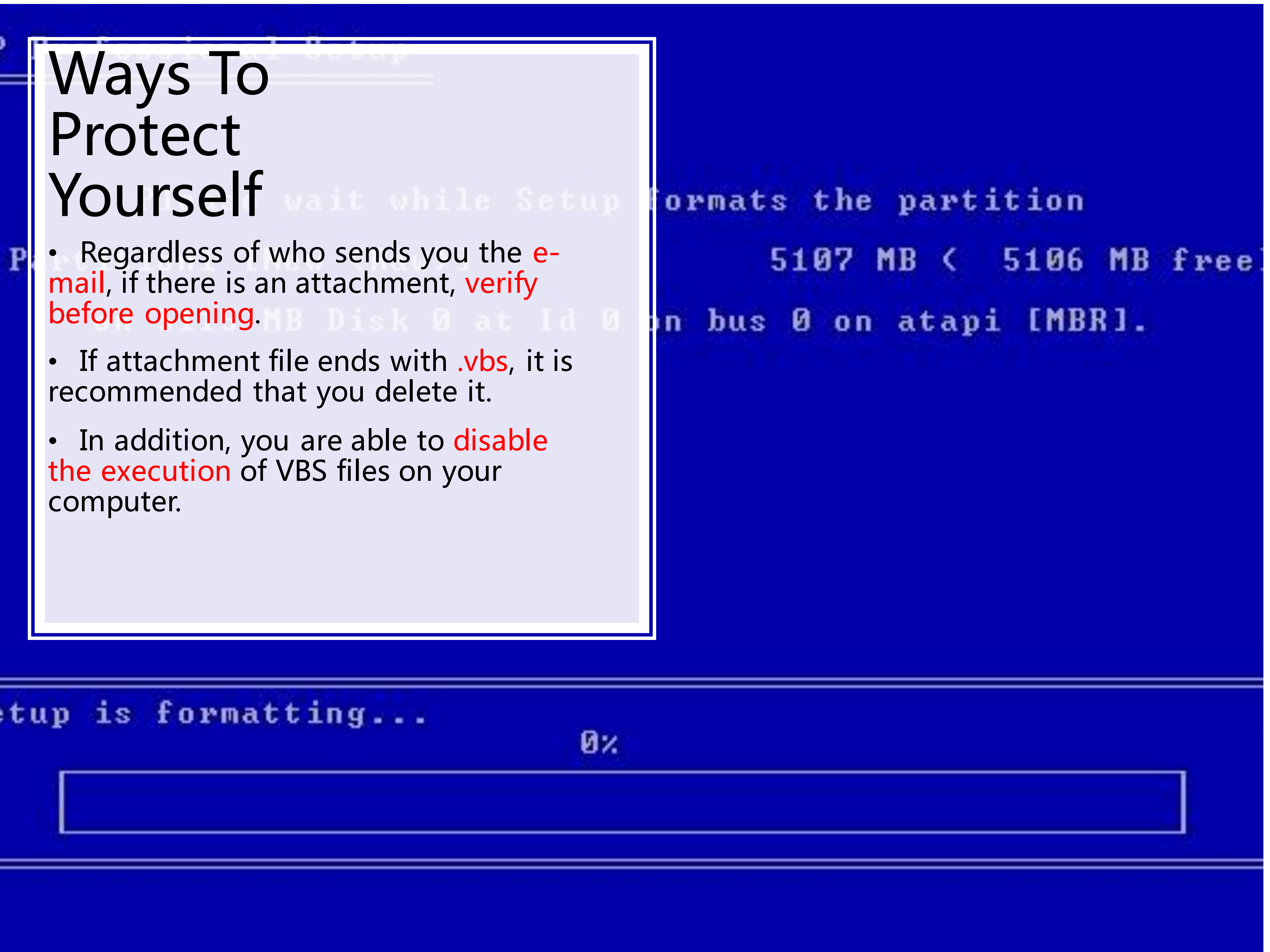


Timeline of ILOVEYOU

- First observed May 5th, 2000, originating in the Philippines.
- Within 10 days, virus estimated to have infected 10% of all networked computers in the world, costing US $15 billion to remove it.
- June 9th, 2000, Microsoft issued Outlook security patch, aimed at closing holes exploited by numerous viruses in the past 18 months.
- The patch also prevented email from directly accessing almost 40 potentially unsafe file types, including Visual Basic Script(VBS).

Ways To Protect Yourself

- Regardless of who sends you the e-mail, if there is an attachment, verify before opening.
- If attachment file ends with .vbs, it is recommended that you delete it.
- In addition, you are able to disable the execution of VBS files on your computer.



```
ormats the partition

5107 MB (  5106 MB free

n bus 0 on atapi [MBR].

tup is formatting...
                          0%
```

Sources

It is now safe to turn off your computer.

- https://www.computerhope.com/vinfo/iloveyou.htm
- http://www.zdnet.com/article/ms-issues-outlook-security-patch/