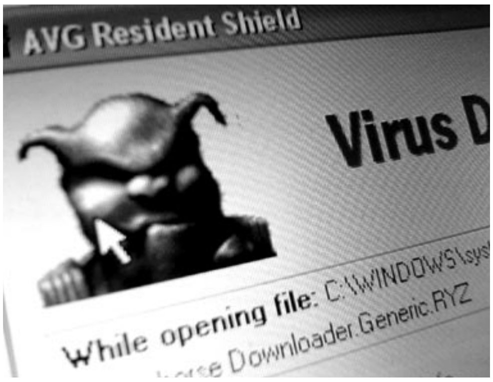
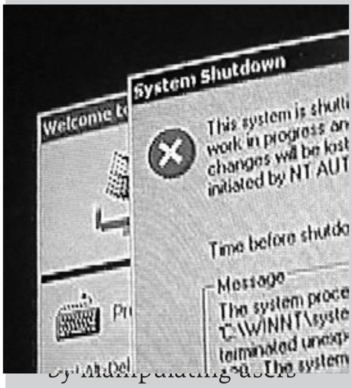
ILOVEYOU Worm


AVG Resident Shield
Virus D
While opening file: C:\WINDOWS\sys
Horse Downloader.Generic.RYZ



The ILOVEYOU worm, also known as VBS/Loveletter and Love Bug worm, is a computer worm written in VBScript.

Description

The worm, first discovered in Hong Kong, arrived in e-mail boxes on May 4, 2000, with the simple subject of "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs".

VBScript
Visual Basic Scripting Edition - an Active Scripting (technology used in Windows to implement component-based scripting support) language developed by Microsoft

Two aspects of the worm made it effective:

- It relied on social engineering to entice users to open the e-mail and ensure its continued propagation.
- It employed a mechanism — VBScripts — that, while not entirely novel, had not been exploited to such a degree previously to direct attention to their potential, reducing the layers of protection that would have to be navigated for success.

Spread

Its massive spread moved westward as workers arrived at their offices and encountered messages generated by people from the East. Because the virus used mailing lists as its source of targets, the messages often appeared to come from an acquaintance and so might be considered "safe", providing further incentive to open them. All it took was a few users at each site to access the VBS attachment to generate the thousands and thousands of e-mails that would cripple e-mail systems under their weight, not to mention overwrite thousands of files on workstations and accessible servers.

Effects

It began in the Philippines on May 4, 2000, and spread across the world in one day (travelling from Hong-Kong to Europe to the United States), infecting 10 percent of all computers connected to the Internet and causing about $5.5 billion in damage. Most of the "damage" was the labor of getting rid of the virus. The Pentagon, CIA, and the British Parliament had to shut down their e-mail systems to get rid of the worm, as did most large corporations.

malware
software designed
to infiltrate or damage
a computer system
without the owner's
informed consent

This particular malware caused widespread outrage, making it the most damaging worm ever. The worm overwrote important files, as well as music, multimedia and more, with a copy of itself. It also sent the worm to everyone on a user's contact list. This particular worm only affected computers running the Microsoft Windows operating system. While any computer accessing e-mail could receive an "ILOVEYOU" e-mail, only Microsoft Windows systems would be infected.

Authorship

The ILOVEYOU worm is believed to have been written by Michael Buen. The Barok trojan horse used by the worm is believed to have been written by Onel de Guzman, a Filipino student of AMA Computer University in Makati, Philippines.

An international manhunt for the perpetrator finally led to a young programming student. On May 11 (one week after the virus spread), he held a news conference and said that he did not mean to cause so much harm. He was unable to graduate because the university rejected his thesis on the basis of its illegality. Helped by a group of friends called the Grammersoft Group, he distributed his virus the day before the school held their graduation ceremony.

Detection

Narinnat Suksawat, a 25-year-old Thai software engineer, was the first person to write software that repaired the damage caused by the worm, releasing it to the public on May 5, 2000, 24 hours after the worm had spread. "Rational Killer", the program he created, removed virus files and restored the previously removed system files so they again functioned normally. Two months later, Narinnat was offered a senior consultant job at Sun Microsystems and worked there for two years. He resigned to start his own business. Today, Narinnat owns a software company named Moscii Systems, a system management software company in Thailand.

Architecture of the worm

The worm is written using Microsoft Visual Basic Scripting (VBS), and requires that the end-user run the script in order to deliver its payload. It will add a set of registry keys to the Windows registry that will allow the malware to start up at every boot.

The worm will then search all drives which are connected to the infected computer and replace files with the extensions *.JPG, *.JPEG, *.VBS, *.VBE, *.JS, *.JSE, *.CSS, *.WSH, *.SCT, *.DOC *.HTA with copies of itself, while appending to the file name a .VBS. extension. The malware will also locate *.MP3 and *.MP2 files, and when found, makes the files hidden, copies itself with the same file name and appends a .VBS.

The worm propagates by sending out copies of itself to all entries in the Microsoft Outlook address book. It also has an additional component, in which it will download and execute an infected program called variously "WIN-BUGSFIX.EXE" or "Microsoftv25.exe". This is a password-stealing program which will e-mail cached passwords.

Barok trojan
this trojan horse
gathers information
such as user name,
IP address and passwords,
and attempts to send the
information to the creator
of the virus

Variants

1. Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs
   Subject Line: ILOVEYOU
   Message Body: kindly check the attached LOVELETTER coming from me.
2. Attachment: Very Funny.vbs
   Subject Line: fwd: Joke
   Message Body: empty
3. Attachment: mothersday.vbs
   Subject Line: Mothers Day Order Confirmation
   Message Body: We have proceeded to charge your credit card for the amount of $326.92 for the mothers day diamond special. We have attached a detailed invoice to this email. Please print out the attachment and keep it in a safe place. Thanks Again and Have a Happy Mothers Day! mothersday@subdimension.com
4. Attachment: virus_warning.jpg.vbs
   Subject Line: Dangerous Virus Warning
   Message Body: There is a dangerous virus circulating. Please click attached picture to view it and learn to avoid it.
5. Attachment: protect.vbs
   Subject Line: Virus ALERT!!!
   Message Body: a long message regarding VBS.LoveLetter.A
6. Attachment: Important.TXT.vbs
   Subject Line: Important! Read carefully!!
   Message Body: Check the attached IMPORTANT coming from me!
7. Attachment: Virus-Protection-Instructions.vbs
   Subject Line: How to protect yourself from the IL0VEYOU bug!
   Message Body: Here's the easy way to fix the love virus.
8. Attachment: KillEmAll.TXT.VBS
   Subject Line: I Cant Believe This!!!
   Message Body: I Cant Believe I have Just received This Hate Email .. Take A Look!

9. Attachment: ArabAir.TXT.vbs
   Subject Line: Thank You For Flying With Arab Airlines
   Message Body: Please check if the bill is correct, by opening the attached file
10. Attachment: IMPORTANT.TXT.vbs
    Subject Line: Variant Test
    Message Body: This is a variant to the vbs virus.
11. Attachment: Vir-Killer.vbs
    Subject Line: Yeah, Yeah another time to DEATH...
    Message Body: This is the Killer for VBS.LOVE-LETTER.WORM.
12. Attachment: LOOK.vbs
    Subject Line: LOOK!
    Message Body: hehe...check this out.
13. Attachment: BEWERBUNG.TXT.vbs
    Subject Line: Bewerbung Kreolina
    Message Body: Sehr geehrte Damen und Herren!
14. Subject Line: Is this you in this picture?
    Message Body: Is this you in this picture?

Legislative aftermath

As there were no laws against virus-writing at the time, on August 21, 2000, the prosecutors dropped all charges against Onel A. de Guzman in a resolution signed by Jovencito Zuno. The original charges brought up against de Guzman dealt with the illegal use of passwords for credit card and bank transactions. The Philippines E-Commerce Law (Republic Act No. 8792), passed on June 14, 2000, laid out penalties for cybercrime. Under the law, those who spread computer viruses or otherwise engage in cybercrime (including copyright infringement and software cracking) can be fined a minimum of 100,000 pesos (about USD$2,000), and a maximum commensurate with the damage caused, and imprisoned for six months to three years.