Computer Viruses Essay, Research Paper

Virus Definition

A computer virus is, simply, a program designed to attach itself to another computer program. Some computer viruses damage the data on your disks by corrupting programs, deleting files, or even reformatting your entire hard disk. Most viruses, however, are not designed to do any serious damage; they simply replicate or display messages.

Most viruses stay active in memory until you turn off your computer. When you turn off the computer you remove the virus from memory, but not from the file, files, or disk it has infected. So the next time you use your computer, the virus program is activated again and attaches itself to more programs. A computer virus, like a biological virus, lives to replicate.

1. Computer viruses infect executable program files, such as word processing, spreadsheet, or operating system programs.

2. Viruses can also infect disks by attaching themselves to special programs in areas of your disks called boot records and master boot records. These are the programs your computer uses to start up.

3. Computer viruses do not damage hardware, such as keyboards or monitors. Though you may experience strange behaviors such as screen distortion or characters not appearing when typed, a virus has, in fact, merely affected the programs that control the display or keyboard. Not even your disks themselves are physically damaged, just what’s stored on them. Viruses can only infect files and corrupt data.

THE LOVE BUG

The subject line read iloveyou. With it came an attached document labeled LOVE-LETTER-FOR-YOU.TXT.VBS.

Before it spent itself–in its first incarnation, it was truly a 24-hour virus–it would affect tens of millions of computers, eventually ring up a toll as high as $10 billion in lost work hours and reopen troubling questions about the safety and security of our vital electronic lifelines. By almost any measure, it was the most damaging virus ever, with at least three times the byte–as more than one punster put it–of Melissa, last year’s electronic femme fatale. Because of its blinding speed, spreading around the world in a hypersonic two hours (vs. six for Melissa).

By week’s end, the work of investigators was further complicated by the appearance of a number of copycat viruses, created either by others or by the Love Bug’s author.

Like a real Asian influenza, the virus first emerged in Hong Kong. From there it sped westward with the sun, lying silently in wait in corporate e-mail accounts until unsuspecting office denizens punched in, logged on and double-clicked on the file. On the other side of the world, in the offices of the German newspaper Abendblatt in Hamburg, system administrators watched in horror as the virus gobbled up 2,000 digital photographs in their picture archive. In Belgium ATMS were disabled, leaving citizens cashless. In Paris cosmetics maker L’Oreal shut down its e-mail servers, as did businesses throughout the Continent. As much as 70% of the computers in Germany, the Netherlands and Sweden were laid low. The companies affected made up a Who’s Who of industry and finance, including Ford, Siemens, Silicon Graphics and Fidelity Investments. Even Microsoft, whose software was the Love Bug’s special target, got so badly battered that it finally severed outside e-mail links at its Redmond, Wash., headquarters.

The bug infected 80% of all federal agencies, including both the Defense and State departments, leaving them temporarily out of e-mail contact with their far-flung outposts. Though Pentagon spokesman Ken Bacon insisted there were other lines of secure cAt the White House, which only a few days earlier had wrangled with Republicans over whether it intentionally destroyed e-mail messages, spokesman Joe says Cecolini. “My Fiendishly created, the Love Bug strikes with a one-two punch. Once you’ve clicked open that fatal attachment and activated its deadly code, the virus either erases or moves a wide range of data files. It singles out in particular so-called JPEG s and MP3s–digital pictures and music–and, like a natural virus, replaces them with identical copies of itself. Then, if it finds the Microsoft Outlook Express e-mail program on your computer, it raids the program’s address book and sends copies of itself to everyone on that list. The Melissa virus grabbed only the first 50 names. Technically, this two-pronged approach makes the Love Bug both a virus and a worm; it’s a virus because it breeds on a host computer’s hard drive and a worm because it also reproduces over a network. As these replicated messages spread, they slowed the Internet traffic to a crawl.

The major antivirus firms quickly posted antidotes–software to neutralize the bug–on their websites, but they were too late to prevent widespread chaos. McAfee received requests for help from 10,000 affected companies on the first day of the outbreak alone.

By contrast, colleges and universities, strongholds of Linux and Macintosh computer systems rather than the targeted Microsoft Windows, got off comparatively lightly.

The difference this time was a mix of shrewdness and ruthlessness. While Melissa sent out its tainted e-mails one by one, sometimes overloading the very server that was supposed to distribute them, the Love Bug spewed them as a single batch–and it didn’t stop at the first 50 names.

Nor would you have been protected if your computer was part of a so-called local area network, or LAN. If you were surfing with Internet Explorer, it would reset your home page to a website in the Philippines, from which it would download a second virus–this one designed to round up all those treasured passwords on your hard drive and ship them off to an e-mail address, also in the Philippines.

Love Bug began to mutate. Either the creator or, more likely, other members of the virus-writing clan started editing the virus and reintroducing it to the Internet with some new, tilted spins. One version had the subject line “FWD: Joke.” Another was written in Lithuanian. One, more devious, bore the subject header “Mother’s Day Order Confirmation”–posing as an e-mail receipt for a credit-card transaction for flowers or a gift for Mom. Perhaps most diabolical of all was the version titled “Dangerous Virus Warning,” with an attached file that cleansed the system of the Love Bug but substituted an equally dangerous one of its own.

The medium may be new, but human nature hasn’t changed: whatever firewalls and antidotes the virus hunters come up with, virus writers will always find a way around them

How to Protect Yourself

–DON’T OPEN E-MAIL from strangers or attachments you weren’t expecting–especially attachments with .EXE extensions

–BACK UP IMPORTANT FILES on floppy discs, Zip drives or other storage devices on a regular basis, so that they can easily be replaced if a virus wipes out your hard drive

–INSTALL THE NEWEST ANTIVIRUS SOFTWARE on your computer, such as Norton Anti-Virus 2000 or McAfee Virus Scan for Windows, or Virex for Macs

–CHECK YOUR SOFTWARE VENDOR’S WEBSITE regularly for updates that will protect against viruses and worms–like the Love Bug–released since your antiviral software was written

Norton

Here’s what Norton AntiVirus does automatically:

Checks system files and boot records for viruses at system startup.

Checks programs for viruses at the time you use them.

Scans your startup drive for viruses once per week.

Monitors your computer for any activity that might indicate the work of a virus in action.

Scan files you download from the Internet.

Checks floppy disks for boot viruses when you use them.

Updates your virus protection at least once monthly.