THE RACE AGAINST MALICIOUS SOFTARE

What Is Malicious Software?

The Internet went from a technological marvel in the late 1980's and early 1990's to something that has become common-place in society today. However, as people log onto the World Wide Web and networks at a continually-increasing rate, the "hidden" threat of encountering malicious software programs also increases. Malicious software typically comes in the form of viruses and worms which "infect" its intended target and rapidly spread within the system or across a network. Exactly how they spread differentiates based on the type of code contained within.

The Nature of the Threat

The most common type of malicious code found in cyberspace today is viruses. These are small pieces of software that "piggyback" on real programs by, for example, attaching itself to a program and running each time the program runs as well. A virus can also reproduce itself by attaching on to another program.[1] Worms are more "intelligent" forms of viruses which replicate by exploiting computer networks and security holes. A copy of the worm searches the network for other machines which contain security holes, copies itself to the new machine, and starts replicating again from there.[2] The main difference is that worms are "self-propagators" – they exploit network vulnerability by spreading without the need of a user, whereas viruses require some form of user intervention to run.

With the presence of malicious software and the potential threats that they serve, the importance of defensive countermeasures are also increasing to a point where it is imperative for virtually every network connected to the Internet. Today, companies ranging from large corporations to small businesses invest substantial amounts of money towards these countermeasures. But it was not always this way. During its advent, malicious software was not considered as an intermediate threat to computer systems, mainly because of industry's ignorance towards them. Over the years, as developers became more technology-savvy, these programs became increasingly sophisticated, forcing industry insiders to recognize their existence and take action against them.

The Evolution of Malicious Software

The term "computer virus" was first given by University of Southern California doctoral candidate Fred Cohen in 1983. He used it to describe a computer program that can "affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself."[3]

In 1986 the first actual computer virus was created by programmers in Pakistan and was coined as "The Brain."[4] It turned out to be a boot-sector virus which infected

DOS formatted 360 K floppy disks and also intercepted the BIOS interrupt for calling disk/drive functions in order to show the original boot sector.[5]

By 1988, industry began to realize the impact that malicious software had on computing. It was then that 23-year-old programmer Robert Morris unleashed a worm that invaded the computers of ARPANET – a large wide-area network for testing new network technologies created by the United States Defense Advanced Research Project Agency.[6] The worm disabled about 6,000 computers on the network by overloading their memory banks with copies of itself. Morris, who confessed to creating the worm out of boredom, was fined $10,000 and given three year's probation.[7]

With the need for some form of defense increasing as the technology evolved, companies began developing anti-viral software. In 1991, Symantec released the first version of the Norton Anti-Virus software – a program that would scan a computer system to find, quarantine, and eliminate files infected with viruses or worms.[8]

Impact on Society

Although malicious software often has the perception that it is only hazardous to the software and computing society, the past five years have proved quite the opposite. Chances are that a substantial number of people outside the computing domain were indirectly affected by some type of malicious code over that time. This is because many applications and services found in society today depend on software which is interconnected by some form of computer network, which in-turn may be controlled by an even larger network or server. Infection of these networks may trigger a "ripple-down" effect, taking down other connected networks as well. This can cause the application controlled by the computer network to malfunction. For example, if the main network from the central location of a large banking company becomes infected, a customer may be unable to withdraw money from one of the bank's automatic teller machines found in another city. This is because the ATM is still connected to the central location network despite not being in its proximity.

Perhaps the most famous case of a software worm affecting society was the blackout which left millions without power in Northeastern America in the summer of 2002. Although it did not directly cause the blackout, the software behind the infamous W32.Blaster worm added to the initial affects and aftermath. The worm had degraded the performance of several communication lines linking key data centers used by utility companies to manage the power grid.[9] Gary Seifert, a researcher at the U.S. Department of Energy's Idaho National Engineering and Environmental Laboratory explains: "It didn't affect the [control] systems internally, but it most certainly affected the timeliness of the data they were receiving from other networks. It certainly compounded the problems."[10] The Blaster worm attacked Windows-based networks and control systems specifically through the open Port 135.[11] These control systems were used to manage large industrial operations such as the electric power grids found in New York, Michigan and Ohio, where the blackout originated.[12] In New York, the worm affected the ability of utilities to restore power appropriately and in time because some of them were running Windows-based control systems with Port 135 open.[13]

The aftermath of the blackout made it clear that malicious software has the ability to cripple society and the way it functions. With the loss of electricity and power, those affected could not operate household appliances or go outside because most stores and services were forced to shut down. Driving was made difficult during the day because stoplights were not functioning and nearly impossible at night because streetlights were left unusable. The affected cities also lost millions of dollars due to the lack of economic activity.

Countermeasures

Although the malicious software available today has increased in sophistication and volume, the technology placed in defensive measures has also increased. Today, everyone from the largest software companies to the smallest home networks have access to numerous anti-virus programs, updates and patches, removal tools, and network security.

As indicated earlier, companies such as Symantec and McAfee annually release anti-virus software in order to combat the ever-changing and increasingly "intelligent" threats. Presently, Norton Anti-Virus stands as the number-one selling anti-virus protection program in the world, boasting the ability to remove viruses, worms, and Trojan horses automatically, detecting spyware and other non-viral threats, as well as blocking more sophisticated codes even before they can enter a computer system.[14] Anti-virus software such as this are also regularly updated to identify and fix the newest loopholes and flaws which malicious code strive to exploit. These updates can be readily downloaded by the end user via a customizable automated download system found within the program.

Certain companies also make available patches to their existing software to not only improve performance and functionality, but to fix security holes and vulnerabilities in the code. For example, about once a year, the Microsoft Corporation releases Service Packs – updates that contain all the fixes and enhancements which the company made available in the previous year.[15] According to Microsoft, their latest release named Service Pack 2 for the Windows XP operating system, has an increased focus on security and protection against malicious software. "[Service Pack 2] is all about security, and it's one of the most important service packs ever released. It provides better protection against viruses, hackers, and worms, and includes Windows Firewall, Pop-up Blocker for Internet Explorer, and the new Windows Security Center."[16]

The Future

As software and computing continues to evolve and play an increasingly-predominant role in society, the quality and potential destructiveness of malicious code will also continue to increase. While malicious code developers continue to produce intelligent software to exploit the weaknesses of companies like Microsoft, these companies will continue to place enormous amounts of money into development of countermeasures. Whoever can stay "ahead" of the other in this game of cat and mouse

will determine how the rest of society is affected. Software is indeed now commonplace amongst society's ever-increasing technological identity, being the driving force behind many routine applications and services. Unfortunately, the presence of malicious code will always cast a dark shadow over it.

Citations

[1] "How Computer Viruses Work," (no date given), Marshall Brain. Retrieved March 24, 2005 from the World Wide Web: http://computer.howstuffworks.com/virus1.htm.

[2] Ibid.

[3] "A Short History of Computer Viruses and Attacks." (February 14, 2003), Brian Krebs. Retrieved March 24, 2005 from the World Wide Web: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50636-2002Jun26&notFound=true.

[4] Ibid.

[5] "A Taste of Computer Security." (no date given), Amit Singh. Retrieved March 27, 2005 from the World Wide Web: http://www.kernelthread.com/publications/security/viruses.html.

[6] "ARPANET." (no date given), (no author given). Retrieved March 27, 2005 from the World Wide Web: http://www.webopedia.com/TERM/A/ARPANET.html.

[7] "A Short History of Computer Viruses and Attacks." (February 14, 2003), Brian Krebs. Retrieved March 24, 2005 from the World Wide Web: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50636-2002Jun26&notFound=true.

[8] Ibid.

[9] "Blaster Worm Linked to Severity of Blackout." (August 29, 2003), Dan Verton. Retrieved March 27, 2005 from the World Wide Web: http://www.computerworld.com/printthis/2003/0,4814,84510,00.html.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] "The World's Most Trusted Antivirus Solution." (no date given), Symantec Website. Retrieved March 27, 2005 from the World Wide Web: http://www.symantec.com/nav/nav_9xnt/.

[15] "Windows XP Service Pack 2." (no date given), Microsoft Website. Retrieved March 27, 2005 from the World Wide Web: http://www.microsoft.com/windowsxp/sp2/default.mspx.

[16] Ibid.