

The Role of the Internet in the Propagation of Malware

Introduction

Businesses of all sizes rely on the Internet as an essential component of their daily operations. The company's Web site is a primary entry point to its current and prospective customers, as well as other key stakeholders; employees conduct the majority of their business operations via the Web; and email has had a profound effect on the speed and efficiency of internal and external communications. All told, email and Web access represent 90 percent of business-critical applications used by small- and mid-size businesses.

Internet tools have dramatically changed the face of the business world, adding extraordinary efficiency and productivity. Unfortunately, these same benefits have also been realized by malware authors. While threats once required months to infect a few thousand computers, the Internet has provided them the means to infect hundreds of thousands in a matter of minutes.

The Evolution of Computer Threats

Computer threats have been a part of our daily computing lives since 1986, when the boot sector virus *Brain* was discovered. Boot sector viruses propagated by writing themselves to floppy disks, then transferring to the user's PC when it booted up. By 1995, boot sector viruses had given way to macro viruses. These were written in script language, and specifically targeted Microsoft Word and Excel documents. Both of these virus types possessed slow, inefficient propagation techniques, relying on users to hand carry them via floppy disks from computer to computer. Desktop antivirus software was sufficient for eliminating these threats.

Much of this began to change in 1999 when the Melissa virus struck. The first email-based threat, Melissa did not need to be hand carried from computer to computer. Instead, it could spread more quickly and easily, using the inherent speed and efficiency of network communications. Future threat types would build on this concept. From email viruses, to network worms, to Web-hosted threats, the Internet would become the new medium of transport.

In addition to its extraordinary propagation benefits, the Internet offered malware authors the capability to post and share their code with their fellow writers. This networking enabled new versions of threats to be developed with just a few modifications to existing code. Even novice programmers, or script kiddies, could develop and distribute new threats to the masses — quickly and easily. Similarly, owners of bot networks and spam email lists began to rent or sell their malicious code and providing writers a natural distribution network for their creations.

Based on this newfound speed and efficiency, desktop antivirus software was no longer sufficient protection, as it could not keep pace with the rate and volume of new and emerging threats.

An Efficient Method of Propagation

As mentioned above, the Internet provided a rich environment for the creation and propagation of computer threats. The whole idea of the Internet is that all computers are connected and can communicate with one another. Malware authors soon realized that they could harness the power of this common network to propagate threats. Rather than the need to infect one computer at a time, these malware authors could now simultaneously take their creations to the masses.

The birth of the Internet provided a mechanism to propagate threats by employing numerous techniques, including email, spam, bots, network worms, and drive-by downloads.

Viruses

The first significant Internet-based threats were propagated via email. Viruses such as Loveletter were sent via email, with the virus as an attachment. Opening the attachment launched the virus, which infected the user's machine. It then sent a copy of itself to every email address in the address book of the victim's email client, using the victim's name as the sender. In this way, other recipients would believe the email had come from somebody they knew. Loveletter infected hundreds of thousands of computers in a single day and caused between \$5 billion and \$7 billion in damages.

To lure the user into opening the attachment, the author included text in the body of the email that told the recipient that the attachment was a love letter to him. This technique was a rudimentary early version of what is now known as social engineering. Simply defined, social engineering is a method employed by malware authors to trick users into infecting their systems. Social engineering takes advantage of the one thing security software can never protect against — the human user.

Spam

The next logical derivative of email-borne threats was spam. Whereas the first email threats behaved as chain letters, relying on individual user error to continue a linear progression for propagation, spam is sent to its intended recipients outright.

Most spam comes in the form of "advertisements" for products or services. Spam is most commonly used to advertise adult Web sites, illegal pharmaceuticals, financial schemes, and other promotional offers. Therefore, most spam is merely a nuisance. However, it is sometimes employed as a vehicle to carry threats such as viruses, spyware, trojans, and rootkits.

The leading technology research firm Gartner estimates that between 2 and 6 percent of spam carries one of these threats. Though this number may seem small, it becomes more significant when coupled with the estimate that between 80 and 95 percent of all email that enters the company's network is spam. Regardless of whether or not it carries a threat, the sheer amount of spam is still of concern to companies, since it can cause a severe impact on network performance.

Network Worms

A network worm has the capability to move seamlessly through the company's network with no dependencies. Because they do not require any user intervention, they can spread rapidly. For example, in July 2001, the Code Red worm infected 359,000 systems within 14 hours, causing more than \$2.6 billion in damages. Similarly, in September 2001, the Nimda worm infected more than 160,000 systems in seven hours, and peaked at 450,000 within 24 hours.

Worms typically spread via operating system vulnerabilities, but they can also be sent as email attachments. Once a worm is on an individual user's system, its built-in SMTP engine enables it to bypass existing email programs completely and move freely throughout the company's network with no user interaction required. Because the worm comes loaded with everything it needs to establish a connection with a mail server, it can send itself to any email addresses it has harvested from the infected computer. Since the worm does not use an existing email application, the operator of the infected computer might not even be aware that a worm is propagating itself.

Worms consume significant amounts of network bandwidth as they replicate and spread freely throughout the network. As a result, network performance can suffer, or it may come to a complete halt. Worms can also carry other threats, including spyware, viruses, and trojans, which can cause additional problems.

Bots

When malware authors wish to send particularly high concentrations of spam, viruses, or spyware, they may employ a bot network to carry out the task. A "bot", short for "Web Robot", is a software program that is automated to perform simple, repetitive tasks over the Internet. On average, a bot network can consist of 20,000 bot-infected computers, also known as "zombies" that are used together in a coordinated fashion to launch threats on a mass scale. Larger bot networks, also known as "botnet" can consist of over a million zombies.

Because bots have the capability to communicate with other network-based services, they are also frequently used to communicate with other computers through various network protocols. Bots can be coupled with spyware to steal sensitive personal information. This information is typically credit card numbers, bank credentials and other consumer-oriented information, but could just as easily be VPN log-ins or other company credentials. They can also be employed to launch a Distributed Denial of Service (DDos) attack, in which large numbers of zombies simultaneously flood the victim's network with millions of connection requests, effectively shutting it down. DDos attacks have targeted such sites as EBay, America Online, Amazon, CNN, E-Trade, and Yahoo.

Drive-By Downloads

A drive-by download is a Web-hosted threat. It is different than the previous threats mentioned, in that it relies on the victim coming to it, rather than being sent to the victim's system. In a drive-by download, threats such as bots, spyware, adware, or trojans are installed with neither the knowledge of, nor any interaction by, the user. When the user visits an infected Web site, the threat is automatically downloaded in the background. The infected site can be a rogue site, developed by a malicious author to appear legitimate, or it can be a legitimate site that has been hijacked by the malicious author and subsequently infected with the threat. In either case, the user typically does not even realize an infection has occurred.

Protecting Against Internet-Based Threats

Ensuring that the organization is adequately protected from Internet-based threats requires a more comprehensive approach to the problem, with multiple layers of security. Though certainly an important first step, desktop security software simply cannot keep pace with the volume, speed, and efficiency of Internet-based threats. This software alone is therefore no longer sufficient to keep the company's network assets safe. For comprehensive protection, traditional desktop security software must be complemented with a robust gateway security solution, which scans both inbound and outbound traffic to detect and remove threats before they reach individual desktops.

The majority of network-based attacks propagate either via email, Web, or the company's internal network, prior to finding an individual user's system. Some threats, such as network worms, prey directly on the company network, with no need for the user's system. As a result, a sound gateway security solution is essential to keep threats out.

Conclusion

Since 1999, the Internet has played an ever-growing role in the propagation of threats. This is due to the overwhelmingly efficient propagation capabilities it naturally offers, as well as the underground community it inadvertently supports. Between the vast number and array of threats available, coupled with the speed and efficiency with which the Internet has enabled them to travel, desktop security alone is unable to keep pace. This has resulted in the need for an additional layer of security at the network gateway to supplement the efforts at the client level.

NETGEAR® ProSecure™ STM Web and Email Threat Management Appliance Solution

The ProSecure STM Appliance uses a unique technology that detects and blocks outbreaks based on their rapid and wide distribution behavior. This approach can detect spam and malware outbreaks as soon as they emerge, and block all associated messages in real time.

The ProSecure STM Appliance features patent pending Stream Scanning Technology that is designed to scan data streams as they enter the network. With Stream Scanning Technology, the NETGEAR STM is able to process large amounts of data in real-time, using a single scan to identify spam, malware, security breaches, or unnecessary applications. This ensures that users on the network receive their email and Web content clean and without delay.

The ProSecure STM Appliance uses a proactive behavioral defense system that eliminates the gap between a vulnerability being exploited and the fix. The NETGEAR solution uses forensic analysis to identify suspicious characteristics of incoming and outgoing network traffic, and neutralizes them until they can be examined more closely.

NETGEAR, the NETGEAR logo, Connect with Innovation and ProSecure are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2009 NETGEAR, Inc. All rights reserved.