Realtime publishers

How to Protect Your Business from Malware, Phishing, and Cybercrime

The SMB Security Series

Malware, Phishing, and Cybercrime – Dangerous Threats Facing the SMB State of Cybercrime

sponsored by

McAfee®

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Malware, Phishing, and Cybercrime—Dangerous Threats Facing the SMB

Malware, phishing and other cybercrime threats have become a persistent problem for businesses. Many organizations do not have the luxury of a dedicated security team that manages endpoint security, monitors networks for malicious traffic, or routinely scans for vulnerabilities. Many rely on a handful of systems and application administrators who are equally adept at managing email and database servers as they are at soliciting business requirements and training end users. They also know something about security but unfortunately they do not have the time or the resources of cybercriminals. Malware, spam, phishing attacks, and directed hacking attacks are part of everyday life in IT. This Essentials Series explains the state of malware and cybercrime today and outlines methods for responding to these threats without demanding inordinate amounts of time or expertise.

Large enterprises are obvious targets of cybercriminals. The well-known security company, RSA, was recently the target of an advanced persistent threat (APT) to steal information about the company's security devices. One of the key steps in that attack was a phishing email message. When an employee opened a spreadsheet attached to the message, malicious code was run that enabled the attacker to install remote control software. From there, the attacker was able to monitor the user's activities and infiltrate other devices on the network.

Cybercriminals do not limit themselves to attacking large businesses. Small and midsize organizations may have valuable information, such as financial data, as well as computing and storage resources attackers can use for other exploits.

Types of Threats to Small and Midsize Businesses

There is a broad array of security threats confronting small and midsize businesses; they can be roughly grouped into three categories:

- Malware
- Phishing attacks
- Other cybercrime activities

Each of these forms of attack presents a distinct set of challenges and requires particular techniques for mitigating the risks.

Malware and Detection Methods

Malware is malicious software. Viruses are perhaps the best-known type of malicious software. These are programs that depend on other programs to spread. Trojan horses, or just Trojans, are programs that appear to perform a legitimate function in order to coax their victims into installing the malware. In addition to different delivery mechanisms, malware can be characterized by what it accomplishes. Key loggers, for example, capture keystrokes, which can be logged and sent to the attacker. These are particularly useful for capturing authentication information such as usernames and passwords. Remote control programs allow an attacker to perform operations on a compromised computer and exploit access to a business' network.

A significant challenge to combating malware is the fact that there are so many malicious programs circulating across the Internet. Antivirus vendors monitor malware infections and related activity and find tens of thousands of new malicious programs every day. Deploying new forms of malware is one way for attackers to try to avoid detection by antivirus software. Even with antivirus vendors constantly updating their detection signatures, the volume of malicious malware makes it difficult to keep up with the pace of new malware generation.

Volume is not the only way attackers try to counter antivirus software; they also use obfuscation techniques. These are methods for masking the malicious code to avoid detection.

For example, malware writers might encrypt their code before distributing it and only decrypt it once the software is ready to run. Encrypted code does not look anything like the original, so signature-based detection methods will not help here. Antivirus vendors have been able to deal with this problem by targeting the encryption/decryption code within a malicious program. That code cannot be encrypted, so it is susceptible to signature-based detection.

Another technique used by malware developers entails inserting extra, random instructions in the code that alter the pattern of the code without altering its function. For example, each time a virus replicates, it may add instructions to add 0 to a variable or multiply some other variable by 1. These operations do not alter the meaning of the code in any way but change the pattern of the binary code making it less susceptible to signature-based detection.

The emergence of self-altering malware, known as polymorphic malware, prompted antivirus vendors to devise a new method of malware detection based on the behavior of a program rather than a pattern in its code. Behavior-based detection simulates code execution in order to detect sequences of steps indicative of malicious software. The execution is done in a way that isolates the code from the host computer so that the malware does not actually damage the system.

Malware developers are constantly coming up with new techniques to avoid detection and improve the effectiveness of their attacks. When new techniques prove successful, they rapidly proliferate. For example, once a polymorphic engine was created to modify the pattern of code without altering its function, that code was widely adopted. More recently, techniques used in the highly sophisticated Stuxnet malware have been detected in other malware.

Malware development and detection are constantly changing in response to each other. One way attackers can avoid the need for sophisticated methods to get their malicious payload installed on a victim's computer is to lure the victim into doing the job for them, and this is one of the objectives of phishing attacks.

Phishing Attacks

Phishing attacks are designed to lure their victims into performing some action that furthers the objective of the attacker, such as visiting a malicious Web site or inadvertently installing malicious software. General phishing attacks target a large number of victims with the same phishing lure or email message. These attacks are enabled by botnets, large groups of compromised computers that are to some degree under the control of the attacker. Botnets can generate large volumes of phishing email messages and other forms of spam.

A specialized form of phishing, known as spear phishing, targets particular individuals. The attack on RSA mentioned earlier, was such a targeted attack. Sophisticated spear phishing attacks use information collected from press releases, social networking sites, and other forms of public information to craft personalized messages. The assumption behind the added research effort is that a personalized message is more likely to be believed by the victim.

Phishing attacks are common elements of larger schemes to compromise a business in order to steal intellectual property, confidential information, or private information about customers or employees.

Cybercrime

Malware and phishing are tools of the cybercrime trade, but they are by no means the full extent of the cybercrime phenomenon. Cybercrime is best understood as an industry with specialized markets for the sale of goods and services as well as a division of labor geared toward the maximization of profits.

Take, for example, the credit card fraud area of cybercrime. Once they have stolen credit card information, thieves can sell this information through online markets where the price for the stolen information is set based on the amount of information provided, the credit limit on the card, and the time since the card information was stolen. Credit card information that includes the security code is more valuable than if only the credit card number is provided.

Market forces also play a role in pricing. Shortly after the Sony network was breached and millions of credit cards were compromised, there was concern in the underground market about the impact of such a large volume of credit cards suddenly coming on the market. As one unnamed hacker told the *New York Times,* "We're keeping a close eye on the Sony story as it would drastically affect the resale of other cards" (Source: *New York Times,* May 3, 2011).

As with most industries, there is a division of labor in the field of cybercrime. The US Federal Bureau of Investigation (FBI) has identified several categories of cybercriminals, ranging from malware developers and project managers to money mules and hosting services. The combination of specialized labor, established markets, and available cyber-infrastructure has enabled the growth of a sizable cybercrime industry.

Although it is difficult to estimate the size of the cybercrime industry, the direct cost of global cybercrime has been estimated to be $114 billion in direct costs, such as stolen money and intellectual property. When indirect costs, such as staff time, are taken into account, the figure could be as high as $388 billion (Source: Net-Security.org at http://www.net-security.org/secworld.php?id=11579).

Small and midsize businesses are not immune to the threats of malware, phishing, and other forms of cybercrime. To mitigate the risk from these threats, businesses of all sizes and types should be in a position to respond.

Responding to Today's Threats

Cybercrime and information security are highly technical areas that demand specialized knowledge in multiple arenas, such as malware, software vulnerabilities, and systems monitoring. Antivirus vendors, for example, must have in-depth knowledge about how malware is written and distributed as well as about global trends related to the spread of infections. IT professionals in general must be aware of the threat of malware and methods for reducing the risk from malicious software.

IT professionals responsible for dealing with security issues must also be knowledgeable about software vulnerabilities and techniques for managing them. Malware often takes advantage of vulnerabilities in legitimate software. For example, a vulnerability in Adobe Flash was used in the RSA attack mentioned earlier. By exploiting that vulnerability, the attacker was able to install a remote control program. (The vulnerability was not publically known at the time of the attack but has since been corrected.)

Systems monitoring with regards to endpoint security focuses on detecting and blocking malicious software. In addition to having adequate antivirus software installed on all systems, IT professionals must understand how to maintain these antivirus systems to keep them up to date, ensure they are properly installed and configured.

The need for specialized knowledge is a common issue for information technology professionals and creates substantial demands on IT staff. This demand for specialized knowledge can often go unmet for several reasons:

- Limited time to acquire specialized skills
- Competing demands for infrastructure and application support
- Virtually all applications, from desktop software to enterprise database management systems, are potential targets

This situation leaves few options for IT professionals. We can deploy in-house security suites that provide a combination of endpoint, email, and Web security tools. This has some advantages, such as full control over the deployment of the software, but it introduces additional complex software that must be configured and maintained. An emerging option of security as a software service offers an alternative model for implementing security controls.

Security as a service enables businesses of all sizes to take advantage of specialized expertise of security vendors who can invest more time, staff, and resources to monitor malware activity and refine business practices to mitigate the risk from security threats. It also allows IT professionals in small and midsize businesses to focus on other business needs by reducing the security burden placed on them.

Summary

Malware, phishing, and other cybercrime activities cost businesses billions of dollars. Security researchers and practitioners have created tools and techniques for addressing these threats, but it is sometimes difficult for small and midsize businesses to dedicate sufficient staff resources to these threats without adversely impacting other IT operations. Security as a service is an emerging alternative model for implementing security controls without inordinate demands on in-house IT professionals.