Global Knowledge®

Expert Reference Series of White Papers

10 Ways Malicious Code Reaches Your Private Network

10 Ways Malicious Code Reaches Your Private Network

James Michael Stewart, Global Knowledge Instructor

Introduction

As of 2010, there are nearly 3 million unique forms of known malicious code, and thousands of new ones are discovered daily. The risk of being infected is greater than ever. The damage caused by an infection can range from a minor annoyance to a catastrophic disaster. The old wisdom continues to ring true: an ounce of prevention is worth a pound of cure.

Most computer users are aware of the importance of security to reduce the threats that could potentially harm a computer or network. For example, anti-virus and anti-spyware are essential defenses in the war against malicious code. However, technology cannot compensate for poor and risky behavior. Thus, proper training and understanding, along with behavior changes, are needed to facilitate a reduction of malicious code infections.

The methods, vectors, or paths that malicious code can use to gain access to your system are increasing as new services or types of communications are developed. In fact, every single possible communication method that exists for legitimate data can be used to transmit malicious data as well. Thus, we all need to be vigilant in keeping our protections current as well as avoiding risky activities.

There are at least 10 ways malicious code reaches your private network that you need to be aware of.

1. E-mail Attachments

Attachments to e-mails are a common method of distribution of malicious code. E-mail is inherently insecure due to its use of SMTP, a plain text-forwarding protocol, and its lack of strong authentication of message senders. The source of an e-mail address can be easily spoofed or falsified as someone that you trust. Often, this alone is enough to trick a recipient into opening an attachment.

Generally, avoid using attachments as a means to exchange files. Instead, use a third-party file exchange system (such as DropBox, Box.net, Drop.io, MediaFire, Windows Live SkyDrive, Foldershare, RapidShare, MegaUpload, Dropload, YouSendIt, SendThisFile, etc.). Thus, when an attachment does arrive, it is suspicious for being abnormal and not the standard method by which common communications take place.

If you receive an attachment and need to determine if it is legitimate, you still need to verify it before opening it. Create a new e-mail (do not reply to the message with the attachment) to the sender and ask for confirma-

tion that they sent the file. Maybe even ask the filename, size, and hash value if you are really concerned. Or, call the person and ask if they sent you an attachment on purpose. If the sender does not confirm the attachment, delete it.

2. Portable Media

Portable media includes any device that can store information. This includes optical discs (CD, DVD, HD-DVD, Blu-Ray, etc.), tapes, external hard drives, USB drives, and memory cards. Any storage device can support both benign and malicious content. The less you know about or trust the source of a device, the more you should be cautious about accepting the device and connecting it to your system. Any media from outside the organization should be highly scrutinized, especially if obtained from a questionable or unknown source.

A possible defense is to use a dedicated scanning system. Every new-to-you media can be scanned at this stand-alone system before it is used on any production system. Assuming the stand-alone scanner system is updated regularly, it will greatly reduce the risk of malware distribution via media. Another option would be to limit data exchanges to file sharing services that do not involve portable media.

3. Visiting Malicious Web Sites

The Web browser is the primary tool used to interact with the Internet, which is a dangerous place. Thus, many threats breach our organizations' defenses through this seemingly innocent client software. Popular and well-known sites are generally not a significant threat; however, any site can be the victim of an attack, which in turn could leave you at risk.

Following hyperlinks sent to you by e-mail or chat could lead to malicious locations. Additionally, some search results might not lead to legitimate locations. Always be cautious about following Web links to domain names you don't generally recognize.

It is difficult to always be aware of the reputation of a Web site are visiting, but you can reduce the risk by using an updated browser, limiting auto-execute features of mobile code, and running anti-malware scanners.

4. Downloading Files from Web Sites

Even when visiting generally trustworthy Web sites, there may be additional risk if you elect to download content to your local system. Take ever greater caution when choosing to download material from any site. Seek out only those locations that are known to be safe and trustworthy. For example, download.com, managed by CNet, is a safe location to download software, because they test and verify every file available through their service.

When seeking out more esoteric content or unique files, you will likely be visiting non-mainstream download locations. These fringe sites put you at greater risk, because they don't have a known reputation and may not have any amount of filtering or screening of offered files.

Downloaded Web content includes both generic files, including software, plug-ins, movies, audio files, etc., as well as mobile code, such as ActiveX, Java, JavaScript, Flash, SilverLight, etc. Any code that comes from an outside source – that is potentially unknown – puts you and your computer system at greater risk.

5. Participation in P2P File Sharing Services

Concern over downloaded, malicious content grows when that code is obtained through a peer file-sharing system. This is not a condemnation of efficient, distributed transmission solutions, but rather the sources of the files exchanged through them. By not knowing or having control over the source of a file, it is possible that malicious code could be included along with the content being sought.

The risk is lower when the content is downloaded legally, but the risk grows when a P2P sharing system is used to access illegal or infringing content. The risk is greater not because the content becomes malicious when it is exchanged outside of ethical channels, but because the providers of the content often include malicious code intentionally. The "poisoning" of the content is a way to further distribute malware, especially remotely controlled tools, through a popular but non-filtered exchange mechanism.

6. Instant Messaging Clients

In many cases, the purveyors of malware look for methods of distribution that will enable them to quickly and broadly transmit their code. The more popular a "thing," the more attractive it becomes as a vehicle for distribution. Malware can be seen as a form of parasite that attaches itself to any popular communication medium.

One increasingly popular communication medium is that of IM or instant messaging. Through chat systems, especially those using installed software clients instead of Web interfaces, the exchange of files is possible. There have been security breaches that allowed remote hackers to upload and/or download files through holes in IM client software. Even with a patched client, it is possible for a user to accept an offered file from an unknown source or follow an offered hyperlink to a malicious Web site.

7. New Devices and Peripherals

A risk that is often overlooked due to its rarity is malware found on brand new devices, right out of their packaging. Mobile phones, digital photo frames, and even media players have been compromised during manufacturing, resulting in malware that makes its way to a customer's computer. This has happened with a well-known, commercial, shrink-wrapped, anti-virus product.

Vendors often outsource the actual construction and pre-production of their products to external manufacturers and assemblers. When computer parts are the product being constructed, especially those with storage capabilities, malware can make its way onto the new device while it is loaded with its software elements if the manufacturer's system is infected. One way to reduce this threat is to not be an early adopter of a product nor the first to grab an updated version of an existing product. Give the rest of the market a few days or weeks to discover malware and other concerns before adding the new device or peripheral to your repertoire.

8. Social Networking Sites

Social networking sites offer up several situations that could allow malware to make its way onto your network. First, there are the social engineering attacks that trick users into accepting fraudulent information that, when acted upon, could compromise an account or the security of a computer. Second, with the proliferation of message posting and exchange services, it is easy to follow hyperlinks to malicious Web sites. Third, some in-site applications, written by malicious entities, attempt to hijack accounts or distribute malicious code.

Many of these threats are discovered by the community or the site moderators within a few hours or days, so these concerns don't remain static for long. However, new attacks and tricks are crafted by hackers constantly. Be suspicious, don't accept offered links, especially for file downloads, and don't be an early adopter of a new application. Give the community a few days to discover the malicious elements and weed them out before you dive in.

9. Social Engineering Attacks

Social engineering is the art of convincing someone to either give up information or perform a task that results in the reduction of security. Large organizations are the most common targets of social engineering attacks; however, mass e-mail-based attacks could show up in anyone's inbox.

Be aware that attackers are trying to trick you into following hyperlinks, downloading files, performing configuration changes, or typing in esoteric commands. Doing so could lead to the direct infection of your system with malware.

Social engineering attacks are often quite subtle. At first glance, or before your second thought, you might not realize that an e-mail or a phone conversation isn't normal. If the hacker can convince you to act before you think or verify, the social engineering attack is successful. If a hacker can trick you into visiting a malicious Web site, malware could be transmitted to your system through Web-based mobile code.

In other attacks, the hacker may encourage you to download a scanner or utility in order to perform some testing or diagnostic function. The tool you download might do what is claimed, but it also may open a remote control connection granting the hacker partial to full access to your system.

A social engineering attack could even be waged by building auto-launch elements onto USB flash drives and leaving them in various locations, such as the restroom counter, the snack room, or near the smoking area. If someone picks up the drive and plugs it into their computer, they probably won't even notice the installation of malicious code, which might corrupt the system or grant hackers remote control access.

Be aware; you are a target of social engineering attacks. The question is will you recognize the attack for what it is, or will you be tricked into harming your own environment.

10. Not Following Security Guidelines and Policies

The last and probably most significant cause of how or why malicious code reaches your private network, or even just your personal computer system, is by not following proper security guidelines and policies. Most organizations of moderate size have made the effort to design a secure infrastructure. This includes prescribing user access policies and providing at least some level of security awareness training.

Failing to abide by security guidelines or purposefully violating security policies will lead to compromised security, often the distribution of malicious code. Security policies are written and implemented for a reason – to reduce the likelihood of a security breach. If a worker fails to abide by the company security policy, they put themselves and the entire organization at risk.

Bypassing filters, using storage devices from outside resources, using unauthorized peripherals, blocking software updates, opening e-mail attachments, participating in unethical file exchanges, and using non-approved software clients are all security policy violations and increase the chance of malicious code infesting the organization.

Every organization and every individual has a vested interest in operating with common sense security guidelines. This will assist in reducing the risk of malicious code infection and allow the organization to be productive in accomplishing missions, goals, or sales, without having to spend resources on recovery.

Write a security policy. Define the acceptable use policy. Hire competent personnel. Train users on how to perform their jobs within the confines of security. Use automated tools to detect and defend. Monitor the environment for abuse, misuse, and compromise. Use common sense. Obey the rules.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course(s):

Certified Ethical Hacker

Cyber Security Foundations

CISSP Prep Course

Security+ Prep Course

For more information or to register, visit **www.globalknowledge.com** or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

James Michael Stewart has been working with computers and technology for over twenty-five years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, CEH, and Security+. He is the primary author on the CISSP Study Guide 4th Edition and the Security+ 2008 Review Guide. Michael has also contributed to many other CISSP and Security+ focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware.

In addition, Michael has co-authored numerous books on other security and Microsoft certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+Security Windows 2000, MCSA Windows Server 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, and iNet+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of the-pants hands-on "street smarts" experience. You can reach Michael by e-mail at michael@impactonline.com.