Vital Security™

Integrated Content Security Solution

Malicious Mobile Code

Technical White Paper

finjan® software

Contents

1 The Internet Today

A large share of the Internet content that users are exposed to is actually in the form of small programs that run locally on the desktop. Most people don't realize that when they visit a Web site, this content is executing automatically on their computer. Corporate employees are exposed to these technologies every day simply by browsing the Web to perform research, buy products or to communicate with business partners and associates.

This concept of distributed computing allows Web users to automatically download and run platform-independent code from all over the world on their own PCs without technical skills. This results in programs that make the Web more dynamic by delivering animation, computation, user interaction, and other functions to the desktop.

In short, programs are dynamically loaded over the network and execute locally, taking advantage of distributed computing horsepower, allowing "fresh" software to be distributed "as needed."

2 Vital Security™

Vital Security detects and prevents malicious attacks before they cause damage. Finjan's products use real-time content inspection and monitoring, plus policy-based behavior-blocking technology that do not require database updates. With no updates needed, Finjan products provide ongoing security out of the box enabling companies to conduct e-business safely.

3 Technology

3.1 Executables

An executable is a file (usually with the ".exe" filename extension) that contains a program that runs on a computer. Executables are most often downloaded from e-mail, the Web or FTP. Most executables are written in machine code (the most elementary programming language) and are thereby capable of performing any function on your PC, including copying, deleting or altering your files. Until now, the industry's best security measure for executables was for companies to tell employees not to open any unknown file with an executable extension (typically .exe). As apparent with the damage caused by the recent MiniZip and Explore Zip worms, PrettyPark.exe, and Happy99.exe, this is not an effective defense.

3.2 Java

Sun Microsystem's Java is a language used to embed applets (small applications) in Web sites. Java applets are executed by the user's browser or in a stand-alone mode with the help of a Java Virtual

Machine application. The risk of using Java is that without proper security controls in the browser, Java applications can access desktop files and send out data to other locations without the user's knowledge or consent.

3.3 Active X

Microsoft's ActiveX is a programming language that can access the operating system of the user's computer. This combination of the Internet and operating system can create powerful desktop applications, however there is a risk that ActiveX controls can be used to access any resource on the desktop to perform malicious activities. ActiveX applications are digitally signed to validate a trusted origin, however this security measure is relatively easy to circumvent.

3.4 JavaScript

Netscape's JavaScript is a common scripting language used to embed applets that are executed by the browser software, rather than the user's operating system. The purpose of JavaScript is to animate a web site with movement and sound, edit user input, perform calculations, and improve overall interactivity. JavaScript has built-in limitations to provide some level of security. It can not access desktop files, operating system, or software applications. JavaScript can, however, modify cookies, launch plug-ins that already reside on the user's desktop, and submit form data to a URL without a user's knowledge or consent.

3.5 Visual Basic Script

VBS is a script programming language used to embed applets into Web sites. A VBS applet operates inside the browser much like JavaScript. The VBS language is restricted from accessing the entire file system or communicating with other web sites, however VBS can create, open, read and write to text files on the user's computer. The risk of VBS is that it may open, read and write text files and launch ActiveX controls without the user's knowledge or consent.

3.6 Cookies

A Web site may use "Cookies" to store a small amount of data on a visitor's disk drive. Cookies are like tags that allow a web site to track its visitors, and provide personalized information for a user when they make repeated visits to a site. Unfortunately, cookies can be used to save passwords for a particular Web page. The inherent danger with this is that if somebody intercepts a user's cookie and finds a password, there is a good chance that the same password is used at multiple locations to protect more sensitive data.

3.7 Plug-ins

Today's browser technology supports the ability to automatically download and install 'plug-in' applications that support user interaction with multi-media data. Although independent software vendors are traditionally responsible sources of such plug-in products, it is possible for well-known plug-ins to be maliciously modified. Since the browser gives users a window to collect plug-in applications, the result is an environment in which uncontrolled software is freely distributed and used, often in contradiction with an established computer security policy.

4 What is the Threat?

Malicious code has been used to steal, alter and erase PC files as well as gain unauthorized access to corporate networks. A malicious code attack can penetrate corporate networks and systems from a variety of access points, including Web sites, HTML content in e-mail messages or corporate intranets.

Today, with 200 million Internet users, new malicious code attacks can spread instantly through corporations. The majority of damage caused by malicious code happens in the first hours after a first-strike attack occurs "in the wild" – before there is time for countermeasures. The costs of network downtime or theft of IP make malicious code a top priority.

Examples of recent malicious code attacks include:

4.1 Back Orifice 2000 (BO2K)

This is a program created and released by the notorious hacker group, Cult of the Dead Cow. It allows anyone to take complete control of another PC and have complete access to hard drive partitions and shared network drives.

Unlike earlier versions that affected consumers and small businesses, Back Orifice 2000 hits large organizations because it runs on Windows NT systems, which are more used by businesses. Also, the updated program is modular, so users can add additional functions. For example, they can hide files or activate a computer's microphone for real-time audio monitoring.

4.2 ExploreZip Worm

Searches your system for Microsoft Word, Excel, and PowerPoint files, and destroys them. Propagated via e-mail. Press coverage of companies hit: Lockheed, Forrester, Boeing, AT&T, Intel, Southern Co., Microsoft, SBC, General Electric, and Electronic Arts.

4.3 MinZip # I, II & III Worms

The original ExploreZip worm was simply run through a compression tool freely available on the Internet. Once compressed, the signature pattern of the attack is changed and becomes invisible to anti-virus scanning engines. The same attack can be compressed and redistributed indefinitely - slipping right pass anti-virus software.

4.4 WinNT.Infis

This is an executable file with .EXE extension that installs itself as a native Windows NT system driver. It is the first known malicious program to install and run in Kernel mode under Windows NT.

4.5 PrettyPark.exe

Reveals the victim's passwords on a number of IRC channels and some reports indicate it is also a Trojan, allowing backdoor access to the victim's system. Sends files of itself to e-mail addresses listed in the user's Internet address book. PrettyPark will run this routine every 30 minutes, without the user's knowledge.

4.6 Happy99.exe

This was a denial of service attack. When someone executes the Happy99.exe attachment, a fireworks display appears on their screen. Meanwhile, in the background, the worm alters the host computer's Internet configuration to keep track of all E-mail or newsgroup activity. The worm then spams itself to the same newsgroups and E-mail addresses to which a user posts. Happy99 caused network slowdowns and crashed corporate e-mail servers.

4.7 eBayla

Blue Adept discovered a security problem that allows eBay users to easily steal the passwords of other eBay users. The exploit involves posting items for bid that include malicious JavaScript code as part of the item's description. When an unsuspecting eBay user places a bid on the item, the embedded JavaScript code sends their username and password to the malicious user by e-mail. From the victim's point of view, nothing unusual seems to have occurred, so they are unlikely to report/complain to eBay. Once a malicious user knows the username/password of the victim's eBay account, he or she can assume full control of the account.

4.8 Russian New Year

A security exploit triggered through the "CALL" function of Microsoft Excel 95 and 97 as well as Microsoft Office 95 and 97. By taking advantage of a known vulnerability in the "CALL" function in Excel spreadsheets hackers can perform hostile attacks on a users PC including transferring files from your desktop to a server outside the corporation. Spreadsheet files can be quietly moved to a browser-using HTML. All 3.x and 4.x versions of Microsoft's Internet Explorer and Netscape's Navigator browsers 3.X and 4.X (except Navigator 4.5) are vulnerable, as well as HTML-aware email applications such as Outlook™ 98. *Finjan would like to emphasize that there are many ways to exploit this severe security flaw and only several variations have been detected.*

4.9 Leningrad

A security exploit that takes advantage of standard HTML and Microsoft Word. The exploit was posted to Woody's Office Watch on January 21, 1999, Volume 4, Number 3, http://www.wopr.com/wow/wowv4n3.html and subsequently followed up on February 2, 1999. Like the Russian New Year, the Word 97 vulnerability, dubbed by Finjan as "Leningrad" can be executed seamlessly using legitimate HTML and exploiting the legitimate "MACRO" function in Microsoft Word™. According to Microsoft in a Security Bulletin issued 1/21/99, "a malicious hacker could exploit a macro code to be run without warning if a user opens a Word attachment that was sent by a malicious hacker, or posted on a web site controlled by the malicious hacker. This malicious macro could possibly be used to damage or retrieve data on a user's system." If you are using Internet Explorer™ 4.x and 5.x, Netscape Navigator™ 4.x and 5.x, or a Web-enabled mail client such as Outlook™ 98, with Word 97 you are susceptible

4.10 Cuicci

A security hole in Microsoft's implementation of Java. Affects the IE 3.x and 4.x. Allows hackers to maliciously exploit Java applets in order to create denial of service attacks. These attacks can be embedded in Web pages or in email attachments. Variations of this attack are circulating out on the Net.

4.11 Cuartango

Cuartango discovered that Microsoft programmers forgot that "copy" and "paste" commands are possible in scripting with Internet Explorer 4 and they did not protect the file input field against this operation. The bug causes Internet Explorer 4.x to upload a file when a browser visits a malicious Web site whose pages contain a simple set of JavaScript instructions.

Despite Microsoft's patch to fix the Curatango bug, and later the son of Curatango, there was yet a third end-run, Grandson of Curatango, that was discovered (and patched within 24 hours by Microsoft). Microsoft calls the attack a "Frame Spoof" and offered the following:

Microsoft has released a patch that fixes a vulnerability in Internet Explorer that could allow a malicious Web site operator to create a false window that imitates a window on a legitimate Web site. The threat posed by this vulnerability is that the false window could collect information from you and send it back to the malicious site.

4.12 Electronic Disturbance Theatre

A dangerous Java applet that attacks third party Web servers (in this case, the Pentagon, the Frankfurt Stock Exchange site, and the President of Mexico's Web site). As detailed in a Wired News article, a Java applet is activated when everyday Web surfers visit a site created by a Mexican political group called the Zapatistas. Just by visiting the site with Java-enabled browsers set "on", users inadvertently trigger a denial-of-service attack on the Pentagon and other target sites.

Programs, by their nature, are inherently buggy and untrustworthy. Technologies such as Java and ActiveX enable these buggy and untrustworthy programs to move to and execute on user workstations. The Web acts to increase the mobility of code without differentiating between program quality, integrity, or reliability. Consider multi-media documents such as Web pages. Such files, regularly created and distributed by non-technical employees, are containers for textual content, graphic images, sound files, and programs. Using available tools, it is quite simple to "drag and drop" code into documents which are subsequently placed on Web servers and made available to employees throughout the organization or individuals across the Internet. If this code is maliciously programmed, or improperly tested, it can cause serious damage.

To learn more about mobile code, please refer to the following resources:

5 Security Site Links

(http://www.finjan.com/site_links.cfm)
http://www.gocsi.com/prelea990301.htm
1999 CSI/FBI Computer Crime and Security Survey
http://www.issa-ne.org/related.htm
Information Systems Security Association, Inc. (ISSA)
http://www.cs.princeton.edu/sip
Princeton University's Secure Internet Programming Site
http://www.cerias.purdue.edu
Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS)
http://www.securityportal.com
SecurityPortal.com - Security News, Security Site Links, Alerts, and more
http://www.rstcorp.com/javasecurity/links
RST's Java Security Hotlist

http://java.sun.com/security
JavaSoft Security Site
http://www.netversant.com/hotinfo/sum.htm
Network Security Survey among IT Executives and Professionals
http://www.microsoft.com/ie/security
Microsoft's Internet Explorer Security Pages - Information, Issues, and Fixes for Microsoft Browsers
http://kimera.cs.washington.edu/related/index
Security Links from Project Kimera at University of Washington
http://www.securityserver.com/cgi-local/ssis.pl/category/java6.htm
Hot links to computer security web sites associated with Java security
http://www.nwnetworks.com/iesf.html
The Unofficial Microsoft Internet Explorer Security FAQ

6 Security Books

Securing Java: Getting Down to Business with Mobile Code
By Gary McGraw and Ed Felten
http://www.amazon.com/exec/obidos/ASIN/047131952X/finjansoftware/002-0821032-0502410

Web Security Sourcebook
By Avi Rubin, Daniel Geer, and Marcus Ranum
http://www.amazon.com/exec/obidos/ASIN/047118148X/finjansoftware/002-0821032-0502410

E-Commerce Security: Weak Links, Best Defenses
By Anup K. Ghosh
http://www.amazon.com/exec/obidos/ASIN/0471192236/finjansoftware/002-0821032-0502410

7 About Finjan

Finjan Software's Vital Security™ is the only complete and integrated Secure Content Management solution in which individual best-of-breed security applications work together in concert to proactively respond to changing security threats today and tomorrow. Supplementing traditional security methods, Vital Security defends enterprises against Malicious Mobile Code using intelligent behavior analysis and comprehensive policy management. Vital Security is designed with High Availability and scalability, for enterprises of all sizes, including those with over 100,000 users. Finjan is recognized by analyst firm IDC as the leader in the worldwide Malicious Mobile Code security market. For more information, visit http://www.finjan.com.

WWW.FINJAN.COM
Printed in the U.S.A.
USA MMCWP2.0 02.04EN