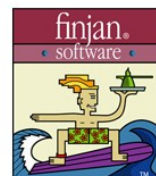


▶ What's the Source of Most Viruses Today? Malicious Mobile Code

Topical White Paper



Why Anti-Virus and Firewalls Are Not Enough

Mobile code is not fundamentally different from any other program executable that runs natively on machines today. What makes mobile code incredibly powerful as well as dangerous is that mobile code can be written by anyone, be distributed seamlessly over the Internet, and can often execute on any platform independent of the operating system or chip architecture. What makes mobile code pervasive is the ubiquitous Internet browser. The browser provides interpreters for mobile code of all types. Today's browser software integrates mailers and Web browsers—both fully capable of executing mobile content present in Web pages and email. What makes mobile code particularly dangerous is that it executes with the privilege of the user—giving the program the capability to access personal files, system resources, and the network. Once mobile code has seized control of the machine, it can destroy data, monitor Web usage, send files back over network connections, and open trap doors into the system.

Mobile code, also known as Active Content, includes Java applets, Java Scripts, Visual Basic Scripts, Macros and Microsoft Windows ActiveX controls. They are commonly found in dynamic Web sites or e-mail and run behind the scenes to provide interactive menus and graphics to computer users. Mobile code can also provide a lot of flexibility and bandwidth optimization.

What is Malicious Mobile Code (MMC)?

With all the end-user benefits that legitimate mobile code brings, there's also a dark side that needs to be considered. Because mobile code executes in your browser's "Local Computer" security zone, it has broad permissions to execute potentially malicious activities such as:

- Stealing passwords and confidential information
- Creating backdoors
- Acting as a transport mechanism for viruses
- Erasing data
- Creating holes in firewalls
- Running programs from client machines
- Reading and writing files on end-user hard drives
- Allowing access to secure company resources

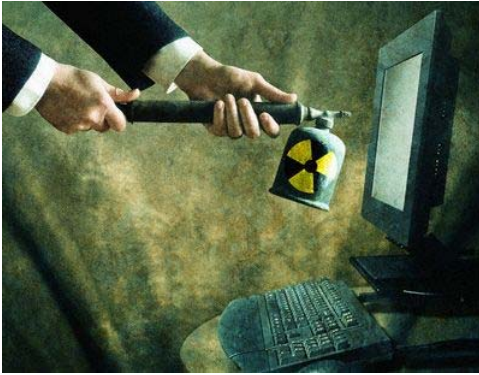
Malicious mobile code can masquerade as something benign such as a screensaver, video game, help file, music download or even an anti-virus application.

"Security concerns have been heightened due to the rash of Web-based viruses (e.g., NIMDA, Code Red, and Bugbear) and malicious mobile code (MMC) that have escaped traditional (signature-based) virus measures... Given the prolific speed at which viruses spread today, they often sneak past traditional anti-virus software and entrench themselves in desktop and server systems before anti-virus vendors can post an appropriate signature."

*Brian Burke, Research Manager
Robert Mahowald, Research Manager
IDC*

How Do You Protect Yourself From MMC?

The best approach to protecting computers and networks against MMC is to implement a strategy that provides a layered solution. A possible security approach could include a proactive code-scanning and behavior analysis engine to catch new MMC and virus outbreaks or variants. This would provide protection to organizations during the time between a new virus outbreak and when a patch is created and deployed in the organization – a window of vulnerability of hours or even days. A traditional anti-virus scanning engine can compliment the proactive code-scanning and behavior analysis engine and provide virus protection against already defined MMC, viruses and worms.



Web filtering and anti-spam solutions are also tools organizations should consider. Web filtering solutions can prevent users from visiting Web sites known to contain mobile malicious code such as many adult and gambling sites. Spam control solutions can reduce the risk of being infected by MMC and other viruses received through unsolicited e-mails.

Recent MMC Attacks

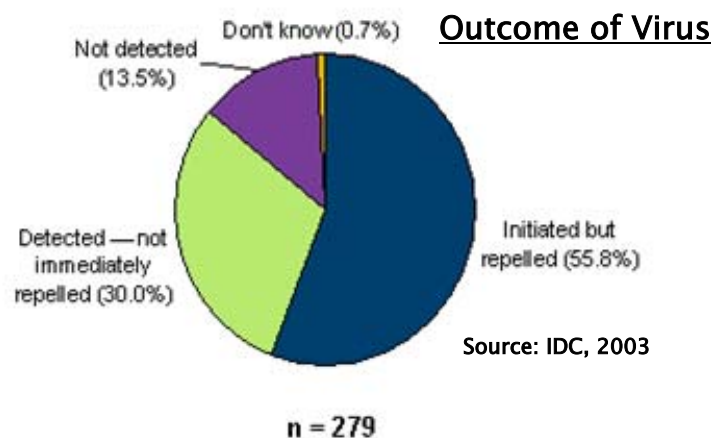
In today's always-on environment, malicious mobile code is one of the biggest threats to computer security systems. Two of the worst viruses to date, Nimda and Code-Red, attacked using mobile code. The Slammer worm is another example and it passed through firewalls and took advantage of a known vulnerability with an available patch — a patch that a lot of organizations failed to apply. In fact, in 2002, 82% of companies were attacked by some kind of virus, even though 99% of them had anti-virus software installed (CSI/FBI 2003 Computer Crime and Security Survey).

Data and Network

Integrity

Legislative requirements in the U.S. such as HIPAA (Health Insurance Portability and Accountability Act) for healthcare, GLBA (Gramm-Leach-Bliley Act) for finance and the EU Directive on Data Protection, are just a few

examples of the need for organizations to have visibility and control over the content traveling into and out of their corporate networks. Combined with today's climate of government oversight and scrutiny into unethical business practices, maintaining the integrity and privacy of information stored inside an organization's network must be a priority. Malicious code, viruses and Trojans can be



introduced onto a local computer and an entire network simply by one individual downloading malicious active content from the Internet. As a result, malicious mobile code can travel, infect and compromise any data stored on a network's SMTP, Web, database or file server.

Reduced ROI

There are a handful of solutions available today that address the problem of malicious mobile code however, there are a few important things to consider. Point products that address a single problem can be less expensive as an initial purchase however, implementation time, IT staff training and ease of management must also be considered. Many IT departments today want to be able to choose best-of-breed technologies to address their content security and management concerns without being tied to a single vendor. Gartner recommends organizations implement content security solutions that integrate best-of-breed technology into one platform allowing network administrators and staff to manage multiple applications from various vendors from one management console.

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 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>.



© 2003 by Finjan Software, Inc., and/or its subsidiaries
Printed in the U.S.A.
USA MMCWP1.0 12.03 EN
WWW.FINJAN.COM

Finjan, Finjan logo, and Vital Security are trademarks or registered trademarks of Finjan Software, Inc. and/or its subsidiaries. All other trademarks are the sole property of their respective owners. The Finjan Software products described in this document are protected by one or more of the following U.S. Patents: 6092194, 6167520, 6480962, 6209103, 6298446, and 6353892 and may be protected by other U.S. Patents, foreign patents, or pending applications.