White Paper December 2003

McAfee SECURITY

McAfee System Protection Solutions

Ricochet Team Server Security Brief, Volume 5

Internet Worms: Self-Spreading Malicious Programs

Table of Contents

Worms are a major threat to the Internet. Their automatic nature makes them powerful and destructive. Using existing and evolving methods of propagation, worms of the future will become increasingly more powerful and harder to contain. Crafted by malicious code developers, worm technology continues to become more destructive, at times causing irreversible damage, as seen in the wake of Code Red and Nimda.

Security Threats, 2003–2008

What will be the biggest security threat over the next five years?

"Super" Worms*	3.71
Polymorphic Code	3.19
Application-Level Attacks	3.12
Massively Distributed Attacks**	3.10
Kernel-Level Holes in OSes	2.95
DDoS Attacks	2.88
Other Worm Attacks***	2.88
IDS Evasion	2.71

* Fast-spreading, multi-platform, multi-exploit, zero-day, metamorphic worms

** Beyond traditional DDoS, including distributed password cracking, distributed port, and vulnerability scanning, etc.

*** Worms spreading beyond the Internet—To telephony and power grid

Source: *Information Security* survey of 220 readers. The threat of "super" worms looms large. *Information Security Magazine's* poll respondents gave the highest mean score to these yet-to-be-seen menaces, and more than 36 percent considered them the single greatest threat

Worm History

The first widespread Internet worm appeared in 1988. A graduate student at Cornell University, Robert Morris, created a worm program that exploited several vulnerabilities and released it to the then-nascent Internet. Morris claimed no malicious intent, stating that the worm was simply an experiment that went awry. Malicious intent or not, the Morris worm impaired over 6,000 Internet-connected computers and caused hundreds of thousands of dollars in clean-up costs. Considering the small size of the Internet and the slow connections in use at the time, this attack was very significant. Given the severe slow-down the Morris worm caused in many government systems, media coverage was plentiful, making this worm one of the first highly publicized computer attacks of its time.

Since then, worm attacks have increased in sophistication. In 2001, Code Red spread to over 300,000 machines in just fourteen hours. This powerful and destructive power translates into a significant cost. According to *Computer Economics*, the associated damage from the Code Red and Nimda worms came to $3.72 billion.

Why Are They Called Worms?

The term "worm" was first applied to self-replicating computer programs by John Brunner in the 1975 sci-fi novel, The Shockwave Rider. In the book, a malicious program spreads itself throughout the government's massive computer system, exposing private data and government secrets. Researchers at Xerox's famous PARC laboratory first applied the term to real-world self-spreading programs.

Worms vs. Viruses

How are worms different from viruses? Worms are malicious programs that spread themselves automatically. Viruses require some form of human intervention to spread. In the early days of personal computing, viruses spread through humans taking infected floppy disks from computer to computer. Due to the rapid growth of e-mail and the decline of floppy disks, most viruses of today spread by convincing a human to open a malicious e-mail attachment. Worms, on the other hand, are able to propagate autonomously. Worms spread by exploiting vulnerabilities in a computer system, then using network connectivity to find and attack other vulnerable systems. The lack of human intervention allows worms to spread much faster than viruses.

Anatomy of a Worm

Worms have three main parts:

- Attack Mechanism
- Payload
- New Target Selection

Attack Mechanism

Worms exploit one or more specific vulnerabilities in a computer system. Buffer overflow vulnerabilities comprise a majority of the vulnerabilities that worms exploit. A worm's attack mechanism exploits the vulnerability in the target system and uses that vulnerability to copy itself onto the target system.

Payload

The payload is the part of the worm code that performs malicious actions against the compromised host. Some worms have no payload; they simply spread themselves and drain system resources. Similarly, a worm's payload can be any type of program. If a worm targets a vulnerability that allows the worm to run its payload at the root or administrator privilege level, the payload will be able to reformat the hard drive, install root kits and backdoor programs, etc. The payload may also search the computer for data, such as credit card numbers, patient records, or other valuable data, then send the data to a central server where the worm's author can collect it. Any number of other malicious activities can be part of a worm payload.

New Target Selection

Once the worm's code is executing on the attacked system, it attempts to spread again. To do this, a worm must locate target computers that are vulnerable to its attack mechanism. The mechanisms used vary in sophistication.

Case-In-Point: Code Red

As an example, Code Red, which spread to hundreds of thousands of IIS Web servers in 2001, caused millions of dollars in damage. Code Red exploited a vulnerability in the Microsoft® IIS Web server. It had three different versions, each one improving the distribution mechanism, which resulted in dramatic acceleration and spreading. The first version of the Code Red worm simply sent HTTP requests containing its exploit code to random IP addresses. Such a simple target selection technique requires a large number of attempted attacks for each successful one. In order for Code Red to successfully infect the randomly selected IP address, the following criteria must be met:

- There is a computer at that IP address
- The computer at that IP address must be running an IIS Web server
- The IIS Web server application must be vulnerable to exploitation (The server is not patched and does not have McAfee® Entercept® running to protect it)

Despite the relative simplicity of this brute force technique, Code Red spread rapidly. A later version of Code Red, Code Red II, improved on the target selection mechanism by selecting target IP addresses that were numerically close to the IP address of the infected machine. For example, if the infected machine's IP address were 192.168.1.134, Code Red II would randomly select IP addresses that began with 192.168.1 before targeting other IP addresses. Since computers on a given network often have similar addresses, this greatly improved the chances that the IP address chosen would actually have a computer at that IP address.

More intelligent, targeted worms may use predefined lists of known servers, targeted attacks against certain organizations, DNS data, or other techniques to more efficiently select potential targets.

How to Protect Yourself from Worms

Internet worms prove that despite the significant effort and money spent on security, software vulnerabilities are still the single biggest security challenge. Simply put, users are left exposed for prolonged periods of time between vulnerability exposure, patch development, and deployment. Due to the relative ease with which new worms can be created, the situation only worsens.

System patching can be an effective solution, but the gap between the exploit appearance and deployment of the patch means that systems are still vulnerable for some time. Furthermore, the time and testing required to deploy patches are significant, meaning the amount of time that systems are unprotected can be large. During that time, users are exposed. This is an unacceptable situation, and there is a clear need for a solution that will either replace

patching or provide an additional security layer until the patch is applied.

Signature-based approaches are not enough. By the same token, behavior-only based technologies fall short of delivering the security intelligence that a robust security signature database can provide. A hybrid approach that uses both protection methods bridges the gap between the two technologies, while providing the benefits of both.

Since the majority of CERT security advisories deal with buffer overflow vulnerabilities, special attention should be given to solutions that address buffer overflows. Simple stack buffer overflow exploitations, as well as more advanced heap-based and non-executable exploitation techniques, should be addressed.

Solutions that detect changes in the integrity of the system are vital. Even more important are solutions that lock down the machine, preventing any modification to the binaries, data, and configuration of the system. Application level security is also becoming increasingly important. Specific systems that address Web servers and other common servers should be considered.

Internet worms continue to be an ever-growing threat. In nearly fifteen years of existence, worms have caused increasingly large amounts of damage. Internet worms vary in degrees of severity, but all have the same basic anatomy and mode of operation. An outbreak of an Internet worm can mean tremendous loss or damage to an organization in the form of time, money, and/or reputation. To combat today's Internet worms, as well as those yet to be discovered, enterprises and organizations need to implement a strong security policy, coupled with advanced intrusion prevention technologies.

About McAfee Security

McAfee Security is a product line of Network Associates® Inc. that protects businesses from security breaches, virus attacks, and blended threats. McAfee Security provides comprehensive network protection through industry-leading anti-virus, encryption, desktop firewall, intrusion detection, vulnerability assessment, and managed security technologies. All McAfee Security products and services are backed by the world-leading anti-virus research organization, AVERT™ (Anti-Virus Emergency Response Team), the team responsible for providing cures for major outbreaks like LoveLetter, Code Red, and Nimda. For more information, McAfee Security can be reached at 888-VIRUS-NO and on the Internet at http://www.mcafeesecurity.com.

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 800.338.8754

Network Associates® products denote years of experience and commitment to customer satisfaction. The PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects—all with service levels to meet the needs of every customer organization. McAfee® Research, a world leader in information systems and security, continues to spearhead innovation in the development and refinement of all our technologies.

 6-sps-ent-iwm-001-1203