



I need
complete network security
that's affordable....
and
I needed it yesterday.

Where Online Hackers Are Headed in 2007: “Coming Soon” to a Website Near You (and Your Hard Drive)!

**Kevin Prince
Chief Security Officer
Perimeter eSecurity
February 2007**



Complete. On Demand. Affordable.

With the advent of powerful anti-virus and anti-SPAM software protecting increasing numbers of computers and networks, hackers are turning their attention to new ways to deliver viruses, crash unsuspecting users' computers, and steal social security numbers, passwords, bank account numbers, etc.

When Microsoft released Microsoft XP Service Pack 2 (SP2) in 2004, they challenged hackers everywhere to find alternate ways to deliver viruses and steal data. This software release, with its built-in security features turned "on" by default, dramatically cut hacker access to millions of computers.

Hackers are a clever, persistent, and creative lot, and their challenges have only increased nominally with the Microsoft enhancements. Even with security turned on, systems remain vulnerable in other ways. But because most of the systems or information with the highest value to hackers has become more secure, they are required to get increasingly creative in their methods.

New attack methods

2005 marked the beginning of a movement towards a new type of attack method. Until then, most attackers would compromise a computer by attacking it with known vulnerabilities (bugs) that allow the attacker to gain control over the system. With firewalls loaded onto many systems, as well as other security features, the "inbound attack" approach became increasingly less profitable.

The new attack methods take advantage of vulnerabilities within the Internet browser. These vulnerabilities allow the attacker to download malicious code, Trojan horses, or other applications in the background by having the user look at a web page on which the malicious code is stored. Some of the new attack methods included luring users to malicious web sites via SPAM, instant messaging, or popular web sites.

Malware code often crashes systems, captures keystrokes containing user id's, passwords, account information or social security numbers. Most users fail to realize that malware creates an outbound connection to the Internet. Because the internal computer is making the request out to the Internet, the security systems assume it is "authorized" traffic, and allows the traffic. This way, a computer makes connections back to the attacker's system without a security query, enabling the hacker to capture information or

do anything they want. This approach defeats virtually all security features designed to stop inbound attacks, since the attack is through an outbound affirmative connection.

2006 brought with it a dramatic increase in this type of attack, which estimates suggest more than tripled those observed in 2005 and continue to increase early in 2007. Efforts to attract users to malicious web sites have increased dramatically. One such effort we observed recently was disguised as a phishing attack. The phishing web site installed malware on the remote computer, even though the users did not enter any personal information.

Stopping new attack types demands strong security posture

The popularity and success of these methods, along with security devices that only block inbound attacks, ensures that this trend will continue and escalate.

Stopping attacks that utilize malware requires a dedication to a security posture that includes a layered approach. Solutions that should be considered to reduce malware in your environment are:

Intrusion Detection/Prevention: Use an IDS/IPS system to do a “deep packet inspection” which will look beyond the header information of the packet and look at the payload, comparing each packet with known attack signatures. Be sure the system is updated, tuned, and monitored 24x7.

URL Filtering: Also known as web site filtering. These solutions prevent internal system from accessing unauthorized sites. All sites are put into any of 50+ categories, and the administrator decides which types of sites should be accessible to employees via the network.

SPAM filtering: Be sure that SPAM is being filtered from the network level, and then on the desktop. Reducing SPAM will keep end users from clicking on links that contain malware.

Policies: An Internet use policy stating what users are allowed to do on the Internet is critical. Systems that have the ability to download peer-to-peer (P2P) software, instant message (IM), or install applications are often the ones burned by attackers. Reduce the

applications and access users have and restrict them to those required to perform their duties.

PC Restrictions: Most operating systems have the ability to restrict the user from installing or downloading applications. This becomes an increased burden on the IT staff, but it is worth it.

Gateway AV: Use gateway AV to stop malicious code from entering your network. Don't rely on the desktop AV to stop all viruses and worms.

Vulnerability Scanning: Be sure you are running scans on all accessible systems and all critical servers to find vulnerabilities. Regularly run a full network-wide vulnerability scan.

The risk mitigation solutions that can keep malware off our systems exist today, but many managers do not use them to get proper protection. A combination of good end user training, policies, and technology, will reduce security risks as they continue to evolve.

By Kevin Prince,
Chief Security Officer
Perimeter eSecurity
www.perimeterusa.com
(800) 234-2175

Founded in 1997, Perimeter eSecurity, is the only provider of complete eSecurity on demand, which offers network security "in the cloud," or directly to the network, for more than 4,000 growing companies nationwide. Headquartered in Milford, CT with seven geographically-distributed operations centers and three redundant data centers, the company is among the fastest growing network security providers. Its website, www.perimeterusa.com, offers a wealth of network security services and webinars that are available to businesses on demand.