

Redefining Endpoint Security: Examining recent changes in security threats and the new ways in which endpoint devices are being exploited by hackers

By Mitchell Ashley, CTO and VP Customer Experience

Originally published in CyberDefense Magazine, August 2004

To date, much of our focus in network security has been on locking down the perimeter and securing internal network resources by utilizing firewalls, intrusion detection/prevention, vulnerability assessment, and good patching practices. In parallel, we have continued to depend on anti-virus and personal firewalls to secure laptops and desktops.



With the start of 2004, a subtle but significant shift has occurred in the way attackers attempt to breach our networks. While parameters have been hardened, the dirty little secret of network security is that the endpoint devices are the real weakness -- and hackers know it. The enormous number of worms, trojans, and spyware that have been introduced into the wild attest to this new approach. Network and security administrators are deluged by the many variants of MyDoom, Netsky, Sober, Sobig, Bagle, Phatbot, Witty, Blaster, and many others.

Let's examine why decentralized attacks like these have become so prevalent. There are two basic methods of breaking into any computer. The first is by exploiting operating system or application software that is improperly configured or contains vulnerabilities that allow the device to be compromised. Most of the commonly deployed security defense systems are directed at preventing attacks of this nature by blocking malicious traffic or reporting known vulnerabilities that need to be repaired.

The second attack approach is to leverage end-user behavior. Many common -- and even desired -- end-user behaviors can be exploited to facilitate an attack. As a result, the attack bypasses traditional defenses such as firewalls and IDS/IPS solutions and has direct, immediate access to core network devices and other endpoints.

How do the new worms and trojans leverage the end user as part of the attack? In the case of MyDoom, malicious payload is delivered when end users open a zip file. Sober.D relies on end users clicking a link to download a security patch contained in a would-be security email bulletin, delivering the worm directly to end users' devices. In the past, security administrators would have ignored end users opening something as common as a zip file and even applauded end users who download a security patch for their computer. Not anymore.

By leveraging end users and their computers, hackers have an almost unlimited number of unsecured corporate and home computers through which to gain access

into our business and government networks. Unsuspecting end users VPN into the network or connect their laptops to the LAN when returning to work and re-infect the network, frequently requiring security administrators to respond to the same attack multiple times.

Considering Endpoint Security

There are two perspectives to take into account when considering endpoint security: protecting individual endpoint devices from attack, and protecting networks from improperly secured and unknown endpoint devices.

Traditionally, endpoint security for laptop and desktop devices has been limited to anti-virus software and the application of security patches and hotfixes. Before the widespread impact of distributed attacks, such as Blaster, MyDoom, and Sasser, most organizations believed anti-virus was sufficient to secure end user devices. Distributed attacks have demonstrated their resilience by bypassing both perimeter and anti-virus defenses. These attacks leverage end user behaviors as part of the attack delivery. While anti-virus is still an important component for securing the endpoint, many organizations have learned the hard way that many worms bypass anti-virus defenses.

Personal firewalls apply many of the same security techniques that network firewalls employ, such as restricting network communications and controlling network access. As a general rule, personal firewalls do a good job of blocking common network attacks (ping responses, port scans, etc.), but they rely on end users to establish firewall security policies when software resident on the device requests communications with the network. These can be valid requests, such as a web browser requesting access to the Internet, or a worm or trojan masquerading as a legitimate program. Keep in mind that unless they are tightly controlled by knowledgeable security staff, most personal firewalls configured by end users are configured for "high end user convenience," rather than proper security.

A new class of endpoint security solutions works to protect the network from unsecured and unknown devices. This approach views all endpoint devices attempting to connect to and use the network as suspect. End users may have disabled security applications (such as anti-virus or personal firewall), neglected to install up-to-date security patches, improperly configured security settings, or installed restricted software (peer-to-peer, file sharing, or instant messaging).

Endpoint security solutions protect against these dangers by prohibiting devices from accessing the network until they meet the necessary security requirements. These solutions test devices for compliance with the organization's security policy in the areas of anti-virus, personal firewall, patches, security settings, and required and restricted software. They also make sure the device has not already been compromised by worms, trojans or spyware. Devices that meet the security requirements are allowed access to the network and are then retested during their connection to ensure continued compliance. Those devices that fail compliance testing are quarantined, and their users are provided with direction and resources for updating the device with the necessary patches and security setting.

Most endpoint solutions require the installation of an agent, either via an executable or downloaded over the network. Installing an agent isn't always practical such as in the case of visitors, contractors, or employees' home computers. Installing agents

also brings with it software compatibility issues, increased help desk support calls, and end user frustration. Next-generation endpoint security solutions offer agent-less, or client-less, technologies that eliminate the need for the installation of agent software on the endpoint device.

About the Author:

Mitchell Ashley is CTO and VP of Customer Experience at StillSecure. He is responsible for the product strategy and development of the StillSecure suite of network security software. Mr. Ashley has more than 20 years of experience in data networking, network security and software development. He can be reached at (303) 381-3830.