TRUE ZERO DAY PROTECTION

The Only Defense Against Evolving Security Threats

March 2008

Abstract

Zero day attacks are a growing threat to corporate networks, because they pass undetected through conventional signature-based defenses. Many, if not most, systems are vulnerable to these attacks. The actual number of infections is staggering, and dealing with them burdens IT departments and impacts corporate bottom lines. The corporate losses are the criminals' gains, as compromised systems feed an underground cyber-economy worth millions and millions of dollars. Rather than relying solely on signatures, businesses need a security strategy that also includes protection from zero day attacks. This white paper explains the mechanisms of zero day threats and shows how the WatchGuard approach of combining application proxy firewall and intelligent layered security provides fundamentally stronger protection for business networks.

Introduction

A corporate user clicks on a link in an email, taking him to a web site. The site serves up a deliberately corrupted media file that contains a snippet of program code. Within seconds, the user's computer is taken over by a criminal and is sending spam emails all over the Internet.

This is just one example of a zero day attack. A zero day attack is an attempt to exploit a vulnerability in computer software or equipment, before that vulnerability has been disclosed and a specific preventive measure exists. Zero day protection, therefore, is the ability to block such a threat, even though the exact mechanisms of the attack are unknown.

"Black hat" hackers are becoming incredibly sophisticated at finding new vulnerabilities and exploiting them before the security community can react. It can take less than a second to compromise a single machine. A zero day worm that exploits a previously undiscovered but widely prevalent security hole can propagate across hundreds of thousands of Internet-connected machines within a few hours. Consider the following examples:

> **Code-Red worm, July 19, 2001.** More than 359,000 computers were infected in less than 14 hours. At the peak of the outbreak, more than 2,000 new hosts were infected each minute.[1]

> **SQL Slammer, July 25, 2003.** At least 75,000 machines were infected, 90 percent of them within the first ten minutes.[2]

> **Storm Worm, January 2007.** Storm spawned a "botnet" of remotely controlled zombie machines, each capable of spreading constantly mutating infections to others through various means. In effect, each variant represented a new zero day attack. By year's end, one source estimated the botnet's size at over 1.8 million infected computers worldwide.[3] The Storm botnet remains a highly active, virulent, and worrisome threat.

True zero day protection has to work from day zero, hour zero, minute zero.

Conventional Defenses and the Zero Day Threat

Most security vendors build their detection strategies around signatures, which are essentially the "fingerprints" of the computer code used to launch an attack. While signatures are a useful element of defense, *any scheme that relies on signatures alone cannot claim to offer true zero day protection.*

The moment an exploit has been released into the wild, security companies that rely on signatures are in a race to obtain samples, build a signature, then test, package, and distribute it. The time from the first attack until the end users have installed the protective signature is termed the "window of vulnerability."
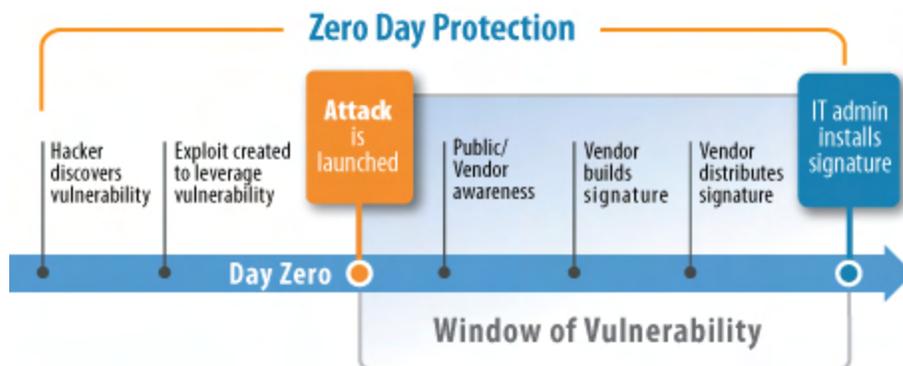
In the best-case scenario, creating and testing a signature can take hours. Fully closing the window by installing the signature can take days, and depends ultimately on the vigilance of end users. However:

- The most virulent Internet worms spread in minutes, not hours or days

- Malware authors have learned how to make their code self-mutating, requiring constant development of new signatures

- Criminals have learned that if their efforts fly under the radar, they can delay discovery of the vulnerability and avoid signature-based security entirely

The Computer Security Institute, which publishes an annual report on the state of network security, concluded in its report for 2007 that given the evolving state of malware, reliance on signatures was leaving defenses "increasingly permeable."[4]

Zero Day Threats: The Harsh Realities

The popular image of a hacker is a teenager, holed up in his bedroom at his parents' home, launching attacks so he can brag about them to his online hacker buddies. Sorry to say, the black hats have grown up. They are organized gangs. They hide behind an array of ever-changing Internet addresses to elude detection, and many work out of foreign countries.

Means, Motive … and Plentiful Opportunities

The potential for zero day attacks lurks everywhere. The National Vulnerability Database, sponsored by the Department of Homeland Security's National Cyber Security Division, listed more than 29,000 Common Vulnerabilities and Exposures (CVEs) as of January 2008. This database is a comprehensive library of vulnerabilities uncovered by "white hat" security researchers. On average, there are 15 new CVEs added per day.[5]

From web browsers and media players to office applications and corporate databases, nearly every type of application has been revealed to have some vulnerability. How do the black hats take advantage of them to compromise machines? Here are some common avenues:

- **Tricking users into opening executable files** masquerading as other file types, sent via email or instant messaging

- **Directing users to visit web sites** that spread infections (drive-by downloads)

- **Sending carefully crafted documents** that contain executable code, taking advantage of application vulnerabilities that allow the code to run (buffer overflow attacks)

For the small to medium-size enterprise (SME), one new hacker technique is especially alarming – the use of personal information, often found on social networking sites, to target individuals within the organization. Vulnerabilities in common office applications allow attackers to send infected documents, seemingly of business value, with enough insider information to prompt the target to open them. In one survey, 32% of respondents said they had experienced a targeted attack directed at their industry or their organization.[6]

Quantifying the Risk

Compromised machines aren't just theoretical. They're a reality. The Microsoft Spyware Removal tool removed malware from more than 8 million computers during the first half of 2007. The infection rate had more than doubled compared to 2006.[7]

ShadowServer, an all-volunteer group of security professionals, tracks botnet activity. As of January 2008, they were tracking more than 2,000 command-and-control servers controlling more than 200,000 zombie machines owned by unsuspecting users.[8] Symantec reported that during the first half of 2007, more than 5 million distinct computers became bot-infected at some point.[9]

No business, regardless of size, is immune. A 2007 survey of security practitioners representing organizations of every size revealed that:[10]

- 52% reported virus incidents

- 25% experienced denial-of-service (DoS) attacks

- 21% uncovered bots within the organization

- 13% detected system penetration

- 10% reporting password sniffing

- 10% suffered web site defacement

- 06% encountered an exploit of their organization's DNS server

This survey was skewed to a population that is more security conscious than the norm. It is likely that the numbers are even higher at organizations that adopt a "see no evil, hear no evil" approach.

Costs and Impacts

The expense in time required to clean infected machines is immense. There are no automated tools or documented steps for cleanup after a zero day attack. Especially when hackers use rootkit techniques, which bury the evidence of their work deep within the operating system, the smartest course is usually to reinstall the operating system and restore files from the last successful backup.

In the meantime, workplace productivity suffers. In one survey, over a six-month period more than one in four users reported their productivity was impacted by an infection, with productivity declines between 21 and 32 percent.

Even more alarming, those users on average waited more than 18 working hours to have the infection repaired.[11] The legal liability for companies harboring infected machines on their networks is an emerging area of law. It is a special concern when those machines contain or access confidential data.

What Do the Black Hats Want?

An entire underground economy has risen around compromised machines. Access to "owned" servers, services for launching "phishing" schemes, rental botnets for spam runs, and malware creation services are all advertised for a fee. These in turn support a marketplace for stolen identities, compromised bank accounts, and credit card numbers. One study tracked activity on an underground server and found more than $1.5 million in transactions over a 24-hour period in one trading channel alone.

To service this underground economy, the hacker is usually not after the data on the computer, but the computer itself and the ability to control it. It could be used as a platform for launching attacks on other, higher-value computers. Or more likely, the aim is to add the computer to a botnet, as a tool for all kinds of criminal schemes.

Hackers have become incredibly sophisticated at hiding their tracks, and typically the only visible sign that a machine has been compromised is a slight slowdown. If the exploit is successful, a hacker can have control of the machine in milliseconds. Typically, the first step after gaining control is to patch the machine's vulnerabilities to improve its security posture. The hacker isn't doing the victim any favors; simply securing ownership by locking out the competition.

Mounting an Effective Defense

Zero day attacks that routinely bypass signature-based detection are especially valuable to the criminal hacker. WatchGuard firewalls enforce security in an entirely different way. Signatures are a secondary element of a multi-layered defense. The twin pillars of WatchGuard's zero day protection strategy are:

- Application proxy firewall
- Multi-faceted detection strategy termed *intelligent layered security*

Understanding how these defenses work separately and in concert is the key to understanding how true zero day protection can be achieved.

Application Proxy Firewall

WatchGuard was an industry pioneer in implementing application proxy technology in a firewall appliance. Even though there are hundreds and hundreds of firewall vendors, WatchGuard remains one of the handful that use an application proxy.

The Traditional Approach: Packet-Based Firewalls

The first firewalls were deployed at large enterprises that needed to handle large amounts of traffic. These first firewalls were packet filters. Packet filters do not process packets as intensively as an application proxy, so they are simpler to design and inherently faster. Despite advances in hardware and processing speed, well-known firewall vendors still rely on their legacy packet-based designs.

To understand a packet filter, consider a packet: a set of data bytes, assembled into a compact bundle for routing over the Internet. Each packet begins with a header that contains information about the contents including:

- Internet address of the sender

- Internet address of the recipient

- Protocol being used

- For most protocols, a port number that the receiving computer uses to direct the packet to the correct application

A packet filter firewall looks at the information in the header. It checks the source, destination, protocol, and port number and if the combination is allowed, it forwards the packet. Most home routers contain packet filter firewalls.

Stepping Up Security: Stateful Inspection and Signatures

A stateful inspection firewall is a packet-based firewall that doesn't just look at the packets individually, but understands what a correct sequence of packets should look like. It understands the state of each connection, and drops packets that are out of logical sequence. Most business-class firewalls are of the stateful inspection type.

For added protection that looks at the data within each packet, some firewall vendors depend on signatures alone. This reactive approach is flawed in dealing with zero day attacks because:

- A signature is written after the exploit is known, which could take anywhere from hours to weeks, or perhaps never if the exploit is uncommon

- Until a signature is applied, systems are highly vulnerable as there is no secondary defense; security is only as strong as the last signature update

- Many end users take an "if it ain't broke, don't fix it" approach to critical network components such as firewalls, and do not patch and update them regularly

Taking a Deeper Look: Application Proxy Firewall

While packet filters look for bad things and filter them out, application proxy firewalls take the opposite approach. They are designed to recognize good traffic, allow it, and block everything else. This approach blocks whole classes of attacks. As one simple example, a number of FTP servers have vulnerabilities associated with the DELE (delete) command, which could lead to outside control of the machine. The WatchGuard application proxy does not recognize use of the DELE command as legitimate traffic – in fact, it protected against those attacks years before specific vulnerabilities were even known.

To obtain this level of protection, an application proxy firewall doesn't simply look at the packet as it flies by. It disassembles the packet, rebuilds and re-sends it. It is called a "proxy" because it handles the connections on behalf of the source and destination machines. At the endpoints, the session proceeds as though each machine is communicating directly with the other. In fact, each is communicating with the firewall.

An application proxy is more processor-intensive than a packet-based firewall. Delivering the benefit of an application proxy with full-speed network performance calls for more than brute-force processing. It requires strategic design. (See *Intelligent Layered Security*, next section.)

The critical security difference between a packet-based and application proxy firewall is easily understood by looking at the seven-layer OSI model. The OSI model is fundamental to modern networking, and governs how data is packaged. A packet inspection firewall can only take action based on the first three layers of the model. A stateful inspection firewall adds the transport layer. An application proxy firewall has the capability to inspect all seven layers and take action based on the topmost application layer, where most zero day threats reside.
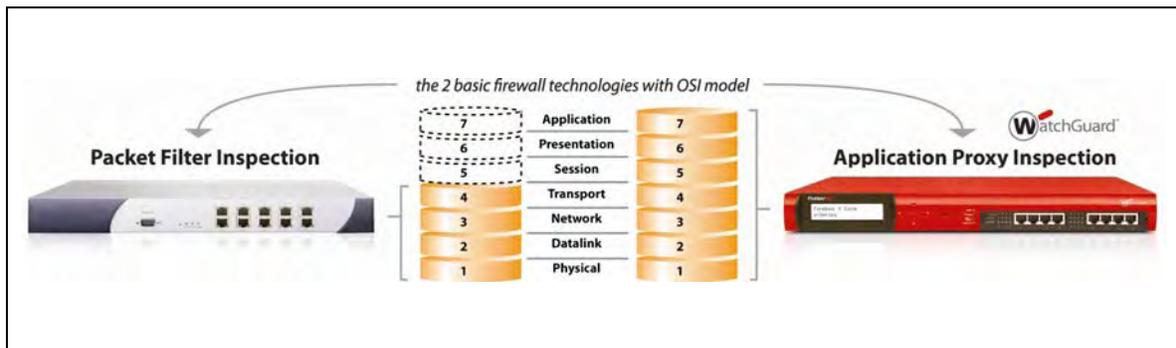
An application proxy makes decisions based on information that packet-based firewalls do not even consider. This includes checks such as:

- Is the packet formatted properly for this protocol?
- Does it contain unknown types of content that could be malicious (.exe files, .scr files, other executable types – even if they have been renamed)?
- Does it contain non-ASCII characters?
- Does it contain dangerous commands?
- Is the amount of data too long for this protocol?
- Does the pattern suggest a potential attacker looking for information about internal systems?

Most significantly, the WatchGuard proxy checks for and validates compliance with Internet standards for the protocol being used (RFC compliance). Whole classes of vulnerabilities, such as buffer overflow attacks, violate standards in some way and the application proxy eliminates the need for many signature checks by enforcing compliance.

The WatchGuard proxy's understanding of applications and protocols is so thorough that if a packet contains benign abnormalities that aren't a security concern, it can rebuild the packet to proper specification before sending it on.

Intelligent Layered Security

Typically, packet-based firewalls check for simple anomalies in the headers or connection, test against a set of signatures, and forward the packet. With a WatchGuard firewall, each connection and packet goes through a series of checks, beginning with the simplest checks first, working from the bottom to the top of the seven-layer OSI model. Any check can strip or modify pieces of the packet, or deny or drop it to eliminate the need for further processing. For the few malicious packets that can survive the gauntlet, signatures at the application layer mop them up.

The intelligent layered security approach allows a WatchGuard firewall to deliver the full zero day protection of an application proxy, with limited impact on network performance. Depending on the port and protocol, only a few checks are needed for most packets. Just a small percentage call for the full scrutiny of layer-seven inspection, augmented by WatchGuard signatures.

The WatchGuard signatures capture specific threats carefully crafted by the black hats to masquerade as benign traffic. For traffic leaving the network, signatures are used mainly to detect and block traffic from machines infected with spyware or bot software, sending rogue instant messages, or participating in peer-to-peer file sharing. For traffic coming into the network, the signatures mainly protect against specific threats aimed at servers that can't be detected by the proxy, such as cross-site scripting or SQL injection.

Most of the other broad classes of threats are effectively trapped without signatures by the first six layers below.
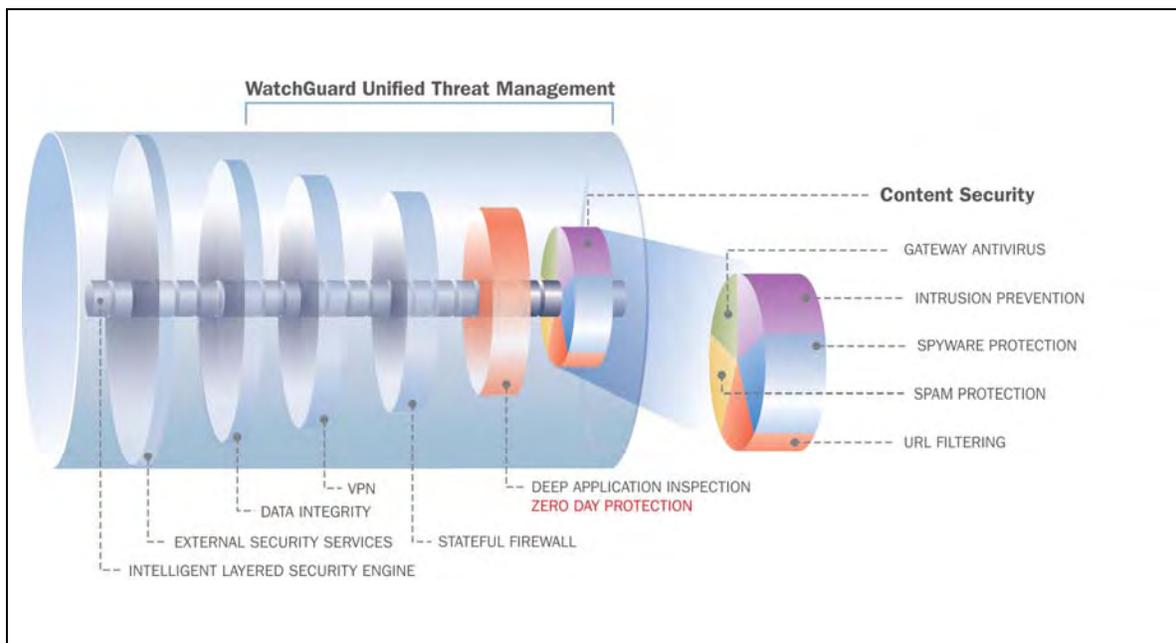
For maximum security, any layer can place the incoming Internet address in the firewall's blocklist – a "penalty box" for misbehaving connections. With this autoblock capability enabled, a WatchGuard firewall drops all further packets from that address for a period of time. This adds

an especially effective element for enforcing zero day security, since few hacking attempts – even previously unknown ones – can proceed without triggering suspicion at some level.

In addition, all firewalls must leave some ports open. These open ports allow access to universal services such as web or email. An attacker probing the open ports for vulnerable servers and services is one of the first signs of an intrusion. A WatchGuard firewall set to autoblock not only denies the probe, but might also send back a response that reports the target doesn't exist. In fact, white hats typically find it difficult or impossible to do a penetration test or security audit of a network protected by a well-configured WatchGuard firewall.

Out on the Border

Think of a packet passing through a firewall as a vehicle at a border crossing. A packet inspection firewall can ask the driver where he's coming from, where he's going, and what he's going to do when he gets there. A stateful inspection firewall does a little more – it can also consider the flow of the conversation, and whether something doesn't seem quite right. If the firewall applies signatures, it can look inside the car, and compare what it sees against a list of contents deemed illegal.

A WatchGuard application proxy firewall with intelligent layered security conducts the same conversation. Then it opens the glove box, pops open the hood, and looks under the seats. It looks for loose screws or false panels. At any point along the way, if it finds anything suspicious, it halts the inspection and denies entry. If necessary, it disassembles parts of the car, tearing it completely apart if it has to. Then, if everything is legal, it puts the car back together and sends it on its way, running better than ever before. All in much, much less than the blink of an eye.

Meeting the Zero Day Challenge

Security is a balancing act between access and security. The most secure network is one that no one can access. At the other extreme, unlimited access is a strategy for disaster. Striking the right balance is a task for IT personnel who understand their organization's needs for effective defense, weighed against the needs of their users.

This is the only approach that can rise to the challenge of the today's hackers. They are incredibly resourceful, technically skilled, and handsomely rewarded for their efforts. They are constantly refining their techniques, and their attacks are swifter and stealthier than even before. A conventional reactive security stance, based on packet filters and signatures, is powerless against the new generation of sophisticated zero day attacks.

Thwarting zero day attacks calls for a proactive security posture that detects and blocks attacks at multiple levels, looks deep into the application layer when necessary, and allows only known good traffic to pass. A firewall that meets those requirements is not only highly protective right out of the gate, but can also be tuned to achieve zero day protection while balancing organizational needs for security and access.

WatchGuard firewalls deliver that protection. For more information about WatchGuard security solutions, visit us at www.watchguard.com, or contact your reseller.

[1] Cooperative Association for Internet Data Analysis (www.caida.org), "The Spread of the Code-Red Worm (CRv2)"

[2] Cooperative Association for Internet Data Analysis (www.caida.org), "The Spread of the Sapphire/Slammer Worm"

[3] MessageLabs Intelligence: 2007 Annual Security Report, p. 12

[4] Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, p. 3

[5] Current statistics are at http://nvd.nist.gov

[6] Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, p. 2

[7] *Microsoft Security Intelligence Report, January through June 2007, Key Findings Summary*, p. 7-8

[8] Current statistics are at http://www.shadowserver.org

[9] *Symantec Internet Security Threat Report: Trends for January-June 07*, p. 15

[10] Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, p. 13

[11] Computing Technology Industry Association, *Summary: Making the Case for Managed Services – The Business Impacts of IT Problems at SMBs*

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest product line – the WatchGuard SSL – makes secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

Part. No. WGCE66521_032608