

The Changing Threat Landscape

by: Oliver Friedrichs, 08/03/2004

<http://www.securitydocs.com/library/2433>

Although Symantec's Internet Security Threat Report confirms a significant increase in 2003 of malicious code that exposes confidential data, enterprise security is evolving to meet the challenge of these cyber attacks. A firewall is no longer just a firewall as newer software includes VPN tunneling and antivirus capabilities. Security point products are being integrated into multi-function security appliances for comprehensive protection. Early warning solutions have emerged that provide 'heads-up' notification of vulnerabilities and precursor threat activity with actionable guidance prior to full-fledged attacks. And more and more companies are choosing to co-source their security device monitoring and management to trusted security providers.

However, the challenge still looms as threats continue to grow in sophistication and intensity. Over 60,000 computer viruses have been identified in the wild with more than 1,700 new Win32 viruses being documented in the second half of 2003. There were more than 2,600 vulnerabilities discovered in 2003—an average of seven per day. And not only are threats to the security of the Internet increasing, but they're also speeding across the Net faster than ever, making it increasingly difficult to defend against them.

Information Security's Challenge

The period of time between the announcement of a vulnerability and the release of an associated exploit continues to shrink, making it increasingly likely that we will see a so-called "zero-day" threat. A zero-day blended threat (i.e., one that uses multiple methods and techniques to spread) could target a vulnerability before that vulnerability is announced and a patch made available. Until the worm outbreaks of August 2003, exploits generally didn't emerge until months (or even years) after a vulnerability had been publicly disclosed. That window is now shrinking -- fast. In fact, last year's Blaster worm used a well-known Microsoft security flaw that had been announced only 26 days earlier. The recent Sasser worm, which began spreading widely on May 1, exploited a hole in a component of the Windows operating system for which Microsoft issued a patch on April 13. The high-profile Code Red threat, released in mid-2001, doubled its infection rate every 37 minutes. Less than two years later, the Slammer worm, which arrived in January of 2003, doubled its infection rate every 8.5 seconds. At this rate, Slammer was able to infect 90% of unprotected servers across the Internet in just 10 minutes. The recent MyDoom worm infected email systems across the world -- at its peak, one out of every 12 emails on the Internet carried MyDoom.

Some traditional security approaches validate the need for advancements. Most current intrusion-detection systems are signature-based and cannot detect zero-day attacks. They can detect only attacks that they're programmed to recognize -- that is, for which they already have signatures. With the threat of zero-day attacks, corporations can't wait for signatures to be developed and installed. Even though security companies have improved their response time from what used to be days or weeks to just hours, the fact remains that the fastest worms now spread more quickly than security companies can respond to with traditional point defenses. It is clear that enterprises need to find fundamentally new ways to protect themselves. What proactive defensive measures might they adopt?

Four promising strategies

Let's look briefly at four strategies that could enable enterprises to stop fast-spreading malicious threats before they penetrate the network.

- **Behavior blocking.** The idea here is to monitor the behaviors of running applications in real-time and block program activity that appears malicious. Consider this analogy from the real world: how do drugs stop viruses in the human body? Viruses typically infect human cells by locating a point on the cell that has a specific shape and then “docking” with that point to inject the viral genes. Such a docking point can be visualized as a piece of a puzzle, for which the virus has a complementary fitting piece. Once the virus docks, the cell opens up and the virus can inject itself. Today’s most advanced antiviral medications work by blocking the docking point on either the cell or the virus, to prevent it from docking with the cell and injecting its genes. With behavior blocking technology, the same thing is done to computer viruses and worms. In this case, key system APIs are blocked -- analogous to the docking points that the worm needs to spread and survive. Without these APIs, the lifecycle of the worm is disrupted.
- **Protocol anomaly protection.** This strategy attempts to stop threats before they ever get onto a machine and cause damage. Many attacks target protocols such as Telnet, HTTP, RPC, and SMTP. Certain programming errors (such as buffer overflows) are used by attackers to compromise or damage a system. These attacks exploit poor programming practices and are quite common. The idea with protocol anomaly protection is to intercept all network communications -- at the perimeter (the corporate firewall), on the hosts, or even potentially in the routing/switching infrastructure -- and ensure that the data flowing through devices adheres to standard Internet protocols. Many worms will intentionally send invalid (not-up-to-specification) data in order to infiltrate a specific hole (vulnerability) in a target computer. If these “not-up-to-spec” communications are dropped so that they never reach the target computer, the worm will be stopped.
- **Virus throttling.** The idea behind this technique, developed by researchers at Hewlett-Packard, is to “sacrifice” a small number of machines for the greater good of the network. In practical terms, most computers regularly interact with a very small group of other computers (for example, the mail server, a few Web servers, the DNS server). Further, most computers don’t establish numerous connections to entirely new computers very often – less than once per second in most cases. Therefore, the HP researchers built a throttling system that automatically limits the number of connections to new computers to one per second. All connections to machines that are already part of the circle of regularly used machines are able to go through without delay, but connections to new computers are “rate limited.” Since threats like Nimda, Code Red, and Blaster basically chose random network addresses, they initiated many new connections to new computers, which is highly anomalous behavior. HP’s technology would limit the spread of those types of threats significantly. Nimda established between 300 and 400 new connections per second. Similarly, Blaster sent 850 packets per second. If rate limited, those threats would not be able to send more than one packet per second, which would drastically slow down or even stop their propagation.
- **Generic exploit blocking.** This technique attempts to protect a new vulnerability against any future attack on that vulnerability. By way of analogy, consider a padlock. Each lock has a set of internal pins that limit the shape of keys that can open the lock. If we examine the set of pins in a lock, we can characterize what a key must look like if it is to be able to open the lock; and we can do this without ever seeing an actual key that opens the lock. We can then use the “shape” of the lock to block any attempt to open the lock no matter what the key looks like. Similarly, any time a new vulnerability is released, researchers can characterize the “shape” of that vulnerability. In other words, they can describe the specific stream of data that must be sent over the network to the vulnerable computer to have any chance of exploiting the vulnerability. Once we have such a characterization, we can produce a signature for this shape that can detect and block any attack (e.g., a worm) that has this telltale “shape.” Generic exploit blocking is sometimes referred to as “generic patching” because the technology provides protection against new vulnerabilities without requiring users to immediately deploy software patches.

Securing the Next Generation

Another finding from the Internet Security Threat Report dramatizes why technologies such as those just described are needed today: critical infrastructure and businesses with significant financial resources are experiencing a high severe attack rate. Indeed, financial services, healthcare, and power and energy were among the sectors hardest hit by severe events in 2003.

Consider power providers. Today, most of the electric utilities in the United States are conducting business on the Internet backbone. That means they're using the Internet or Internet-reachable machines to trade electricity, and any of those machines could be compromised by a fast-spreading new threat. Major telecommunications providers, meanwhile, are migrating more and more telephone service onto the Internet. In December 2003, AT&T, Qwest Communications, and Time Warner Cable all announced plans to roll out voice-over-Internet-protocol (or VOIP) technology. But a simple worm that caused even moderate network congestion could devastate traditional phone service that relied on the Internet.

As the Internet continues to control key aspects of our everyday lives, it is essential that enterprises explore strategies such as those described above in order to protect this global network – and themselves. Only through such approaches will the next generation of Internet computing be secure.

Oliver Friedrichs is a senior manager at Symantec Security Response, where he oversees the development of Symantec DeepSight Threat Management System, which notifies customers of global viruses, hackers or blended threats, and collects data about the assaults as they happen.