

Computer Technology Review®

TECHNOLOGY SOLUTIONS FOR SYSTEMS INTEGRATORS, VARS & OEMS

The Threat from Within: The Evolution of Cyber Attacks

By Michael Rothschild

Since the dawn of computer networking, there has been an ongoing game of cat and mouse between hackers and network security engineers. Hackers continuously refine their attacking methods, while network security engineers continue to deploy technology to foil the hackers' attempts and keep the network secure. Attack vectors in the early 1980's were not particularly sophisticated, yet required the hacker to possess an incredible amount of knowledge in order to launch these relatively low level attacks. Hackers were primarily fringe loners looking to simply disrupt operations and gain notoriety in the hacking underworld.

Today, significantly more sophisticated and damaging attacks plague networks. These new and sophisticated attacks are stealthy and strike in the form of zero day attacks, worm storms and targeted attacks. Hackers are no longer fringe elements, but rather organized, career criminals that launch precision or targeted attacks in order to hold for ransom, destroy and steal information — all with a financial profit in mind.

What Is Hitting My Network?

The sophisticated attacks which are commonly affecting networks today primarily fit into four categories.

Zero-Day Attacks – The vast majority of security products today rely on attack signatures, a “fingerprint” by which the product can identify and stop the attack. Zero-day attacks are designed to take advantage of a vulnerability that is unprotected until a signature is isolated, produced and deployed. Hackers taking advantage of this seven to 30 hour window have a very easy and effective way to fly under the radar of most security products. Examples of these attacks include Slammer, Sasser and a number of attacks exploiting Microsoft vulnerabilities including Zotob.

Known Attacks – These are attacks that are already in the “wild” but continue to plague networks. This may be due to new variants that are released or more commonly because enterprises have not deployed the new signatures or patches in order to be protected against the specific attack. In some cases, network devices cannot be taken off-line to be patched which leaves them vulnerable indefinitely.

Targeted Attacks – Whereas hackers used to cast a wide net and attacked any and all available networks, today's methods employ a surgically precise method. When hackers target specific industries or companies, the typical seven to thirty hour time frame needed to isolate, produce and deploy a signature or patch may stretch from days to weeks. Because of its targeted nature, it is harder for security vendors to isolate the attack thereby giving the hacker more time to do damage. Recent targeted attacks included those launched against The UK Ministry of Defense, eGold, RIAA and others.

Worm Storms – Worm storms may be unleashed at any time. Some have signatures associated with them and others don't. Typically, these worm storms are released with fast self propagation built in. Worm storms are particularly effective when hackers use a zero-day attack to spread the attack as there is no patch or signature to impede their propagation. It is not uncommon for worms to release many variants in rapid succession and be able to circumnavigate the globe in hours whereas it used to take days to weeks. Such worms also may include a timed detonation. In such cases, the worm infects the computer at any time, yet

wreaks havoc at a specific predefined date and time in order to have maximum impact.

The Fallacy of Protecting the Gates

Back in the days of old, castles and villages were protected with thick walls, a drawbridge, and a moat to protect the perimeter of the castle. The mindset was that the “bad” would always come from the outside. The security design in most of our networks comes from the same mindset, where perimeter defense is deemed essential in order to protect the network from being attacked. As a result, the multilayered security which we have dutifully deployed is outward facing with nothing protecting us from the evil that lurks in our midst.

A recent study released by the US Secret Service and CERT indicates that a substantial network security threat actually initiates from within. Whether taking advantage of known vulnerabilities, unguarded modems, VPN access, default passwords or passwords which should have been disabled, our own virtual castle is at risk from security threats in our midst. The US Secret Service/CERT report indicates that “75 percent of the insider (attacks) were identified through manual procedures only”, meaning that no

security device actually detected the attack. 42 of the attacks were found through system failure which by all measures indicated that the castle had been sacked.

By faithfully relying on security devices that (a) protect the network perimeter and (b) rely on signature-based technology, the hackers have now devised attacks to take advantage of this paradigm. The storm is just over the horizon, but the evil lurks within.

Best Practices for Internal Network Defense

In order to avoid the brewing cyber security storm an Internal Network Defense device needs to be deployed. There are several crucial requirements to keep in mind when selecting and deploying an Internal Network Defense security device.

Internal Deployment – Though your perimeter is probably adequately protected using a variety of technologies such as firewalls, anti-virus, IDS and IPS, none of these products are addressing (or were designed to address) the attacks that occur internally. It is essential that the solution must protect the internal network for attacks that occur from within.

Speed and Accuracy – Attacks are propagating across networks at breakneck speed. Waiting for a signature to be produced is out of the question. Other anomaly detection technologies utilize Cisco NetFlow information which can delay detection of attacks from sever-

al minutes to hours. While this is an improvement over waiting for signatures to be generated, there is still a window by which a substantial portion of the network can become infected. As a result, an important requirement is that suspect traffic is stopped immediately within seconds rather than minutes, hours or days. Additionally, the information gleaned from our device must be accurate and actionable without causing false positives or negatives.

Vendor Agnostic – Analysts and network experts alike recommend that security be deployed in a layered, best-of-breed approach. Any vendor that claims that their solution can address all potential security threats (both internal and perimeter threats) should immediately raise suspicions. When considering an Internal Network Defense solution, it should be completely compatible with any and all security solutions which have already been deployed. It should be able to operate without having to make any policy, configuration or architecture changes to the existing network.

Non-Signature Based – Many of the traditional security devices rely on signatures which are easily defeated by the attacks mentioned earlier. As a result, the technology used to address Internal Network Defense must be non-signature based.

Multi-Factor Detection – There are newer generations of

technology on the market which are non-signature based and find attacks by detecting anomalous events within the network. While this method improves detection of some attacks, it alarms in some cases where there is no attack (false positive) while missing other attacks (false negative). As a result, Internal Network Defense technology should never rely on one detection methodology to determine if the traffic in question constitutes an attack. Multiple engines which can take the “network pulse” from several different vantage points are essential. By correlating information gleaned from different detection methodologies, results are considerably more reliable and actionable than relying on just one indicator.

Flexible Active Response – Once the alarm information is timely and accurate, the security device must be able to offer a number of response options including the ability to stop the traffic automatically, manually or on a needed basis (through a panic mode or emergency response). These options empower the network administrator to immediately have traffic stopped without any manual intervention, allow for a review and response posture and allow for a preset panic mode to respond.

Simple Deployment – Finally, deployment should be simple and straightforward. The requirement of many vendors to

deploy inline introduces issues having to do with scalability and redundancy. Inline deployment often also requires major rewiring and routing changes to the network. A good alternative is to look for technologies that can sit out-of-path and interact with the network infrastructure to shut down switch ports or leverage quarantine VLANs when appropriate. It eliminates many of the headaches of having to develop a redundancy plan for security devices that do not offer built in redundancy and eliminates the need to re-architect the network.

The old security response paradigms held by companies must be updated in order to effectively address the new and extremely virulent attacks such as zero-day and targeted attacks, as well as worm storms. It is no longer sufficient to rely on signature-based technologies to address new security concerns and it is no longer plausible to assume that all attacks will come from outside the network. For a company to securely protect its network it needs to deploy best-of-breed internal network defense devices. By following best practices noted above, attacks can be kept out of our virtual castle whether the evil lurks outside or from within. **CTR**

Michael Rothschild is the director of marketing for CounterStorm, Inc. (NY, NY)

www.counterstorm.com



CounterStorm™

CounterStorm, Inc.
15 West 26th Street, 7th Floor
New York, NY 10010
Phone: 212.206.1900
Fax: 212.242.2975

Sales: sales@counterstorm.com

Federal Sales: fedsales@counterstorm.com

Marketing: marketing@counterstorm.com