

The Gathering Storm: The Future of Cyber Attacks

By Dave Zwieback

Cyber attacks are increasing in speed and sophistication, and are causing more damage than ever. Incidents like the widely reported Zotob attacks are severely impacting operations of companies and causing billions of dollars in lost revenues and cleanup costs. Moreover, according to the FBI, the actual damage from cyber attacks is far greater than reportedⁱ.

The main perpetrators of attacks are groups of criminals, who are actively targeting companies in order to disrupt their operations or steal valuable data. To maximize financial gain, criminals are using sophisticated zero-day and targeted attacks that cannot be stopped by commonly deployed security defenses.

Zero-day attacks exploit previously unknown software vulnerabilities. It takes days or weeks for software vendors to release patches and for security vendors to release signature updates, which enable detection of the latest attacks. Until patches and signatures are released and fully deployed, companies remain without protection. The SANS Institute confirms that the time to download and apply critical security patches now exceeds a network's survival time.

Furthermore, it is nearly impossible for vendors to generate signatures or patches in time to protect from targeted attacks. Such attacks are customized to disrupt operations

or steal information from specific companies and industries, and are designed to avoid detection.

Clearly, a cyber security storm is gathering; in fact, by many accounts, it has already begun. Unprepared businesses are seeing their operations interrupted—or even permanently disabled—by successful attacks. To enable business continuity, and prevent costly, widespread damage, companies must implement multi-layer defenses, including effective protection from destructive zero-day attacks.

The Evolution Of Cyber Attacks

Many of today's devastating cyber attacks rely on computer worms to spread and cause damage. A worm is a self-propagating malicious program that replicates from system to system by exploiting software vulnerabilities. The concept of a computer worm dates to 1978, when a prototype was first demonstrated at Xerox PARCⁱⁱ. A decade later, the Morris worm became the first attack to seriously disrupt the small, experimental network called the internet. Unleashed in 2000, the VBS/Loveletter was one of the most destructive worms in history, causing more than 10 billion dollars in damageⁱⁱⁱ.

While a decade ago worms appeared months after vulnerabilities were discovered, today's zero-day attacks exploit

vulnerabilities within hours of—and in some cases, hours prior to—their disclosure. While the time-to-exploit has decreased by *at least* a factor of 30, the time required to protect from vulnerabilities has not decreased as substantially. It still routinely takes vendors days to release patches or signatures for critical vulnerabilities, and in large environments it takes even longer to deploy them. As a result, until such patches and signatures are released and fully deployed, companies are defenseless against attacks.

An even more troubling recent development is the emergence of targeted attacks, which aim to disrupt operations or steal valuable information from individual companies or businesses in a particular industry. Targeted attacks often rely on zero-day vulnerabilities, but unlike the headline-grabbing worm storms, they are usually stealthy, making them difficult to detect. As a result, it takes software and security vendors even longer to offer any protection.

In a recent example, an outsider was able to quietly access to as many as 40 million credit and debit cards from CardSystems Solutions using a targeted attack that was undetected for over a year.^{ivv} In addition to impacting millions of cardholders, this attack has effectively put CardSystems Solutions out of business. Other examples of recent targeted attacks include the industrial espionage case in Israel^{vi}, and the ongoing attempts by foreign entities to steal sensitive information from US government agencies and companies^{vii}.

The future of cyber attacks is clear: they are increasing in number and speed, are becoming more targeted and difficult to detect, and are causing more damage. Although Zotob is considered a relatively mild attack, it still cost companies \$100,000

on average to clean up after it^{viii}. This figure does not include damage due to business interruption.

The Causes Of The Storm

Profit-seeking groups of criminals are the driving force behind many of today's attacks, and the major cause of increased attack frequency, sophistication and resulting damage. Cyber thugs commonly use extortion to force their targets to pay or face attacks intended to cripple the business. Moreover, computer criminals are available for hire, and are used by unscrupulous businesses to disrupt operations of their competitors or conduct industrial espionage.

The other major factor in the severe impact of network attacks is the platform monoculture that pervades most companies today. 90% of all computers run a Windows-based operating system, and most users also rely on an office suite and internet browser made by Microsoft^x. The dramatic success of attacks such as the Sobig and Blaster worms, which resulted in the largest downtime and clean-up costs in history, is a direct consequence of platform homogeneity.

Another factor contributing to the gathering storm is ever-increasing software complexity. For example, a recent version of Windows contained 40 million lines of code^x. There are typically 2 defects found in every thousand lines of code, so any large system has thousands of bugs of varying severity^{xi}. Even if a small percentage of all defects present a security risk, every release of software invariably includes new vulnerabilities will be found and exploited, especially since criminals groups are now conducting vulnerability research professionally.

Moreover, to stay competitive, businesses are becoming more reliant on a mobile, geographically dispersed workforce, and require open networks with suppliers, customers and partners. A compromised laptop can be the source of especially dangerous attacks, because it often has complete access to internal, trusted networks.

To further exacerbate the situation, currently deployed defenses are unable to curtail zero-day and targeted attacks. Perimeter defenses such as firewalls, proxies and content filters are powerless to stop even known attacks that originate and spread inside trusted networks. Patch management and signature-based systems (IDS/IPS, anti-virus) cannot detect zero-day attacks. Host-based solutions must be installed on *all* vulnerable hosts to offer effective protection, a time-consuming goal which is not realistically achievable given the prevalence of mobile and third-party devices on today's networks. Even network-based anomaly detection systems do not respond in time to prevent widespread, costly damage.

In The Eye Of The Storm: The Impact

Without appropriate defenses, cyber attacks are continuing to cause damage, severely impacting business continuity and daily operations of many companies. In fact, critical infrastructure such as banking, transportation, and healthcare systems is at risk. The Sasser worm disabled X-ray machines, forcing an attacked hospital to redirect emergency patients. mi2g analysts report that a few of the more publicly known attacks of 2003 such as Sobig and Klez caused over 80 billion dollars in clean-up costs worldwide.

The impact of network attacks is increasing as criminal groups target specific companies and industries with a barrage more sophisticated and malicious than ever before. Unprepared companies may be forced out of business as a result of these attacks, or lose considerable value due to stolen intellectual property or degraded operations. Furthermore, there is evidence that nation-states possess the tools and know-how required to attacks other countries' critical infrastructure.

Preventing The Storm

In order to prevent the storm, a layered defense is required, which must include conscientiously applied protection at the perimeter, on the network interior, and at the host. Moreover, a critical component of a successful defense-in-depth strategy must include systems that constantly monitor network traffic and can identify known, zero-day and stealthy targeted attacks without relying on signatures. Because time-to-exploit is getting shorter, such systems must have automatic defense capability to stop attacks in seconds without human intervention, preventing widespread damage.

The CounterStorm Solution

CounterStorm provides immediate defense against network attacks. CounterStorm-1 is the only network security appliance that detects and stops zero-day and targeted attacks in seconds. Through a unique correlation of behavioral attack recognition, anomaly detection and a dynamic honeypot, CounterStorm-1 immediately quarantines affected machines, preventing widespread damage. Companies already using CounterStorm-1 have realized significant cost savings, limited network downtime and increased protection of valuable corporate assets.

CounterStorm-1 deployment will:

- Enable operational continuity and reduce network downtime by working in an active and real-time mode to stop attacks in seconds and keep vital IT services and networks running during attacks.
- Protect critical information and assets by reinforcing existing security infrastructure and promoting a best of breed approach. This is achieved by integrating with and strengthening current network security investments, adding an additional layer of security to high-value and mission-critical information assets.
- Decrease administrative burden with flexible automated responses and centralized, web-based management and forensic/drill-down reporting, saving time and effort by dramatically reducing daily preparation and monitoring requirements.
- Lower IT costs by preventing costly, widespread damage and greatly reducing investigation as well as cleanup costs.

CounterStorm has developed its advanced patent-pending technologies under research grants from the Defense Advanced Research Projects Agency (DARPA) and the U.S. Department of Homeland Security. A recognized leader in network security, CounterStorm won two concurrent Small Business Innovation Research (SBIR) awards from DHS--the first time in DHS history two Phase II SBIR grants were awarded simultaneously.

CounterStorm's solutions are deployed in large financial organizations, healthcare institutions, media services, academic institutions, federal and local government

agencies, military agencies, and other leading organizations.

Conclusion

To reduce the risk of successful attack, many organizations have implemented comprehensive defense-in-depth security initiatives, yet most remain unprotected from increasingly destructive known, zero-day and targeted attacks, especially those that originate inside trusted networks. To reduce the risk of successful zero-day and targeted attacks, organizations must deploy network security solutions for the network interior that accurately identify malicious intent within seconds, and automatically stop today's and tomorrow's attacks.

About the Author

Dave Zwieback

Dave is the Technical Director of inkcom, which specializes in infrastructure and security architecture. He can be reached at zwieback@inkcom.com.

© 2005 CounterStorm, Inc.

May not be reproduced without the express written permission from CounterStorm, Inc.

Bibliography

- ⁱ Red Herring. FBI Gets Tough on Cyber-Crime. September 26, 2005. <http://www.redherring.com/Article.aspx?a=13728>
- ⁱⁱ Xerox Palo Alto Research Center. PARC History. August 12, 2003. <http://www.parc.xerox.com/about/history/default.html>
- ⁱⁱⁱ Wikipedia.org. Timeline of notable computer viruses and worms. November 1, 2005. http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms
- ^{iv} Sullivan, Andy. Hackers score big by thinking small, experts say. June 21, 2005. <http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,102654,00.html?source=x1545>
- ^v Marlin, Steven. Unauthorized Data Access At CardSystems Began In April 2004, Bank Says. July 22, 2005 <http://informationweek.com/story/showArticle.jhtml?articleID=166401530>
- ^{vi} Millard, Elizabeth. Spyware as Corporate Espionage Threat. July 19, 2005 http://www.toptechnews.com/news/Spyware-as-Corporate-Espionage-Threat/story.xhtml?story_id=10300A9PHD5P
- ^{vii} US-CERT. Targeted Trojan Email Attacks. July 8, 2005. <http://www.us-cert.gov/cas/techalerts/TA05-189A.html>
- ^{viii} Keizer, Gregg. Summer's Zotob Attack Cost Each Company \$100K To Clean Up. October 26, 2005. <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=172900790>
- ^{ix} w3schools.com. Browser Statistics. November 11, 2005. http://www.w3schools.com/browsers/browsers_stats.asp
- ^x Wikipedia.org. Source lines of code. November 3, 2005. http://en.wikipedia.org/wiki/Source_lines_of_code
- ^{xi} Heinz, Lauren. Preventing Security-Related Defects. November 8, 2005. <http://www.sei.cmu.edu/news-at-sei/features/2002/2q02/feature-1-2q02.htm>