ciphertrust.com

November, 2004

Choose Your Weapon: Fighting the Battle against Zero-Day Virus Threats

Introduction

In January 2004, the computer virus known as "MyDoom" created mass disruption to corporate resources and reputation as it spread quickly through e-mail networks worldwide.

At its peak, MyDoom infected one in every five e-mails transmitted over the Internet.[1] The worm broke records set by previous malware, such as SoBig.F, to become the fastest-spreading virus ever. This incredible propagation speed left many networks vulnerable despite the presence of anti-virus software. Anti-virus programs rely on signatures created by the anti-virus vendor, but this process takes time. The independent testing laboratory AV-test.org found the response times to range from just under seven hours to almost 30 hours[2], with the four leading vendors (Sophos, McAfee, Symantec, and Trend Micro) clocking in at no fewer than 12 hours.

Unfortunately, the speed of MyDoom and subsequent virus and malware attacks ensures that the damage is done by the time the anti-virus vendors have published their signature. For corporations, this means that simply deploying a signature-based solution is no longer good enough. They need to take additional steps to prevent these rapidly deploying new threats, or "Zero-Day" attacks, from causing serious disruption.

Virus and Malware Attack Consequences

Attacks from viruses and other malicious code have serious consequences for businesses and other organizations providing e-mail. These include:

System Downtime

E-mail has evolved to become the primary communication method for most organizations, and the loss of e-mail due to attack can severely affect enterprise operations. Beyond the immediate financial expenses involved in restoring the network, an attack on your enterprise e-mail system can also result in lost hours and days for employees.

Resource Depletion

The costs of cleaning up an e-mail system after an attack are significant. IT teams are forced to spend considerable time and money repairing damage to servers and the network. Worse still is the prospect of checking and cleaning individual workstations.

Administration

In the past, when a new vulnerability was discovered, network administrators scrambled to apply security patches from the makers of their anti-virus software and manually reviewed quarantine lists for virus-infected messages. Software manufacturers release patches so frequently that network administrators cannot reasonably be expected to keep up with them all, particularly within a change-controlled environment. As stated by Gartner Research, "Enterprises will never be able to patch quickly enough. After all, attackers have nothing else to do."[3] The staggering damage caused by recent virus and malware attacks is clear evidence that manual intervention to institute emergency measures or review quarantined messages is rarely effective against rapidly propagating threats.

Compliance and Liability

With the recent Federal regulation of information security policy through legislation such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA)

[1] *http://www.nationmaster.com/encyclopedia/MyDoom*

[2] *http://www.esecurityplanet.com/views/article.php/3316511*

[3] *Pescatore, John - Gartner. "Management Update: Mount a Solid Defense against Worms and Viruses," 9/15/04*

and Sarbanes-Oxley Act (SoX), enterprises are charged with protecting data residing in mail servers and on other internal systems. Security breaches violate these regulations, exposing sensitive data and opening the door to serious sanctions and costly litigation.

Credibility

Falling victim to a Zero-Day attack can also result in lost trust from business partners and customers. According to Gartner, "Enterprises that spread viruses, worms, spam and denial-of-service attacks will find not only that malicious software can hinder their profitability, but also that other businesses will disconnect from them if they are considered to be risky." While an attack may not be your fault, it is most certainly your problem.

Zero-Day Virus Protection

In light of the emergence of rapidly propagating threats, the most critical part of any anti-virus solution is now its ability to identify these new threats, regardless of whether they are viruses, worms, hybrids or something entirely new. Corporations must be sure that they are protected by a solution that detects all malicious threats, even those that have not yet been identified.

Any e-mail security solution designed to protect enterprise networks should consist of multiple technologies designed to ensure that viruses, worms and other malware never get past the gateway. This "cocktail" approach provides multiple levels of defense and should include most, if not all, of the following features:

Attachment Filtering

Attachments frequently contain the "payload" of a virus. Detecting and blocking them at the gateway, before they ever reach the mail server, is critical. "Deep inspection" of all attachments to protect against dangerous file types is absolutely necessary. To ensure accuracy and security, the binary code contained in attachments should be scanned to determine the actual file type, rather than relying on signature files and file extensions. In addition, an effective e-mail security solution should inspect all .zip files before allowing them to pass through the gateway.

Protect end-users from themselves. *E-mail security differs greatly from traditional network security, which uses tools such as firewalls, VPN and intrusion detection. Because e-mail is deemed "safe" traffic, every e-mail – good or bad – passes through the firewall and enters the enterprise network. And because most e-mail threats– spam, phishing, viruses etc. – are sent with a profit motive, spammers and hackers continually create new threats.*

Anomaly Detection

Today's best-of-breed e-mail security appliances identify and respond to abnormal behavior in mail flow. By monitoring "normal" e-mail traffic rates across the Internet, appliances can immediately identify spikes in traffic that are often the first signal of a Zero-Day attack. Once these spikes are recognized, the units can take appropriate action to prevent infiltration of the network.

Anti-Spam

Increasingly, spam is a common carrier of viruses and other malicious code. The techniques used by spammers to evade detection are just as effective for virus writers. An effective anti-spam solution must analyze every characteristic of an e-mail message to differentiate between spam and legitimate messages. By using an array of detection and analysis techniques to "score" messages based on their likelihood of being spam, in addition to providing deep inspection of messages, an effective e-mail security appliance will detect and block viruses and worms that use spamming techniques.

Threat Updates

In order to remain ahead of the multitude of threats that face enterprise e-mail systems, appliances in the field should be fed a constant stream of updates from a central server for the purpose of responding to new threats and continually optimizing the on-board software. Ideally, these updates will be based on data gathered from other active units in different companies and organizations, Internet tracking and scanning, and research and analysis. Some key contributors to automatic updates should include:

Reputation Service – By constantly observing and analyzing e-mail traffic across the Internet, reputation services identify good e-mail sender behavior – those senders who consistently prevent spam, viruses, and other unwanted e-mail from being sent from their servers. An effective reputation service allows e-mail security appliances to achieve higher levels of accuracy in determining good e-mail, thus reducing false positives for their customers.

Bulk E-mail Detection – An efficient bulk e-mail detection service should leverage a network of enterprise users across multiple industries to maintain a database of spam signatures and allow real-time queries.

Content Filtering – Identifies keywords used in virus attacks and provides updated policies to allow immediate response. Content filtering dictionaries are populated with words, phrases, weighted word lists and text patterns, and should be updated frequently.

Secure Platform

An increasingly common technique used in assaults on large corporations is to make a conventional hacker attack on an organization's e-mail defenses prior to a targeted virus attack. E-mail security appliances should protect the entire e-mail system from attack via an e-mail firewall and intrusion prevention capabilities, allowing them to detect and block attacks such as denial-of-service and buffer overflows.

Secure Web-Based Mail

For corporations that use them, corporate WebMail products are another vector of attack for e-mail systems. Any e-mail security appliance that offers WebMail access must ensure that it protects the enterprise from a range of mail threats, including cross-packet attacks, directory traversal attacks, path obfuscation, shell access attacks and database access attacks.

Policy Enforcement

Enforcing content and policy compliance across the entire e-mail system is the first, and quite possibly most important, step to ensuring compliance with federal privacy and security regulations like HIPAA and SOX. By providing comprehensive content filtering, monitoring and reporting capabilities, an effective e-mail security appliance helps corporations improve productivity, reduce liability and save valuable network resources.

Recycled Threats

While Zero-Day protection is the most critical component of effective virus control, a more traditional signature-based anti-virus engine is still necessary. Deployed correctly, this system provides assurance that older, known viruses will not trouble your network. E-mail security appliances that integrate a robust anti-virus solution into their core reduce the administrative

burden of managing multiple platforms and allow anti-virus to become part of a unified e-mail policy.

Conclusion

Protecting e-mail systems from viruses and malware is imperative for enterprises. The threats faced every day by e-mail systems are real, and the consequences of failing to shield the network at the gateway are severe.

An effective e-mail security solution must be able to provide the enterprise with a multi-faceted approach to fighting viruses, worms and other malware. In addition to addressing the dangers posed by viruses and worms such as MyDoom and SoBig.F, anti-virus solutions must also focus on viruses that have already left their mark, yet continue to recycle throughout the Internet. A multi-faceted approach, including attachment filtering, anomaly detection, anti-spam, secure WebMail and a secure platform must be incorporated in order to successfully protect the network on all levels.

About IronMail

IronMail is the leading provider of robust protection to stop viruses and other malware before they reach the mail server. IronMail combines and integrates multiple security technologies to detect and block the most dangerous attacks, virus and malware outbreaks. IronMail Zero-Day Virus Protection is proven, tested every day in the most demanding environments in the world, including businesses, government agencies and educational institutions. IronMail's success as the complete messaging security solution has made CipherTrust the leader in messaging security.

To learn more about IronMail and how it can protect your enterprise e-mail system, visit CipherTrust on the Internet at www.ciphertrust.com.