SONICWALL

EXECUTIVE BRIEF: HOW CYBER CRIMINALS CAN BYPASS YOUR REPUTATION MANAGEMENT

The evolution of reputation management for email security

Abstract

As technology advances, cyber criminals develop new tactics to carry out new attacks. Real-time Blackhole List (RBL) was developed in 1997 and was the foundation of today's DNS-based Blackhole List (DNSBL) format. But cyber criminals carry out attacks that undermine and bypass IP reputation management systems. Hence, it is important to for security professionals to evolve and stay ahead of the curve to prevent these attacks.

How cyber criminals bypass IP based reputation management

As IP reputation systems have grown in popularity, hackers have increasingly focused significant resources towards undermining IP reputation systems. Threat actors are increasingly using phishing emails over spam in order to masquerade as a trusted source and use your corporate email system and your employees against you. Phishers cloak themselves in the guise of trusted partner or friend, and phishing emails are focused on either compromising legitimate mail severs at companies with good reputations, or cracking web mail accounts at ISPs and ASP's, such as Yahoo® or Gmail®. This allows cyber criminals to avoid or delay listing on traditional IP reputation systems by sending bad email mixed with good email from the compromised servers of legitimate businesses.

Although cyber criminals do manipulate their IP addresses, they do not manipulate all aspects of a phishing or spam message uniformly. Like other profit-making entities, cyber criminals cut overhead costs by reducing complexity. They tend to reuse IP addresses, as well as content, layout, hyperlinks and images. This presents an opportunity: an additional defensive layer of reputation identification and management beyond IP addresses alone.

To prepare for future email threats, you must understand the lessons of the past.

How we got here: The evolution of reputation management

The original email reputation management system began with the Real-time Blackhole List (RBL). The very first RBL was developed in 1997 by Paul Vixie for the Mail Abuse Prevention System (MAPS). Referring to a network link that drops rather than forwards incoming traffic, Vixie intended the "blackhole" in this case to drop email traffic from sites that directly sent or enabled spam. The original RBL consisted of a list of suspect sites transmitted to subscribing systems administrators over Border Gateway Protocol (BGP). Subscribers could then apply the list to block TCP/IP traffic from those sites.

While RBL reputations presented a significant step forward in managing spam, it also presented inherent challenges. MAPS meticulously worked to verify sites for accuracy before publishing them to the list. While this helped reduce false positives, it also significantly delayed subscribers' ability to respond to attacks quickly. Over time, MAPS developed RBL clients that integrated with email software to enable administrators to customize their own RBL to reject incoming email on a per-server basis.

The MAPS RBL laid the groundwork for the development of the DNS-based Blackhole List (DNSBL) format. The Domain Name System (DNS) Internet service translates domain names/hostnames to IP addresses (forward DNS) and IP addresses to their associated domain names/hostnames (reverse DNS) with the help of a DNS server. Rather than being simply a discreet list, a DNSBL added multiple standards for dynamically listing and delisting IP addresses. DNSBL service providers could then distribute updated lists via the Internet Domain Name Service (IDNS) using a standardized format. Early developers of DNSBLs added such criteria as whether a sending mail server used potentially exploitable open relays or proxies, or whether a mail server sent spam to a "honey pot" system designed to attract and gather spam for identification and analysis.

Today, there are dozens of DNSBL services available and most email servers can query these services to verify the reputations of IP addresses. However, these services apply different standards for adding, removing or retaining IP addresses on their lists. Subsequently, some service lists may not contain potentially dangerous IP addresses, or erroneously include valid ones.

Conclusion

Emails are a critical threat vector that cyber criminals constantly use to carry out attacks. Phishing emails have been found to be the ground zero for most of the successful attacks on an organization's network. With the rise of spear-phishing and whaling attacks, malicious emails are increasingly indistinguishable from legitimate business communications. Therefore, it is imperative that you evaluate your reputation management to make sure it delivers an effective defense against the emerging email threats.

Learn more. Read our solution brief, "Using advanced reputation management to combat email threats."

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com