

Anti-SPAM Solutions The Next Generation

By Paul Serrano

For obvious reasons, spammers, phishers and virus writers would prefer to hide their identities. They spoof message headers, hide links within message bodies and use countless other techniques to disguise themselves in the hopes of sneaking into Email inboxes and avoiding prosecution. The latest SPAM techniques have become so sophisticated and so varied that there needs to be a new way to counter the threat.

Content Inspection Is Not Enough

Unfortunately, many enterprises rely on an e-mail security solution based solely on message content; identifying the source of a particular message never enters the equation. While this approach is moderately effective when dealing with messages that contain specific spam identifiers, it is completely ineffective at stopping spam that employs new techniques such as header spoofing, embedded links or a myriad of other methods of sneaking past enterprise gateways and into your e-mail inbox.

E-Mail Security with Reputation

A comprehensive approach to e-mail security involves examining both message content AND sender history. By evaluating senders based on their past behavior, a more accurate picture of their intentions and legitimacy can be discerned. Has the sender engaged in spamming, virus distribution or phishing attacks? If they have, an effective reputation system knows and flags the message. Has the sender even been seen before? If not, a reputation system should pay close attention to ensure that the sender is not a "zombie" machine being controlled remotely by a hacker.

Reputation systems add value to corporate e-mail security efforts in multiple areas:

- Increased effectiveness - If a known spammer tries to use a new technique to evade detection, an accurate reputation system will still recognize the origin of the message, causing it to be blocked. E-mail security solutions that do not employ reputation will be unable to maintain their effectiveness against new threats.
- Decreased server load - By identifying and blocking known "bad" IP addresses, reputation systems can reduce the intake of messages into the network by up to 50%. This is critical in handling the constantly increasing load of mail.

Since their inception, reputation systems have advanced significantly, both in concept and in the technology behind them.

Reputation Systems Defined

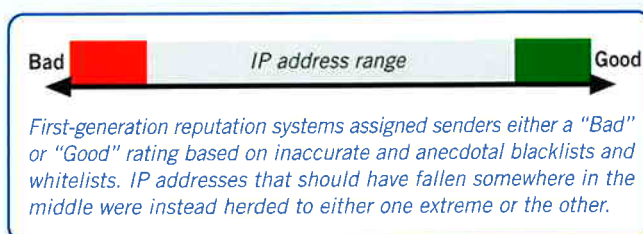
Quite simply, a reputation system keeps track of whether a sender typically engages in good behavior (such as sending legitimate e-mail messages), bad behavior (such as sending spam or malicious code) or something in between. By tracking sender behavior over time, CipherTrust's database of sender reputation is constantly growing and being refined. An examination of the relatively brief history of reputation systems shows a rapid progression:

First-Generation Reputation Systems

In the "early days" of spam (circa 2001), simple blacklists and whitelists (BL/WL) seemed like an appropriate response to the nuisance messages that had begun to show up in inboxes around the world. Blacklists contain the IP addresses of known spammers, phishers and virus senders, and whitelists contain the IP addresses of senders known to be legitimate. Referencing these lists allowed companies to filter a segment of their total mail flow, momentarily curbing the onslaught of spam messages. Practically overnight, the shortcomings of blacklists and whitelists became painfully obvious:

- Black / whitelists are reactive, not proactive, Black / whitelists are anecdotal., Black / whitelists are error-prone, Black / whitelists are slow AND It's not a black-and-white world.

While there are certainly other mitigating factors behind the decline in blacklist and whitelist effectiveness, in the end, the failure of these lists as e-mail security solutions was largely due to their inability to factor message quality into the equation.



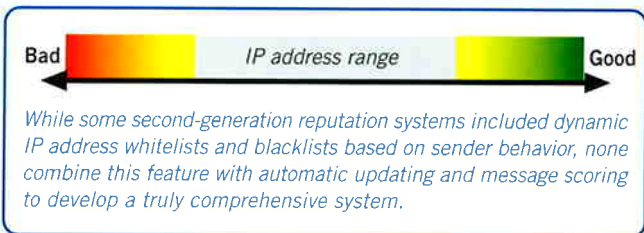
Second-Generation Reputation Systems (2G)

The next iteration of reputation systems built on the failure of blacklists and whitelists to maintain control over the spam flood. While the lists remained an integral component, new features briefly increased 2G reputation systems' efficiency

and effectiveness. With time, however, spammers adapted their habits to evade detection.

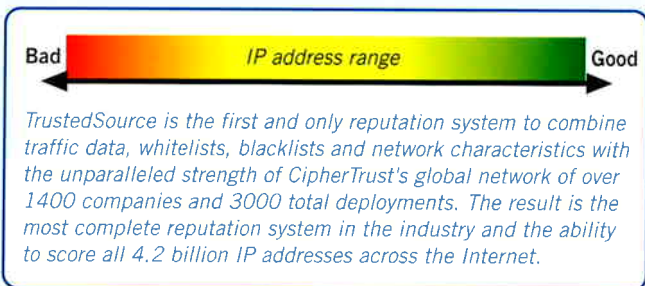
Among improvements seen in second-generation reputation systems were:

- Dynamic lists., Automatic updates AND Message scoring



TrustedSource: The Next Reputation System

Spammers are more clever than ever, so today's reputation systems must be equally sophisticated. An effective reputation system must be dynamic, comprehensive, precise and based on actual enterprise mail traffic in order to keep the spammers from gaining any advantage. To that end, CipherTrust developed TrustedSource, the most precise and comprehensive reputation system available. TrustedSource keeps enterprises ahead of the spammers in the ongoing battle for the inbox by leveraging research generated by CipherTrust's industry-leading network of customers. In developing TrustedSource, CipherTrust has succeeded in defining a reputation for every IP address in use across the Internet (all 4.2 billion!), not just those that have been encountered in the past.



With the largest enterprise customer base in the industry, CipherTrust researchers have access to more data, and more complete data, than any other vendor. With so many units deployed and so much data available to study, researchers were able to extract a sample that accurately represents the flow of e-mail across the entire Internet.

Persistence Testing - Guilty until Proven Innocent

Rather than give the benefit of the doubt to unknown or unfamiliar senders, TrustedSource takes a "guilty until proven innocent" approach to reputation scoring. By examining the frequency with which we have seen e-mail activity from a particular IP address and the quality of the sent messages (via IronMail's Message Profiler), TrustedSource assigns the address a probability of being a spammer or zombie machine that has been taken over by hackers and used to send spam, viruses or

other unwanted messages. Based on information gathered from IronMail units in the field, CipherTrust identified approximately 50 million IP addresses that send approximately 70% of all e-mail on a daily or nearly daily basis. The other 30% comes from IP addresses that have not been previously encountered, and of those messages, over 95% are spam, viruses or other undesirable messages, leading CipherTrust researchers to the conclusion that IP addresses that are encountered for the first time are more than likely zombie machines. CipherTrust typically identifies over 18,000 new zombies an hour using this principle.



Constant Feedback

The more unwanted messages IronMail units encounter, the better they get at detecting and stopping them. TrustedSource provides constant updates on sender status to CipherTrust; these updates are then sent out to other IronMail units in the field via CipherTrust's Threat Response Updates (TRUs), creating a cycle of feedback that benefits all parties involved (except the spammers) and allows IronMail to achieve the highest level of accuracy in distinguishing the good e-mail from the bad.

Conclusion

A traditional e-mail security approach that relies solely on identifying messages based on content and/or characteristics, or an approach that relies solely on blacklists and whitelists, is incapable of generating adequate data about senders. In order to accurately identify messages as wanted or unwanted, corporations must embrace an approach that blends message examination with a comprehensive reputation system like TrustedSource for identifying dangerous IP addresses based on sender history.

By combining the IronMail Message Profiler and the CipherTrust TrustedSource reputation system, IronMail users have a significant advantage over users of other e-mail security solutions; even more importantly, they have an unmatched advantage over spammers, virus writers, phishers and other malicious senders. ■ Paul Serrano is the Senior Marketing Director of Asia Pacific.



The Leader in Messaging Security

www.ciphertrust.com

(852) 2598 9280