

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years, and is uniquely qualified to be the global security solutions provider to organizations of all sizes.

Secure Computing Dynamic Quarantine

Problem

Spammers, virus writers, and malicious hackers are becoming increasingly sophisticated in methods of attacking network systems. The most destructive mechanism typically utilized today is the use of thousands of zombie machines tied together into a single botnet.

The use of zombie machines to send spam and viruses, and to launch DDoS attacks is increasing exponentially. In fact, Secure Computing TrustedSource™ now detects over 240,000 new zombies per day sending unwanted or unauthorized e-mail messages. Virus outbreaks are commonly caused by botnet masters unleashing their zombie machines to send millions of messages containing the virus payload.

Secure Computing TrustedSource tracks all IP addresses sending e-mail from around the world. By monitoring e-mail sending behavior and patterns TrustedSource is able to assign a very accurate, granular reputation score to each address. This reputation score is utilized by all IronMail® appliances to perform a threat assessment of inbound messages, and based on the threat level of the inbound message IronMail will take action to block, throttle, or allow the message to be processed through the IronMail SpamProfiler™.

Zombie machines typically have never sent e-mail and so when an e-mail is received from a zombie machine by an IronMail appliance, TrustedSource occasionally will not have enough information about a sending IP address to make a determination about the threat level posed by a message from that IP address. These messages are categorized as “suspicious.”

During a virus outbreak or spam attack, defensive signatures can be developed once the attack is recognized. Those signatures then need to be disseminated to the e-mail security systems. This can take hours to occur and during this time networks are very vulnerable. To meet these zero-day attacks requires a proactive defensive mechanism to shut down the window of vulnerability.

Solution

Secure Computing Dynamic Quarantine™ is an additional layer of defense to protect networks from suspicious messages sent by zombie machines. Dynamic Quarantine will temporarily hold a suspicious message until an accurate assessment can be made, so that the threat posed by that message can be determined. Holding these messages in Dynamic Quarantine gives TrustedSource time to see if there are multiple copies, identical or similar, of the suspicious message being received from other IronMail appliances around the world, signifying that the message is indeed unwelcome.

The Dynamic Quarantine process works as follows:

- Messages enter the IronMail appliance and a TrustedSource lookup is performed immediately. Known bad messages are dropped and the other messages are passed into the message analysis process.
- The message is broken into its component parts – header, body content, attachments, etc.
- IronMail examines the message component parts, identifying the component parts such as what type of attachment (.doc, .pdf, .zip, etc.) and the size/makeup of those parts.
- Based on the results of the examination of the component parts, IronMail applies rules to determine if the message should be moved to Dynamic Quarantine.
 - These rules will determine how long a message should be quarantined.

