Cisco IronPort Outbreak Filters: Block Hard-to-Detect Email Threats

The Challenge

As global spam volumes decrease, the number of blended threats continues to rise. Traditional email approaches to fighting blended threats are not fully able to address the Internet as an attack vector and are therefore not successful. According to recent data from Cisco Security Intelligence Operations (SIO), there is a dramatic rise in targeted attacks, such as malware; financial and password phishing; advanced persistent threats; and scams involving bank transfers, charities, hotels, and inheritances. These attacks are traditionally difficult to detect since, unlike pharmaceutical and weight control spam, they are sent in low volume (often one or two emails) and contain custom URLs that have not been identified or categorized. Low-volume, targeted attacks are more profitable and harder for security specialists and end users to detect.

The Solution

Cisco IronPort™ Outbreak Filters offer next-generation threat prevention for hard-to-detect email threats. These innovative filters deliver the industry's first solution dedicated to blocking targeted email attacks. Cisco IronPort Outbreak Filters have three primary elements: advanced rule sets, dynamic quarantine, and Outbreak Intelligence from ScanSafe.

Advanced rule sets: Cisco SIO threat researchers manage an extensive set of targeted attack heuristics. Cisco SIO researchers have built the world's largest body of real-life targeted attacks and have studied them to identify significant patterns and common characteristics. This allows Cisco to create and refine rules that better identify never-before-seen threats on the first try.

Dynamic quarantine: Cisco applies current dynamic quarantine capabilities in order to perform deep content and contextual inspection. The dynamic quarantine provides a configurable delay of suspicious messages, which enables an additional layer of protection when a message is first received.

Outbreak Intelligence from ScanSafe: Suspicious links are rewritten so that they point to Outbreak Intelligence for deeper inspection and analysis. Once a user clicks on a link, the dynamic web content runs through our virtualized environment and is scanned to determine any malicious data. This service comprises numerous content analysis scanlets, which analyze every piece of content contained within the web page, including images, files, scripts, and obfuscated code. All content undergoes structural and behavioral analysis to determine if malware is present. If malware is identified, the specific piece of infected content is blocked while the safe content is allowed through to the end user. Rewriting the URL to point to Outbreak Intelligence scanning provides protection for the user, regardless of which device they use to follow the link.

Summary

With the ever changing threat landscape it's even more important for businesses to protect their assets. Cisco is the first vendor to provide real time protection of hard to detect, low volume email born threats. Backed by SIO, Cisco IronPort Outbreak Filters utilizes multi-vector threat protection to provide unmatched email security.

For More Information

Cisco IronPort Email Security Appliances: http://www.cisco.com/en/US/products/ps10154/index.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C78-676366-00 07/11