White Paper

Mitigating Email Virus Attacks

Since the early 1990s, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, over 100 billion corporate email messages are exchanged.[1] With this level of use, email is vital to businesses worldwide.

Email Under Siege

With email at the heart of businesses, security is a top priority. Mass spam campaigns are no longer the only security concern. Today, spam and malware are just part of a complex picture that includes inbound threats and outbound risks.

A Broadening Inbound Threat Landscape

More Organized

Email attacks have become increasingly complex and sophisticated. Skilled criminals now form enterprises to create malware, discover exploits, build kits to install malware, and sell botnet spam networks and DDoS services. Others sell services that make these ventures more successful. To improve deliverability of payloads and malicious links, criminals offer programs that test spam against open-source spam filters as well as low-volume spam-bot networks that stay under the radar of many blacklist services.

More Personal

Attacks have become significantly more targeted as well. By scouring social media websites, criminals find information on intended victims and socially engineer spear phishing emails. These relevant emails targeted to individuals or population segments contain links to websites hosting exploit kits.

Less than 48 hours after the April 15, 2013 Boston Marathon attack, Cisco's blog reported two massive spam campaigns claiming to contain news concerning the attack. The emails led to websites hiding malware behind embedded YouTube videos about the bombings.[2]

[1] The Radicati Group, Inc, *Email Statistics Report,* 2012-2016.
[2] Williams, Craig. *Massive Spam and Malware Campaign Following the Boston Tragedy*, April 2013.

More Exposure

Employees once checked text-based email from a workstation behind a company firewall, but today they interact with rich HTML messages from multiple devices, anytime and anywhere. HTML provides more avenues for blended attacks, while ubiquitous access creates new network entry points that blur the lines of historically segmented security layers.

Outbound Email Risks

The increasing amount of business-sensitive data and personal identifiable information (PII) sent via email means the potential for outbound leakage is great. In March 2012, an employee at the Wayne County Department of Personnel/Human Resources in Michigan mistakenly attached to an email a spreadsheet containing the names, addresses, birth dates, and social security numbers of over 1000 Wayne County employees. The email was sent to about 1300 people, and it is unclear how many people opened the original message.[3]

In many countries, any email with PII must be sent encrypted. If any unauthorized person can read unencrypted emails, an organization is not in compliance with PCI DSS, HIPAA, GLBA, or SOX, depending on the industry. Hundreds of highly variant regulations add to the complexity and importance of outbound control. Most security solutions offer no way for senders to retract a PII violation or know whether recipients have read the message.

The Cost of Inadequate Protection

Given the widespread level of basic protection against unsolicited and malicious email, companies may think they are adequately protected, but new methods are constantly being developed to elude this level of defense. The costs of security breaches then nullify any short term savings gained from settling for basic protection.

In July 2012, the controller of a small fuel supplier in southern Georgia clicked on an image-embedded link in an email appearing to come from the U.S. Postal Service. The email passed basic spam filters and contained no malware attachments, but clicking the embedded link loaded content from a site hosting the BlackHole exploit kit, infecting the controller's PC with the Zeus Trojan. Able to record and export usernames and passwords, the criminals involved transferred over $300,000 out of the company's bank accounts.[4]

Indirect expenses and reputation damage add to the total cost. Table 1 describes the costs per attack to 361 organizations in 2011.[5]

Table 1. Overall Organizational Costs per Attack

Size of Organization	Monetary Loss*	Remediation Cost*	Reputation Cost*
Up to 1000 users	$327	$558	$2,346
From 1000 to 5000 users	$233	$484	$1,436
More than 5000 users	$290	$833	$1,553

* Per infected user.

[3] OSF DataLossDB, *Incident 5895*, March 2012.
[4] Brian Krebs, *Uptick in Cyber Attacks on Small Businesses*, August 2012.
[5] Cisco, *Email Attacks: This Time It's Personal*, June 2011.

Outbound mistakes can damage brand equity, customer trust, and a company's email reputation - a rogue internal sender may drastically reduce an entire company's ability to send email to legitimate recipients. Mistakes may also come with fines for regulation violations. In February 2011, Cignet Health, a hospital in Maryland, received a $4.3 million fine for violations involving 41 patients.[6]

The Challenge

Effective email protection requires a global, multi-protocol threat perspective and an infrastructure that can respond rapidly. Several things must be added: scalability, flexible outbound compliance and encryption capabilities, and the ability to avoid burdensome demands on the infrastructure.

Cisco® Email Security delivers **advanced threat defense, superior data security**, and **simplified management**, while lowering total cost of ownership and reducing administrative effort.

Advanced Threat Defense

Fast and comprehensive email protection using the largest threat detection network in the world

Cisco's defense starts with Security Intelligence Operations (SIO), an in-house threat research team that provides a 24x7 view into global traffic activity. SIO analyzes anomalies, uncovers new threats, and monitors traffic trends; automatic policy updates are then pushed to multi-protocol network devices every three to five minutes.

SIO is constantly tracking over 200 parameters, including:

- SIO Blocklist/Reputation lists domains, URLs, IP addressed and files to be blocked
- Spam traps catch emails that may not pass through Cisco appliances
- Honeypots find attackers so Cisco can analyze their methods
- Crawlers scan the web, making note of malicious content
- Deep files inspections apply analytics to spot malicious content
- Domain/WHOIS information is used to build a database of malicious domains

> "Cisco innovation and insight has led email security for ten years. We have been using their solution campus-wide with great success for a long time. It gives us confidence for the future."
> **— Dr. Damian Bucher, Zentrum für Informationsverarbeitung, Westfälische Wilhelms-Universität Münster, Germany**

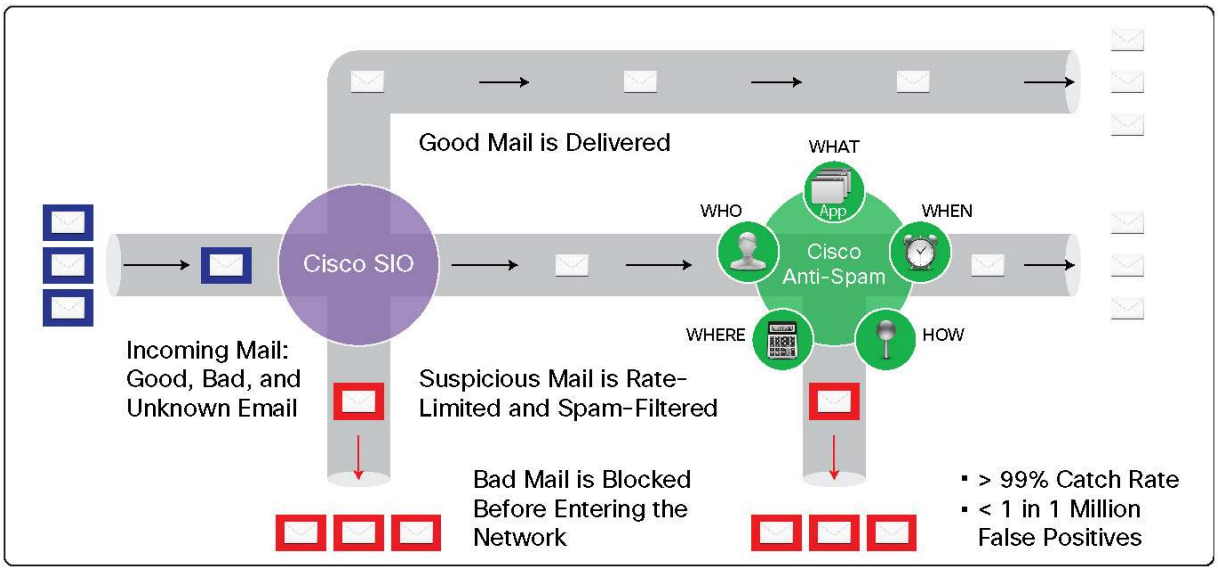
Anti-Spam

The highest spam capture rate, with an industry-low false positive rate of less than one in one million

Spam is a complex problem that demands a sophisticated, multilayer solution. To stop spam from reaching inboxes, Cisco Anti-Spam combines an outer layer of filtering based on the reputation of the sender and an inner layer of filtering that performs a deep analysis of the message. Reputation filtering stops 90 percent of spam before it even enters the network, allowing the solution to scale by analyzing a much smaller payload. Figure 1 shows how Cisco Anti-Spam works.

[6] U.S. Department of Health and Human Services, HHS imposes a $4.3 million civil money penalty for violations of the HIPAA Privacy Rule, February 2011.

Figure 1. Cisco Anti-Spam



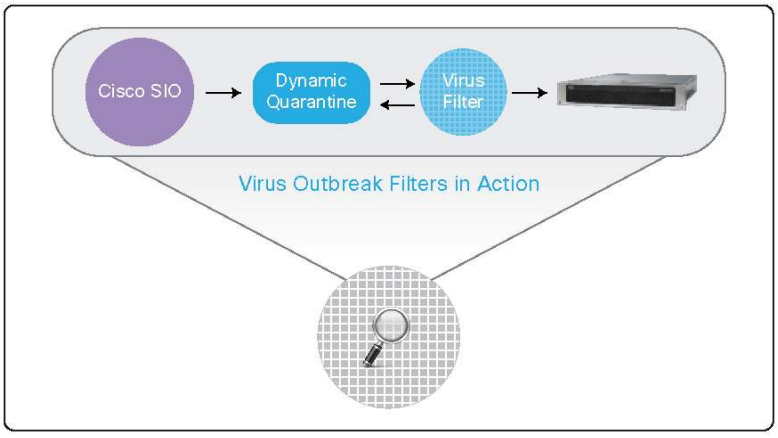
Antivirus

The industry's only proven zero-hour antivirus solution that protects against new viruses in less than 60 minutes

Cisco Virus Outbreak Filters provide a critical first layer of defense against new outbreaks an average of 13 hours ahead of signatures used by traditional reactive antivirus solutions. The Cisco Threat Operations Center (TOC) analyzes SIO data and issues rules to quarantine suspicious messages worldwide (Figure 2). As the TOC learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Messages with attachments are held in quarantine until Sophos or McAfee releases an updated signature.

Find an up-to-date list of the last 20 virus outbreaks: http://tools.cisco.com/security/center/home.x#~alerts.

Figure 2. Cisco Virus Outbreak Filters

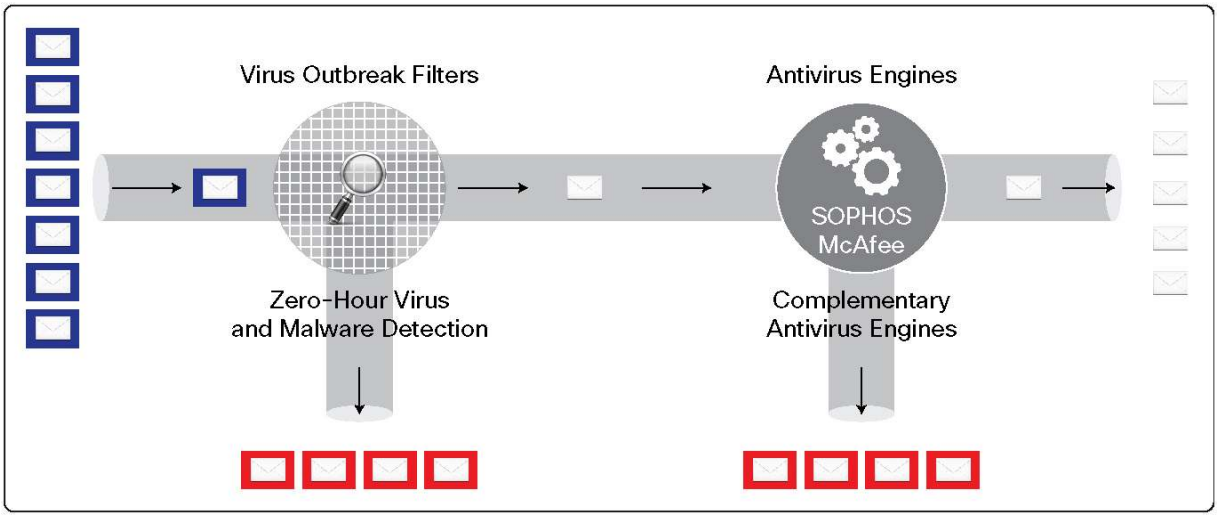


Outbreak Filters also protect against blended threats by rewriting URLs linked in suspicious messages. When clicked, the new URLs redirect the recipient through the Cisco Web Security proxy. The website content is then

actively scanned, and the Outbreak Filters display a splash screen warning the user that the site contains malware.

A choice of antivirus engines and the ability to run them in tandem to dual-scan messages provides the most comprehensive protection (Figure 3).

Figure 3. Cisco Antivirus and Outbreak Filter



Superior Data Security

Effective, accurate, and simple DLP policy enforcement and email encryption

Data Loss Prevention

Zero to compliant in 60 seconds

Data loss prevention (DLP) filters are included with Cisco Email Security solutions. Through Cisco's partnership with RSA, the leader in DLP technology, the email security solution supplies more than 100 predefined policies covering government and private sector and custom company-specific regulations. Remediation choices include BCC, notify, quarantine, and encrypt.

RSA's Information Policy and Classification Research Team created and automatically updates predefined policies with proven methodology for best-in-class accuracy. With a filter such as HIPAA, GLBA, or DSS, outbound email can be automatically scanned and encrypted accordingly.

For companies needing a complex custom policy, the building blocks necessary for customization are readily available and make the process quick and easy.

Encryption

Complete sender control, no extra overhead

The sender of an encrypted message receives a read receipt once a recipient opens a message. Secure replies and secure forwards are automatically encrypted to maintain end to end privacy and control. To recall a message, the sender can lock or expire a key at any time. Cisco Email Security is the only solution to offer per-message, per-recipient encryption key revocation that can be done by either the sender or the admin.

Cisco Registered Envelope Service provides user registration and authentication as a highly available managed service, with no additional infrastructure for clients to deploy. For enhanced security and reduced risk, only the key is stored in the cloud - message content goes straight from the sender's gateway to the recipient.

Simplified Management

Complete control, always up-to-date

A centralized, custom consolidated System Overview dashboard provides system and work queue status, quarantine status, and outbreak activity, among other critical metrics. The centralized quarantine system provides a single location for email users to self-administer their spam quarantines and administrators to manage policy and DLP quarantines.

> "With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam [are] a reality."
> **— Kenichi Tabata, Komatsu Ltd., Japan**

Threat message detection rules and updates apply automatically without down-time or the need for human intervention. The result is hands-off management and superior protection.

Why Cisco

Cisco delivers market-leading solutions at scale and in the method that makes sense for your organization.

Cisco offers the following appliance-based, cloud-based, and hybrid solutions:

Cisco Email Security Appliance (ESA) keeps sensitive data on-premise, with strong performance and easy management.

Cisco Email Security Virtual Appliance (ESAV) provides quicker deployment, scalability on demand, and the operational efficiencies gained from using existing investments.

Cisco Cloud Email Security provides a flexible deployment model for anytime, anywhere email security.

Cisco Hybrid Email Security gives you advanced control of messages on-site while taking advantage of the cost-effective convenience of security in the cloud.

Cisco Managed Email Security provides the performance and security of an on-premise Email Security Appliance with the confidence of Cisco's Threat Operations Center management.

Learn More

Find out more at http://www.cisco.com/go/emailsecurity. Evaluate how Cisco products will work for you with a Cisco sales representative, channel partner or system engineer.

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 C11-728635-01 06/13