Detect and Deflect Targeted Attacks and Zero-Day Threats with Cisco Outbreak Filters

Email-based outbreaks can be devastating. They can overwhelm limited IT resources and quickly bring down whole systems. There's a reason the virus analogy has remained pervasive in IT: Regardless of whether an outbreak is a regional epidemic or full-blown pandemic, once it gets into your system, it can spread fast and bring your system down.

What Is a Virus Outbreak?

Of the email-based attacks that occur on a daily basis, the following criteria qualify for outbreak status:

1. A new malicious attack profile (or a new variant of an existing known attack)
2. Has moderate to significant damage potential
3. Has a widespread distribution (multiple instances identified from varied sources)

If an email-based attack satisfies the above criteria, the Cisco Threat Operations Center (TOC) investigates the incident and issues outbreak rules to protect our customers.

Cost of IT Outbreaks

Although outbreaks in IT no longer grab the headlines as they did with LoveBug and Melissa, they can still cause significant damage—and they continue to be increasingly costly. Leaps in malware evolution, combined with faster exploits of zero-day attacks, have turned some small, isolated incidents into fast-spreading outbreaks.

- 10 Worst Computer Viruses of All Time
- 10 Most Destructive Computer Worms and Viruses Ever, October 12, 2010
- 10 of the Most Costly Computer Viruses of All Time, May 29, 2012

Best Practices for Outbreak Defense

The strength of your IT security posture can make the difference between safe or compromised systems. When investigating outbreaks, epidemiology organizations have developed a set of recommended practices that typically include the following steps:

1. Verify the diagnosis and identify the existence of the outbreak.
2. Map the spread of the outbreak.
3. Develop and implement control and prevention systems.

IT standards boards recommend something similar. Maintaining enterprise security in today's complex and dynamic threat landscape requires ongoing vigilance—and a multilayered defense approach that includes intelligent, context-aware security solutions capable of protecting networks, data, and end users from both known and emerging risks in real time.

Targeted attacks are among the top security concerns for modern enterprises. Cisco Security Intelligence Operations (SIO) has identified the increasing prevalence and correlated impact of these hard-to-detect attacks, including advanced persistent threats (APTs) and spearphishing, also known as targeted attacks. According to recent research by Cisco, the overall annual cost of infections caused by targeted attacks is more than US$1.2 billion.[1] Yet most organizations are unaware of these attacks until they are well under way—and damage is done.

The goal for many cybercriminals—regardless of their preferred method for launching an attack—is stealing data for profit, either by using the data themselves or selling it to a third party. Data targeted for theft ranges from banking credentials to intellectual property to patient health information. In addition, the “big data” that businesses now generate, store, and collect offers a wealth of high-value information that enterprising criminals can surreptitiously collect over time with help from malware and, increasingly, from targeted attacks.

As part of Cisco Email Security, Cisco Outbreak Filters assess the threats of inbound and outbound messages. These filters are the industry’s first custom-built engine dedicated to blocking targeted email attacks utilizing refined rule sets and dynamic quarantine. This paper examines best practices for defending against email-borne outbreaks with this solution.

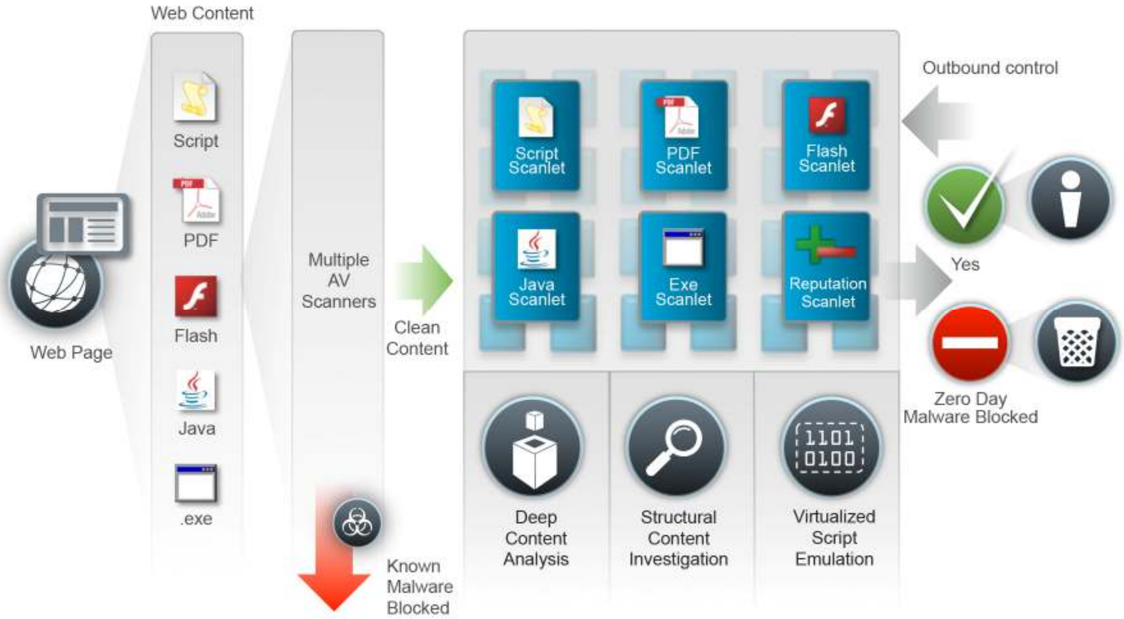
Identifying and Blocking Threats in Real Time

Cisco extends threat protection capability at the gateway. Cisco Outbreak Filters work with Cisco SIO from the cloud to identify and block email-borne threats in Cisco Email Security.

The system scans all inbound and outbound web traffic in real time for new and known web malware by using multiple signature-based antimalware scan engines and multiple heuristic detection engines. Vastly different from traditional signature-based antivirus, this intelligence is based on artificial intelligence (AI), using the billions of web requests it sees per day to learn what web traffic is “good” and “bad.” This intelligence means malware can be blocked without the need to wait for signature updates—and that the window of opportunity for zero-day threats is effectively eliminated.

[1] "Email Attacks: This Time It’s Personal", Cisco, 2011: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

Figure 1. Zero-Day Malware Architecture



As illustrated in Figure 1, when an end user visits a webpage, that page is deconstructed by the intelligence systems in Cisco SIO down to the components on that page, such as HTML, scripts, Flash, and PDFs. Once all web content is passed through multiple antivirus engines to remove known threats, the “clean” traffic is analyzed again in real time in order to identify and block zero-day threats. The system uses “scanlets” to scan each piece of content in parallel using three different techniques designed to accurately detect zero-day malware: deep content analysis, structural content investigation, and virtualized script emulation.

- **Deep content analysis** is the examination of content to identify malicious intent. Through this process, content is compared to the known “normal” statistical model that is kept accurate through AI learning. For example, does an animated GIF have only one frame? Does an image file contain executable code or other anomalous content?
- **Structural content investigation** examines the structure of the content, again looking for signs of potential risk. For example, based on content analyzed by Cisco SIO, it could be determined that a new obfuscated executable file has a 95 percent probability of being malicious. Such a determination is achieved by scanning the page content using various types of scanlets, such as reputation scanlets and scanlets for Flash, Java, PDF, archives, executables, file anomalies, and more. These scanlets run in parallel to ensure high performance.
- **Virtualized script emulation** is especially important for examining dynamic web content such as scripts. Running the script within the cloud infrastructure of the Cisco Outbreak Filters allows for monitoring of malicious behavior, such as a hidden redirect or “drive-by” downloads attempting to edit user settings on a computer. If malicious behavior is detected, the script is blocked and not allowed to pass to the end user.

Cisco Outbreak Filters: Staying Ahead of Targeted Attacks

Targeted email attacks are growing in prevalence following a decline in spam. According to Cisco SIO, spam volume dropped from more than 379 billion messages daily to about 124 billion messages daily between August 2010 and November 2011—levels that had not been seen since 2007.[2] One key factor for this decline was the takedown of major botnets, such as Bredolab and Rustock.

But even before some of the biggest botnets were taken offline, many cybercriminals had started to channel more resources into developing and launching targeted attacks instead of mass spam campaigns. The reason: Targeted scams need only a single response from a recipient to be considered successful, whereas mass spam campaigns require a much higher response rate. Launched primarily via email, targeted attacks represent less than 1 percent of the inbound spam messages that organizations face globally; however, they are very effective in that even highly aware users can fall victim to these scams.

Targeted attacks are categorized as:

- **Advanced persistent threats (APTs):** These messages are sent as part of a broader attack that attempts to break into an organization's network over an extended time period.
- **Spearphishing and whaling:** These messages are targeted toward specific individuals in an attempt to steal money or information. An example is a targeted attack on an organization's accounts payable group in an attempt to install software that steals the organization's banking information.

Targeted attacks use data that can be harvested easily, such as from company websites and social networking sites like Facebook and LinkedIn. By including city names or a target's name, or making an email appear to be from a friend or business associate, attackers increase their chances of success. They know the weakest link in the security chain is the general end user—and that social engineering provides the highest level of returns.

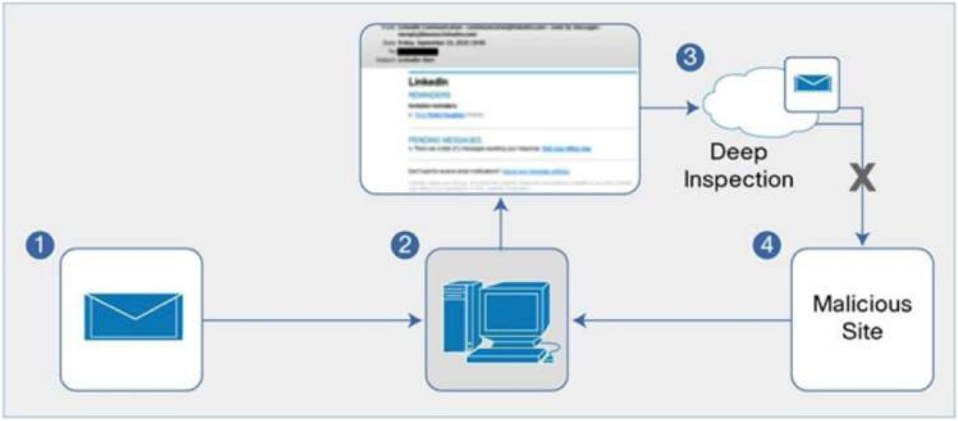
Cisco Outbreak Filters help enterprises detect and deflect targeted attacks through the following:

- **Advanced rule sets:** Cisco SIO threat researchers manage an extensive set of targeted attack heuristics; they have captured 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 to better identify never-before-seen threats on the first try. Targeted attack heuristics combine intelligence gained from Cisco SenderBase and security appliances, as well as content derived from known attacks. This intelligence is used to evaluate various aspects of each message, such as the URLs, headers, and message body, to identify threats within the message. These heuristics work with other Cisco Outbreak Filters rules to determine if a given message is a targeted threat.
- **Dynamic quarantine:** Cisco applies dynamic quarantine to immediately isolate suspicious messages. Quarantined messages are continuously re-evaluated by Cisco Outbreak Filters.

[2] Cisco 2011 Annual Security Report, Cisco, 2011: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

- **Leveraging SIO:** Using Cisco SIO through the cloud, suspicious links in email are rewritten so that they point instead to the cloud-based system for deeper inspection and analysis. (As an example, http://www.threatlink.com would become http://secure-web.cisco.com/auth=X& URL=www.threatlink.com.) Once a user clicks on a link, the dynamic web content runs through Cisco's virtualized environment and is scanned to determine the presence of malicious data. This service comprises numerous content analysis scanlets, which analyze every piece of content contained within the webpage, 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 Cisco Outbreak Filter scanning provides protection for the user, regardless of which device they use—laptop, smartphone, tablet, etc.—to follow the link.

Figure 2. A simple flow of Cisco Outbreak Filters using Cisco Outbreak Intelligence



The basic process of Cisco Outbreak Filters is outlined in Figure 2.

1. An incoming email is scanned by Cisco Outbreak Filters. The refined rule set identifies it as a potential phishing or targeted attack email and handles it as configured on the appliance. By default, a disclaimer is prepended to the email text identifying it as a phish, and the URL contained in the email is rewritten.
2. The email with the rewritten URL is delivered to the user's inbox.
3. If opened, this rewritten email link sends the user to a public proxy where the webpage content is intercepted and scanned in the cloud in real time.
4. If malware is detected on the page, a blocked page message is served up to the user and information about the URL is passed from the Cisco Outbreak Filters system back to Cisco SIO. Otherwise, the user is given a choice: (1) Surf the page through the proxy, (2) or go directly to the site.

What Outbreak Filters Detect

Cisco Outbreak Filters are organized into four categories: malware, phishing, scam, and virus-infected emails. They detect more than 20 different types of commonly used scams. The following list covers some of the types of attacks Cisco Outbreak Filters can detect:

- Phish
- Charity
- Robbed abroad
- Seminar
- Inheritance
- Financial URL
- Bank transfer
- Fake cashier's check
- Money mule
- Loan
- Financial phone
- Fake deal

The list of attack types dynamically changes, keeping up with the current trends that cybercriminals use in their attempts to get users to click on URLs and/or email attachments.

A Proactive, Multilayered Approach to Security

New threats continue to appear at a rapid rate, with several thousands of new types of malware detected each month. Attacks are more targeted and utilize multiple malware variants, diminishing the likelihood of antimalware vendors obtaining every new malware sample for signature development. Email-borne threats are harder to detect because they are sent in low volume and contain custom URLs that have not been identified or categorized. These trends underscore the need for enterprises to practice a more proactive and multilayered approach to securing their network, data, and end users.

Cisco Outbreak Filters are designed to help enterprises defend against threats delivered by email or via the web. Cisco provides the most effective solution against new and known web malware by using a combination of multiple, correlated detection technologies, automated machine-learning heuristics, and the industry's largest web data set. The system analyzes several terabytes of web code each day and has compiled a proprietary web data set that goes back to 2004. Cisco Outbreak Filters dynamically quarantine suspect email messages and use Cisco Outbreak Intelligence to check the safety of URLs, keeping targeted attacks at bay.

Cisco Outbreak Filters are connected to Cisco SIO, the world's largest cloud-based security ecosystem that provides early warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks from today's most sophisticated threats.

Why Cisco?

Security is more critical to your network than ever before. As threats and risks persist, along with concerns about confidentiality and control, security is necessary for providing business continuity, protecting valuable information, maintaining brand reputation, and adopting new technology. A secure network enables your employees to embrace mobility and securely connect to the right information. It also allows your customers and partners to conduct business with you more easily.

No organization understands network security like Cisco. Our market leadership, unmatched threat protection and prevention, innovative products, and longevity make us the right vendor for your security needs.

For More Information

The best way to understand the benefits of using Cisco Outbreak Intelligence or Cisco Outbreak Filters as components of your overall enterprise security strategy is to participate in the Try Before You Buy program for Cisco Email Security. To receive a fully functional evaluation appliance to test in your network, free for 30 days, visit http://www.cisco.com/go/emailsecurity.

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

C11-727467-02 11/13