WHITE PAPER

ASSESSING THE IMPACT OF SPAM ZOMBIES ON BROADBAND SERVICE PROVIDERS

INTRODUCTION

Once considered little more than an annoyance, spam has become an enormous problem affecting Internet users and broadband service providers. Well-known viruses, worms, and Trojan horses get the headlines, but spam is arguably a more pervasive and insidious threat because it affects every Internet user—directly or indirectly—and it lacks a comprehensive solution analogous to antivirus software programs. Spam frustrates users by overloading their e-mail boxes with volumes of useless and unwanted messages.

Beyond the annoyance and inconvenience, spam causes real damage to both users and service providers. "Phishing" scams cause unwary users to reveal valuable personal information such as credit card numbers or passwords, suffering monetary damages as well as losing time and privacy. Spam can carry malicious code viruses such as distributed denial-of-service (DDoS) agents. On the service provider side, spam overloads e-mail servers, delaying or preventing the delivery of legitimate e-mail messages. It uses up bandwidth, ultimately forcing the service provider to invest capital for additional capacity to support legitimate mail crowded out by spam. Spam can cause disruptions to service when service providers are blacklisted as spam sources because of the activities of their users—real or spoofed. And the impact on marketing can be profound: Acquiring a public reputation as a spam source makes it more difficult for a service provider to compete for broadband subscribers in a highly competitive marketplace.

AN OPPORTUNITY TO DIFFERENTIATE SERVICE

Although most users consider spam senders disreputable or worse, they target their anger at the service provider. A common response is "I don't care where it's coming from, I want you to stop it!" One study finds that 74 percent of customers believe that their Internet service provider (ISP) should be responsible for fixing spam problems (Gartner Group). Despite the growing sophistication of e-mail filters and antispamming techniques, the average home and small-business users look to their service provider to ensure spam-free e-mail. They are far from a silent majority: According to *PC Magazine*, AOL alone receives 250,000 spam-related complaints every day.

Spam also represents a business opportunity for the service provider that successfully and creatively addresses the problem. A spam-free ISP can both attract subscribers from other ISPs and develop additional revenue from spam services. In a recent research report, Gartner Group reports that:

- To reduce the amount of spam received, 36 percent of users would switch ISPs.
- As many as 24 percent of users are willing to pay for spam blocking.

ANTISPAM TECHNICAL ALLIANCE LOOKS TO THE SERVICE PROVIDER

The Internet community itself looks to the service provider for answers to spam. The Antispam Technical Alliance has developed technical standards and promotes collaboration in the community to address the spam problem. Their initial set of recommendations[1] target service provider practices with specific suggestions such as:

- Detect and quarantine compromised computers (zombies).

[1] "Antispam Technical Alliance Technology and Policy Proposal," Version 1.0, June 22, 2004

- Implement rate limits on outbound e-mail traffic.
- Develop complaint-reporting systems.

ASSESSING THE SPAM PHENOMENON

The first generation of spammers used the simplest of approaches: Send out thousands or millions of e-mail messages from their own e-mail accounts. Responding to complaints, service providers answered with an equally simple remedy—the user blacklist. Based on mail volumes, subject line and message analysis, and user complaints, the service provider identified spammers and barred them from the network, a simple policy that was easily enforced.

Spammers quickly switched to a new technique using open mail proxies. In brief, an open mail proxy is a server that accepts connections from any network address, acting as a blind intermediary to virtually any other network address. To the recipient (and the intervening network infrastructure), the spam message seems to originate from the mail proxy, effectively masking the sender's true identity. Service providers responded with a second kind of blacklist, this time of known mail servers that were sending spam. In response to the server blacklist, spammers developed an even more sophisticated method of attack—the spam zombie.

By infecting unprotected computers with a Trojan horse program, a spammer effectively recruits an army of unwitting users who can be activated by a remote command to launch a spam attack. Such an attack has characteristics similar to a DDoS attack: The large number of attacking machines makes it difficult or impossible either to identify the source of the attack or to take effective corrective action in real time without causing massive disruptions to legitimate users.

ZOMBIES: PCs HARNESSED FOR MALICIOUS INTENT

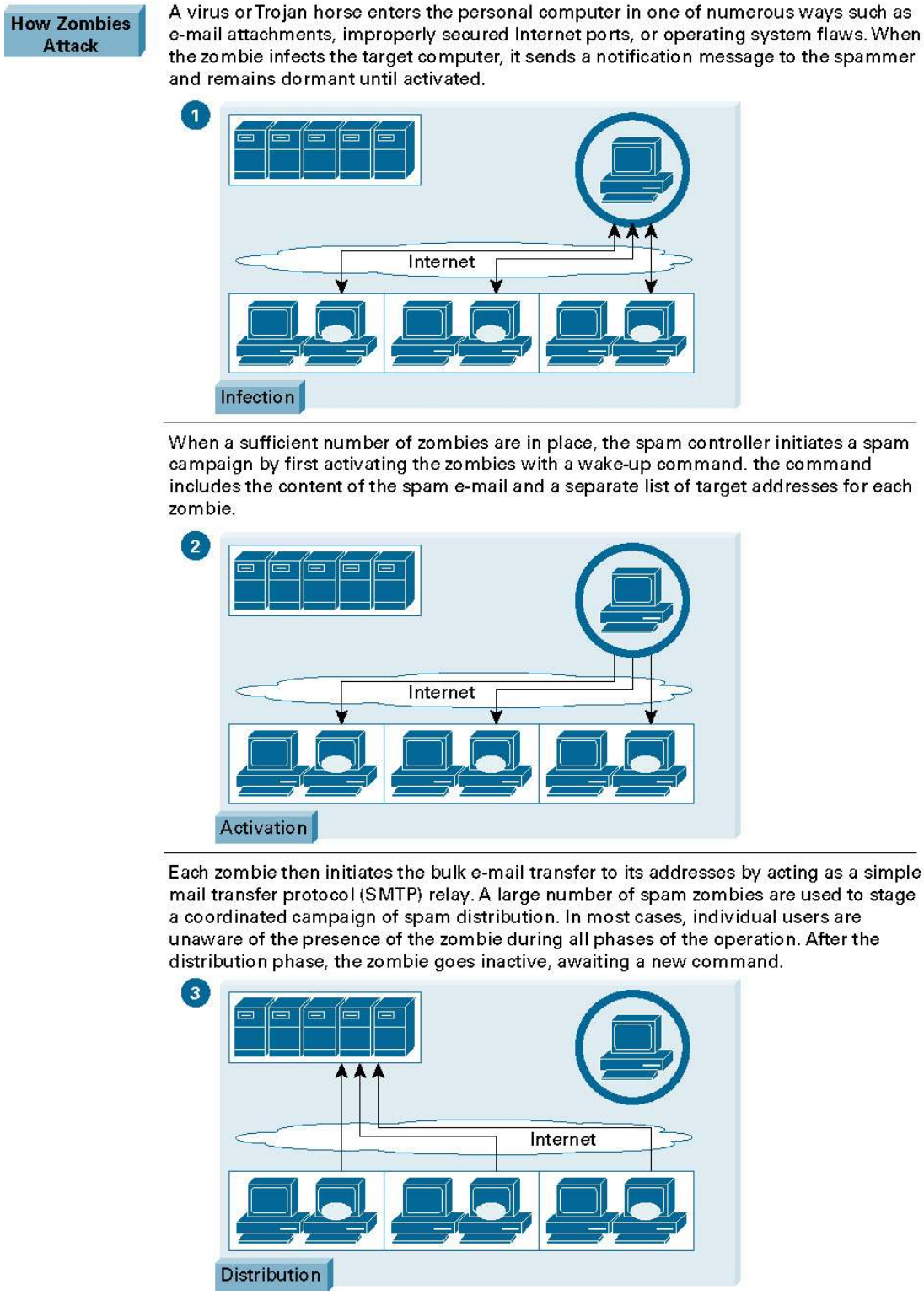
Spam zombies are by far the most insidious method of spamming yet developed. Today's broadband networks are particularly susceptible to zombie infection because many users remain continuously connected to the network, providing opportunities for spammers to discover and attack insecure computers.

Zombies are a massive problem—and the problem is growing. Industry experts estimate that the percentage of infected PCs on broadband networks is at least 1 percent, and may be as high as 10 percent. (Refer to "How Zombies Attack" in Figure 1 for a better understanding of the zombie mechanism.)

BLOCKING SPAM ZOMBIES AT THE SOURCE

With spam zombies becoming the spammers' method of choice to overload and circumvent existing spam protection mechanisms, the Internet community must adapt and develop new strategies to mitigate their negative effect. Although existing spam protection techniques such as black-listing, message text analysis, and filtering provide a means to filter out and remove spam messages when they reach mail servers, broadband service providers need effective solutions that block zombie-generated e-mail messages from ever leaving the broadband access network and reaching their designated mail servers. Such an approach eliminates the significant advantages spam zombies offer spammers—a means to distribute. A spam attack from a multitude of sources that frequently change IP addresses.

Figure 1
How Zombies Attack



Spam zombies deploy techniques that make them very difficult to identify at the mail server because messages originating from a single "spam campaign" are delivered from a vast number of zombie sources. Traditional techniques such as blacklisting or statistical prevention become ineffective, and, although text-pattern detection methods can eventually detect such an attack, the computational resources required to perform such detailed message analysis slows down mail servers in a way that is directly proportional to the size of the attack created.

Identification becomes possible and scales more effectively in the broadband network, which is the source from which the zombies operate. A solution that is capable of transparently monitoring all traffic in the network and efficiently identifying and blocking spam zombie mail without affecting the performance or availability of broadband resources can offer new ways for the Internet community to shut down this insidious distribution technique.

FIGHTING SPAM ZOMBIES WITH CISCO SERVICE CONTROL: A FORENSIC APPROACH

The most effective approach to zombie-driven spam is to identify the offending parties, that is, the PCs that are sending the spam. When infected machines are identified, then the service provider can quarantine them (deny network access) to protect the network and also notify the network users about the infection so that they can take corrective action.

How is the source of the spam identified? Fortunately, although zombies can hide the identity of their true originator, they leave distinctive "fingerprints" in network usage patterns, readable by sophisticated network forensics available with advanced Cisco® Service Control solutions. Their weak point is the number of SMTP sessions they generate as part of a spam campaign. Extensive testing at service provider customers of Cisco Systems® shows that it is technically feasible to develop network rules that can identify zombie attacks in real time to a high degree of reliability.

Identifying a source of zombie spam requires a network element that can monitor network traffic and has the following core capabilities:

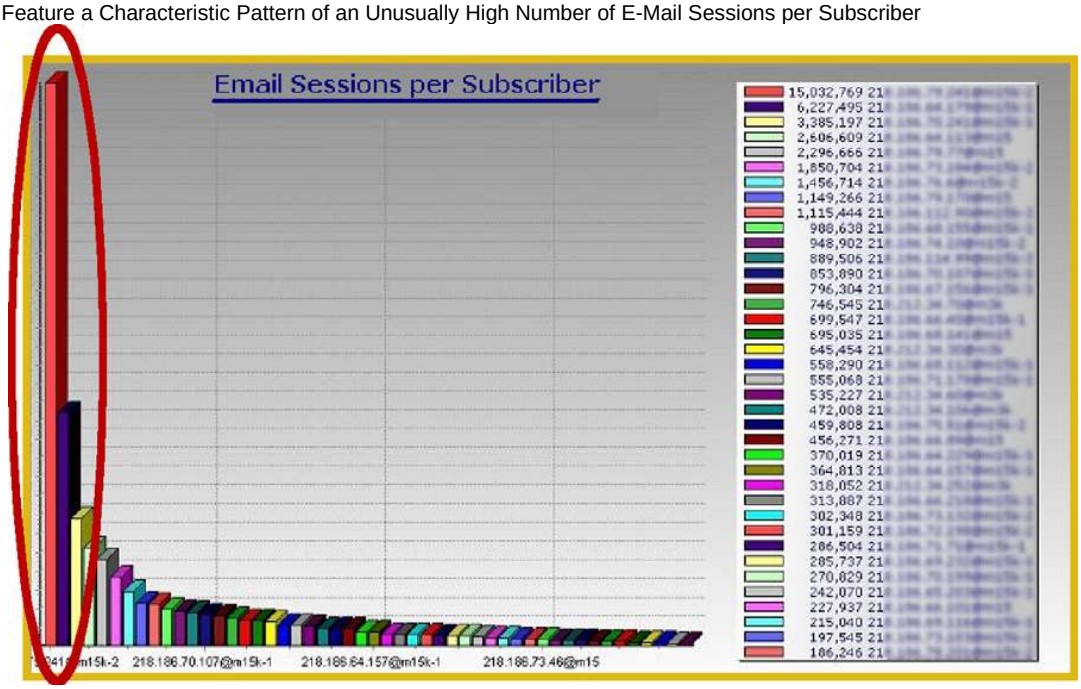
- *Deep packet inspection*—A solution must be able to perform deep packet inspection and classify network packets to SMTP mail protocol flows. Using deep packet inspection, a solution can accurately account for the type of SMTP traffic generated by subscribers and identify suspicious patterns that exist in zombie mail traffic.
- *Maintenance of flow and subscriber state*—When a certain flow of packets is determined to be of the SMTP protocol, the solution must be able to track the total number of such flows generated by a given subscriber. By tracking the number of SMTP sessions, the solution can identify subscribers generating an unreasonable number of sessions demonstrating a zombie pattern, that is, attempting to distribute mail to a large number of recipients.
- *Destination-based classification of e-mail traffic*—To further distinguish between zombie mail traffic and legitimate e-mail, a solution must be able to track the number of destination mail servers an individual subscriber uses in any period of time. This helps distinguish between legitimate activities (use of the ISP's own mail servers or a small set of off-net servers) to zombie activity (use of a multitude of off-net servers).
- *Ability to control traffic of e-mail and HTTP applications*—To create a solution that automates the mitigation process, a solution must be able to control zombie traffic through rate limiting or blocking as well as by using HTTP redirect capabilities to proactively inform subscribers that they have been compromised.
- *Built for performance*—In order to maintain visibility and control of application traffic, as well as respond immediately to suspected e-mail spam, the network element must be purpose-built to manage traffic streams under load. Without this capability, and with the volume of traffic traversing the network, the ability of the solution to manage e-mail spam is quickly compromised.

Deep packet inspection at Layer 4–7 and the ability to maintain "state" is a powerful means to identify anomalies in network traffic generated by spam zombies. Unless a solution can maintain state, it has difficulty spotting such irregularities. Adding state allows a solution to differentiate, for example, between 1000 1-KB messages generated as 1000 independent sessions or a single 1-MB mail session. Stateless solutions can only count packets and cannot easily differentiate between a multitude of small sessions or a single large one. Moreover, by

tracking a subscriber's state across multiple logins, a Cisco Service Control solution can identify spam zombie activity even if it is conducted over multiple subscriber broadband sessions or uses different IP addresses. Stateful application and subscriber awareness allow the service provider to quickly identify spam zombie activity from a particular subscriber, block their e-mail transmissions, and redirect the infected subscriber to a site where the system can be purged of the zombie infection.

Figure 2

Zombie Attacks Feature a Characteristic Pattern of an Unusually High Number of E-Mail Sessions per Subscriber



Service Control Analysis of E-Mail Sessions per Subscriber

PROTECTING NETWORKS FROM SPAM WITH CISCO SERVICE CONTROL

As the spammers move to more sophisticated technologies, so must the service provider. Layer 3 devices lack the intelligence and speed to mount an effective defense. What is needed is an application-aware, powerful network device that can identify the attack, protect the network, and notify the subscriber. Advanced Cisco Service Control technology offers service providers an off-the-shelf tool that can greatly reduce the volume of zombie-generated spam on their networks without costly infrastructure overhauls.

Using stateful deep packet inspection, Cisco Service Control solutions offer service providers a powerful tool in the fight against spam. They have the intelligence and speed needed to identify spam, protect the network, and notify subscribers:

- The solution must be both application- and subscriber-aware. The Cisco Service Control solution monitors and analyzes traffic in more sophisticated ways than Layer 3 devices such as a routers or switches. Furthermore, its comprehensive ability to maintain and manage state provides a quick and efficient method to automate the detection and mitigation of spam zombie activity.
- The solution must operate at multigigabit wire speeds and be able to handle today's high-volume traffic without creating a bandwidth bottleneck, and the Cisco Service Control solution also satisfies this criterion.

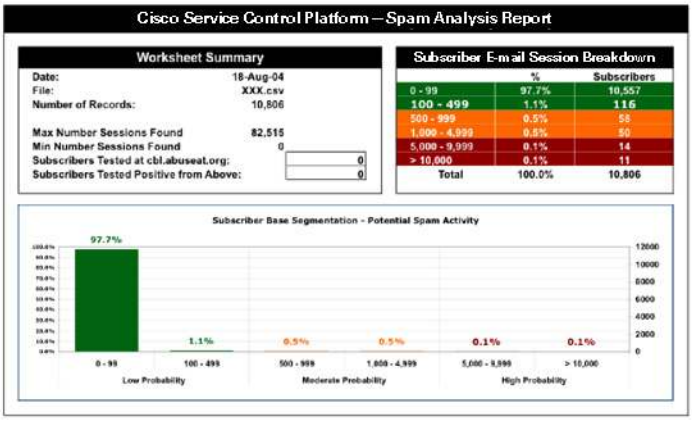
Cisco Service Control can effectively fight zombies using a three-stage approach:

- *Identify* the zombie machines—A Cisco Service Control solution can detect the characteristics of a zombie attack in the early stages, often the first few thousand messages, typically a small percentage of the total targeted number of spam messages.

- *Protect* the network from the attack by quarantining the zombie machines—When a suspicious traffic pattern is identified, action must be taken immediately to minimize the damage. Fast reporting allows the network administrator to intervene during the early stages of an attack and limit the amount of spam that gets through the network.
- *Notify* the users so they can take corrective action—Users whose PCs are infected are unaware of the infection. Therefore, in addition to stopping the zombie attack originating from their machines, the zombie solution should promptly notify the subscribers so that they can take corrective action. This notification provides an immediate demonstration of service value, and provides the service provider with an opportunity to upsell the subscriber to premium levels of service.

Figure 3
Customer Case Study—The Value of the Cisco Broadband Spam Control Solution

Sample Spam Analysis Report



Zombie Fingerprints

In conjunction with several of its service provider customers, Cisco identified several distinctive patterns indicative of zombie attacks. By monitoring these patterns for service provider customer during a typical 24-hour period, Cisco discovered the following:

- 1 percent of subscribers generated more than 1000 SMTP sessions
- 0.1 percent generated more than 10,000 sessions (refer to graph)

To validate the suspected spamming activity, Cisco then compared the list of high SMTP session users to published spam listings. Many of the +1000 group—and virtually all the +10,000 group—were listed as major spammers.

BENEFITS OF ZOMBIE-FREE NETWORKS

Broadband service providers have been fighting spam for years, with varying degrees of success. Although the emergence of the zombie can be viewed as an additional problem in a pressure-packed industry, mounting an effective defense offers tangible benefits:

- *Differentiation in the marketplace*—When consumers have so many options for broadband service, it becomes increasingly important to differentiate product offerings. Taking proactive steps to reduce spam on the network is one way that an ISP can create unique and compelling positioning to differentiate itself from the competition.
- *Defense against IP blacklisting*—If a significant number of the ISP's customers are infected and involved in zombie attacks, other service providers can respond by blacklisting the ISP's entire IP address range, effectively cutting off all legitimate users from initiating remote e-mail transactions. The ensuing disruptions erode subscriber loyalty and can increase customer turnover.
- *Building subscriber loyalty*—For the subscriber who is the victim of a zombie infection, the ISP that offers prompt notification, online help, and proactive customer support will grow customer loyalty.
- *Sales opportunity*—The notification process also represents an opportunity to offer the subscriber premium tiers of security service and security products such as antivirus software and firewalls.
- *Bandwidth recapture*—As the volume of spam traversing the network is reduced, additional bandwidth is made available for subscriber use, with no capital investment. This benefit applies only to solutions that stop spam at or near the source. Spam filters that operate on the user's PC may reduce the amount of spam that the user sees, but they do little to free bandwidth.

CISCO SERVICE CONTROL OFFERS PROVIDERS MORE THAN SPAM CONTROL

Beyond its powerful application as a spam killer, Cisco Service Control brings a range of network-management capabilities to the service provider. It optimizes network bandwidth based on application type and priority, reducing cost by eliminating unnecessary upgrades and improving overall subscriber performance. Cisco Service Control solutions comprise hardware and software, introducing a programmable network element that monitors and classifies network usage in real time. A Cisco Service Control platform is a comprehensive solution that helps enable broadband service providers to identify subscribers, classify applications, apply service-level guarantees of performance, and meter and charge for any IP service running on a provider's transport.

Primary capabilities of the Cisco Service Control solution follow:

- The Cisco Service Control solution offers a true capability to reliably and accurately classify traffic by application and subscriber.
- The solution offers programmability, helping ensure the solution is adaptable and extensible to emerging threats to network security.
- All classification is performed in real time, providing an unsurpassed ability to support gigabit line rates in a carrier-grade configuration.
- Minimal network reconfiguration is required to deploy an intelligent and transparent network overlay, allowing providers to minimize additional investment and amortize the solution over multiple offerings.

Using Cisco Service Control technology, broadband operators can better manage network resources, improve network performance and reduce operational costs, and develop new types of broadband services and offerings.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Pa/LW7944 02/05

Printed in USA