The spam economy: the convergent spam and virus threats

A Sophos whitepaper

May 2005

SUMMARY

Spammers, virus writers and hackers were once distinct communities with distinct motivations. However, the success of spam has brought the three together in an underground economy with a single purpose: to make money from unsolicited email. This paper examines how the convergence of the spam and virus threats is developing a new spam economy. It details the level of protection that businesses need to combat the threats, and demonstrates how Sophos can help keep organizations spam- and virus-free. A glossary of spammers' tricks and related terms is included at the end of the paper.

Introduction

The spammers' goal is simple – to make money from unsolicited commercial email, either from their own scams or products, or on behalf of other parties, such as porn or gambling sites. With more and more organizations deploying anti-spam protection, accomplishing this goal has become much harder for spammers and has led to the emergence of an elaborate industry that constantly develops, tests and adapts new tactics to defeat an organization's filters – something virus writers have been doing for years.

According to security firm Sandvine, "Many service providers report an upsurge in spam traffic immediately following a worm attack."[1]

Spammers are turning to various illegitimate providers more often to meet the demand for the specialized tools and services needed to make spamming more effective. The various relationships include:

- Virus writers and hackers supplying the infrastructure needed to deliver spam.
- Spammer services supplying specialized skills and resources.
- Spamming software coordinating spammer services and managing campaigns.

While it is true that people still write viruses for other reasons, an economic incentive is driving innovation in the virus and hacker communities in a different direction – namely quietly hijacking, rather than noisily vandalising, computer systems. Previously, these groups just wanted to gain notoriety, which meant causing obvious damage. Now they have a financial incentive, which changes the aim of viruses and makes everyone a target.

Armed with these new tools and resources, spamming operations have evolved from individual efforts, to an entire community, to a massive underground economy powered by spammers, virus writers and hackers, all intent on making money through unsolicited email.

The coordinated efforts of this new illicit community is just another tactic in the ongoing technology race between spammer and anti-spam vendor that is perpetuated by rapid innovation and increasingly sophisticated tools.

The threat to business

Findings from a report produced by Nucleus Research[2], which conducted in-depth interviews with employees at 82 Fortune 500 companies, identified the following:

- The average employee receives nearly 7500 spam messages per year, up from 3500 in 2003.
- Average lost productivity per year, per employee, is 3.1%, up from 1.4% in 2003.

The high level of cooperation which is now being seen within this underground community means that companies are faced with increasing volumes of spam, representing a continuous and significant business threat. Spam presents serious security and resource risks that can affect an organization's infrastructure by:

- Overloading systems, clogging mailboxes, reducing productivity, defrauding recipients, and draining morale.
- Increasing the frequency, severity and cost of virus attacks and related threats, such as damage to reputation from inadvertently sending spam or viruses.

Figure 1 shows the how all tiers of an organization's IT infrastructure are vulnerable to the separate and convergent

threats of spam and viruses, from the outer tiers, down to the individual workstations and back out again to mobile, remote users.

The evolution of spammer tactics

Originally, spammers used their own servers and simply devised techniques to avoid blacklists. They progressed to disguising messages and disabling spam filters. Today, they rely on virus writers and hackers to provide a constant supply of servers to hide their identity and generate huge volumes of mail.

A typical spam message will combine several techniques. For example, it might:

- Originate from a virus-infected or hijacked system on a consumer or business network.
- Incorporate multiple redirected URLs to avoid detection of known spam websites.
- Use both text and HTML message obfuscation to disguise content.
- Incorporate multiple hashbuster strings to avoid signature detection.
- Add a word salad to poison statistical filters and further avoid signature detection.

Table 1 demonstrates how spammers have developed increasingly sophisticated techniques to get around the technology designed to block spam. The early avoidance tactics began in early 2002. Since then, significant new tactics have emerged approximately every six months.

Virus tactics

Approximately 40% of spam is now sent from hijacked consumer systems, and over 800 new viruses are discovered each month – many looking for new ways to take control of computers for the purpose of sending spam. Once infected, these hijacked computers act as zombies, waking up and operating at the virus writer's or hacker's command, and providing a service to spammers until they are disinfected from within the organization or blocked by blacklists. Viruses often include methods to replenish the supply of zombie machines, such as using built-in SMTP engines to forward themselves to email addresses found on a user's hard disk.

As well as gateway and desktop protection, companies need to protect their users' home and laptop computers.

The technology and tactics used by virus writers give spammers ready access to a constant supply of servers that can:

- Act as proxies and relays to hide message routing.
- Steal the identity of the original owners, and use these legitimate credentials to bypass blacklists or take advantage of whitelists to get their messages through.

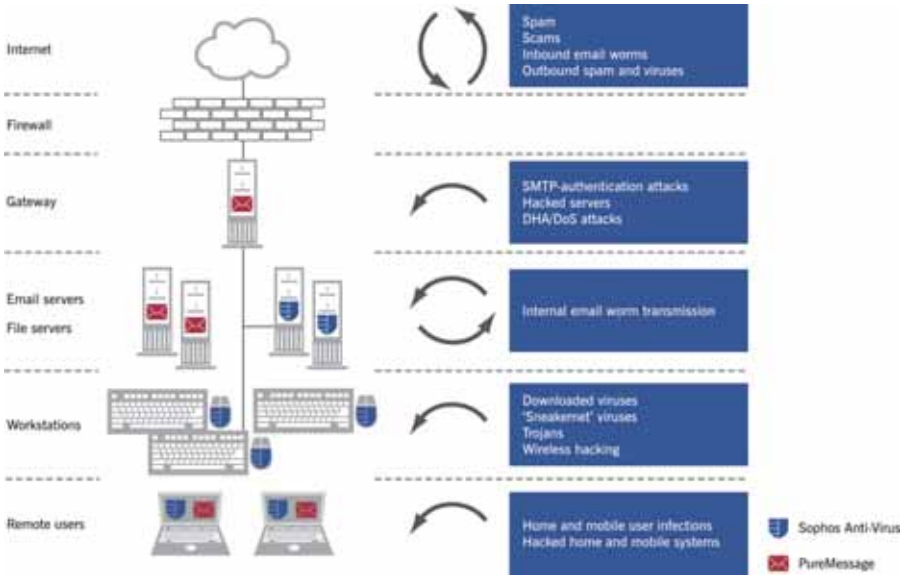

Figure 1: Sophos products protect all levels of the IT infrastructure

- Conduct Denial of Service attacks to shut down Denial of Service blackhole lists (DNSBLs).
- Conduct Directory Harvesting Attacks.
- Supply temporary websites and email accounts by abusing free, publicly available webmail hosting services, such as Yahoo, MSN or Hotmail.

Spammer software

As well as having access to a host of new techniques and a huge network of servers, spammers are also aided by the emergence of specialized software known as ratware. Readily available on the internet, ratware allows sophisticated spam attacks to be generated automatically, enabling the involvement of small cottage industry spamming operations as well as the traditional professional spammers.

Using ratware, spammers need only enter their message and the software automatically coordinates the services and manages the campaign. The software offers the ability to:

- Disguise the message using various tactics
- Choose from a variety of recipient addresses
- Choose from a list of available spam servers
- Generate and send the message
- Monitor the campaign on an ongoing basis.

Spammer services: a summary

With vendors responding to previously unseen spamming techniques by developing new detection methods, the technology needed to bypass email filters and deliver spam has become more complex. As a result, the services and resources being designed and employed by spammers are driving the overall sophistication of spam attacks.

Figure 2 summarizes the network of providers that spammers have access to, and demonstrates how:

- Spamming software providers sell programs, such as ratware, to help manage spam campaigns.
- Guaranteed delivery services devise tricks to bypass publicly available spam filtering.
- Virus writers, hackers and web-services abusers provide anonymous, hijacked, server networks for use as websites, spam servers, proxies and relays.

Stage	Spammer tactic	Tactic's purpose
Avoid	Short-lived sources, open-proxy relaying and spoofed addresses	Avoid blacklists by constantly changing addresses
Disguise	Text randomization features, including hashbusters and word salad Image spam and HTML obfuscations within message content	Avoid signature-based detection by making each message unique Disguise messages from content-based spam filters
Disable	Direct attacks against anti-spam technology, including filter poisoning and Denial of Service attacks against DNS blackhole lists (DNSBLs)	Render automated and machine learning-based spam filtering technology ineffective Shut down important anti-spam resources
Hijack	Direct attacks against businesses, including hacking and virus attacks to hijack systems, and phishing attacks to damage reputation	Maintain a supply of unblocked servers to send spam Abuse organization's credentials and customer relationships

Table 1: Evolving spammer tactics

- Message tracking, link redirection, and other services, such as the "Valid from" and "List removal" options, formed in response to the US CAN-SPAM legislation, provide spammers with specialized services to measure response, hide server addresses, and maintain a veneer of regulatory compliance.
- Address providers use Directory Harvest Attacks and other means to grow their lists of recipient and sender addresses.
- Bulletproof hosting services provide spammers with unregulated internet access.

The business need for consolidated protection

Organizations are under attack at every level of the IT infrastructure, and need a multi-faceted, integrated approach to protection. As the spammer community is certain to carry out increasingly aggressive attacks, organizations need to redouble their efforts to protect their resources, reputations and relationships. Problems that businesses may face when attempting to keep pace with new spamming tactics include:

- The deployment of a diverse set of single-purpose security solutions.
- Security functions, such as network, email and virus protection, not being integrated.
- Internal expertise and resources not keeping pace with today's increasingly sophisticated spam attacks.
- Existing systems not addressing the current environment of continuous attacks.
- Protection against external attacks not being successful in detecting and isolating compromised internal systems.

One option is to educate users about the threats that exist, but the best route that organizations can take is to ensure that they have implemented multi-tier, multi-threat defenses that block spam, detect viruses and enforce email policies. In addition, they should harden email systems by turning off exploitable email server practices, such as unauthenticated non-delivery bounces and email relaying, including SMTP-authentication relaying. Most organizations prevent the use of mail servers as open relays, but continue to allow authenticated users to relay messages through their servers. Doing so exposes the server to SMTP-authentication attacks, enabling hackers to gain access to the mail server and use it as a relay. Preventing all relaying by discontinuing this practice will protect an organization's reputation as a legitimate sender.

Table 2 demonstrates that one of the significant weapons that businesses can rely on in their armory is the anti-spam industry. As each spammer tactic has developed, anti-spam vendors have countered continually with evolving defenses.

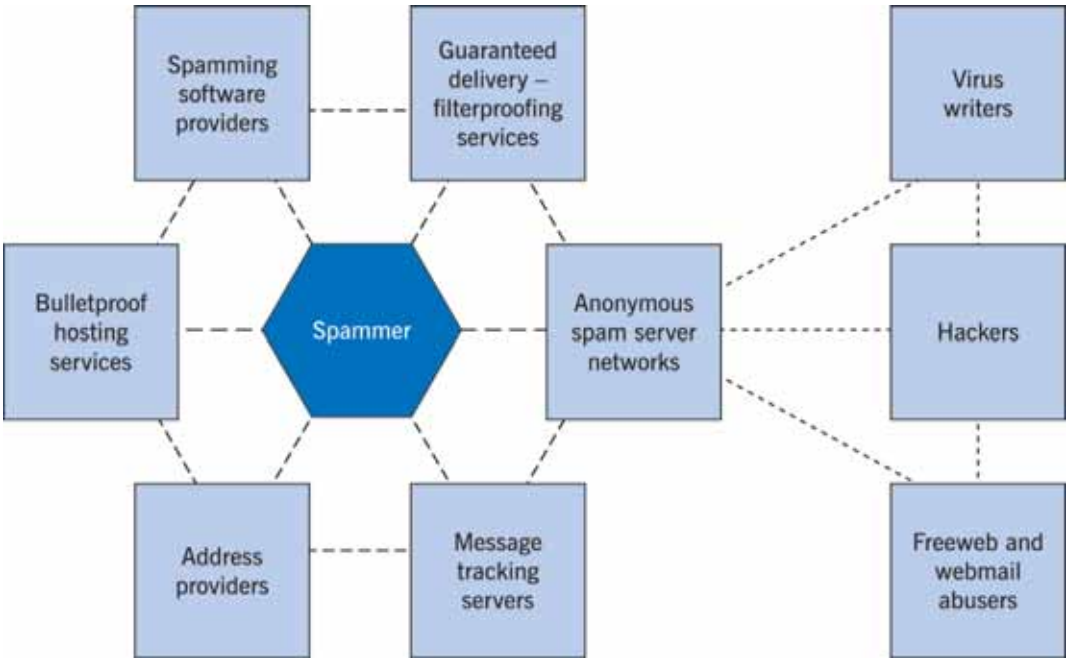

Figure 2: Spammer services

Sophos provides total protection

Sophos is a trusted, global provider of integrated security software, protecting businesses against viruses and spam, and enforcing corporate messaging policies. Sophos is uniquely positioned to deliver the experience and technology needed to secure organizations against the risks posed by the spam economy. SophosLabs™, a global network of threat research centers, develops effective detection methods and provides 24-hour analysis and protection. Rapid response procedures ensure that customers are automatically protected as new spamming tactics arise.

Sophos PureMessage™ provides total protection against spam and viruses at the gateway. It blocks up to 98% of spam, and allows businesses to create and enforce powerful email policies to reduce further the threat of unwanted email entering, or leaving an organization. PureMessage is complemented by the round-the-clock protection against viruses and malicious spyware that Sophos Anti-Virus brings to desktops, file servers, and even remote users. Both Sophos Anti-Virus and PureMessage use Genotype™ detection technologies which respectively provide pro-active protection against families of viruses and variants of spam campaigns. Sophos's integrated multi-layer technology is fully scalable, with flexible management tools that enable large organizations to define policies, and manage and deploy protection across multiple servers and systems.

By providing consolidated protection against the convergent spam and virus threats, Sophos offers organizations significant business and operational efficiencies, and lowers the total cost of ownership of anti-spam and anti-virus security.

Conclusions

Spam and viruses are ongoing and rapidly evolving security threats. With the increasing aggressiveness of spam campaigns and the growing sophistication of spammer networks, businesses need to implement protection throughout their organization from a vendor that has visibility and expertise in all areas of the overall problem. Sophos's advanced technologies provide effective consolidated protection – not just against spam, but also against viruses and malicious spyware – helping businesses stay one step ahead of the spam economy.

Further reading

For more information about spam, viruses, best practice, and Sophos products, visit www.sophos.com.

Sources

1 www.sandvine.com. Press release: *Spam Trojans a growing problem for ISPs*, 2 June 2004. Trend analysis: *Spam Trojans and their impact on broadband service providers.*

2 www.NucleusResearch.com.

Spam delivery mechanisms	Anti-spam defenses
Standard servers	Manual blocking of known spam senders
Rapid address changes to avoid blocking	Creation of public, shared DNSBLs to track addresses
Abuse legitimate servers by sending spam through open relays and SMTP-authentication attacks	Relaying no longer permitted, supplemented by blacklists
Proxy servers to hide source addresses	Blacklists
Infected consumer and business systems	DNSBLs and sender authentication track consumer IP ranges and legitimate senders

Table 2: The evolution of defenses against spam delivery mechanisms

Glossary of terms

Term	Description
Authentication	A means of validating an email's source.
Bayesian filtering	A statistical approach to determining whether an email is spam. Based on probability inference techniques pioneered by English mathematician Thomas Bayes.
Blacklists	A list of known spammers, from which no email will be accepted.
Denial of Service	Where a hacker sends attachments or other unusual or excessive traffic in an attempt to bring down email systems.
Directory Harvesting Attack	When a spammer bombards a domain with thousands of generated email addresses in an attempt to collect valid email addresses from an organization.
DNS blackhole list	Domain Name System blackhole lists (DNSBL) – commercial lists of networks that either allow spammers to use their systems to send spam, or have not taken action to prevent spammers from abusing their systems.
DoS	See Denial of Service.
Filter poisoning	Including large amounts of legitimate content to poison Bayesian, lexical, machine-learning and other statistical filters.
Hacker	Someone who intentionally breaches computer security, usually to cause disruption or gain confidential information, such as financial details.
Harvesting	See Directory Harvesting Attack.
Hashbusting	Using randomly generated strings and word combinations to make each message's signature unique and defeat spam signature databases.
Image spam	Sending messages with little or no body content apart from a link to embedded images, thereby providing minimal information for filter analysis.
IP address	Internet Protocol address.
Message tracking	Embedding unique information into subjects, links and images to track which email addresses open and respond to spam messages.
Non-delivery reports	Sending false message bounces (non-delivery reports) to mislead the recipient into opening the message.
Obfuscation	Spammers' attempts to hide data to prevent its detection. Also, using HTML and Cascading Style Sheets (CSS) layout and scripting tricks to hide the message within HTML body content.
Open relay	An SMTP email server that allows the third-party relay of email messages. The relay feature is a part of all SMTP-based servers and it has legitimate uses, but spammers and hackers have learned how to locate unprotected servers and hijack them to send spam.
Phishing	This involves creating a replica of a legitimate web page to hook users, often using spam, and trick them into submitting personal or financial information or passwords.
Proxy server	A server that makes requests to the internet on behalf of another machine.
Proxy relaying	Relaying messages through open proxies – typically hijacked systems – to hide the actual source IP address and avoid DNS blackhole lists.
Randomization	Using randomly generated synonyms and other polymorphic tricks to make each message unique.

Ratware	Software that spammers use to automate spam campaigns, coordinate spam services, and generate, send and track spam messages.
Relay	see Open relay
Sender authentication	see Authentication
Sneakernet	The medium by which electronic information is manually transferred from one computer to another by floppy disk, CD or other format.
Spoofing	Using familiar-looking internal or external email addresses to avoid detection based on the "from" address.
URL redirection	Using public redirection services to disguise destination URLs.
Whitelist	A list of external email addresses, IP addresses and domains trusted by the entire organization or individual users. All mail from these addresses is delivered, bypassing the spam filters.
Word salad	Adding a long list of legitimate words at the end of a message to poison adaptive spam filter databases and avoid signature-based detection.
Zombie	An insecure web server or computer that is hijacked and used in a DoS attack or to send spam.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.COM