



A Guide to Spam and Related Threats

Being open for business is synonymous with being online. Your employees need to communicate at various locations and access various types of business information stored electronically. But the openness of online business activity is synonymous with danger. The danger starts with spam, the top security threat to businesses today, which began as unwanted advertising, but is now so much more.

This guide will help you understand today's evolving, interrelated online threats to your business, and what you can do about them

The most recent figures available at the time of writing (i.e. for October 2006) showed spam accounting for 72.9% of all emails processed by MessageLabs

Spam: Key Concepts

Nearly all threats to your business begin with spam. Spam first appeared back in the 1990s. The quirky term for unsolicited bulk email is generally believed to have been inspired by the classic Monty Python sketch where every item on a menu included spam – whether you wanted it or not. Whatever the truth about the name's origin, the problem quickly escalated.

While viruses have been around for about 20 years, in 2003 the first exclusively spam-related virus, named "Sobig," emerged. Since then, most viruses – and especially those grabbing the headlines – have been spam-related. Specifically, they've focused on building "**botnets**".

A botnet comprises a number of Internet-connected computers that, unknown to their users, have been set up to forward spam, viruses, and other valuable information to other computers. This not only affects those computers' performance; it also generates a phenomenal amount of data on the users (passwords, online purchases, etc.) that can then be used to further target victims with other attacks.

Botnets played a fundamental role in driving global spam levels to their all-time high in summer 2004, when spam accounted for 90% of email traffic – and some predicted the death of email. Spam/botnet percentages did recede, but they are rising once again.

Currently, a vast majority of spam emanates from botnets, which almost exclusively consist of home-based machines. Smaller size businesses tend to take fewer security precautions than large enterprises and so they represent easier prey for the botnet builders, however businesses of all sizes are at risk.

Disturbingly, botnet controllers already have the **spyware** tools that make it easy to decrypt passwords and usernames stored "securely" within a remote computer's web browser.

Like any good spy, spyware is designed to go about its work unnoticed and without attracting suspicion. Fundamental to its success is its use of a range of convincing disguises to gain access to your network.

Spyware may be hidden in spam email attachments, websites or free downloadable software (e.g. games). Often, it relies on pop-up windows that include innocuous-looking "OK" or "Click Here To Read" buttons which, when clicked, result in the spyware being downloaded.

One technique in widespread use is the so-called "drive-by install". As you surf the web, a pop-up box appears on your screen, apparently alerting you that a virus or trojan has been installed on your computer. But by clicking the "OK" button to remove the virus or trojan, you inadvertently download adware, for which an adware company is paying the scam's originator a fee of, say, 25 cents a shot to install their product.

By clicking on the attachment or weblink, or by downloading the software, you unwittingly install the spyware on your computer. It can then track everything you do when you're online, in some cases, even down to the keys you press when you're inputting a password.

Before you're even aware there's a problem, high-value data – about your business, the way you work, your products and the knowledge underpinning them – will be turned against you or used to defraud you.

Spyware represents a highly effective industrial/commercial espionage tool that offers big rewards for those who design it or take advantage of its ill-gotten harvest of data. And because of the Internet's global reach, attacks can come from many directions, particularly countries where perpetrators are free from constraints imposed by legislation or regulation.

Whatever its means of gaining access to your computer, today's spyware is both clever and tenacious. Because it usually consists of a number of components, removing just one of these will not be enough to get rid of it.



It's also very possible that soon, by gaining access to Personal Storage Folders, spyware will be used not just to profile the users of infected botnet computers but also *most of the people they regularly correspond with*.

It's vital to recognize that this kind of intelligence gathered by spyware can be harnessed to conduct increasingly sophisticated **"phishing"** attacks targeting organizations like yours. This is spam, but with a different objective.

Phishers send out counterfeit but legitimate-looking emails (e.g. purporting to originate from the recipient's bank) designed to dupe the recipient into supplying high-value, confidential business data. By including, for instance, a reference to a genuine transaction that recently took place between the bank and the recipient, the email looks all the more credible and is more likely to succeed in attracting a "bite."

Exacerbating threats like these is spyware's increasing ability to conceal itself from a computer's operating system and even from advanced desktop security hardware and software solutions. Similarly, with banks moving towards more secure authentication processes to protect their customers, scammers are even developing spyware that can hijack online banking sessions after two-step authentication has been completed.

Latest Patterns in Spamming

Who are the spammers? It's estimated that 80-90% of spam originates from about 15-20 perpetrators around the world. Sometimes they're out to disrupt communications. But more often they're looking to make money, by renting out their botnets to advertisers, or to those looking to gain access to others' commercially valuable data.



In addition to their ploys to get you to open dangerous emails, spammers are developing new tricks to defeat traditional protection measures. An October 2006 spam surge gave witness to two particularly sophisticated techniques:

- **"SpamThru"** – a spam-sending trojan, with new strains regularly released in order to evade detection by traditional anti-virus systems. SpamThru is also designed so that if the botnet operator's command-and-control channel gets disrupted, he or she can regain control by accessing just one machine on the botnet. SpamThru uses a variety of tricks to neutralize anti-virus software, such as, for example, inserting dummy addresses to override genuine anti-virus update URLs.
- **"WarezoV"** – a particularly aggressive trojan, with tens of thousands of copies of each variant sent out in numerous batches. Because each batch sent out differs subtly, they can sidestep traditional anti-virus protection measures. During one 24-hour period, MessageLabs seized over 900,000 copies of this trojan. Although WarezoV's precise purpose is unclear, it certainly seems to be connected to the hike in worldwide spam levels.

The year 2006 also saw a particularly big rise in **"link spam"**. Link spam is a very effective way of delivering spyware or other malware to your computer.

Link spam works very simply. You receive an email that looks harmless – it just contains a hyperlink to a website. But what you don't realize is that the website contains spyware (or in some instances, a virus) which automatically downloads when you click on the link. Your machine is infected – and confidential data is suddenly at risk.

For some time now, spammers have been evading traditional text-scanning anti-spam measures by sending their messages in images, such as .jpeg files. Spammers would also randomize their images, making detection more difficult. However, now that those tricks have been identified and protected against, spammers are switching to a new format: **PDF Spam**.

PDF spam now accounts for around 20% of spam. MessageLabs first saw large-scale PDF spam in the middle of June 2007, when a "spam run" or "campaign" was started to "pump and dump" a German stock.

It's estimated that 80-90% of spam originates from about 15-20 perpetrators around the world.

In terms of volume, spam grew by around 70% during the month, pushing up overall email volumes by 33%

Many new types of spam start primitively, and PDF spam was no exception. This first spam run included exactly the same document in each message, making it easy to stop the messages using PDF hashes or “fingerprints” (like MD5 for example). But make no mistake, spammers continue to come up with new techniques, and PDF spam will change as well.

Superthreats and Spam

As you can see, the boundaries between different types of messaging and web-related threat are blurring and converging to produce a new breed of “**superthreats**” – the first of which appeared in 2003 when viruses and spam first merged to create a whole host of messaging security problems.

Spyware is playing the key role in both of these trends. The information it leaks out is underpinning scammers’ efforts to deploy the other weapons in their arsenal in a much more precise and targeted way – effectively equipping them with a sniper’s rifle instead of a blunderbuss.

Not only are the threats becoming more precise, they are also becoming stealthier, as large-scale attacks generate media coverage and so prompt businesses to improve their defenses. Spammers and scammers are increasingly employing their better targeted attacks to stay under the media and security radar for longer.

Spam the Top Threat

Because of its evolution from advertising medium to superthreat delivery mechanism, spam remains the undisputed number-one messaging and /web-related threat to your business.

Statistically, today it dominates the threat landscape – and yet it still continues to grow and become more dangerous: it’s growing:

- The most recent figures available at the time of writing (i.e. for October 2006) showed spam accounting for 72.9% of all emails processed by MessageLabs
- This represented an increase of 8.5% compared with the previous month – the sharpest rise in spam levels since January 2006
- In terms of volume, spam grew by around 70% during the month, pushing up overall email volumes by 33%

- Most of this increase in global spam was caused by an explosion in “botnet” activity Compare the 72.9% headline figure for spam with the corresponding figures for viruses (around 1% of all emails) and phishing (around 0.5% of all emails) – and you soon get a sense of the scale of the spam problem confronting your business.

The Cost of Spam

While spam is now a familiar feature of the email landscape, it represents an unwelcome cost to your organization. Spam pushes down productivity and eats away at your profitability. Your staff spends a lot of time identifying and deleting unsolicited emails, which also clog up your network.

You also know your computers are a target of organizations or individuals intent on harming you. And this should be a powerful stimulus to ensuring that you’ve got reliable, hassle-free and, above all, cost-effective security measures in place. For companies like yours, defense really is the best form of attack.

The MessageLabs Solution

Not surprisingly, more and more businesses are now opting for an outsourced, managed messaging security service as the best solution to their needs. Covering email, web and IM, an integrated service of this kind can divert traffic before it reaches your network, filtering out anything harmful or suspicious – even previously unknown malware which conventional security packages won’t pick up. Eliminating the need to constantly upgrade in-house systems and expertise, it takes the headache – and the risk – away.

MessageLabs provides services that offer particular benefits because they can deal with individual threats and their convergence into superthreats as it is happening.



For example, the linking of detection mechanisms is already paying dividends. At MessageLabs, we incorporate a heuristics mechanism in our email system and, by linking this to our web security services; in this manner we are able to track threats as the scammers mix and match their vectors of choice (email, web, or instant messaging).

Moreover, we're also using data generated by our scanning of billions of emails and our intensive profiling of scam messages to pinpoint the geographical location of scam gangs – data that could help break up the gangs and hold them to accountable.

Through leading-edge capabilities and imaginative initiatives, MessageLabs really is helping businesses fight back. As MessageLabs offers a managed anti-spam service, our customers benefit from seamless, continual system improvement. Combined with our industry leading development capabilities and our 24 hours per day, 7 days a week support, MessageLabs customers are always protected against emerging spam threats.

For a free 14 day trial, call us at **866.460.0000** or visit www.MessageLabs.com.

Additional Resources from MessageLabs

White Papers

<http://www.messagelabs.com/resources/whitepapers>

MessageLabs Intelligence Reports

<http://www.messagelabs.com/intelligence.aspx>

Case Studies

<http://www.messagelabs.com/resources/casestudies>

Free Trials - Web, Email and IM Security Services

<http://www.messagelabs.com/trials/free>

Industry Reports

<http://www.messagelabs.com/resources/industryreports>

PDF spam now accounts for around 20% of spam. MessageLabs first saw large-scale PDF spam in the middle of June 2007, when a “spam run” or “campaign” was started to “pump and dump” a German stock.



Americas
AMERICAS HEADQUARTERS

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
T +1 952 830 1000
F +1 952 831 8118

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong
T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 14
90 Arthur Street
North Sydney
NSW 2060
Australia
T +61 2 9409 4360
F +61 2 9955 5458

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
T +65 6232 2855
F +65 6232 2300

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
1 Great Portland Street
London, W1W 8PZ
United Kingdom
T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands
T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium
T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastrasse 9
85774 Unterföhring
Munich
Germany
T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999