

## security threat report // Q1 08

### First quarter of 2008 at a glance

This report, looking at the events and trends that emerged during the first quarter of 2008, is designed to help users and businesses keep abreast of today's threats in order to better defend against attack.

#### Web threats increase

The web now hosts an unprecedented number of threats, with Sophos discovering a new infected webpage every 5 seconds. This is an average of more than 15,000 every day, three times more than in 2007. Sophos also discovered that a new spam-related webpage appears almost every 3 seconds.

#### Data leakage grows

High-profile losses of customer details were reported from both US companies Hannaford and Advanced Auto Parts. Companies remain under pressure to become compliant with new payment card industry (PCI) guidelines. Ironically, the largest reported data breach so far this year followed Hannaford's implementation of the guidelines, highlighting that even the most vigilant of companies are not immune to data loss.

#### Email threat declines

Only 1 in every 2500 emails are infected, compared to 1 in every 909 in 2007.

#### High profile arrests announced

In February, authorities in Canada apprehended 17 people suspected of running the largest zombie network ever discovered in the country. It was believed to have included almost one million compromised computers and spanned 100 countries.<sup>1</sup> March saw 18-year-old New Zealander, Owen Thor Walker plead guilty to six charges of using computers for illegal purposes. He admitted to playing a key role in infecting 1.3 million computers around the world, installing revenue-generating adware and stealing data worth US \$20 million.<sup>2</sup>

## Web threats

The web continues to be the preferred way for malware authors to deliver their attacks. Our growing dependence on the web for purchasing and gathering information makes it an ideal hunting ground for cybercriminals chasing poorly protected users.

In 2007, SophosLabs® – our global network of researchers and analysts – discovered a new infected webpage every 14 seconds – today that figure has dropped to 1 in every 5 seconds; 79 percent of these are legitimate websites.

It is not just small so-called “mom-and-pop” sites that are affected. In March, a Euro 2008 soccer ticket website was hacked by cybercriminals in order to infect unwary fans’ computers.<sup>3</sup> January saw reports of thousands of websites belonging to Fortune 500 companies, government agencies and schools being infected with malicious code.<sup>4</sup> In February, UK broadcaster ITV was the victim of a poisoned web advert campaign, designed to deliver scareware to Windows and Mac users.<sup>5</sup>

Even companies in the security industry have suffered attacks. Trend Micro’s malware analysis pages were compromised for a few days early in 2008.<sup>6</sup> This was not the first example of a security company’s website being hacked, with Symantec and Computer Associates both reportedly attacked.<sup>7</sup> Even a Mac security forum suffered from vast amounts of spam pushing hardcore porn and malware.<sup>8</sup>

Mal/Iframe and Mal/ObfJS continue to dominate the chart, as they did in 2007, with attackers taking advantage of vulnerabilities in websites and on web servers to implant malicious code. Web users should surf from a fully protected machine, while companies need to ensure their web servers are protected against attacks. To learn more about how you can safeguard your web server, read SophosLabs’ technical paper, [Securing websites](#).<sup>9</sup>

## Where is malware hosted?

The results of research into which countries contain the most malware-hosting websites reveal some interesting changes when compared to the 2007 Sophos Security Threat Report.

The US has experienced unprecedented growth in this area, hosting almost half of all infected websites. The country has almost doubled its contribution to the chart compared to 2007, when it was responsible for hosting less than a quarter of compromised websites.

China, which in 2007 was responsible for hosting more than half of the infected websites on the web, has returned to its 2005 standing, playing host to just a third of infected websites. A newcomer to this top ten is Thailand, which in the first quarter of 2008, accounted for 1 percent of the infected websites found by Sophos.

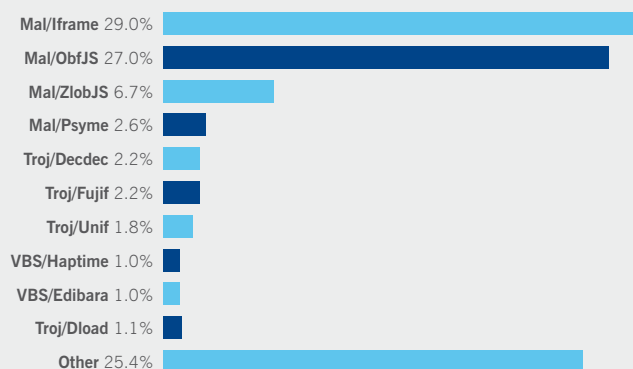
Poland and The Netherlands, which were present in the 2007 chart at positions six and nine respectively, have escaped this quarter, with both countries hosting too few malicious sites to be listed.

## Email threats, spam and phishing

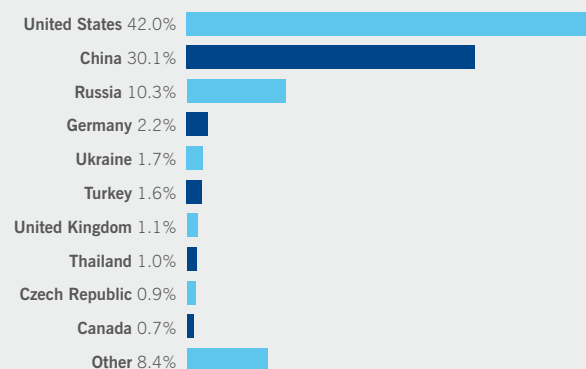
In the first quarter of 2008, only 1 in 2500 emails was found to be carrying malware – 40 percent less than in 2007. Rather than incorporating malware into the email in the form of an attachment, cybercriminals are using unsolicited email to provide links to compromised websites. Ironically, there is still a common belief that unsolicited email, or spam, is a non-threat. With virtually all of it unwanted, and a large proportion linking to infected websites, organizations would be wise to address this problem before they become a victim.

Sophos experts have discovered many Pushdo campaigns during the first part of 2008. Some of the techniques used have been technically sophisticated in an attempt to avoid detection.<sup>10</sup> These techniques involve changing the type of packers used, in which the malware tries to obfuscate itself. Pushdo, despite being at the top of this list, has not spread as far and wide as mass-mailing worms we saw in 2003 and 2004, including Netsky, Bagle, and Sobig – two of which are still listed in this top ten.

Top ten malware found on the web in Q1 2008



Top ten malware hosting countries in Q1 2008



## Spam

Spam continues to plague computer users, with Sophos research revealing that 92.3 percent of all email was spam during the first quarter of 2008. Millions of new messages are analyzed automatically by Sophos each day, and these are used to refine and update existing spam rules. Sophos currently detects over 99 percent of all spam.

Sophos finds a new spam-related webpage on average every 3 seconds - 23,300 each day. This calculation includes pages registered on “freeweb” sites, such as Blogspot, Geocities, etc. Sophos predicts this number will increase so long as its authors are making money from such ruses. By ensuring that spam messages are quarantined and not delivered to the recipient, businesses can not only save time and money, they can also help protect their users from emails linking to infected sites.

In an attempt to defeat sender reputation-based filters, the spammers who relied heavily on botnets are trying to abuse free webmail services, such as Hotmail, AOL AIM and Gmail. A recent and notable spam campaign using this technique was “Canadian Pharmacy”. Some of their campaigns were exclusively sent from webmail accounts. Experts believe that the rise in webmail spam might be related to spammers having bypassed CAPTCHA techniques – a challenge response test used to determine that the user is human.<sup>11</sup>

The Dirty Dozen chart shows that the US has decreased its contribution to the spam problem, relaying only 15 percent of spam, compared to one fifth in 2007.<sup>12</sup>

Sophos experts are also monitoring a large number of Chinese, domains that are being promoted by spam campaigns. Interestingly, there is a 2008 promotion inviting people to register .CN domains for a mere 1 Yuan (USD 14 cents).<sup>13</sup> Such a low cost is attractive to spammers, as they can register hundreds of new domains and rotate them every few minutes during a spam run in order to bypass spam filters that use URL blocklists.

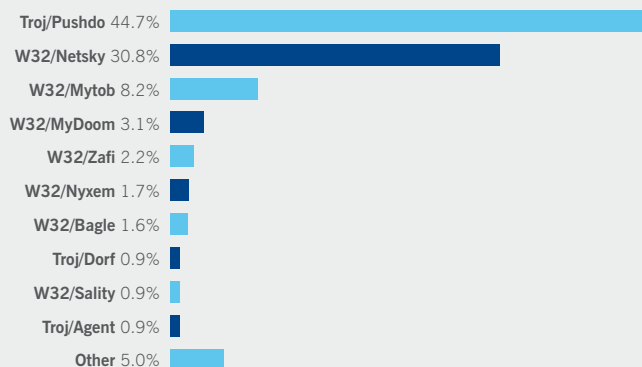
## Phishing

Phishing remains a big problem for banks and other financial institutions. It also poses a problem to large online companies, such as eBay and PayPal. Sophos measured the number of phishing emails targeting these two organizations in 2007, and found that during the first quarter of 2007, 59 percent of phishing campaigns targeted at least one of them.<sup>14</sup>

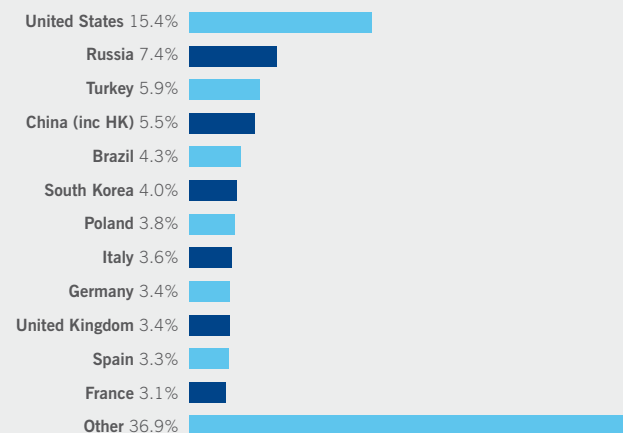
In the first quarter of 2008, however, Sophos has recorded a massive decrease in the number of campaigns targeting eBay and PayPal. PayPal has been the target in slightly over 15 percent of phishing campaigns, while eBay has accounted for just less than 4 percent of all campaigns. Heightened user awareness may be responsible for phishers looking elsewhere to lure in unsuspecting victims to bogus websites. Computer users need to remember to be vigilant when entering confidential data online, and only to do so from a fully protected computer.

SophosLabs spam experts have also seen a rise in spear phishing activity – which targets specific organizations – this year. Many educational institutions in the US have been attacked as have various webmail services. While most users have learned how to recognize most standard phishing attempts, they are more likely to trust – and therefore be conned by – emails that purport to be sent from the company’s IT or HR department, and so businesses need to exercise vigilance in this area.

### Top ten threats spread by email attachments in Q1 2008



### Dirty dozen: the top spam-relaying countries in Q1 2008



## Data leakage

News stories about organizations, from businesses to government agencies, losing sensitive data still dominate the press.

In March 2008, it was reported that the credit card numbers of 4.2 million customers had been stolen from the supermarket chain Hannaford Bros using malware installed on servers at the grocery chain's stores in New England and Florida.<sup>15</sup> The credit card details were then sent overseas. According to media reports at the time of writing, the Secret Service is continuing its investigations and approximately 1800 fraud cases have already been reported as a result of the incident. The high profile breach resulted in a letter of apology from Hannaford's CEO Ron Hodge being placed in every customer's shopping bag.

March also saw US motoring parts retailer, Advance Auto Parts announcing that hackers had gained access to the financial information of 56,000 of its customers, through an attack which affected 14 of its stores worldwide.<sup>16</sup>

Details of how the information was stolen have not been made public, and the identities of the hackers are currently unknown. Advance Auto Parts says it is working with the authorities to assist in the investigation.

Questions remain as to how hackers managed to plant malware even in companies that are PCI compliant. Sophos experts remind businesses that achieving compliance must not lead to complacency. While no security system is perfect, it is worth remembering that the more effort required to steal a company's data, the less attractive a target it becomes.

2008 will surely see more high profile companies forced to make an embarrassing admission to their clients that they have suffered from a hacker attack and had their data stolen.

## More Mac malware and vulnerabilities

Although still tiny when compared to the Windows malware problem, Mac users are not being left unscathed when it comes to malware attacks.<sup>17</sup> During the first quarter of this year, Sophos discovered a new Trojan designed to scare users into purchasing bogus security software, poisoned web adverts that would lead to either a Mac or Windows infection, and vulnerabilities that affected Mac users just as easily as Windows lovers.<sup>18</sup>

With Apple Macintosh's market share on the rise, it seems likely that hackers will increase their attempts to outfox a user population which has often - incorrectly - believed itself to be immune from many internet security threats.

## The future

While the idea of protecting your data has been revamped and reintroduced to the market by many in the security industry, it is not a new concept. Security issues over the last 15 years have revolved around protecting information – from the macro viruses of the early 90s that tampered with and deleted information to today's large-scale data thefts.

Just as technological advancements help legitimate marketers and sales teams to focus their efforts on specific markets quickly, efficiently and cost-effectively, they have also made life easier for hackers. For both the good and the bad guys, improved technology has led to improved return on investment.

This is not the time for companies to bury their heads in the sand and hope no one notices any gaping security holes in their network. Today, attacks are sophisticated, well funded and at large. Putting in place an up-to-date security policy that defends your web and email gateway, proactively protects your endpoint computers and mobile devices, and educates your users on appropriate and acceptable online behaviour can make an organization a very unattractive target indeed.

## Sources

- 1 <http://www.sophos.com/news/2008/02/botnet-busted.html>
- 2 <http://www.sophos.com/news/2008/04/owen-walker.html>
- 3 <http://www.sophos.com/news/2008/03/euro2008.html>
- 4 [http://www.theregister.co.uk/2008/01/08/malicious\\_website\\_redirectors/](http://www.theregister.co.uk/2008/01/08/malicious_website_redirectors/)
- 5 <http://www.sophos.com/news/2008/02/poisoned-adverts.html>
- 6 <http://www.sophos.com/security/blog/2008/03/1186.html>
- 7 <http://news.bbc.co.uk/1/hi/sci/tech/409980.stm>
- 8 <http://sunbeltblog.blogspot.com/2008/03/oops-macvirusorg-hosting-porno-malware.html>
- 9 <http://www.sophos.com/security/technical-papers/>
- 10 <http://www.sophos.com/security/blog/2008/03/1233.html>
- 11 <http://www.scmagazine.com/uk/news/article/789445/cybercrooks-beating-captcha-send-spam/>
- 12 <http://www.sophos.com/news/2008/02/dirtydozfeb08.html>
- 13 <http://www.cnnic.cn/html/Dir/2007/12/27/4953.htm>
- 14 <http://www.sophos.com/news/2007/10/paypal.html>
- 15 <http://www.sophos.com/news/2008/03/hannaford.html>
- 16 <http://www.sophos.com/news/2008/04/advance.html>
- 17 <http://www.sophos.com/news/2008/03/imunizator.html>
- 18 <http://www.sophos.com/news/2008/02/poisoned-adverts.html>

## About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

**To find out about Sophos products and how to evaluate them, please visit [www.sophos.com](http://www.sophos.com)**

© Copyright 2008. Sophos Plc.

All registered trademarks and copyrights are understood and recognised by Sophos.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

**SOPHOS**  
secured.