SOPHOS

Security threat report update

07/2008

This report gives a comprehensive insight into the events and trends that emerged during the first half of 2008, and helps businesses to stay ahead of today's increasingly covert threats.

SOPHOS

Security threat report: **July 2008**

Overview

Since the virus threat first appeared on the business radar in the mid-1980s, the nature of the menace has changed considerably.

Spreading slowly via floppy disks, and knowing nothing of network drives or email, let alone the internet, early viruses were written by mischief-makers, keen to gain notoriety and kudos for their creations, or to create mindless damage. The motivation has changed over recent years and malicious software (malware) is now largely in the hands of organized criminal gangs, who have no interest in creating headlines for themselves, but do want to steal identities, hijack computers and compromise them in order to send spam, and blackmail companies with distributed denial-of-service attacks.

Financially motivated criminals are creating and spreading new malicious code at an accelerated rate. According to independent testing organization av-test.org, there are now over 11 million unique malware samples in its collection.

SophosLabs™ – a global network of researchers and analysts – receives approximately 20,000 new samples of suspect software every single day. Many of these samples are Trojan horses, designed to silently steal information from computer users or compromise their PCs and take control of them.

SophosLabs is also encountering some highly crafted viruses (as opposed to Trojans) that are reminiscent of the deliberately complicated malware of the early 1990s, such as complex polymorphic viruses which go to great lengths to try to avoid detection by anti-virus software.

This "conveyor belt" of computer crime has led to masses of new malware being pumped out onto the internet every day, in the hope that some of it might slip past innocent users' anti-virus defenses, and make them the next victims.

Six months at a glance

Total number of different malware threats in existence – over 11 million

Biggest malware threat – SQL injection attack against websites

New web infections – 1 new infected webpage discovered every 5 seconds

Spam-related webpages – 1 new page discovered every 20 seconds

Top malware-hosting country – US with 38%

Top spam-relaying continent – Asia with 35%

Email with infected attachments – 1 in 2500

Spam in business email – 97%

New types of spam – Cell, Facebook and backscatter spam

Top host for malware – Blogger (Blogspot.com)

Once again, increased flexibility in working practices, new and more complex operational threat methods, and a raft of new scams have continued to place a heavy burden on businesses and the threat landscape remains challenging for the months ahead.

Malicious webpages

Our growing dependence on the web for making purchases and gathering information makes it an ideal hunting ground for cybercriminals chasing poorly protected users, and the web has become the primary vector by which hackers try to infect business computers with malware.

In 2007, SophosLabs discovered one new infected webpage every 14 seconds. In the first six months of 2008 that figure rose to one every five seconds, or an average of 16,173 malicious webpages every day – and 90 percent of these webpages are on legitimate sites which have been hacked.

The following is just a tiny sample of the hundreds of thousands of affected websites around the world which have fallen victim to a malicious attack and demonstrates that it is not just small-scale sites that are affected:

- **January 2008** Thousands of websites belonging to Fortune 500 companies, government agencies and schools were infected with malicious code.[1]
- **February 2008** UK broadcaster, ITV, was the victim of a poisoned web advert campaign, designed to deliver scareware to Windows and Mac users.[2]
- **March 2008** A Euro 2008 soccer ticket website was hacked by cybercriminals in order to infect unwary fans' computers[3] and anti-virus firm Trend Micro found some of its webpages had been compromised.[4]
- **April 2008** Cambridge University Press's website was compromised and visitors to its online dictionary were subject to attempts to run unauthorized hacker's script on their computers.[5]
- **June 2008** As the Wimbledon tennis tournament opened in the UK, the Association of Tennis Professionals (ATP) website was infected.[6]
- **July 2008** Sony's US PlayStation website suffered an SQL injection assault which put visiting consumers at risk from a scareware attack.[7]

One of the reasons the web is so popular with attackers is that innocent sites can be compromised and used to infect large numbers of victims. However, it is not just the unsuspecting visitor who is the victim – the owner of the website also suffers.

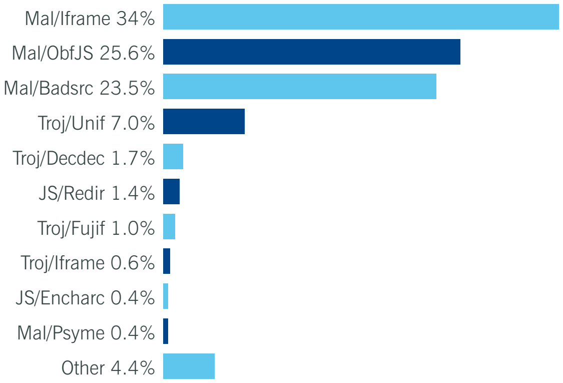
This is particularly apparent with one of the major headline grabbers of the first half of 2008 – SQL injection attacks which exploit security vulnerabilities and insert malicious code (in this case script tags) into the database running a website. The attack works when user input, for instance on a web form, is not correctly filtered or checked and unexpectedly executes as code, peppering the database with malicious instructions. Recovery can be painful, and there are numerous cases of website owners cleaning up their database only to be hit again a few hours later.

The best solution is prevention. Published advice about preventing SQL injection attacks can be found on the SophosLabs blog[8] and in an advisory published by Microsoft at the end of June 2008.[9]

Aside from SQL injection, the first half of 2008 has also revealed other trends in web-based malware. Hackers use established websites like Blogspot and Geocities, that make it easy for people to create their own sites, to host their malware because new pages are trivial to set up without requiring identification. In addition, some security products struggle to protect their users against malware on these sites for fear of blocking legitimate pages. In June 2008 Blogger (Blogspot.com) was responsible for hosting 2 percent of the world's web-based malware, making it the primary host of malicious code worldwide.

Malware families found on the web

The following chart shows the top malware discovered on websites in May and June 2008.



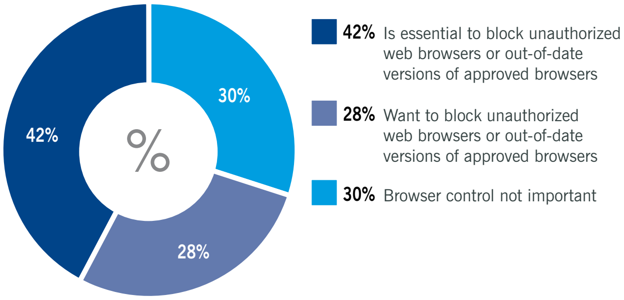
Top malware hosted on websites

The chart is dominated by malware commonly associated with SQL injection attacks. For example, a Mal/Iframe attack can be invisible to the naked eye, exploiting simple HTML code to place a pinprick-sized element 1x1 pixel in scale, through which malware can be run from a third-party website. Used in conjunction with an SQL injection attack, this can be an effective weapon for hackers.

Controlling web browsers inside the enterprise

Hackers have increasingly turned to compromising legitimate websites by inserting malicious code that redirects browsers to sites hosting malware. Similarly phishers have been taking advantage of vulnerabilities and security weaknesses in web browsers to trick users with authentic looking replicas designed to collect sensitive personal and company information which can then be used for financial gain.

A well-managed web browser, where vulnerabilities are patched and options are appropriately set, helps to preserve the integrity of corporate networks. Indeed, 70 percent of system administrators want the ability to block unauthorized web browsers or out-of-date versions of approved browsers inside their organization.



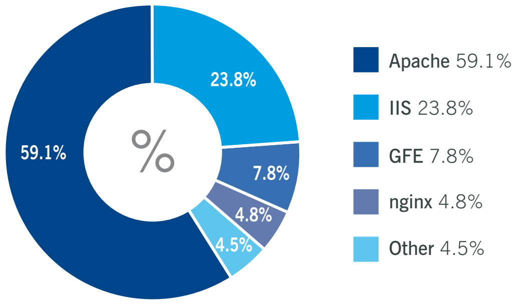
Sophos web poll, 304 respondents, 16 May – 4 June 2008

The 30 percent of administrators who do not consider browser control to be important might want to revisit this issue since unauthorized browsers generate real security and productivity issues. Setting down a policy that controls which web browser and version type employees can use, administrators are simplifying the job of keeping the web secure, which is particularly important in light of the increased malware activity on the web.

Aside from the risks posed by cybercriminals, "browser wars" have opened up a competitive, fast-paced and varied landscape. Beta versions and updates of popular browsers are entering circulation on a near daily basis, some incorporating media streaming and file-sharing capabilities, making it increasingly difficult for administrators to secure the endpoint computers in their organization.

Web server infections

The chart shows which web server software is most commonly used on infected websites.



Web server software most commonly hit by web infections Jan–Jun 2008

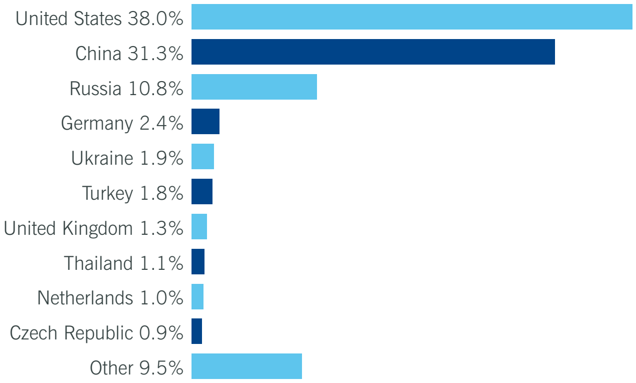
Almost 60 percent of web-based threats in January to June 2008 have affected Apache servers. This is a notable increase from the level seen during 2007, when Apache web servers accounted for less than 49 percent of web-based infections. A large number of Apache servers are hosted on Linux or some flavor of UNIX, highlighting the fact that malware is not just a Microsoft problem.

While it is true that there is less malware written to target Linux and UNIX, the websites are not necessarily safe from attack. This is because the attacks target the website – not just the server – and often attempt to embed scripts or redirections to malicious code.

Top malware-hosting countries

The chart showing which countries contain the most malware-hosting webpages reveals some interesting changes:

- **The US** – tops the chart with just under two in every five infected webpages based there.
- **China** – topped the chart in 2007 and was responsible for hosting 53.9% of infected pages on the web, but has returned to its 2005 positioning, serving up just a third of the poisoned pages on the internet.
- **The Czech Republic** – a new entrant on the list, hosting just under than 1 percent of all of the world's malware on the web.
- **France, Canada, Taiwan and South Korea** – were present in positions six, seven, nine and ten respectively in the 2007 chart but now have too few malicious sites to appear on the chart.



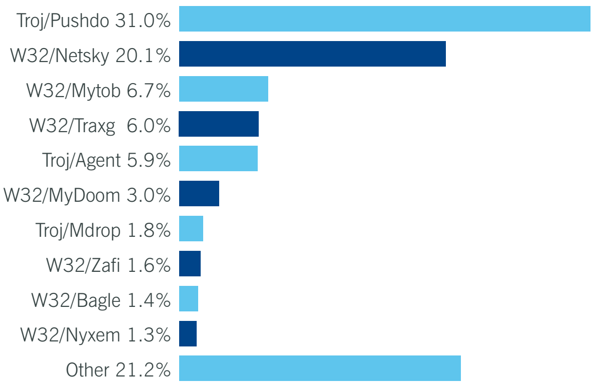
Top malware-hosting countries

Email

Malicious email attachments

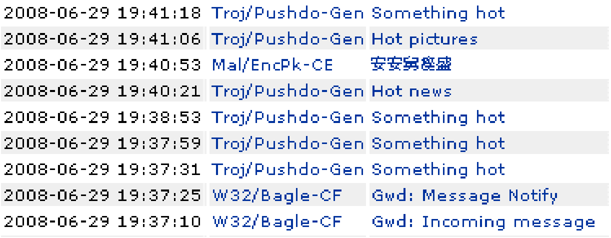
Only 1 in every 2500 emails examined during the first six months of 2008 was found to contain a malicious email attachment, compared to 1 in 332 in the first half of 2007.

The chart shows the top families of malware spreading via email attachments in January to June 2008.



Top ten viruses families spreading via email attachments

Pushdo's rapid dominance of the email attachment malware chart – accounting for almost a third of all reports during the first six months of 2008 is significant, having not made an impression in the statistics collected for 2007. However, although being at the top of the chart it has not spread as virulently as the mass-mailing worms like Netsky, Bagle and Sobig that were first seen in 2003 and 2004.



```
2008-06-29 19:41:18 Troj/Pushdo-Gen Something hot
2008-06-29 19:41:06 Troj/Pushdo-Gen Hot pictures
2008-06-29 19:40:53 Mal/EncPk-CE    安安舅癡盛
2008-06-29 19:40:21 Troj/Pushdo-Gen Hot news
2008-06-29 19:38:53 Troj/Pushdo-Gen Something hot
2008-06-29 19:37:59 Troj/Pushdo-Gen Something hot
2008-06-29 19:37:31 Troj/Pushdo-Gen Something hot
2008-06-29 19:37:25 W32/Bagle-CF    Gwd: Message Notify
2008-06-29 19:37:10 W32/Bagle-CF    Gwd: Incoming message
```

Five minutes in malware – rapidly spammed Pushdo campaign

The Pushdo Trojan is spammed out using a rapidly changing subject line and claiming, for example, to have attached photographs of a nude Angelina Jolie or Nicole Kidman. Typically the Trojan drops another piece of malware (called Pushu) which itself then downloads further malware, such as a rootkit, from the internet.

The Pushdo campaigns use sophisticated techniques in an attempt to avoid detection, including obfuscating the code using different types of packer. Although Pushdo has been seen infecting users predominantly via email, it has also used web-based attempts to infect users.[10]

The second most prevalent malware spreading via email attachments is Netsky, written by German teenager Sven Jaschan and spreading since 2004 – proving that a worrying number of users have not updated their anti-virus defenses for over four years.

Email links to malicious webpages

The huge change in the numbers of infected attachments in emails does not mean that email itself is less of a threat. It is **how** email is being used to infect users' computers that has radically changed.

Rather than incorporating malware into the email in a form of an attachment, cybercriminals are using unsolicited email, or spam, to provide links to compromised websites. Unfortunately, there is still a common belief that spam is not a threat but with virtually all of it unwanted, and a dangerous proportion linking to infected websites, organizations should secure their email and web gateways just as fastidiously as their desktops and laptops.

Targeted malware

The first half of 2008 has seen very focused malware attacks, which are designed to infect specific individuals and corporations rather than the internet community at large. Like spear-phishing (described below), targeted malware attacks are small-scale, usually sent as if from a member of your own company (in other words somebody you are more likely to trust), and typically designed to get the user to click on an infected email attachment.

In April 2008 there was a specifically targeted email campaign sent to chief executive officers of various companies. The emails all related to federal subpoenas, pretended to be from the US Federal courts, and tried to frighten their hand-picked recipients into opening a dangerous attachment.[11]

Apple malware

Apple Macs

The Apple malware problem is currently tiny compared to the situation for Windows users. However, since the emergence of the first financially motivated malware for Mac OS X in late 2007[12] there have been more attempts by hackers to infect Mac computers.

In February 2008, Sophos discovered a new Flash-based Trojan, Troj/Gida-B designed to scare users into purchasing bogus security software, using poisoned web adverts that would lead to a scareware attack that worked equally well on Mac and Windows computers.[13]

The OSX/Hovdy-A Trojan, discovered in June 2008, is capable of infecting Mac OS X computers and attempts to steal passwords, open firewalls to give access to hackers, and disable security settings. It takes advantage of the recently reported ARDAgent vulnerability in Mac OS X, to gain root access. Once a computer has been exploited, the hacker can gain complete control of the compromised Mac – covering their tracks by disabling system logging.[14]

There are several reasons why Mac users should be wary:

- A higher level of security complacency in the Apple community, with many Apple users incorrectly believing that they are immune from the problem of internet security threats, risks making Mac users a soft target for future hacker attacks.
- The use of Intel-based chips in Apple Mac hardware has made use of Windows on Macs more common, so Macs are more likely than before to be harboring and spreading Windows malware.
- The first half of 2008 has seen record laptop sales reported by Apple, with some users disgruntled with Windows Vista attracted to the Macbook brand.[15] As the marketshare for Apple Macs increases, Sophos believes that users are likely to see more attacks launched against their personal computers.

Nevertheless, with so many Windows home users seemingly incapable of properly defending themselves against the avalanche of malware and spyware being created for their platform it seems sensible to suggest that some of them should consider switching to the Apple Mac platform. This suggestion is made not because Mac OS X is superior – but because there is simply significantly less malware currently being written for it. So cybercriminals looking to maximize their return are likely to stick mostly to attacking Windows computers for the foreseeable future.

However, the likelihood is that there will continue to be malware written for Apple Macs, and Mac users should continue to follow safe computing best practices like running an anti-virus product and keeping up-to-date with security patches.

iPhone

There is no disputing that the 3G version of the iPhone is going to prove more attractive to business and internet users than its predecessor owing to its superior internet connectivity and its cheaper price point. This increased marketshare, however, may in turn herald more concerted attempts by criminals to take advantage of the devices in future.

Although simple malware has been seen,[16] the Apple iPhone has not yet been the target of commercially motivated hackers.

However, security flaws have been found in Apple's mobile email application and Safari browser, and the company has been criticized[17] for not patching these flaws in the iPhone at the same time as its other computers running versions of Mac OS X.

One thing that Apple iPhone users do need to be aware of is that they may be more vulnerable to phishing attacks than their desktop counterparts:

- Because they have to enter URLs via the touch-sensitive screen, iPhone users may be more willing than when using a real keyboard to click on links to what they assume is their online bank, eBay and the like in unsolicited emails.
- In the iPhone version of the Safari web browser, a URL embedded in an email is not displayed before it is clicked on, so iPhone users might be more susceptible to scams as it is harder for them to tell if the web link they are about to select is, for example, to a bogus banking website.

Furthermore, the issue has been raised that with the Apple iPhone's browser displaying only partial URLs in its address bar, it makes it easier for cybercriminals to fool users into believing they are on a legitimate website.[18]

Linux malware

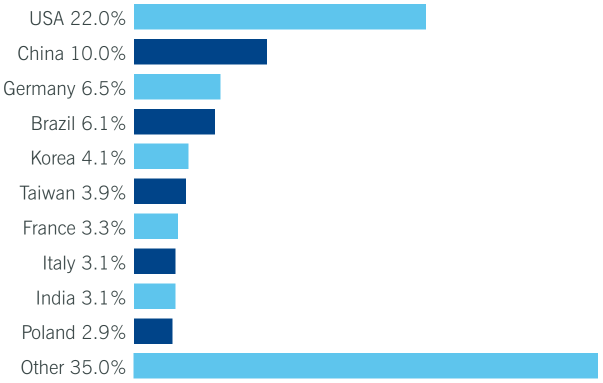
Apple is not the only non-Microsoft platform to be under threat of malware attack. In February 2008, Sophos reported that a six-year-old Linux virus, RST-B, was being seen in surprising quantities infecting Linux computers and servers.

After releasing a free tool and carrying out further research, SophosLabs found several thousand Linux computers with root level infections of Linux/RST-B, allowing hackers to use the Linux computer to control botnets (networks of compromised computers). It should be noted that only root level infections were examined; figures for compromised non-root accounts would have resulted in even higher reports of infestation.

Examination of the statistics revealed that most of the infections were in the USA* as can be seen in the chart.

Interestingly, Japan, which is a large market for Linux, comes in at eleventh position with 2.3 percent of infections.

Linux users are encouraged to investigate the free Sophos tool to check if they are also infected by RST-B.[19]



Linux/RST-B infections

* *Sophos would like to acknowledge the assistance of Accretive Networks for its help in producing these statistics*

Spam

Email spam

Email spam continues to plague computer users. By June 2008, the level of spam had risen to 96.5 percent of all business email, up from 92.3 percent in the first three months of the year. Corporations are now facing the fact that only one in 28 emails is legitimate.[20]

During the first six months of 2008, Sophos experts discovered on average 8,330 new spam-related webpages each day, approximately one every 20 seconds. The peak was in January when there was a major outbreak of the Storm worm – at its height an astonishing 1 in 6 of all emails pointed computers to a maliciously infected webpage.[21] This contributed to a high of one new spam-related webpage every three seconds. Fortunately, subsequent months did not see a comparable spam and malware campaign.

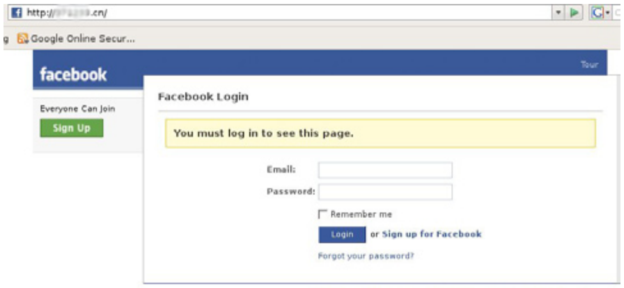
China

There is a growing trend for spammers to host their content and websites on Chinese web servers. This has caused problems for some security companies because it is harder to get visibility on Chinese domain name information than it is for other countries. There are also language and cultural issues which have conspired to make it more difficult to get some offending websites taken down promptly.

From the criminals' point of view the use of Chinese domain names is attractive, as they do not have to change their domain so regularly and may be able to operate for a longer period of time.

Phishing campaigns

Sophos continues to see widespread phishing email campaigns targeting the users of online financial institutions, and popular auction and payment websites. In recent months social networking websites like Facebook have also caught the interest of phishers.[22]



http://[redacted].cn/

You must log in to see this page.

Email:

Password:

□ Remember me

A Facebook phishing website

Spear-phishing

There have also been more sophisticated targeted attacks against particular organizations and individuals. The technique, known as spear-phishing, involves emails that have been personalized to a specific domain or organization. They appear to come from a trusted source, such as a member of IT staff at the same company as the recipient, and ask for usernames, passwords, and potentially other personal information, sometimes redirecting recipients to a bogus version of the company website or intranet. Those who reply to these messages will inadvertently be supplying information that the phisher can use for malicious purposes, such as identity fraud.

The University of Waterloo[23], Oak Ridge National Laboratory[24] and the University of Minnesota[25] are amongst the many organizations to have been on the receiving end of this kind of attack.

Spear-phishers can easily generate the victims' addresses by using spammers' software that, for example, combines given names and family names. They might also have exploited a list of employees by finding a directory on a network such as Facebook or LinkedIn. And because the phishing emails are sent only to a single domain, it is less likely that they will appear on a security vendor's radar.

It is important to remember that phishing campaigns are not specific to any one operating system, and can affect any internet user regardless of whether they use Microsoft Windows, Mac OS X or a brand of UNIX. Because they exploit trust and human nature rather than software they are likely to continue to be a problem for the foreseeable future.

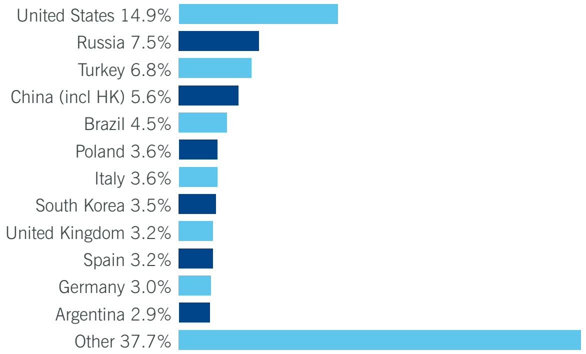
Botnets

Virtually all spam is sent from compromised computers (called "bots" or "zombies") that unbeknown to their innocent owners are being used by hackers to send out large volumes of spam, launching distributed denial-of-service attacks, or stealing confidential information. Typically they are home users who are not properly protected with up-to-date anti-virus software, firewalls and security patches.

It is important that more be done to raise awareness amongst computer users about the importance of keeping their PCs secure.

Dirty dozen

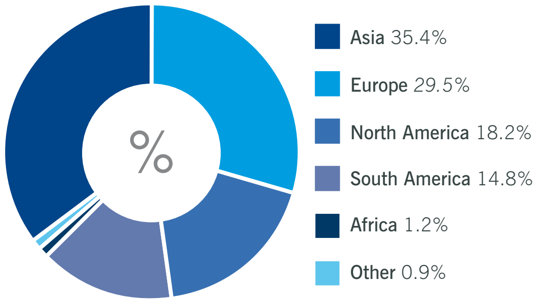
The list of "dirty dozen" spam-relaying countries in April to June shown in the chart and reflects a concern that botnets are having an increasing impact in nations with growing economies as these begin to appear in the chart.



"Dirty dozen" spam-relaying countries Apr–Jun 2008

- **The US –** has decreased its contribution to the spam problem, relaying less than 15 percent of all spam compared to a fifth in the same period in 2007.
- **China –** has also dropped from its earlier second position in the chart, having been displaced by Russia and Turkey.
- **Argentina** – the fastest growing economy in South America is a new addition to the chart this quarter, knocking France out of the chart to take 12th place and now responsible for relaying 2.9 percent of the world's spam email.
- T**urkey** – has risen from ninth place and 2.9 percent in the second quarter of 2007, to third place and 6.8 percent so far this year.

Viewed by continent, the breakdown of spam-relaying countries shows Asia as delivering more than one-third of all spam.



Spam-relaying continents Apr –Jun 2008

Backscatter spam

A noticeable spam trend during the first half of 2008 was the growth in the number of non-delivery report (NDR) messages generated by mail systems that accept spam messages during an SMTP session. If there is a delivery error (for instance, “mailbox full” or “user doesn’t exist”), the system attempts to send a bounce message back to the supposed original sender.

The bounce message is directed to the email address found in the envelope sender information (the Return-Path header) in the original message. Because this address has been forged in most spam messages, the bounce message is delivered to a mailbox of a sender who did not send the original spam message. This is known as “backscatter spam”.

Specific addresses or domains that are favorites of spammers can be the target of hundreds, or even thousands, of backscatter spam messages every day.

Cellphone spam

Another growing method for spammers to spread their messages is via SMS texts sent to cellphones.

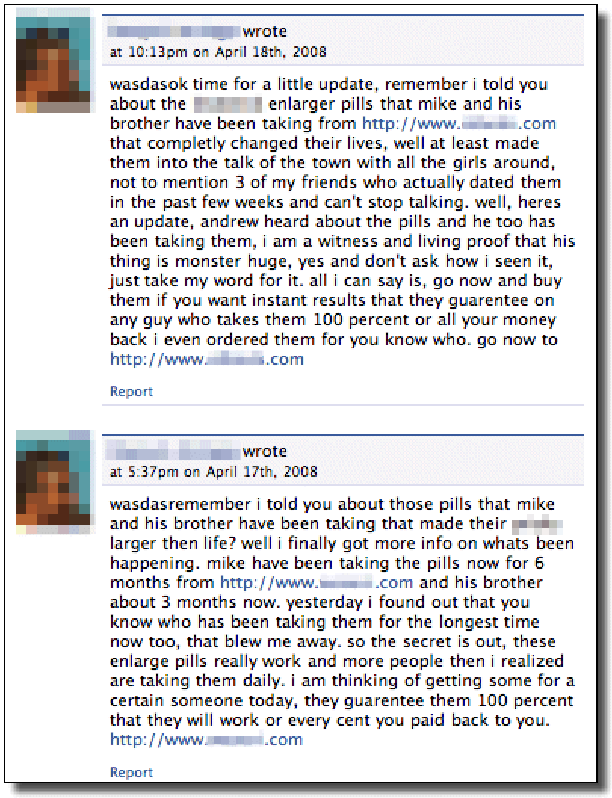
According to the Internet Society of China, 353.8 billion spam messages were sent to the country’s cellphone owners in the last year. As a consequence, China’s 574 million mobile phone users, receive on average over 600 spam messages each year. Of the 438,668 spam complaints received in June 2008, 39.17 percent were regarding fraudulent texts and 36.28 percent were commercial adverts.[26]

The problem is not confined to China, however. For instance, in April 2008, the switchboard of Dublin Zoo was swamped after at least 5000 people were spammed an SMS text message to their cellphones telling them to ring a number urgently and ask for a fictitious person.[27] The number was that of the main phoneline to Dublin Zoo and the fake names all animal-related (Rory Lion, Anna Conda, C Lion or G Raffe according to the news reports). Zoos in Houston[28] and Brownsville, Texas[29] suffered from similar attacks in the following month.

Spamming a lot of people via text message is an effective way of generating a flash-flood denial-of-service attack against the telephone system of an organization. As mobile operators give away more and more free texts per month as part of their calling-plans, and make available SMS web gateways that can be exploited by hackers, we may see more spammers using SMS to clog up phone lines.

Social/business-networking spam and malware

Social networking websites, like Facebook, MySpace, Bebo and other Web 2.0 sites, have exploded in popularity in the last few years – a trend that has not gone unnoticed by cybercriminals. Computer users, used to an onslaught of unsolicited email in their inbox, appear to be less cautious when messages arrive via other routes, such as instant messaging or Facebook.[30]



[redacted] wrote
at 10:13pm on April 18th, 2008

wasdasok time for a little update, remember i told you about the [redacted] enlarger pills that mike and his brother have been taking from http://www.[redacted].com that completly changed their lives, well at least made them into the talk of the town with all the girls around, not to mention 3 of my friends who actually dated them in the past few weeks and can't stop talking. well, heres an update, andrew heard about the pills and he too has been taking them, i am a witness and living proof that his thing is monster huge, yes and don't ask how i seen it, just take my word for it. all i can say is, go now and buy them if you want instant results that they guarentee on any guy who takes them 100 percent or all your money back i even ordered them for you know who. go now to http://www.[redacted].com

Report

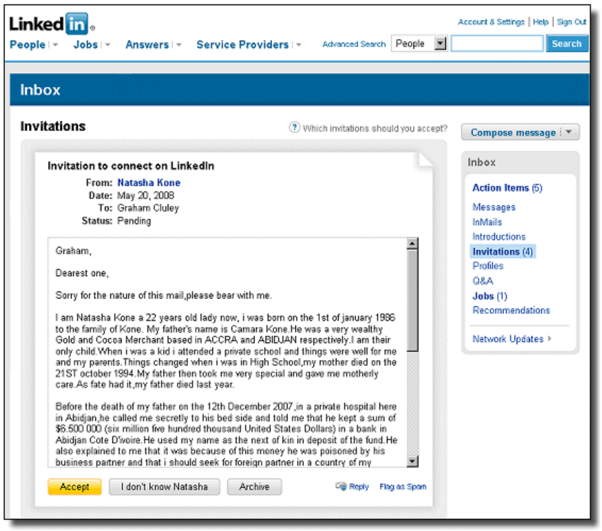
[redacted] wrote
at 5:37pm on April 17th, 2008

wasdasremember i told you about those pills that mike and his brother have been taking that made their [redacted] larger then life? well i finally got more info on whats been happening. mike have been taking the pills now for 6 months from http://www.[redacted].com and his brother about 3 months now. yesterday i found out that you know who has been taking them for the longest time now too, that blew me away. so the secret is out, these enlarge pills really work and more people then i realized are taking them daily. i am thinking of getting some for a certain someone today, they guarentee them 100 percent that they will work or every cent you paid back to you. http://www.[redacted].com

Report

Facebook spam

Industry networking website LinkedIn has also not been immune to attack, with phishers and scammers using the site to target successful business people. In May 2008 a '419 scam' sent via the LinkedIn website claimed to come from a 22-year-old woman living in the Ivory Coast who had been left $6.5 million by her deceased father.[31]



Invitation to connect on LinkedIn

From: Natasha Kone
Date: May 20, 2008
To: Graham Cluley
Status: Pending

Graham,

Dearest one,

Sorry for the nature of this mail,please bear with me.

I am Natasha Kone a 22 years old lady now, i was born on the 1st of january 1986 to the family of Kone. My father's name is Camara Kone.He was a very wealthy Gold and Cocoa Merchant based in ACCRA and ABIDJAN respectively.I am their only child.When i was a kid i attended a private school and things were well for me and my parents.Things changed when i was in High School,my mother died on the 21ST october 1994.My father then took me very special and gave me motherly care.As fate had it,my father died last year.

Before the death of my father on the 12th December 2007,in a private hospital here in Abidjan,he called me secretly to his bed side and told me that he kept a sum of $6.500 000 (six million five hundred thousand United States Dollars) in a bank in Abidjan Cote D'ivoire.He used my name as the next of kin in deposit of the fund.He also explained to me that it was because of this money he was poisoned by his business partner and that i should seek for foreign partner in a country of my

LinkedIn scam

Malware authors have also looked with greedy eyes at the pool of potential victims available to them on social networking sites:

- **May 2008** Vkontakte, the most popular Russian social-networking site with over 12 million members, was struck by a worm which spread via the system, wiping files from hard drives.[32]
- **December 2007** Google's Orkut networking site in December 2007 was struck by malware which used a cross-site scripting (XSS) attack to infect hundreds of thousands of members' profiles.[33]

As more and more companies put defenses in place at their email gateway, and home users are protected by their ISP or web email account provider, criminals may have to become more inventive in how they deliver their messages and malware. While the current level of Facebook, Bebo and LinkedIn spam is still dwarfed by email spam, there are likely to be more attempts to use Web 2.0 websites to spread malware and spam in the future.

Arrests and the law

With international computer crime authorities joining efforts in a bid to bring down hackers, malware authors and spammers, the past six months have seen more arrests and harsher sentences for criminals involved in high-profile financially rewarding computer crimes.

Below are some of the cases that made the news in the first half of 2008.

January 2008 Three men who constructed an elaborate email scam which involved them claiming that they had throat cancer, pleaded guilty in a New York court house to stealing more than $1.2 million. The men sent emails which claimed to come from a victim of terminal throat cancer who wanted to distribute $55 million to charity. One of the gang, Nnamdi Chizuba Ainsiobi, is then said to have telephoned recipients, disguising his voice to pretend he was that suffering from the disease.[34]

February 2008 An American teenager pleaded guilty to seizing control of hundreds of thousands of zombie computers, including some that were based at the Weapons Division of the US Naval Air Warfare Center in China Lake, California and at the US Department of Defense, using them to display cash-generating adverts.[35]

March 2008 Lee Shin-ja, the former CEO of Korean security company Media Port, was charged with distributing bogus anti-spyware software to over a million people, allegedly earning over 9.2 billion won (approximately US $9.8 million) since 2005 with a free anti-spyware program that displayed fake security warnings and directed internet users to purchase Media Port's Doctor Virus clean-up solution.[36]

March 2008 A Chinese court handed out jail sentences of between six and a half and eight years to four men who used a Trojan to steal internet bank account information.[37]

April 2008 Edward "Eddie" Davidson, was jailed for 21 months and ordered to pay $714,139 to the IRS after he was found guilty of tax evasion and falsifying email headers in hundreds of thousands of spam messages. By marketing perfume and luxury watches and by manipulating the stock market with pump-and-dump scams Davidson allegedly made at least $3.5 million.[38]

April 2008 An Israeli court jailed three members of the Modi'in Ezrahi private investigation firm after they were found guilty of using a Trojan to steal commercial information.[39]

May 2008 22-year-old Thomasz Grygoruk was sentenced to three years in jail, after being found guilty of stealing personal information from thousands of people over the web in a five-year spree, using a combination of Trojans and fake banking websites.[40]

May 2008 Mark Richman and Nathaniel Seidman, the owners of a company based in Boca Raton, Florida, were fined $75,000 under the CAN-SPAM act for sending unsolicited spam messages with faked headers and lurid subject lines in an attempt to promote websites such as sexyfriendsearch.com.[41]

May 2008 Authorities in the USA and Romania charged a total of 38 people suspected of running an international crime ring that sought to steal from thousands of consumers, targeting hundreds of financial institutions through phishing emails and SMS text messages.[42]

June 2008 19-year-old Jason Michael Milmont admitted to being the programmer of the Nugache malware which infected Windows computers, turning them into a sophisticated P2P-controlled botnet with between 5,000 and 15,000 compromised PCs at any one time. Milmont used stolen bank information to take over victims' accounts, and order goods to be sent to vacant addresses in the Cheyenne, Wyoming area.[43]

State-sponsored cybercrime

Countries are spying on each other all across the world for political, commercial and military advantage and it would be naive to think that nations would not take advantage of computers and the internet to assist them in their espionage activities.

During 2007 it became common for countries to openly accuse each other of engaging in spying via the internet, for example with the Chinese military being blamed for a cyberattack on a Pentagon computer system in September 2007. Concern about state-sponsored cybercrime climaxed at the end of 2007, with a discovery that MI5, the British Security Service, had written to 300 chief executives and security chiefs at UK companies warning them of the "electronic espionage attack".[44]

The first six months of 2008 have seen more reports of alleged government sponsored cybercrime – and even though it can be extraordinarily difficult to prove an attack has been endorsed by a state, rather than being the act of a independent group of hackers 2008 is likely to bring more claims of countries attacking and spying on each other via the internet.

April 2008 Der Spiegel reported that the BND – Germany's foreign intelligence service – used spyware to monitor the Ministry of Commerce and Industry in Afghanistan. Confidential documents, passwords and email communications are said to have been compromised by German spies, and sent to the BND's headquarters. The news followed revelations that the BND had intercepted emails between Spiegel journalist Susanne Koelbl and Afghanistan's Commerce Minister Amin Farhang, and resulted in a diplomatic row between the countries.[45]

May 2008 Senior Indian government officials in New Delhi were said to have confirmed that Chinese hackers targeted the Ministry of External Affairs and the National Informatics Centre, which provides the network backbone for central and state government, as well as other administrative bodies in India. The unnamed officials were quoted as saying that this is China's way of gaining "an asymmetrical advantage" over a potential adversary.[46]

May 2008 Belgium also accused the Chinese government of cyber-espionage, claiming that hacking attacks against the Belgian Federal Government had originated in China, and are likely to have been at the bequest of the Beijing government. Separately, the Belgian minister of foreign affairs told parliament that his ministry had been the subject of cyber-espionage by Chinese agents several weeks before.[47]

In truth, there is simply not enough evidence to say whether these or other attacks are state-sponsored rather than coming from the desk of a government worker or a teenager's bedroom. Governments need to think carefully before accusing another of spying via the internet unless they have strong proof.

However, these reports do underline the importance of everyone making computer security a priority and there is no doubting the importance of securing critical computers inside government from hackers whether motivated by politics, espionage or money. The advice for companies, organizations and governments alike is to keep their malware defenses up-to-date and ensure that proper security is in place to prevent intruders (be they cybercriminals or foreign government spies) from stealing information.

sophos**labs**

Strategic global insight from SophosLabs

Through the powerful integration of cross-threat expertise, automated systems and leading-edge technology, SophosLabs has the global visibility and 24/7 research operation to provide the proactive protection and rapid response that businesses need to safeguard their security, productivity and regulatory compliance. Its expertise underpins all Sophos's web, email and endpoint security and control solutions. SophosLabs' alert services, ZombieAlert and PhishAlert inform organizations if any of their computers have been compromised and turned into zombies, or if their brand is being used in phishing campaigns.

SophosLabs' broad base of data sources includes:

- Spam traps in over 50 countries, providing instant visibility of new spam campaigns
- Global email traffic from thousands of customer deployments
- Third-party resources that report and share threat information
- Data-sharing partnerships with search engines
- Millions of daily feeds of malicious URLs.

To find out about Sophos products and how to evaluate them, please visit **www.sophos.com**

Sources

1. www.theregister.co.uk/2008/01/08/malicious_website_redirectors
2. www.sophos.com/news/2008/02/poisoned-adverts.html
3. www.sophos.com/news/2008/03/euro2008.html
4. www.sophos.com/security/blog/2008/03/1186.html
5. www.sophos.com/security/blog/2008/04/1292.html
6. www.sophos.com/news/2008/06/infected-tennis-sites.html
7. www.sophos.com/news/2008/07/playstation.html
8. www.sophos.com/security/blog/2008/07/1545.html
9. www.microsoft.com/technet/security/advisory/954462.mspx
10. www.sophos.com/security/blog/2008/05/1425.html
11. www.sophos.com/security/blog/2008/04/1311.html
12. www.sophos.com/news/2007/11/mac-osx-trojan.html
13. www.sophos.com/news/2008/02/poisoned-adverts.html
14. www.sophos.com/news/2008/06/machovdyA.html
15. www.macworld.com/article/133145/2008/04/profit.html
16. www.sophos.com/security/blog/2008/01/975.html
17. blog.washingtonpost.com/securityfix/2008/07/apple_iphone_four_months_behin_1.html
18. 'iPhish: Phishing Vulnerabilities on Consumer Electronics', by Yuan Niu, Francis Hsu, Hao Chen, University of California, www.usenix.org/events/upsec08/tech/full_papers/niu/niu.pdf
19. www.sophos.com/security/blog/2008/02/1062.html
20. www.sophos.com/news/2008/07/dirtydozjul08.html
21. www.sophos.com/news/2008/01/storm-timezone.html
22. www.sophos.com/security/blog/2008/01/963.html
23. www.ist.uwaterloo.ca/security/vulnerable/20080403/20080526.html
24. www.eweek.com/c/a/Security/Oak-Ridge-Speared-in-Phishing-Attack-Against-National-Labs
25. www1.umn.edu/oit/security/OIT_ARTICLE_003725.html
26. news.xinhuanet.com/english/2008-07/17/content_8563615.htm
27. www.sophos.com/blogs/gc/g/2008/05/08/zoowatch-continues
28. www.sophos.com/blogs/gc/g/2008/05/07/cellphone-spam-clogs-up-phone-lines-at-houston-zoo
29. www.sophos.com/blogs/gc/g/2008/05/20/mobile-phone-monkey-business-strikes-at-another-zoo
30. www.sophos.com/blogs/gc/g/2008/05/04/facebook-spam
31. www.sophos.com/news/2008/05/linkedin.html
32. www.sophos.com/blogs/gc/g/2008/05/22/russian-social-networking-worm-wipes-hard-drive-files
33. www.sophos.com/security/blog/2007/12/900.html
34. www.sophos.com/news/2008/01/nigerian-scam.html
35. www.sophos.com/news/2008/02/sobe.html
36. www.sophos.com/news/2008/03/lee-shin-ja.html
37. www.sophos.com/news/2008/03/zhang.html
38. www.sophos.com/blogs/gc/g/2008/05/01/prison-for-colorado-spam-king
39. www.sophos.com/blogs/gc/g/2008/04/29/i-spy-with-my-private-eye
40. www.sophos.com/blogs/gc/g/2008/05/30/new-zealand-hacker-jailed-in-computer-fraud-and-blackmail-case
41. www.sophos.com/blogs/gc/g/2008/05/07/sexy-friends-to-spam-no-more
42. www.sophos.com/news/2008/05/phishing-gang.html
43. www.sophos.com/news/2008/06/milmont.html
44. www.sophos.com/news/2007/12/mi5-china-internet-spy.html
45. www.sophos.com/blogs/gc/g/2008/04/28/german-spooks-deploy-spyware-against-afghan-ministry
46. www.sophos.com/blogs/gc/g/2008/05/09/china-crisis-now-india-claims-hackers-are-attacking-it-from-behind-the-bamboo-curtain
47. www.sophos.com/news/2008/05/belgium.html