MARSHAL SECURITY TRENDS: SPAM, PHISHING, MALWARE
by Marshal Threat Research & Content Engineering Team

Volume 2

Security Threats

January - June 2007

Executive Summary

Spam

- Overall spam volumes remain high, but growth has leveled off compared to the rapid growth experienced at the end of 2006.
- Image spam has declined markedly to under 20% of all spam, after a peak of over 50% in January 2007.
- The proportion of plain-text spam, and spam using remote linked images, has risen. Plain text spam now represents 27% spam, up from 15% in January.
- Average spam message size has reduced from 10Kb to 6Kb as image spam has declined.
- Health spam continues to dominate as the top spam category representing nearly one-half of all spam.
- Stock “pump and dump” spam has declined markedly to under 10% after its peak of nearly 50% in February 2007.
- The US remains the top spam source at single country level with 17% of all spam, and Europe is the leading continent with 37%.
- A new spam type utilizing attached PDF documents first appeared in June 2007.

Phishing

- Overall phishing levels declined to just 0.4% as a proportion of all spam.
- The top phishing source country was Spain, accounting for 17% of total phishing attacks.
- Major phishing targets remain banking institutions. Phishing targets change every few weeks as phishers move to target new victims.

Malware

- Botnets remain a big problem as the prime distributors of spam.
- Malware is more sophisticated and is using stealth techniques to hide from detection.
- Spam is increasingly being used to help distribute malware by “advertising” its presence via links in messages.
- The Web is being used to distribute malware more and more, chiefly via exploiting vulnerabilities in Web browser applications.

MARSHAL™
Secure. Protect. Comply.

Introduction

This report has been prepared by the Marshal Threat Research and Content Engineering Team (TRACE). It is a review of the trends and developments in spam, phishing and malware during the period from January through to June 2007. It also comments on the malware that underpins and sustains the global spam phenomenon.

TRACE researches the areas of spam, phishing, and general malware. It is also responsible for the anti-malware defense and updates to unique Marshal features and functions such as SpamCensor, in Marshal's comprehensive suite of content security solutions.

TRACE data and analysis are continually updated and accessible online at www.marshal.com/trace.

Spam Volume

The TRACE team monitors spam volume through its Spam Volume Index (SVI), which tracks the spam received by a representative sample of domains. The index shows that the overall spam volume remains high, although it has leveled off over Q2/2007 compared to the rapid growth experienced in 2H/2006.

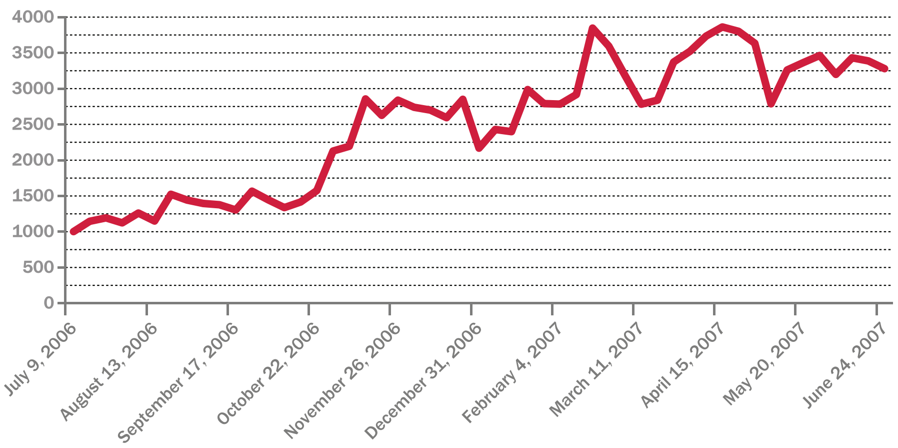


Figure 1: Marshal Spam Volume Index (SVI)

Spam Categories

Health spam, promoting pharmaceuticals such as weight loss pills and performance enhancing drugs, continues as the number one spam category comprising nearly one-half of all spam. Stock spam, which touts penny stocks in order for the spammers to make a financial gain, also was extremely prevalent, making up nearly one-quarter of all spam over the period. At 13.5%, product spam, which pushes items such as replica watches and cheap software, came in third.

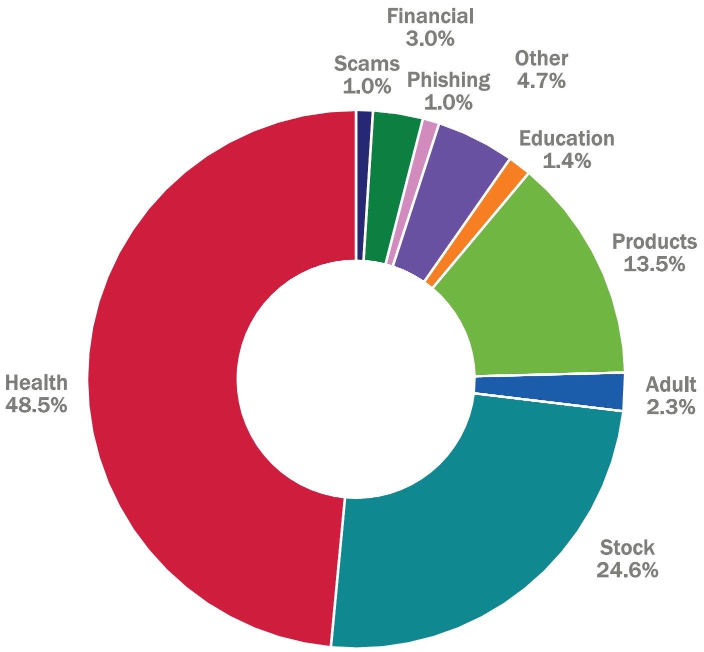


Figure 2: Spam by Category Six Months Ending June 2007

Figure 3 illustrates the weekly changes between the three major spam categories and illustrates how stock spam has dropped markedly over Q2/2007. We cannot say with precision why stock spam has declined in this way; however, possible reasons include:

- overuse of stock spam leading to declining returns to spammers
- interruption of stock spammers operations for some reason – e.g. law enforcement
- improvements to spam filtering technology.

MARSHAL™
Secure. Protect. Comply.

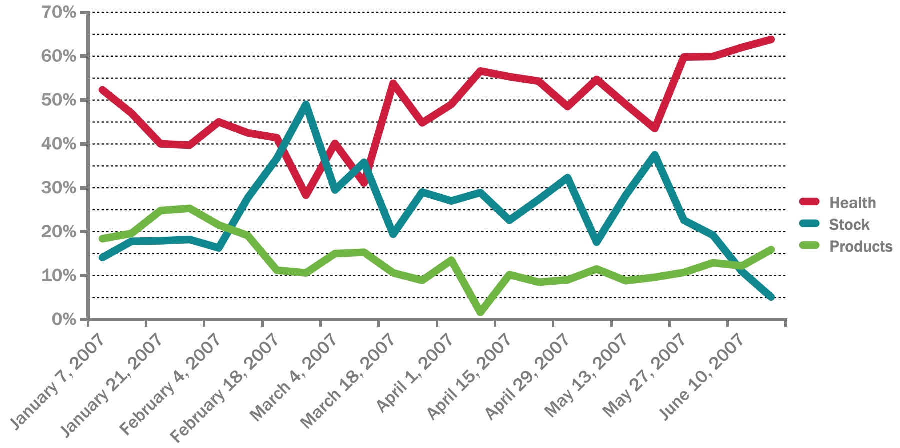


Figure 3: Major Spam Categories Jan-Jun 2007

Spam Sources by Country

Where spam comes from provides an interesting insight into how spammers distribute spam. About 70% of all spam originates from a dozen countries, mostly from compromised computers that are part spam-generating botnets. At the top of the list for the first half of 2007 is the United States, followed by China and Korea.

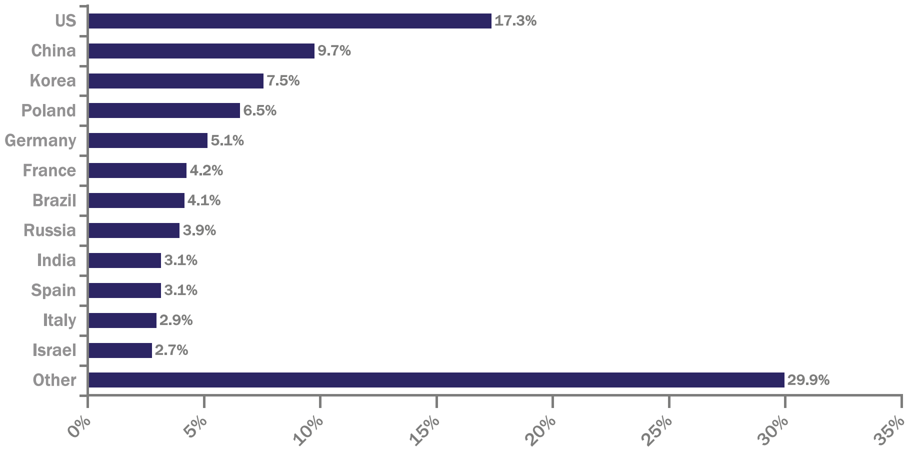


Figure 4: Top Spamming Countries

Secure. Protect. Comply.

Spam Sources by Continent

When the statistics are reviewed by continent, a slightly different picture emerges. Europe tops the list with many of its countries contributing to global spam, notably Poland, Germany, France, Russia and Spain.

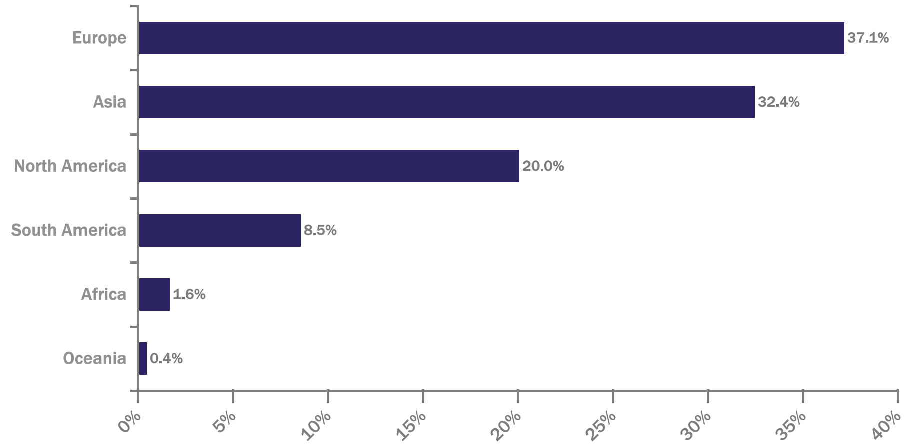


Figure 5: Top Spamming Continents

Spam Message Structure

Image Spam

During the second half of 2006 rising volumes of image spam emerged as a significant problem. Email servers everywhere strained to cope with the extra volume and anti-spam filters struggled to maintain detection rates owing to high variability and advanced randomization techniques in the images. Image spam peaked at more than 50% in January 2007 but has since fallen to less than 20% - most likely as a result of improved image spam detection. Notable over the period was a reduction in stock image spam, whereas health image spam continued largely unabated.

MARSHAL™
Secure. Protect. Comply.

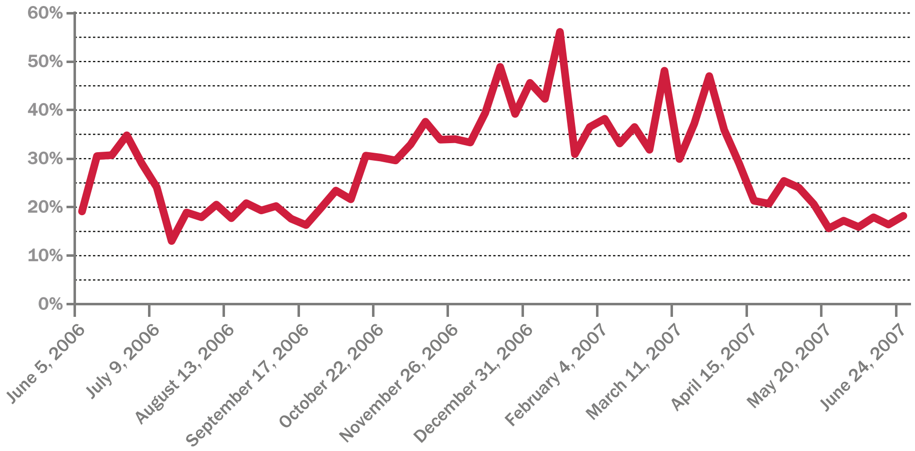


Figure 6: Image Spam June 2006 – June 2007

Text Spam

During the same time that image spam decreased, we saw a corresponding increase in the use of "tried-and-true" text spam - messages consisting only of plain text. Over the past six months, plain text spam has increased from 15% to 28% of spam, as seen in Figure 7.

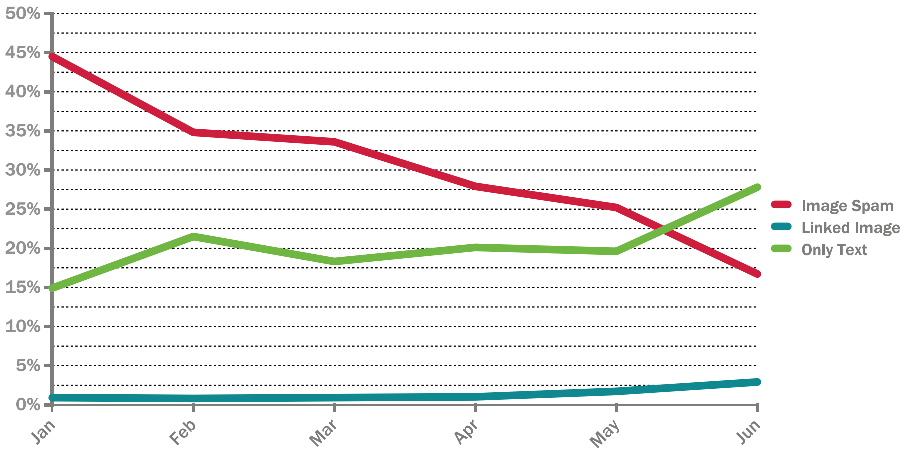


Figure 7: Trends in Spam Message Structure

Linked Image Spam

There has also been an increase in linked image spam, where the image is retrieved from the Web, as opposed to being attached to the message. This old technique gets around general image scanning technology implemented at email gateways while still allowing the spammers to hide their text in an image. The downside for the spammers is that URL links can be monitored and managed using URL blacklist databases [1]. Figure 8 shows that over the last six months, the proportion of spam with URLs has risen to 64% in June 2007 from its low of 55% in January 2007.

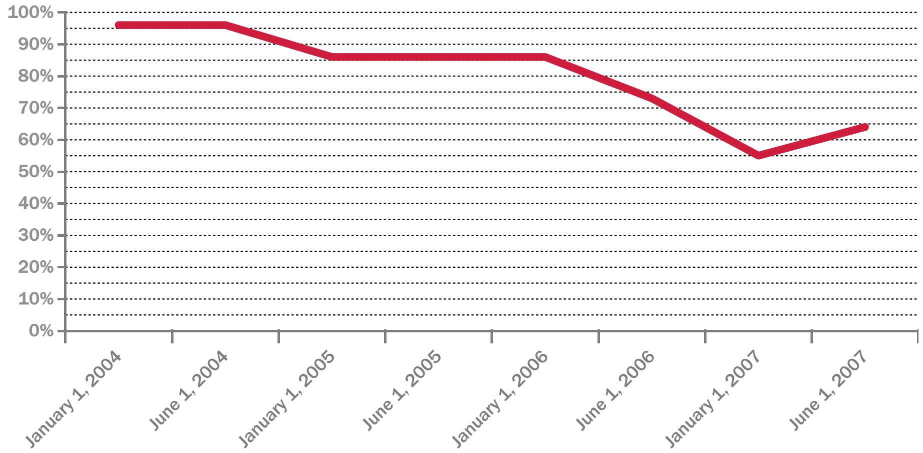


Figure 8: Proportion of Spam with URLs

Stock spammers have been among the first to re-adopt linked image technique instead of attaching images to their spam messages and are now seeking to host their images on remote Web servers.

Spam Size

In addition to the decline in image spam, the average size of spam has also declined – now hovering just under 6Kbs as depicted in Figure 9.

[1] Such as Spam URL Real-time Blocklists – http://www.surbl.org.

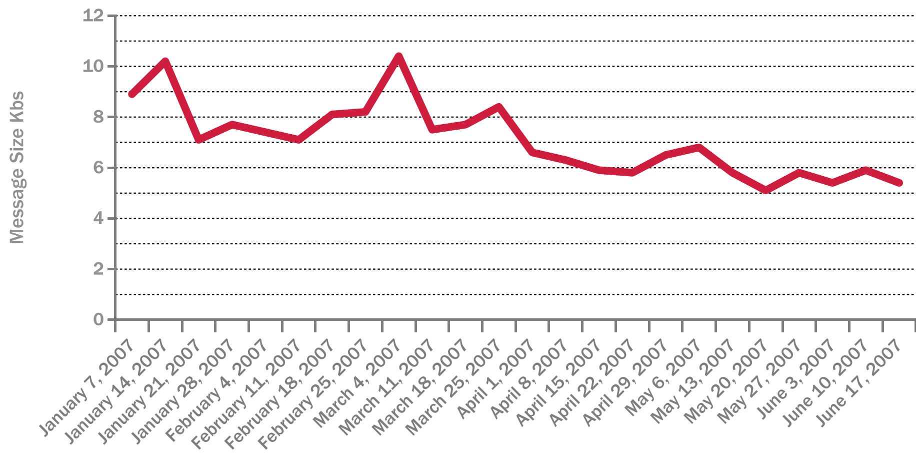


Figure 9: Average Spam Message Size

New Spam Types

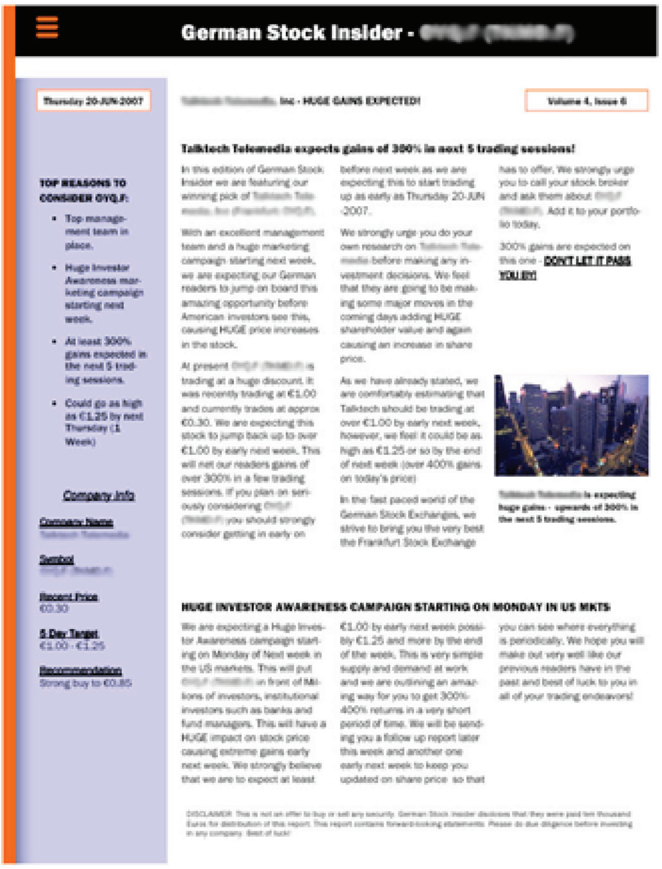
In August 2006 we observed the appearance of attachment spam where the message was contained within an attached Microsoft Word document. It was in low volume, and came and went very quickly – most probably a failed experiment by spammers.

PDF Spam

In June 2007, PDF spam made its first appearance. The PDF attachment in the form of a professional looking stock spam advertisement is an unsettling although expected new direction that the spammers have taken. It is too early to predict whether the PDF spam is yet another experiment or will represent a new phase of spam.

There are two key reasons behind the appearance of PDF spam. The first is related to the demise of image spam. Spammers are constantly seeking new means of fooling spam filters. For the first quarter of this year they achieved this using image spam. But as spam filtering technologies have improved throughout 2007, image spam has faded. The spammers are now experimenting to see what success they can have defeating spam filtering by placing their advertisements within a PDF.

The second reason is about apparent legitimacy. Pump 'n' dump spam has also been declining and one factor contributing to this has been its overuse. Recipients of pump 'n dump spam are more aware and wary of this activity now. Spammers believe that by using PDF attachments and with professional looking design and authentic looking documents they can add an air of legitimacy to their "investor opportunities". It remains to be seen if they are correct.



German Stock Insider - [redacted]

Thursday 20-JUN-2007

[redacted] Inc - HUGE GAINS EXPECTED!

Volume 4, Issue 6

TOP REASONS TO CONSIDER OYQ.F:

- Top management team in place.
- Huge Investor Awareness marketing campaign starting next week.
- At least 300% gains expected in the next 5 trading sessions.
- Could go as high as €1.25 by next Thursday (1 Week)

Company Info

Company Name
[redacted]

Symbol
[redacted]

Recent Price
€0.30

5 Day Target
€1.00 - €1.25

Recommendation
Strong buy to €0.85

Talktech Telemedia expects gains of 300% in next 5 trading sessions!

In this edition of German Stock Insider we are featuring our winning pick of [redacted]. before next week as we are expecting this to start trading up as early as Thursday 20-JUN -2007.

With an excellent management team and a huge marketing campaign starting next week, we are expecting our German readers to jump on board this amazing opportunity before American investors see this, causing HUGE price increases in the stock.

At present [redacted] is trading at a huge discount. It was recently trading at €1.00 and currently trades at approx €0.30. We are expecting this stock to jump back up to over €1.00 by early next week. This will net our readers gains of over 300% in a few trading sessions. If you plan on seriously considering [redacted] you should strongly consider getting in early on

We strongly urge you do your own research on [redacted] before making any investment decisions. We feel that they are going to be making some major moves in the coming days adding HUGE shareholder value and again causing an increase in share price.

As we have already stated, we are comfortably estimating that Talktech should be trading at over €1.00 by early next week, however, we feel it could be as high as €1.25 or so by the end of next week (over 400% gains on today's price)

In the fast paced world of the German Stock Exchanges, we strive to bring you the very best the Frankfurt Stock Exchange has to offer. We strongly urge you to call your stock broker and ask them about [redacted]. Add it to your portfolio today.

300% gains are expected on this one - **DON'T LET IT PASS YOU BY!**

[redacted] is expecting huge gains - upwards of 300% in the next 5 trading sessions.

HUGE INVESTOR AWARENESS CAMPAIGN STARTING ON MONDAY IN US MKTS

We are expecting a Huge Investor Awareness campaign starting on Monday of Next week in the US markets. This will put [redacted] in front of Millions of investors, institutional investors such as banks and fund managers. This will have a HUGE impact on stock price causing extreme gains early next week. We strongly believe that we are to expect at least €1.00 by early next week possibly €1.25 and more by the end of the week. This is very simple supply and demand at work and we are outlining an amazing way for you to get 300%-400% returns in a very short period of time. We will be sending you a follow up report later this week and another one early next week to keep you updated on share price so that you can see where everything is periodically. We hope you will make out very well like our previous readers have in the past and best of luck to you in all of your trading endeavors!

DISCLAIMER: This is not an offer to buy or sell any security. German Stock Insider discloses that they were paid ten thousand Euros for distribution of this report. This report contains forward-looking statements. Please do due diligence before investing in any company. Best of luck!

Figure 10: PDF Stock Spam Example

MARSHAL

Secure. Protect. Comply.

Phishing

Phishing as a proportion of spam received declined over the period and now is hovering at just 0.4% of all spam.

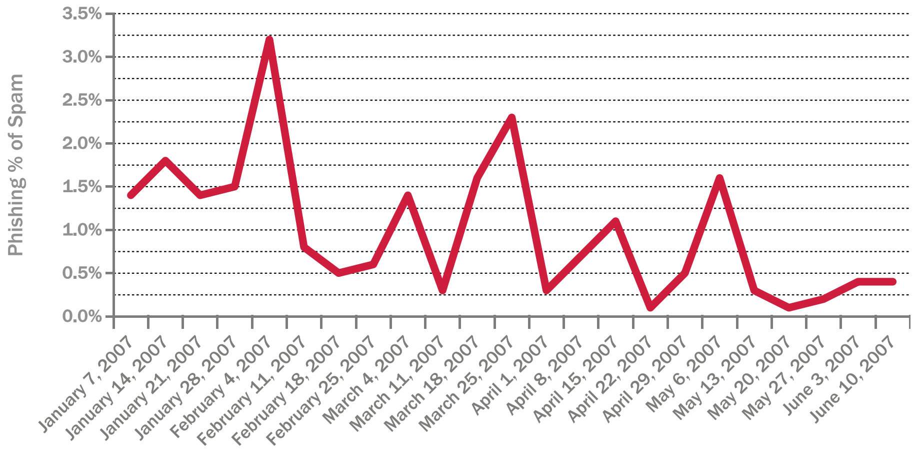


Figure 11: Phishing as a Proportion of Spam

By Country

By country of origin, Spain was the top source of phishing email at nearly 17% for the January – June 2007 period, followed closely by the US at 16%. However, European countries as a group accounted for one-half of all phishing email.

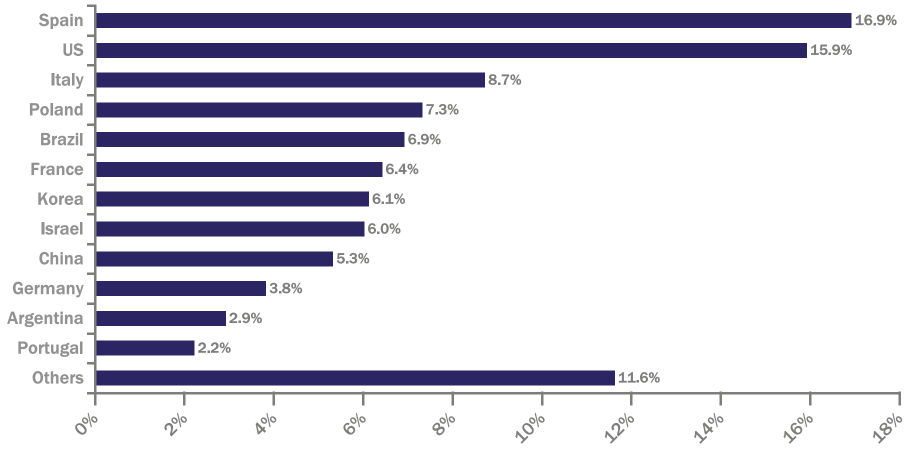


Figure 12: Top Phishing Countries

Secure. Protect. Comply.

Judging by similarities among phishing messages, a handful of phishing groups appear to dominate, selecting specific organizations for a few weeks, then moving on to new targets. While different financial institutions are being targeted at different times, other organizations like PayPal and eBay are consistently targeted at a lower, yet significant level.

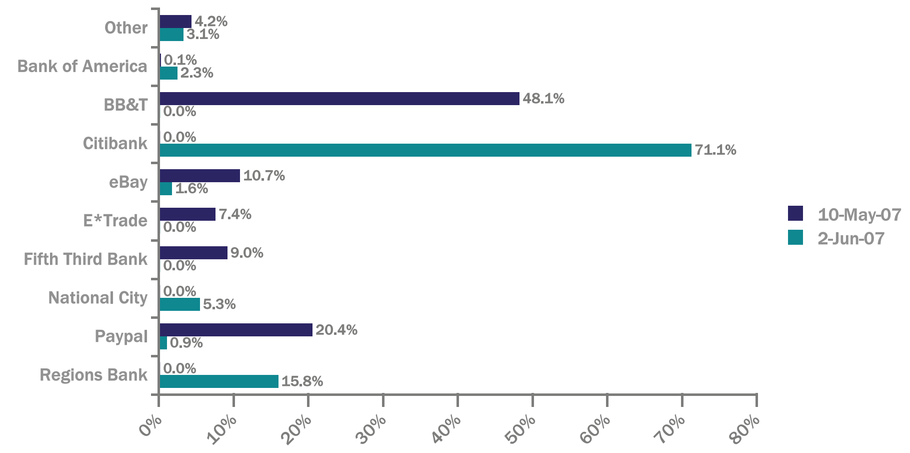


Figure 13: Phishing Targets in May and June 2007.

Malware Trends and Observations

Malware continues to evolve rapidly. The people behind malware are professional criminals looking for a financial gain either by stealing personal information or by acquiring control of computers to serve as extra members of their botnets. Some key points emerge from our observations of malware over the last six months:

- Botnets remain a major problem. Most spam is sent via botnets, and many types of malware seek to deploy spambots. The tools used to control botnets are advanced and rapidly evolving. They can, for example, push out new components or instructions to the bots.

- Malware is more sophisticated. Features such as disabling anti-virus or competing malware, and gathering information about the computer environment so that the best exploit can be deployed are examples of the new level of sophistication these devices have reached [2].

[2] See Rustock: Analysis of a Spambot - http://www.marshal.com/trace/traceitem.asp?article=217

MARSHAL™
Secure. Protect. Comply.

- Malware is harder to detect. Remaining undetected is the key for continuing success of malware. Rapidly morphing code, rootkits, low priority processes, and other stealth methods continue to be used to hide processes from both the victim and anti-virus technology.

Spam and Malware Distribution

Email remains a prime method for malware distribution. There are a number of ways this is achieved:

- Email containing "traditional" virus attachments, which when executed, are self-propagating. The amount of email with attached viruses has declined in recent years, and is currently sitting at around 0.2%.

- Email containing Trojan attachments, which do not self-propagate when executed. These are often spammed out in large numbers using existing botnet infrastructure. An example is the "Storm Worm", where we saw several different 'runs' in December 2006, January 2007 and April 2007.

- Email containing links to malicious code hosted on remote websites.

The last method is where we have observed increased activity over the last six months. Spam is one of the prime mechanisms used to deliver the "advertising" for malware hosted on remote websites. Over the past six months we have seen an increase in spam that:

- Contains simple links to executable files which require users to download and execute the file

- Has links to websites hosting malicious code that exploits vulnerabilities in the user's browser and other software

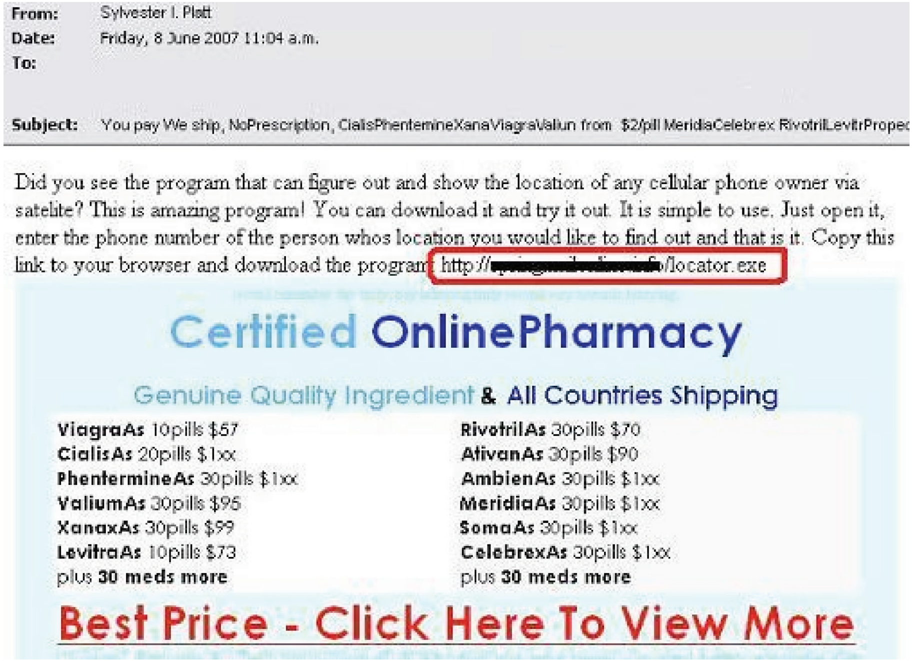
Often the spam contains social engineering to entice users to click on the link. In April 2007 we saw spam with links advertising 'Hot pictures of Britney Spears' that, when clicked, exploited a vulnerability in Windows animated cursor files [3].

In other cases, little social engineering is used. In June 2007, we saw the emergence of compound spam that contains both traditional-looking spam and a simple unrelated malware link that appears to hitch a ride or "piggyback" on the spam message [4]. The distinction between spam and malicious email is becoming increasingly blurred.

[3] Microsoft Windows ANI file Exploit - http://www.marshal.com/trace/alertsitem.asp?article=177

[4] Piggyback Spam - http://www.marshal.com/trace/traceitem.asp?article=232

Secure. Protect. Comply.



From: Sylvester I. Platt
Date: Friday, 8 June 2007 11:04 a.m.
To:

Subject: You pay We ship, NoPrescription, CialisPhentemineXanaViagraValiun from $2/pill MeridiaCelebrex RivotrilLevitrPropec

Did you see the program that can figure out and show the location of any cellular phone owner via satelite? This is amazing program! You can download it and try it out. It is simple to use. Just open it, enter the phone number of the person whos location you would like to find out and that is it. Copy this link to your browser and download the program http://[redacted]/locator.exe

Certified OnlinePharmacy

Genuine Quality Ingredient & All Countries Shipping

ViagraAs 10pills $67	**RivotrilAs** 30pills $70
CialisAs 20pills $1xx	**AtivanAs** 30pills $90
PhentermineAs 30pills $1xx	**AmbienAs** 30pills $1xx
ValiumAs 30pills $96	**MeridiaAs** 30pills $1xx
XanaxAs 30pills $99	**SomaAs** 30pills $1xx
LevitraAs 10pills $73	**CelebrexAs** 30pills $1xx
plus **30 meds more**	plus **30 meds more**

Best Price - Click Here To View More

Figure 14: "Piggyback" spam has links to malware hitching a ride on otherwise traditional-looking spam.

Web Browsing Threats

The Web is increasingly being used to spread malware. Recent research by a team at Google found some 450,000 websites distributing malicious code[5]. Attackers are choosing browser exploits as their weapon of choice, while security researchers are ever more focused on Web browser vulnerabilities. There are a number of reasons for this:

- Increased popularity of the Web and Web applications
- Increased capabilities of Web browsers to execute code or launch external programs
- Propensity for the software on end user computers to be badly managed and seldom updated, allowing easy exploitation of known vulnerabilities

In many cases all that is needed for malware to be downloaded and executed is for a vulnerable user to browse to a compromised website.

[5] The Ghost in the Browser: Analysis of Web-based Malware - http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

The tools used by the attackers are sophisticated and automated. In June 2007 we saw an attack that compromised thousands of normally trusted websites[6]. The tool used, dubbed MPack, was capable of determining which browser type and version the user was using and subsequently serving up a suitable exploit based on that information.

Conclusion and Some Thoughts on the Future

After the manic floods of new image spam in late 2006, growth in spam volume has slowed somewhat. However, despite the slowing in growth, the overall volume of spam remains at historically high levels. A drop in proportion of image spam suggests that the technique is no longer as effective in evading filters – representing a small victory for the anti-spam industry. Whether this respite is the lull before another storm or reflects some fundamental changes in spamming methods is unclear.

The financial motive of the malware underworld that sustains spam appears to remain strong. It seems to remain lucrative to steal data and control networks of computers. For this reason, we are not optimistic that spam is going to recede in the near future. We believe that some of the trends we have identified in this report will continue:

- The overall volume of spam will remain strong.

- Spammers will continue to try a range of new tricks – such as PDF spam – in an attempt to avoid anti-spam filters.

- The use of spam to spread malware via attachments or links to malicious websites will continue to grow.

- The Web will increasingly be used to distribute malware, with continued focus on exploiting browser vulnerabilities.

In summary, enterprises need to continue to be vigilant as spammers will invariably keep reaching into their bag of tricks. For our part, TRACE will continue to monitor and research spam and the wider threat landscape to better equip our customers with the tools and knowledge to help protect against the inevitable emergence of new threats in the future.

We hope that you have found this report interesting and informative. If you have any questions or comments we would very much like to hear them. You can email us at trace@marshal.com.

[6] MPack Hacks Thousands of Websites - http://www.marshal.com/trace/traceitem.asp?article=237

MARSHAL™
Secure. Protect. Comply.

MARSHAL™

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com