MARSHAL TRACE REPORT

MARSHAL™
Secure. Protect. Comply.

Marshal Security Threats: Spam, Phishing, Malware

By Marshal Threat Research & Engineering Team
December 2007

CONTENTS

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 in 2007. It also comments on the malware and botnets that underpin and sustain the global spam phenomenon.

TRACE researches the areas of spam, phishing and malware. It is also responsible for the anti-malware defense and updates for Marshal's suite of content security solutions, including MailMarshal's SpamCensor, and Zero Day updates.

Data and analysis from TRACE is continually updated and accessible online at www.marshal.com/trace.

EXECUTIVE SUMMARY

- Total spam volume increased by over 50% in the latter half of 2007, reflecting the evolution and refinement of the major spam-sending botnets.
- Spammers reacted to better anti-spam techniques by improving their botnets and simply sending even greater volumes of 'ordinary' spam.
- Stock 'pump n dump' spam declined to an almost insignificant 1% of spam after its peak of nearly 50% in February 2007.
- Health spam, touting pills and potions, continued to dominate as the top spam category, representing nearly 70% of all spam.
- The proportion of image spam declined further to under 5%, as spammers reverted back to plain text and HTML formats during the latter half of 2007.
- Spammers experimented with new formats in 2007, including PDF, Excel, and MP3 file attachments, but these formats were short-lived.
- Overall phishing levels remained around 0.5% as a proportion of all spam during the second-half of the year.
- Major phishing targets remained the banking institutions. However, these targets changed every few weeks as phishers constantly sought new victims.
- Botnets remain a big problem as the prime distributors of spam and reached new heights of sophistication and capability in 2007.
- The distinction between spam and malware became increasingly blurred

as the spam-sending botnets sought to expand their networks by using email to 'advertise' the presence of malware on websites.

- There was a marked shift to using the Web to distribute malware, involving both hacked websites and spammed forums and blogs that were used to drive users to websites hosting malicious code.

FACTS & FIGURES

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 SVI shows spam volume increased markedly in the second half of 2007, following relatively modest growth in the first half-year. The huge increase in spam reflects the evolution and refinement of the major spam-sending botnets – notably the Storm botnet from July onwards. The sharp rise in November-December 2007 not only reflects more spam, but also the typical Christmas spam spike – a phenomenon we have observed for the past three years running.

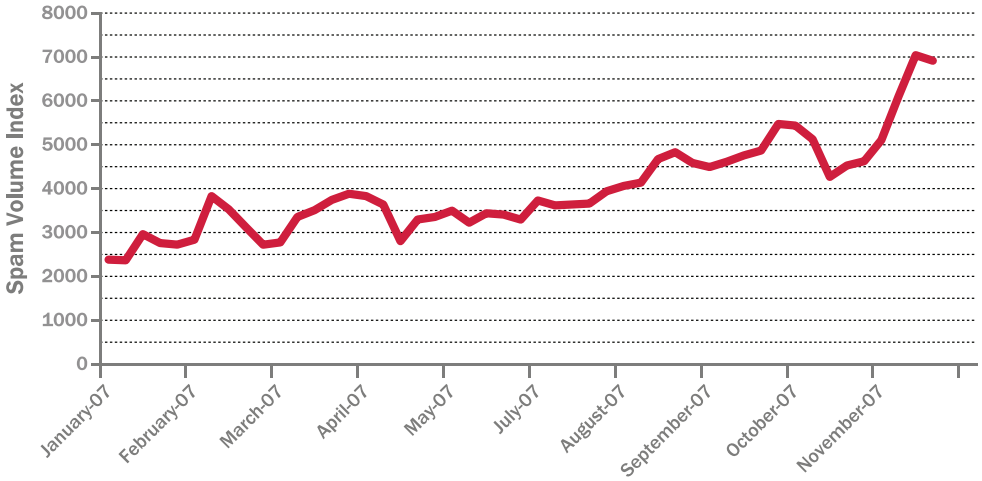

Figure 1: Marshal Spam Volume Index (SVI)

Spam Categories

Health spam, promoting pharmaceuticals such as weight loss pills and performance enhancing drugs, consolidated its position as the dominant spam category. Figure 2 is a snapshot of spam categories in December 2007 and it shows the health category comprising nearly 70% of all spam. Male sexual organ enlargement spam is especially prevalent in this category

and, at times, a single type of this spam comprised one third of all the spam received in the TRACE spam traps during November-December 2007. Product spam, which pushes items such as replica watches, and cheap software, was the second largest category at 26% of all spam.

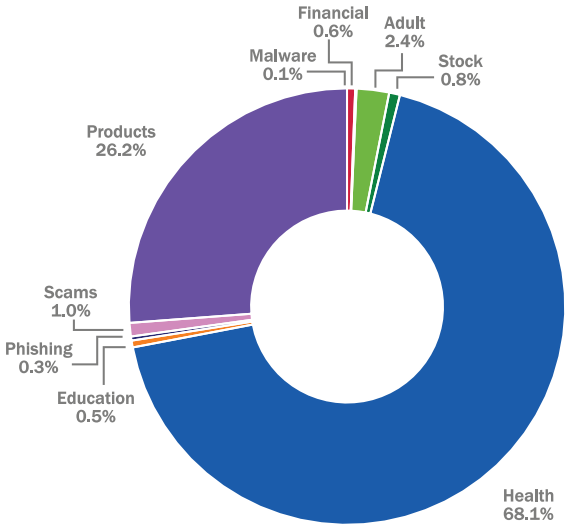

Figure 2: Spam by Category, December 2007

Stock spam, which touts penny stocks in order for the spammers to make a financial gain, has been subject to the biggest change during the year. The July-December 2007 period saw stock spam dwindle to almost nothing. By year-end it represented less than 1% of all spam - a major turnaround when compared to its peak of nearly 50% in February 2007. We cannot say precisely why stock spam has declined in this way; however, likely reasons include:

- Overuse of stock spam leading to declining returns to spammers
- Interruption of stock spammers operations from the actions of securities regulators and law enforcement authorities

Figure 3 illustrates the weekly changes between the major spam categories and illustrates how stock spam has dropped markedly over the year. Although the reduction in stock spam is welcome news, the overall volume of spam remains high - reminding us once again that spammers, as always, are quick to adapt to new circumstances.

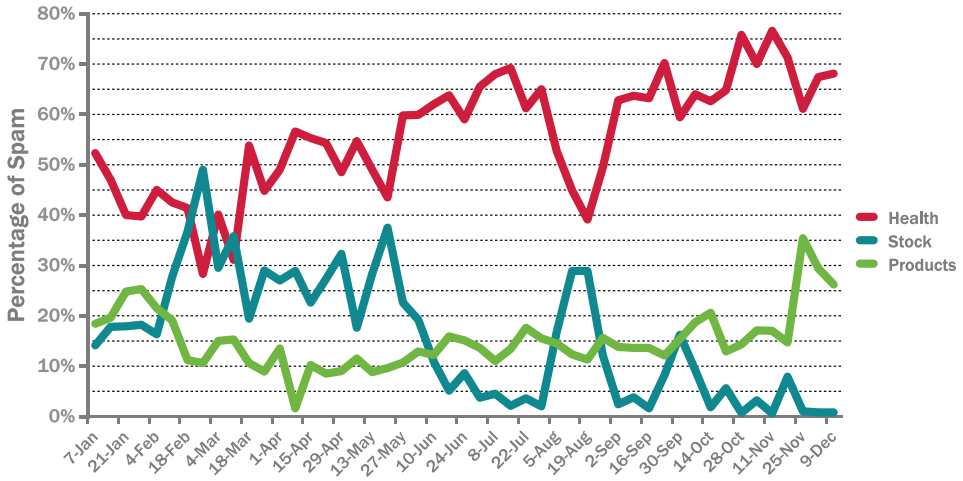

Figure 3: Major Spam Categories January-December 2007

Spam Sources by Country

Where spam comes from provides an insight into how spam is distributed. About 70% of all spam originates from fifteen or so countries. As most spam is sent by spam botnets, this pattern reflects the number of compromised computers, or 'bots', in those countries. As of December 2007, the United States was the leading source of spam. Russia was the biggest mover in late 2007 and jumped to second place with nearly 10% of all spam. Also of interest was China and South Korea, both traditionally major sources of spam, dropping down the table.

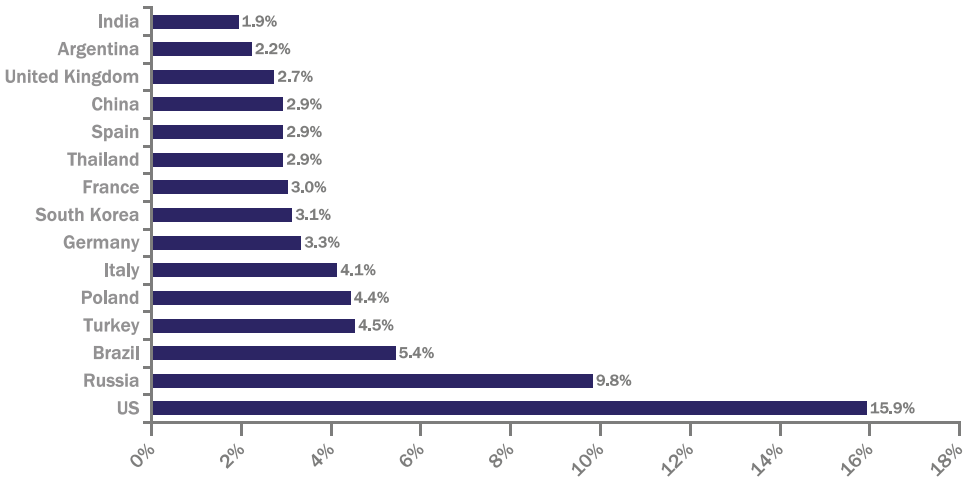

Figure 4: Top Spamming Countries, December 2007

Spam Sources by Continent

When the spam statistics are analyzed by continent, Europe tops the list, with many of its countries contributing to global spam, notably Russia, Poland, Italy and Germany.

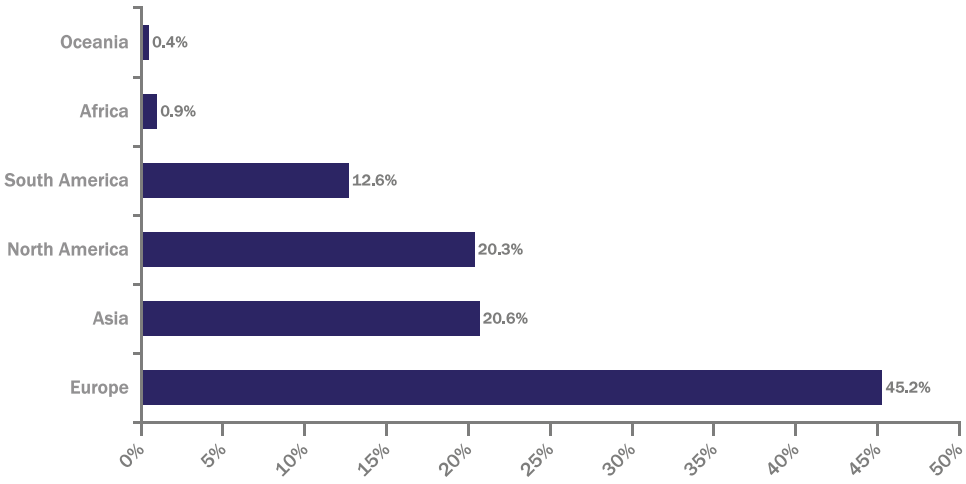

Figure 5: Spam Sources by Continent, December 2007

Spam Message Structure

The latter half of 2007 marked a shift back to more traditional spam formats. Spammers moved away from image spam towards more ordinary, plain text and HTML spam formats. Figure 6 shows some overall trends in spam message structure, with a decline in image spam to just under 5% and a noticeable increase in the use of plain text spam during August and September 2007.

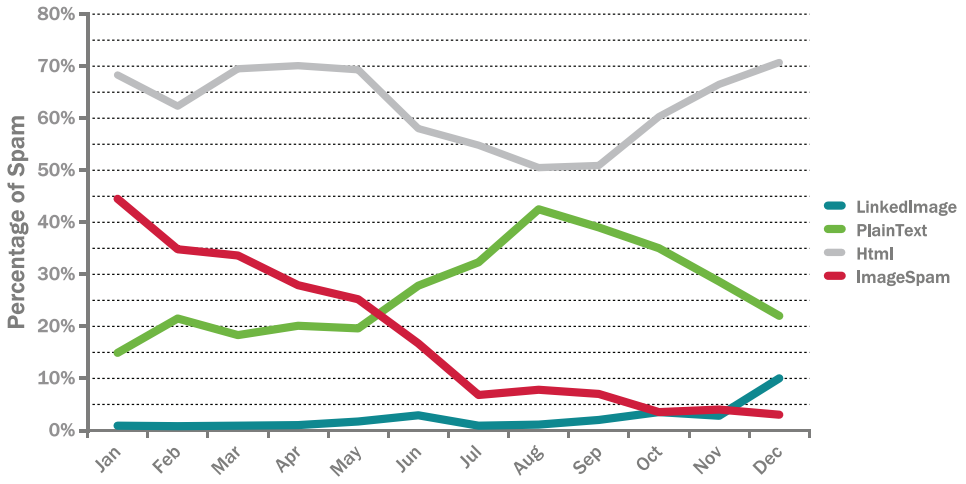

Figure 6: Trends in Spam Message Structure

Spammers Experiment with Attachments

As spammers moved away from image spam, they also experimented with different ways to send spam in attachments. During the second half of 2007, a number of different techniques were tried, notably the use of PDF attachments containing the spam message. Figure 7 shows the PDF spam spike in August, which, at times, peaked at over 20% of all spam received.

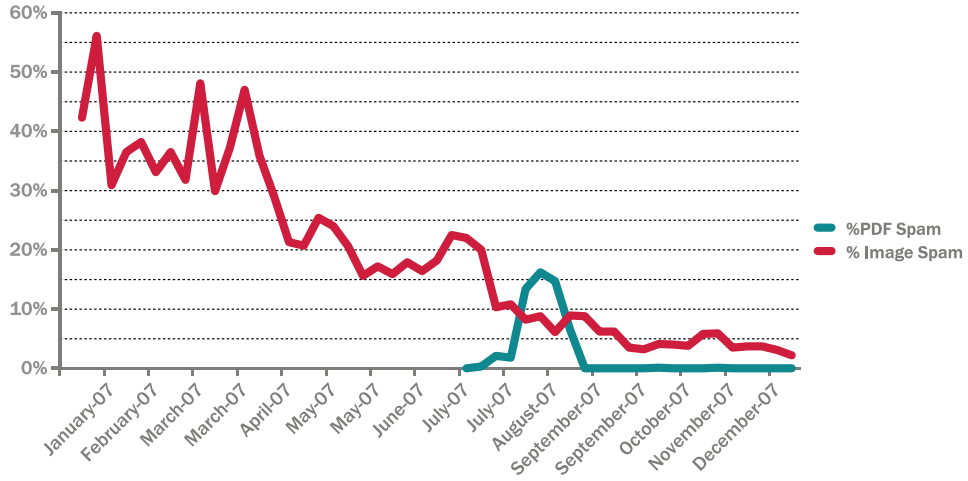

Figure 7: Attachment Spam as Percent of Total, January – December 2007

Spammers also experimented with delivering their messages via other attachments including ZIP, Text and Excel attachments[1], and even "audible spam" using MP3 files.

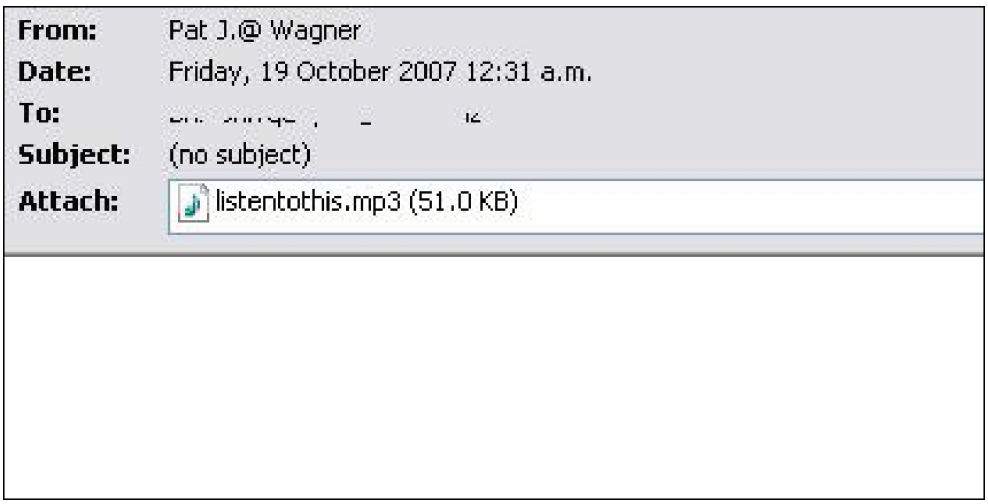

Figure 8: Example of MP3 Attachment Spam

1 Excel and text spam: What next - http://www.marshal.com/trace/traceitem.asp?article=270

All these new techniques were short-lived, suggesting a low success rate from these new spam mechanisms. In the end, spammers reverted back to the 'tried and proven' text and HTML formats, as Figure 6 shows.

Spam with URLs

During 2007 there was also major turnaround in the amount of spam containing URL links. Figure 9 shows that over the year, the proportion of spam with URL links rose to over 90% from its low of 55% in January 2007.

Once common in almost all spam, URL links in spam declined in 2006 as stock spam and image spam gained prominence. Stock spam has no need for URLs because it merely touts the advantages of a particular stock, and some image spam types hide the URL in the image so that you have to type it into your browser to access the website. The resurgence of URL links in 2007 reflects the decline in both stock and image spam.

The upside of this development is that URL filtering has once again become a very useful anti-spam weapon. URL filtering works by extracting any URLs from a spam message and querying them against a database of known 'spammy' URLs. Figure 9 shows the corresponding increase in effectiveness of URL filtering just with MailMarshal's URLCensor over the period.

Figure 9: Proportion of Spam with URLs

Spam Size

In line with the move back towards typical plain text and HTML email, the average size of spam has also declined – now hovering just under 4KB as depicted in Figure 10.

Figure 10: Average Spam Message Size

Phishing

During the second half of 2007, phishing spam remained reasonably consistent, hovering around 0.5% of total spam received.

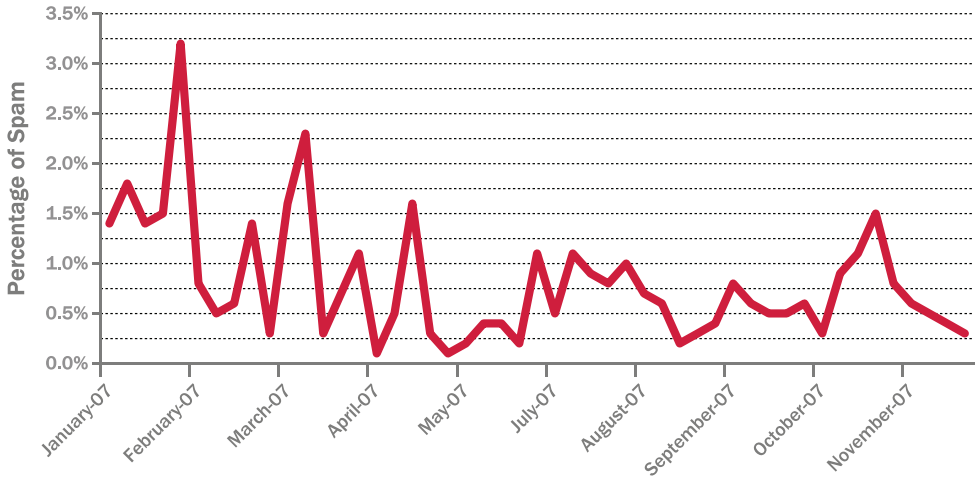

Figure 11: Phishing as a Proportion of Spam, January – December 2007

Phishing by Country of Origin

By country of origin, Spain was the top source of phishing email at 16% in December 2007, followed closely by Italy at nearly 15%. During the last six months, the US has slipped several places and now sits at only 3.5%. Interestingly, the dominance of Spain and Italy is quite a different profile from spam as a whole, where the US and Russia top the list (see Figure 4).

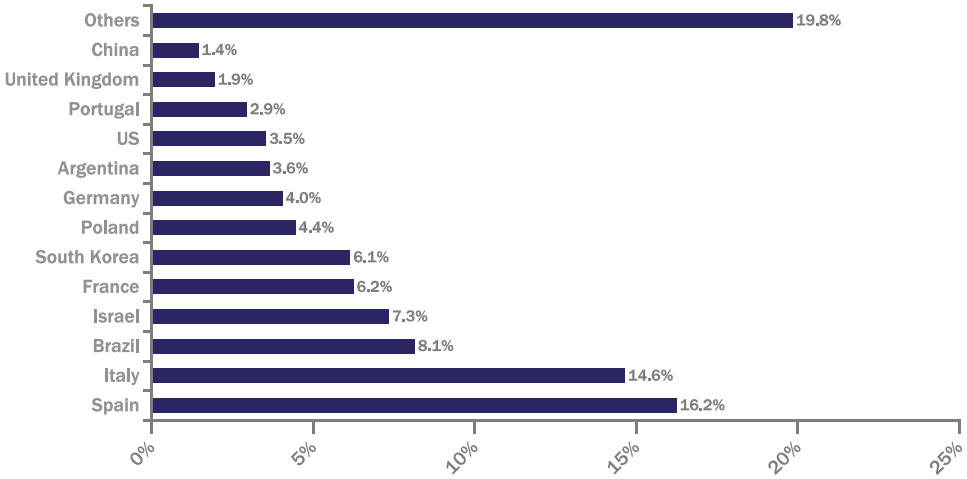

Figure 12: Top Phishing Countries, December 2007

Phishing Gangs and Targets

Judging by similarities among phishing messages, a handful of groups seem to dominate, suggesting phishing has become a specialized activity. One particular group, the Rock Phish Gang, is estimated to be responsible for over one-half of all phishing emails[2]. This gang's phishing emails are distinctive and dominate the daily phishing catch.

The major phishing gangs select specific targets to build their scam around, usually financial institutions, although other organizations like PayPal and eBay are consistently targeted at a lower, yet still significant, level. Each target may be used for a few weeks or more before moving on to new targets. The following charts in Figure 13 show two different snapshots of this targeting. In both early November and early December 2007 the chief target was NatWest Bank. Among the second tier, the Bank of Scotland and Citizens Bank were targeted in early November but not in early December, when HSBC, Citibank and Fifth Third bank were targeted.

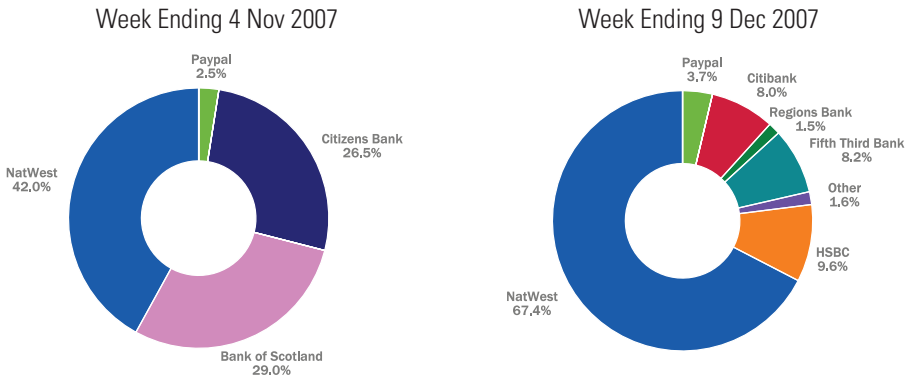

Figure 13: Phishing Targets in November and December 2007

2 Rocky Gang: Pervasive Phishers - http://www.marshal.com/trace/traceitem.asp?article=190

THE THREAT LANDSCAPE

Malware and Botnets

It would be incomplete to discuss spam without commenting on the malware and criminal activity that sustains it. Distributing spam and malware is firmly in the domain of professional criminals looking for financial gain. In the last six months, cyber-criminals have, unfortunately, reached new heights of sophistication and capability. The following are some key points that emerge from our observations of malware and botnets over the last six months of 2007.

Botnets Remain the Major Problem

The vast bulk of spam is sent via botnets, and spam is increasingly dominated by the large volume campaigns from the major botnets:

- Earlier in this report, we noted that a particular type of male sexual organ enlargement spam comprised 33% of all the spam captured by the TRACE spam traps in November and December 2007.

- Another group, which we call the 'Celebrity Gang' owing to their habit of using celebrity names in the malware they spam out, was responsible for over 20% of all spam in the same period[3].

Not only have the large botnets taken over in terms of spam volume, they have also evolved to reach new levels of sophistication. During the middle of 2007, the Storm botnet grew rapidly following mass spamming of emails containing links to websites hosting malicious code. The websites not only hosted executable files that could be downloaded by users, but they also hosted malicious code that attempted to exploit a number of different known browser vulnerabilities. The Storm botnet also uses:

- Its own peer-to-peer protocol with multiple command servers, making it difficult to disable

- Fast-flux networks with rapidly changing DNS records to distribute load and reduce the effectiveness of blacklist IP blocking[4]

- Proxy redirection where back-end servers hide behind many front-end hosts - usually compromised home computers

- Encrypted communications between nodes, making it harder to track and allowing the botnet to be segmented for renting to third parties[5]

---

3 Celebrity spam gang are major players - http://www.marshal.com/trace/traceitem.asp?article=389&thesection=trace

4 Cyber-criminals up the ante with fast-flux - http://www.marshal.com/trace/traceitem.asp?article=259&thesection=trace

5 The Changing Storm - http://www.secureworks.com/research/blog/index.php/2007/10/15/the-changing-storm

These kinds of developments elevated botnet sophistication to new levels in 2007 and were behind the large increases in spam, particularly in the second half of the year.

Increasingly Professional Criminal Cybereconomy

The groups behind spam and botnets are sophisticated and highly organized. They operate in a thriving underworld marketplace where services, software tools, and software development are freely bought and sold. Computer skills are no longer necessary to execute cybercrime. Malware authors, who may not even commit crimes themselves, simply develop and sell the tools, some of which come complete with support services[6]. This marketplace is increasingly competitive and there is evidence that the price for acquiring tools is decreasing[7].

Botnets, for example, have become tools that are bought, sold or rented. In one recent case a botmaster leased his botnet for as little as US$200 per week for 6,000 bots[8]. With this low outlay, a spammer can send 100 million spam messages or more. The potential profit for spammers is now considerable. In one recent court case, a spammer admitted to earning US$250,000 profit[9]. It is this sort of money that is driving ever greater volumes of spam.

Spam and Malware are Increasingly Blurred

The distinction between spam and email-borne malware is not clear-cut anymore. Botnets are used to distribute spam and malware alike. At one moment, a particular botnet campaign might be a garden-variety Viagra spam run; at the next, it could be a campaign with a malicious file attached to the email or a link to a website hosting malicious code. Increasingly, spam contains both an advertising message and malicious code, or links to malicious code (Figure 14). In terms of content filtering, the question today is no longer "is it spam?", rather it has become "did it come from a bot?".

---

6 Cyber-crime for sale - http://pandalabs.pandasecurity.com/archive/Cybercrime_2E002E002E00_-for-sale-_2800_II_2900_.aspx

7 Mpack Clearance Sale - http://www.symantec.com/enterprise/security_response/weblog/2007/07/mpack_clearance_sale.html

8 True crime: The botnet barons - http://www.infoworld.com/article/07/12/17/50FE-busted-botmen_1.html

9 High-earning spammers face tougher sentences - http://www.networkworld.com/community/node/22659

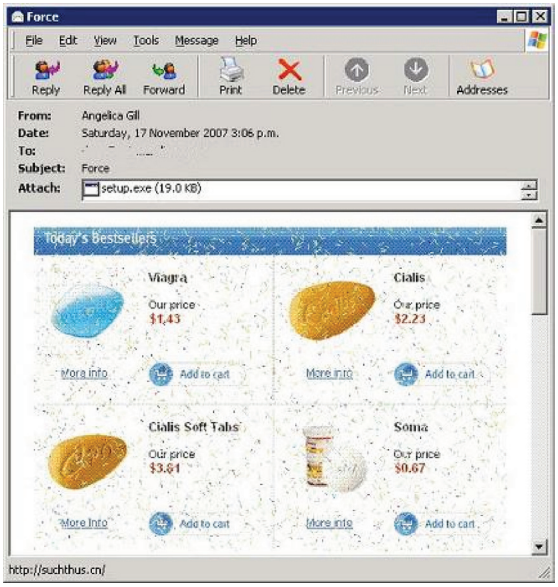

Figure 14: Combined Spam and Malware Example

Malware Distribution Shifts to the Web

In our last Security Report in June 2007, we noted that malware was increasingly being distributed via the Web. There are a number of reasons for this.

- The increasing popularity of Web activities, especially forums, blogs and social networking sites with their rich user interaction
- Increased capabilities of Web browsers to execute code or launch external programs
- Propensity for the software on end-user computers to be managed badly and seldom updated, allowing easy exploitation

These elements are changing the way cybercriminals are distributing malware. The second half of 2007 saw the distribution of malware via the Web on a scale never seen before. Some of the techniques we observed were:

- **Email mal-advertising.** We saw large campaigns involving email 'mal-advertising' with email spammed out with a URL link pointing to malicious code hosted on a Web server. The link can be as simple as a link to an executable which needs the user input to download and execute it. Or the website may host malicious code that seeks to exploit known browser vulnerabilities. The mid-year Storm phenomenon was a good example of mal-advertising in action.

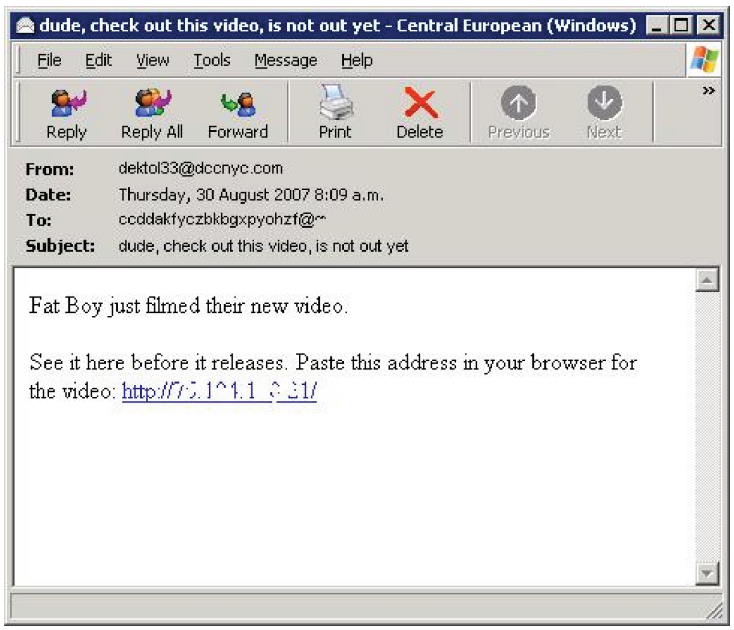

Figure 15: Storm Email 'Mal-advertising' a Website Hosting Malicious Code

- **Hacking of legitimate websites.** Instances of legitimate websites being hacked continue to happen at regular intervals. In November we saw the Monster.com website infected by a malicious IFrame that directed users to a website that served up a range of exploits[10]. We also saw the hacking of MySpace profile pages, in particular that of Alicia Keys, where users were diverted to a malicious website by means of a large background image hyperlink[11].

- **Mass spamming of blogs and forums.** In late 2007 we saw evidence of bots that post URL links and keywords to many online forums and blogs. This served to increase the search engine rankings for the attacker's malicious Web pages that were crammed full of those same keywords. The end result is that users searching for seemingly innocuous terms may end up at websites hosting malicious code[12].

- **Use of real Web services accounts to send spam.** During the year we saw accounts at several Web services, including Hotmail, Gmail and YouTube, used to send spam. Spammers had found a way to create valid accounts en-masse and then used them to send spam via the legitimate email servers hosted by the service[13].

---

10 Monster.com hit with another malware attack - http://www.securecomputing.net.au/news/97730,monstercom-hit-with-another-malware-attack.aspx
11 MySpace profiles install spyware - http://www.marshal.com/trace/traceitem.asp?article=388
12 Malware 'Spread-by-Web' continues - http://www.marshal.com/trace/traceitem.asp?article=445
13 YouTube used to send spam - http://www.marshal.com/trace/traceitem.asp?article=331

CONCLUSION

While image spam and stock spam died away, the overall volume of spam continued to increase in 2007. While some attempts were made by spammers to use new techniques such as PDF attachments, spammers largely reacted to better anti-spam technology by improving their botnets and simply sending a greater volume of 'ordinary' spam. Currently, it is not uncommon for enterprises to report spam accounting for over 90% of their inbound email.

Despite the increased efforts of law enforcement agencies to crack down on spammers and their botnets, spam grew even worse in 2007. It seems that whenever a spamming gang is caught, there are others that jump up in its place. The financial motive of the cybercriminal underworld that sustains spam appears to remain strong. The cost of acquiring the tools and services needed to send spam is also reducing. For these reasons, we are not optimistic that spam is going to recede in 2008.

Predictions for 2008

- The technical sophistication of the Storm botnet is just the beginning. The major botnet operators will further refine their technology and other groups will seek to emulate them, driving even greater volumes of spam in 2008.

- The use of spam 'mal-advertising' to lure users to websites hosting malicious code will continue to grow strongly. More and more, these attacks will look and feel 'legitimate' to the end user.

- The shift to using the Web to distribute malware will continue as cybercriminals seek to exploit the growing use of Web services such as forums and blogs, as well as users' propensity not to update their software.

- The massive growth in popularity of social networking sites like Facebook, MySpace and LinkedIn, as well as the share sites like YouTube, will guarantee increased attention by cybercriminals. User suspicion levels are lower when accessing such familiar sites. Information gleaned from these sites will also be used for targeted attacks, for example, to promote items of interest like videos of a favorite sports team or a new music video.

- The use of newer technologies, notably instant messaging and Internet telephony, to spread spam and malware will increase as cybercriminals seek to exploit easier, unprotected systems.

Recommendations

Enterprises and computer users need to continue to be vigilant as cybercriminals get ever more professional and sophisticated. Receiving email and browsing the Web, now involves more risk then ever before. Here are our recommendations for 2008:

- Good anti-spam protection is imperative. Ensure that your spam filtering systems employ defense-in-depth by using multiple technologies for maximum resiliency.
- Take steps to secure Web browsing at the gateway, including the restriction of executable and other content that can be downloaded by users.
- Keep Web browsers and other desktop software meticulously up-to-date, as many malicious websites utilize old, known exploits.
- Educate users about the new dangers of email and browsing, to ensure they avoid following links in unsolicited email and are suspicious of unexpected download prompts when browsing.

TRACE will continue to monitor and research spam and the wider threat landscape to 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, please email us at trace@marshal.com.

CONTACT MARSHAL

EMEA
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

MARSHAL™
Secure. Protect. Comply.