MARSHAL8e6™

Marshal8e6 Security Threats:
Email and Web Threats

By Marshal8e6 TRACELabs January 2009

Contents

Introduction:

This report has been prepared by the Marshal8e6 Threat Research and Content Engineering Team (TRACE). It covers key trends and developments in Internet security over the last six months, as observed by TRACE security analysts.

TRACE researches spam, phishing, Web exploits and malware. It is also responsible for the anti-malware defense and updates for Marshal8e6'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 http://www.marshal.com/trace.

Summary

- Spam volumes rose strongly in 2008 and TRACE estimates that global spam volume exceeded 150 billion messages per day at its peak.
- Spam declined by 50% overnight in November when a hosting provider called McColo that was hosting control servers for several spam botnets was taken offline.
- One major spamming botnet, Srizbi, is yet to recover from the McColo shutdown, although spam volume is rebounding again through Mega-D, Rustock and other botnets.
- Blended attack spam which directs users to Web pages hosting malicious code via URL links rose strongly in mid-2008, peaking at 33% of all spam. However, this dropped to a more typical level of 1% by the end of the year.
- Health-related spam, usually promoting cheap online drugs, continued to dominate, constituting 70% of all spam.
- Phishing volume rose in 2008 peaking at nearly 4%of all spam as the major spamming botnets Srizbi and Pushdo began to 'phish' more actively. However, after the McColo shutdown phishing declined to less than 1%.
- Browser vulnerabilities continued to be a key attack vector for criminals.
- Literally millions of legitimate Websites are now hosting malicious code. Mass Website attacks by botnets are one of the most concerning developments of 2008.
- Criminals are increasingly abusing free Web services such as file hosting, blogs, and other services, to host spam landing pages and malicious code. They are also using sophisticated Search Engine Optimization techniques to drive users to their infected Web pages.
- The social networking sites MySpace, Facebook, Bebo, and others came under attack by malware called Koobface that spread links to other users in an effort to distribute malware.

Email Threats

Spam

Spam remains a huge problem for enterprises. Not only does spam consume valuable network resources, it remains a popular conduit for the distribution of malware, phishing and scams. At its peak, TRACE estimates that global spam volume exceeded 150 billion messages per day in 2008. Organizations typically report that spam represents anywhere from 75-95% of their inbound email.

Spam Volume

2008 was a rollercoaster year for spam. The first half of the year saw strong growth in spam volume, fuelled by the rise of several dominant spamming botnets. The second half of the year was characterized by a plateau, then sudden drop off in spam volumes as several of those same botnets were disabled.

At TRACE, the proxy for spam volume movements is our Spam Volume Index (SVI), which tracks the volume of spam received by a representative bundle of domains that we monitor. The Marshal SVI showed an 85% increase in spam from January to June 2008. Spam volume appears to have peaked mid-year, and then started to fall away from September onwards. Then, on November 11, an ISP called McColo, which was hosting control servers for several major botnets, was disconnected from the Internet[1]. Spam literally dropped by over 50% overnight as the botnets became effectively disabled. Spam volumes in mid-November were at the lowest levels we have seen since mid-2007. Of course, no one really expected this situation to last very long and volumes increased once again in December as some botnets came back on stream and others gained extra business.

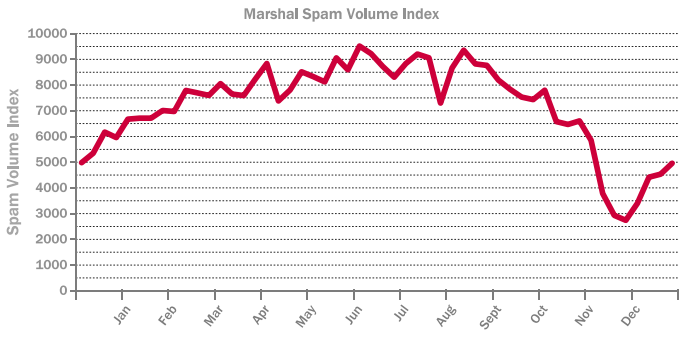


Figure 1: Marshal Spam Volume Index (SVI)

Botnet Sources of Spam

The vast majority of spam is churned out from a mere handful of botnets. During 2008 TRACE undertook extensive research into spam and its botnet origins and posted its findings on the TRACE Website. In our last report we highlighted that 75% of spam came from just three botnets, and that the top seven spamming botnets were responsible for 90% of all spam (Figure 2).

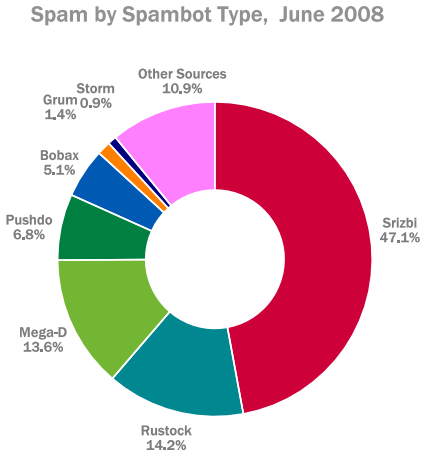


Figure 2: Spam by Spambot, June 2008

Removing any doubt about the dominance of these botnets, the McColo shutdown in November demonstrated the impact of disabling them, by substantially reducing the volume of spam in circulation. Post-McColo, the situation looks substantially different. Srizbi has all but disappeared. However, the other major botnets with control servers hosted at McColo (Mega-D and Rustock) eventually recovered and continue to spam strongly. In the aftermath of McColo, another botnet, Xarvester, has managed to gain market share and is now one of the leading sources of spam (Figure 3 and 4).

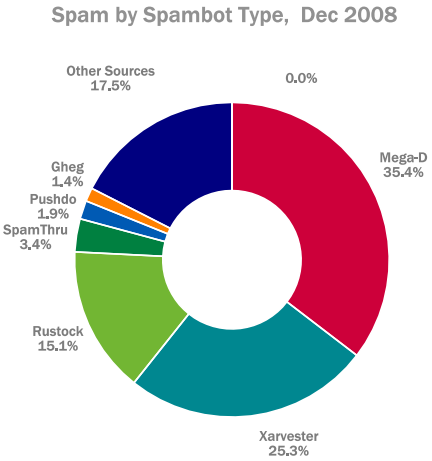


Figure 3: Spam by Spambot, December 2008

Figure 4 illustrates the shifting sands of the spam botnets in their quest for control of your inbox. The Srizbi botnet dominated spam for much of 2008. In fact, Srizbi was largely responsible for driving spam volumes up during the first part of the year. At times, Srizbi was responsible for 50% of all the spam received in the TRACE spam traps during 2008.

Along with Srizbi, other major spam botnets had varying fortunes in 2008. Rustock grew strongly around mid-year due to several aggressive malicious “news” spam campaigns that often ended up infecting systems with the Rustock bot as well as other, more obvious, rouge ‘anti-virus’ malware[2]. Mega-D (also known as Ozdok), Pushdo (also known as Cutwail),

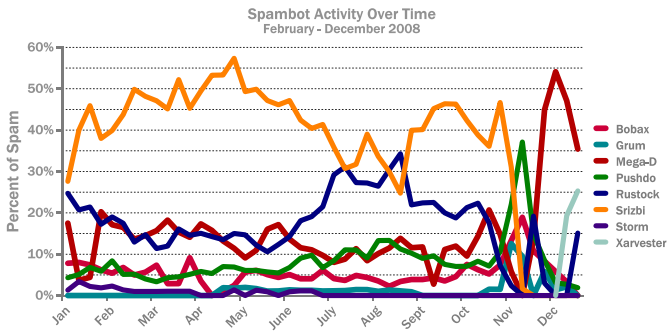


Figure 4: Spambot Activity over Time, February – December 2008

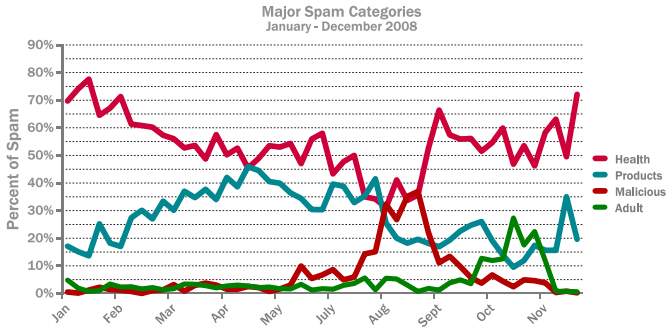
Bobax (also known as Kracken), and Grum maintained a constant presence throughout the year. Meanwhile, the infamous Storm slipped in importance mid year and finally faded away to nothing in October[3].

Some of these botnets consist of hundreds of thousands of compromised computers. Just after the McColo takedown, Srizbi was estimated at 450,000 bots[4]. In our lab, we have measured individual bots sending spam at rates of up to 25,000 messages per hour. We estimate the Srizbi botnet, at its peak, was capable of some 60-80 billion spams per day.

Spam Categories

During 2008, we saw several significant shifts in the types of spam we were seeing, reflecting the changing fortunes of the various affiliate programs that the spammers and botnet operators sign up for (Figure 5).

Figure 5: Rise in Product and Malicious spam



Health spam remains dominant

Health spam, largely touting cheap online drugs, started and ended the year at around 70% of all spam. One of the most popular and persistent programs spammed is 'Canadian Pharmacy' one of the brands of Glavmed, a major affiliate program that pays spammers to promote their Websites[5].

Figure 6: 'Canadian Pharmacy' affiliate spam program

In October, the US Federal Trade Commission and the New Zealand Department of Internal Affairs took action and seized the assets of a competing affiliate program, called Affking, which was behind some of spam's most voluminous and notorious brands such as 'VPXL', 'ManSter', 'MegaDik', and 'King Replica'. During 2008, TRACE was pleased to assist the authorities in their investigations into the activities of this group[6]. The demise of this group had a noticeable, but minor impact on spam levels, as the botnets appeared to quickly switch to other programs.

Product spam rises, then falls

Product spam rose early in the year to almost 50% of all spam, but has since fallen back to around 20%. Product spam promotes fake watches such as replica Rolex, Patek Philippe, Bvlgari and Tag Heuer, as well such things as designer handbags, shoes, pens and accessories, most commonly counterfeits of high profile brands like Ugg, Prada, Versace and Dior.

Adult dating spam is briefly popular

Our adult-related spam category consists of two types: porn and dating. It was dating spam that rose strongly in October and November, a large part of which was spammed out from the Mega-D botnet prior to the McColo shutdown. This "dating" spam arguably falls into the scam category as the intention of it appears to be for 'Russian girls" to establish contact with a victim, establish a rapport and then request money for 'travel' expenses[7].

Malicious spam skyrockets in mid-year

During July to September, TRACE observed a huge increase in malicious spam that peaked at over 30% - one in every three spam messages - in August (Figure 5). This Blended Attack spam consists of "mal-advertising" – using URL links to drive users to Websites hosting malicious code that attempts to install malware on the victim's computer. A large portion came from the Srizbi botnet seeking to expand its bot army even further. The Rustock botnet, too, was behind numerous malicious spam campaigns using dramatic celebrity, or current affairs subject lines, and even mimicking CNN Daily News alerts[8] (Figure 8).

Figure 7: Dating Spam 'Scams'

Figure 8: 'CNN News' malicious spam from the Rustock botnet

The scale of these malicious spam campaigns was a major departure from what we have seen in the past. A popular payload during this period was fake antivirus software, which seems to 'scan' the victim's computer, 'find' lots of malware, then request money for the full software (Figure 9). Often during such attacks, unknown to the user, other malware was also installed silently in the background - including spambots that perpetuate more spam.

Figure 9: Fake Anti-virus was spammed out mid-year

Gambling spam increases noticeably

Gambling spam, which promotes various online gaming sites, increased significantly, peaking at some 13% of spam in November 2008. This probably reflects the increasing popularity of online gaming and the wealth of dubious sites out there. In October, TRACE observed spam campaigns encouraging the download of executable gaming clients[9].

Figure 10: Spam promoting online gaming increases

Spam Message Structure

In contrast to the extensive experimentation of 2006 and 2007 that leveraged image obfuscation and randomization techniques, spam in 2008 looked 'normal'. There is roughly a 70:30 split between HTML formatted spam and plain text spam. Image spam has dropped away and now represents only 1 or 2 % of all spam (Figure 11). Instead of fancy tricks, it seems spammers now rely on simplicity, social engineering and sheer volume to push enough of their messages through the anti-spam filters.

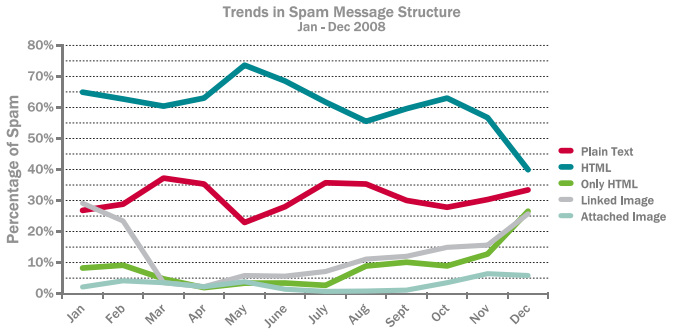


Figure 11: Trends in Spam Message Structure

In late 2008 we saw an upsurge in the use of small HTML-only message bodies, with little or no readable text and a linked image retrieved from the Web. Spam also often used typical non-delivery receipt (NDR) subject lines (Figure 12).

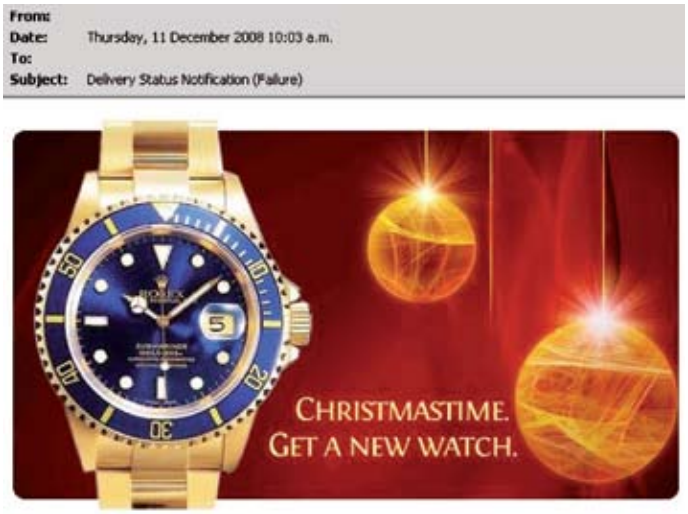


Figure 12: HTML-only spam with an image retrieved from the Web and NDR subject

Phishing

The proportion of phishing in spam generally rose throughout 2008, reversing last year's trend. One of the reasons for this was that the major spamming botnets like Srizbi, and Pushdo, in particular, started to 'phish' whereas in 2007, phishing was largely absent from their activities. There was a distinct peak in phishing activity in October/November as numerous campaigns were mounted by several botnets[10] (Figure 13).

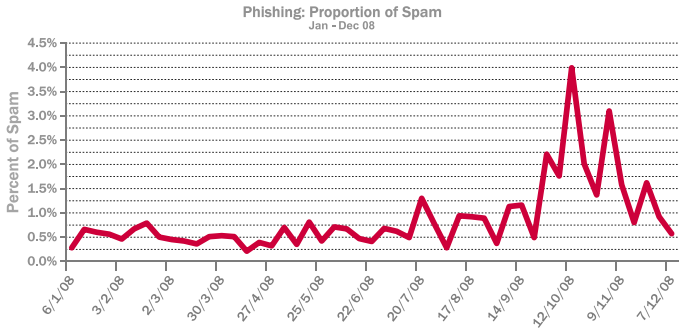


Figure 13: Phishing as a Proportion of Spam

Phishing follows a simple formula. Essentially, phishing spam looks like legitimate email that asks you to confirm your login security details. You link to what you think is your bank's Website and use your login name and password. However, the link that the phishing email provides, in fact, points to a false Website that looks authentic, but is in fact controlled by the phishers. As a result, the cyber criminals gain access to your bank account details which they can then use to steal your money or sell on to other criminals as part of a wider identity fraud.

Given the nature of phishing, it is not a surprise that major financial organizations, particularly those in the US, are targeted. Figure 14 shows the major US phishing targets at the end of December 2008.

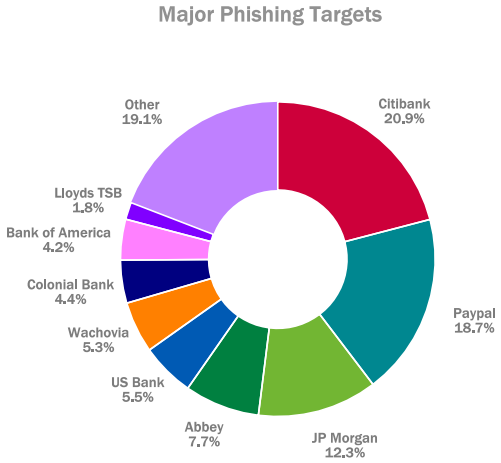


Figure 14: Major Phishing Targets, Dec 2008

Email-borne malware

In the past, email-borne malware such as the mass-mailing viruses Netsky, Bagle and MyDoom, were the chief concern of email administrators. These viruses still exist, but in volume terms they now form a very small part of the malware in incoming email – around 0.05% or less. Traditional anti-virus software deployed at the email gateway usually protects against these viruses.

Most of the malware attachments that TRACE observes today in email are spammed out from the major botnets. The Pushdo botnet is particularly notorious for this activity.

Most days it is seen spewing all forms of email with malicious attachments. The attachment itself can vary, but it usually contains a sophisticated downloader that often avoids standard anti-virus detection. The malware seeks to download further components from the Web, which may function as an information stealer, a spambot, or fake anti-virus depending on the purpose of the campaign.

TRACE documented several cases during 2008 of Pushdo's malicious email[11]. A favorite subject line – which is still being used – is one purporting to be a UPS Tracking ticket number. The executable file is located inside a zip attachment masquerading as an invoice (Figure 15).

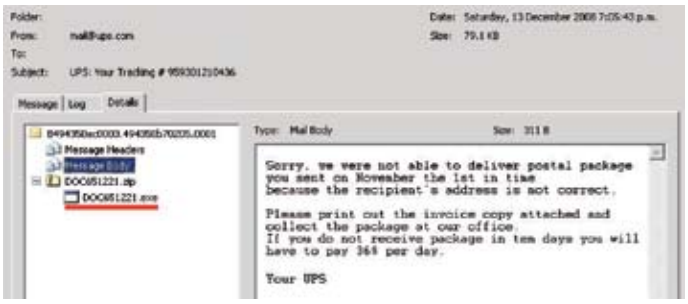


Figure 15: Fake UPS notification containing malware downloader from Pushdo botnet.

As the malware-laden email from the botnets is essentially spam, it can be identified using the same means as spam. Anti-spam filters, whether they use reputation or heuristics, play an important part in blocking malware as part as a defense-in-depth strategy.

Web Threats

Simply browsing the Web is an increasingly risky business. Feature-rich browsers, plug-ins, and advanced Web applications have brought with them a whole new range of potential vulnerabilities. And attackers are exploiting these vulnerabilities to distribute their malware on a scale not seen before. This section covers a few major Web security exploits and themes that TRACE has observed over the last six months.

Browser Vulnerabilities

The browser itself remains a key attack vector. As we highlighted in our last report in June, some 45% of Internet users are potentially at risk from simply running old or un-patched browsers[12].

Web browser vulnerabilities are commonly exploited when users visit Websites hosting malicious code, usually JavaScript. The Websites themselves are often legitimate sites that have been hacked, as opposed to specific sites that have been set up by the criminals.

Even if you are fully up to date with your browser software, there are no guarantees of security. As we were writing this, another significant, un-patched, vulnerability in Microsoft Internet Explorer was discovered and was being exploited by malicious JavaScript code hosted on legitimate Websites[13] (Figure 16).

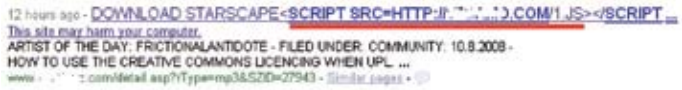


Figure 16: Legitimate sites hosting malicious code snippets

This attack follows a similar theme to those we saw earlier in the year where literally millions of Websites were affected by SQL Injection attacks launched by the Asprox botnet. Each bot searched Google for .asp pages that contained specific terms and then launched a SQL Injection attack against the Websites returned, to insert malicious JavaScript into the pages on each site. The JavaScript itself directed users automatically to Websites hosting various exploits[14]. Over 1.5 million legitimate Websites were affected.

In our view, this style of mass Website attack is one of the most concerning issues to arise in 2008. The explosive growth of these attacks, and the use of botnets to promulgate them, is worrying - it is highly likely we shall see more of this style of attack in the future.

Criminals Use Free Web Services

Criminals have been quick to utilize the wealth of free Web hosting and other services being offered by various vendors. During the last six months, TRACE has documented the following cases:

- Use of YouTube's Channels to direct users to other Websites[15]
- Microsoft's Windows Live Spaces and SkyDrive used to host malicious files and spam landing pages[16] [17]
- Google's Notebook used to host spam landing pages[18]
- Google's Blogspot pages hosting 'blogspam' – spam posted to blogs – that direct users to other Websites hosting spam or malicious content[19]

Figure 17: Windows Live Spaces page hosting malicious code

Search Engine Optimization

Like any owner of a Website, criminals are interested in driving increased traffic to their pages. During the last six months, TRACE observed operations using sophisticated Search Engine Optimization (SEO) techniques to increase the chances of their Web pages being returned higher up in search engine queries.

One operation used millions of search terms covering almost any topic imaginable to influence as many searches as possible[20] [21]. Users entering seemingly innocuous search terms like 'ski Alaska' were presented with malicious links surprisingly high up in the search results (Figure 18).

Another SEO operation we observed used top search terms from Google's Hot Trends service to help drive users to Websites hosting malicious code[22].

These cases underline the need for users to always be vigilant when presented with any links whether they are in an email or search engine results.

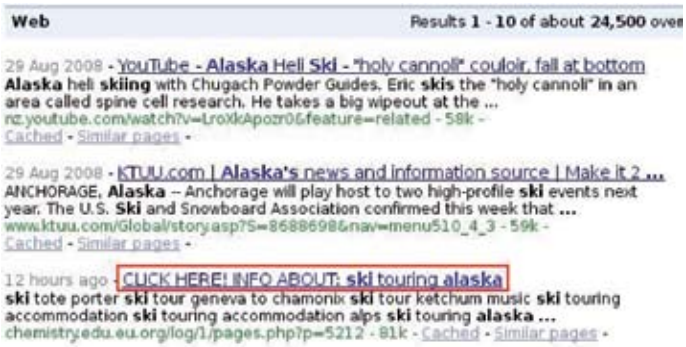


Figure 18: SEO techniques push up search engine rankings

Exploitation of Social Networking Websites

As widely predicted by many, including TRACE researchers, social networking sites came under increasing attack during 2008.

One piece of malware, known as Koobface, drew lots of attention. Koobface works by infecting user profiles, and then using mechanisms such as Facebook's private messaging system to spread messages containing links to other users. After clicking on the link the user is taken to another Website hosting malicious code. Koobface is now known to target facebook.com, myspace.com, bebo.com, friendster.com, myyearbook.com, and blackplanet.com. In one case we investigated, the Website mimicked YouTube. The profile picture of the Facebook friend, the account where the link was originally sent from, was included in the page to make it look as if they posted the video[23] [24].

Figure 19: Fake YouTube site linked from Facebook message.

Conclusion and Predictions for 2009

Spam remains a huge problem for enterprises, with a handful of major spamming botnets being responsible for the bulk of spam, phishing and email-borne malware distribution. During 2008, with the help of TRACE's research, some of the major botnets behind spam emerged from the dark and the anti-spam community took action against them, with some success. Despite this success, and perhaps inevitably, spam volume is bouncing back and new spamming malware is already delivering ever more spam.

Over the longer term, the botnet operators will learn from the McColo incident and evolve their control systems. They may adopt a more resilient peer-to-peer or layered model where control servers are harder to access and spread among many hosts – much like the Storm botnet. However it develops, the key challenge for all in the security community is to keep exposing and maintaining the pressure on these botnets. As November's events show, it can have a positive impact on spam, and by association, on malware distribution.

As the world increasingly conducts its business through the Web, browser vulnerabilities will continue to be a major attack vector, with attackers continuing to exploit both old and new vulnerabilities.

The exploits we have highlighted in this report illustrate one of the essential problems of the Web 2.0 world: the Web is alive with rich Web applications, free Web services, hosting and user-generated content. The potential for emerging security issues in this environment is high. Attackers will continue to focus their efforts in this area by targeting Web applications, and abusing free Web services. The result is that, in many cases, we can no longer automatically trust legitimate Websites. As we highlighted in our last report, social engineering will also remain a key theme for attackers. The various campaigns we have seen over the last six months have shown us that simple social engineering ploys still appear remarkably effective.

Marshal8e6 sees the following six threats as the major issues to be dealt with in 2009.

1. Spam Botnets – The success of the McColo take down gives us great hope for the future; this had a profound effect on Spam volumes. Unfortunately the controllers of the affected Botnets were able to bring their command servers back online long enough to re-point their bots at new network locations and so spam volumes have recovered somewhat, but the decline of the Srizbi Botnet proves that this method of addressing Botnets can and does work. The negative side of this is that the increased pressure on the Botnet operators will force them further underground and we may see them develop ever more complex command and control networks.

2. Legitimate Websites Serving up Malware – Spammers, hackers and malware writers are increasingly exploiting seemingly harmless, legitimate Websites to serve up malware. Blogspot, free hosting services, and even Auntie Martha's online healthfood Website have been targets for hackers to pervert and exploit for hosting malware. There are numerous reasons why this is occurring; traditional URL filtering typically fails to identify the change in threat status of a compromised legitimate Web site fast enough, someone else takes the blame and has their site blocked as malicious and the hackers can hide their malicious payloads behind the good reputation of legitimate sites when users have their guards down. This trend is likely to revolutionize the way that Web security vendors classify Websites and assume sites as inherently safe or unsafe.

3. Social Networking Sites – The massive growth in popularity of sites like Facebook and LinkedIn, as well as the share sites like YouTube will continue to be a major target in 2009. The biggest reason for this is that user suspicion levels are lower when accessing familiar sites such as these and typically will open messages purporting to be from these sites. The owners of these sites need to improve the capability they currently have in place for protecting their users from these risks. These sites are quick to develop new capabilities to stay ahead of competition and attract new users, but are slower to protect their Websites from misuse.

4. Blended Email Attacks – This is a growing issue requiring integrated defence across email and Web security technologies that deliver effective real time malware scanning, reputation services and a good blend of signature and non-signature scanning technologies.

5. Virtualization – Many companies today are running or have run projects to consolidate their server infrastructure, the next target for many is the security infrastructure. At present there are few vulnerabilities known, but with the increasing reliance on virtualization, the attackers will begin to target and probe for vulnerabilities.

6. Growth in the Use of Free Web Services to Launch Attacks - Criminals are increasingly using and abusing free Web services such as file hosting, blogs and even Web-based email services such as Hotmail to launch and host their attacks. This will become more common with the decreasing effectiveness of CAPTCHA checks to prevent automated account creation and because organizations blindly trusting such services at their email and Web security gateways.

Beyond 2009, Marshal8e6 sees the growing importance of Secure Web Gateways. We anticipate that they will expand to also include Email traffic and other protocols which could be a further driver for even more market consolidation as today's traditional Email Security products will be embedded into these new emerging complete Web security products.

In summary, 2009 promises to be a busy and interesting year. Based on what we observed in 2008, today it is even more important for organizations to select their IT security partners very carefully that the partner has the right mix of experience, sustainability and perhaps most important of all, high level of technical innovation in predicting and addressing the threats of tomorrow.

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.

Endnotes

1 http://www.marshal.com/trace/traceitem.asp?article=815
2 http://www.marshal.com/trace/traceitem.asp?article=740
3 http://www.marshal.com/trace/traceitem.asp?article=786
4 http://blog.fireeye.com/research/2008/11/not-to-sound-the-panic-alarm.html
5 http://spamtrackers.eu/wiki/index.php?title=Glavmed
6 http://www.marshal.com/trace/traceitem.asp?article=797
7 http://pandalabs.pandasecurity.com/archive/From-Russia-with-Love.aspx
8 http://marshal.com/trace/traceitem.asp?article=725
9 http://www.marshal.com/trace/traceitem.asp?article=782
10 http://marshal.com/trace/traceitem.asp?article=777
11 http://www.marshal.com/trace/traceitem.asp?article=723
12 http://www.marshal.com/trace/traceitem.asp?article=701
13 http://www.marshal.com/trace/alertsitem.asp?article=837
14 http://www.marshal.com/trace/traceitem.asp?article=661
15 http://www.marshal.com/trace/traceitem.asp?article=780
16 http://www.marshal.com/trace/traceitem.asp?article=783
17 http://www.marshal.com/trace/traceitem.asp?article=782
18 http://www.marshal.com/trace/traceitem.asp?article=835
19 http://www.marshal.com/trace/traceitem.asp?article=722
20 http://www.marshal.com/trace/traceitem.asp?article=746
21 http://www.marshal.com/trace/traceitem.asp?article=753
22 http://www.marshal.com/trace/traceitem.asp?article=783
23 http://www.marshal.com/trace/traceitem.asp?article=729
24 http://www.marshal.com/trace/traceitem.asp?article=839

MARSHAL8e6™

Corporate Headquarters
Marshal8e6

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Marshal8e6

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Marshal8e6

Suite 1, Level 1, Building C
Millennium Center
600 Great South Road
Aukland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720