MARSHAL TRACE REPORT

MARSHAL™
Secure. Protect. Comply.

Marshal Security Threats: Email and Web Threats

By Marshal Threat Research & Engineering Team
July 2008

CONTENTS

CONTENTS	2
INTRODUCTION	3
EXECUTIVE SUMMARY	3
EMAIL THREATS	4
Spam	4
Spam Volume	4
Source of Spam	5
Spam Categories	7
Spam Message Structure	9
Webmail Spam	10
Phishing	10
WEB THREATS	12
Browser Vulnerabilities	12
Mass Website Hacks	13
Blended Threats	14
PREDICTIONS	15
Recommendations	15

INTRODUCTION

This report has been prepared by the Marshal 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 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 http://www.marshal.com/trace.

EXECUTIVE SUMMARY

- Criminals are moving en masse to the Web to distribute malware on a scale not seen before; the browser and browser plug-ins are key targets, with more than 45% of Internet users potentially at risk from running old or unpatched browsers

- Much malicious code is now hosted on legitimate websites that have been compromised, as opposed to sites criminals have specifically set up; this makes URL filtering or site reputation services less effective as previously 'safe' sites may now contain threats. The other event which further reduced the effectiveness of URL Filtering and reputation is the DNS flaw identified by Dan Kaminsky early in 2008 and the ISPs delay in patching their DNS servers.

- Malicious spam, which incorporates URL links to websites hosting malicious code, rose sharply as the major botnets sought to increase the size of their botnets and to distribute third-party malware. (Note: As this report was going to print, malicious spam accounted for 30% of all spam.)

- Webmail spam from providers such as Yahoo, Hotmail and Gmail, using accounts automatically created using Captcha-breaking methods is a worrying new development rendering IP reputation and message header inspection less effective because the source and header are legitimate

- Spam continued to increase in volume, showing a doubling for the year ending June 2008

- About 75% of spam comes from just three botnets; the top seven spamming botnets are responsible for 90% of spam

- The worst spam offender is the Srizbi botnet, which is hard for infected users to detect and capable of pumping out 63 million messages in an 8 hour day. At times, Srizbi has been responsible for nearly 50% of spam; Rustock and Mega-D botnets are also prolific botnets. (Note: As this report was going to print, Rustock was challenging Srizbi as the chief spamming botnet)[1].

- Product spam, pushing replica watches and fake designer accessories, has increased significantly, challenging the supremacy of health-related "pills" spam

- Image spam has slowed to less than 1%, while experiments with other attachment types has ceased as spammers concentrate on high volume, simpler text and html formats, with attention grabbing subject lines to encourage social engineering

- Although some of the major spam botnets are getting in on the phishing act, Phishing remains constant at about 0.5% of spam

- Several mass website attacks occurred in the last six months, including one SQL injection attack that affected over 1.5 million legitimate Websites. This botnet-driven activity is one of the most concerning new threats to emerge in the last six months. This has seen numerous data theft issues and unauthorized web page changes or substitutions.

EMAIL THREATS

Spam

Spam remains a huge problem, having clearly evolved beyond a mere nuisance. Not only does spam consume valuable network resources, it remains a popular conduit for the distribution of malware, phishing and scams.

Spam Volume

During the first six months of 2008, spammers continued their unrelenting invasion of our inboxes. Organizations typically report that spam represents anywhere from 75-95% of their inbound email. Global spam volume is now estimated to exceed 100 billion messages per day[2].

At TRACE, our 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 shows a doubling of spam volume for the year ending June 30, 2008. Interestingly, spam

1 Please reference http://www.marshal.com/trace/spam_statistics.asp for up to date statistics.

2 http://en.wikipedia.org/wiki/E-mail_spam

volume appears to have peaked around May 2008, and current volumes have receded from that high point. This growth in spam volume reflects the evolution of the major spamming botnets – as we shall explore next.

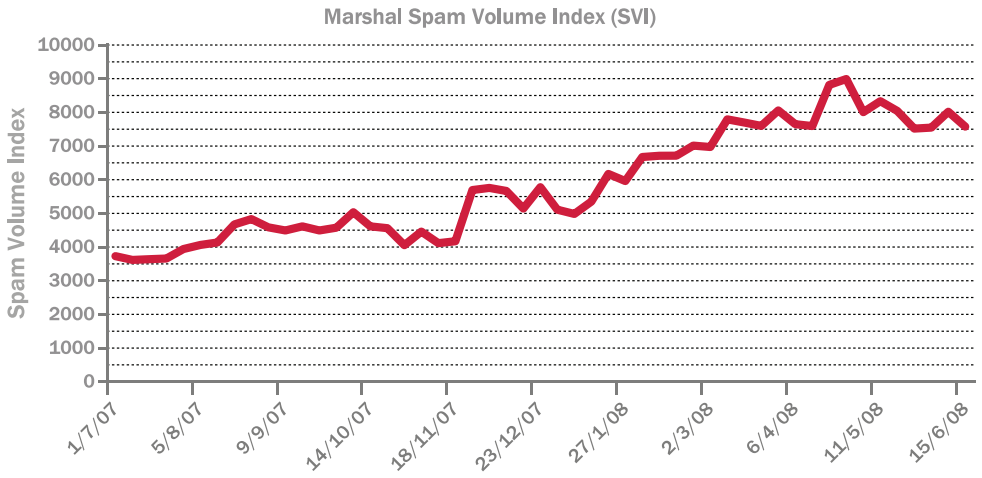


Figure 1: Marshal Spam Volume Index (SVI)

Source of Spam

So where does all this spam come from? The answer is that the vast majority of it is churned out from a mere handful of botnets. Over the last six months TRACE has done extensive research into spam and its botnet origins. The results are surprising. We estimate that approximately 75% of spam comes from just three botnets. The top seven spamming botnets are responsible for a whopping 90% of spam (Figure 2).

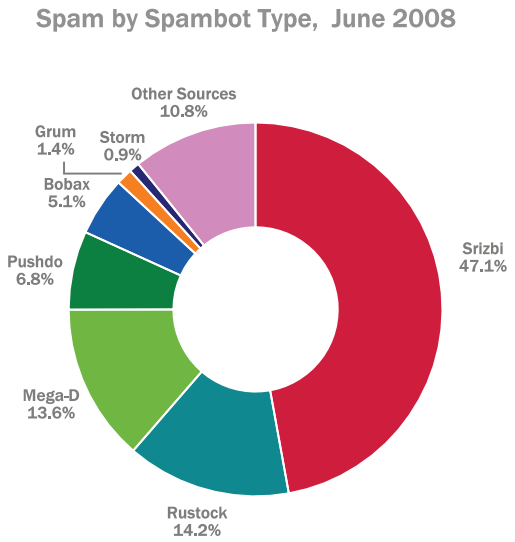


Figure 2: Spam by Spambot, June 2008

The most outstanding thing about this chart is the total dominance of Srizbi which, at times, has exceeded 50% of all the spam received in the TRACE spam traps (Figure 3).

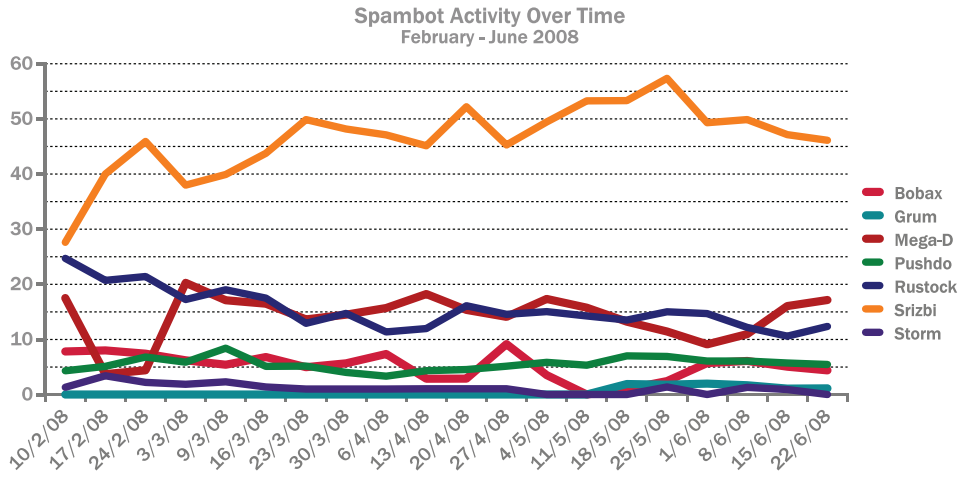


Figure 3: Spambot Activity Over Time, February – June 2008

Note Srizbi's rapid rise in February, which coincided with the beginning of an aggressive malicious spam campaign involving celebrity, "you look stupid" and other social engineering hooks to entice users to click on the link provided.

Srizbi is extremely stealthy, operating in full-kernel mode and using its own TCP stack, making it hard to detect on a computer. In April 2008 Srizbi was estimated at 315,000 bots[3]. At TRACE we have observed individual Srizbi bots pump out spam at a rate of 25,000 spam messages per hour, making the botnet capable of spamming 7.8 billion messages per hour. Assuming an average 8 hour day, this equates to some 63 billion messages per day. Such is the power of the modern spam botnet.

Along with Srizbi, the other major spam botnets, namely Mega-D (aka Ozdok), Rustock, Pushdo (aka Cutwail, Pandex), Bobax (aka Kracken and Hacktool.spammer) together account for nearly 90% of spam. Meanwhile, the infamous Storm has now slipped in importance to just less than 1% of spam. (Note: as this reports was going to print, Rustock was challenging Srizbi as the chief spamming botnet owing to a large scale and sustained malicious spam campaign).

Of course, the picture as represented by Figure 3 above is constantly changing as spam operations get interrupted, in some cases, by better anti-malware defenses or law enforcement, and, otherwise, by spambot software upgrades or replacements.

3 http://www.secureworks.com/research/threats/topbotnets/?threat=topbotnets

All of the spambots mentioned here are template driven, that is to say, once established on a computer, the spambot will contact a control server, download a spam template and a list of email addresses and proceed to spam. Sometimes more than one botnet will be spamming messages with links to the same websites, suggesting spammers have access to multiple botnets. In February 2008, TRACE noticed no less than five botnets - Srizbi, Mega-D, Rustock, Bobax and Pushdo – all promoting links to the "express herbals" brand website[4] peddling male enhancement pills.

Spam Categories

The six months ending June 2008 saw significant shifts in spam types (Figure 4). Early in the year health spam, particularly male organ enlargement messages, accounted for nearly 70% of all spam. Health spam had been the dominant type for the previous two years.

Product spam rises

Steadily, product spam has been on the rise and now rivals health spam as the biggest genre of spam being sent worldwide. In the past the vast majority of products on offer were fake watches such as replica Rolex, Patek Philippe, Bvlgari and Tag Heuer. Now, the fake watches are still on offer (Figure 5), but we also have designer handbags, shoes, pens and accessories, most commonly counterfeits of high profile brands like Ugg, Prada, Versace and Dior[5].

Most of the major botnets are in on the action - Pushdo, Mega-D and Srizbi have all been seen sending out huge volumes of spam pushing these imitation products.

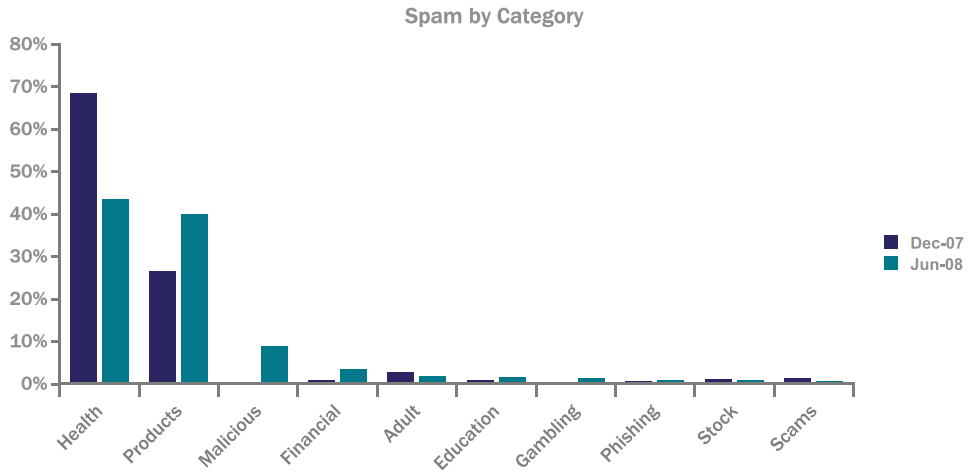


Figure 4: Spam By Category December 2007 and June 2008

4 http://www.marshal.com/trace/traceitem.asp?article=567&thesection=trace

5 Product Spam is the New King - http://www.marshal.com/trace/traceitem.asp?article=635&thesection=trace

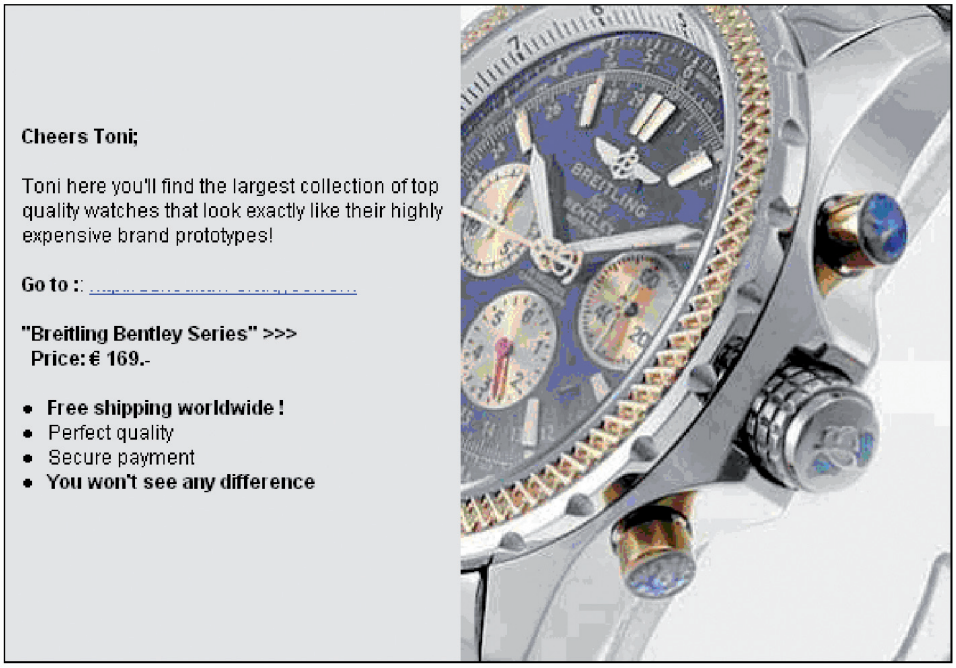


Figure 5: Example Replica Watch Product Spam

Malicious spam also increases

Also significant in Figure 4 is the substantial rise in malicious spam which does not seek to promote a product but, instead, leads to your PC being compromised. Here, spam is "mal-advertising" - driving users to websites hosting malicious code that attempt to install malware on the victim's computer. At TRACE we observed a huge increase in malicious spam that reached 10% of all spam in June 2008. (Note: as this report was going to print, this figure has increased further to 30%). A large portion was sourced from the Srizbi botnet seeking to expand its bot army even further. Lately, the Rustock botnet, too, has been behind numerous malicious spam campaigns[6] using dramatic celebrity or current affairs subject lines such as:

- Video of rampage in Tokyo
- Angelina Jolie dies in plane crash
- Clinton says: Hiliary cheated on me
- Subprime crisis FINALLY over: feds report
- Homeless man wins lottery
- Plane crashes into White House, injuring hundreds

The size of this increase in malicious spam is a major departure from what we have seen in the past. Some of these campaigns result in the

6 http://www.marshal.com/trace/traceitem.asp?article=681&thesection=trace

installation of multiple pieces of malware on a PC, including the spambots that perpetuate the spam. It would appear that not only are the botnet operators seeking to increase the size of their spamming botnets, they are also trying to install other malware in the same attack. In addition to advertisements for pills and fake bags, spammers may be turning to malware distribution as a significant new activity and revenue source.

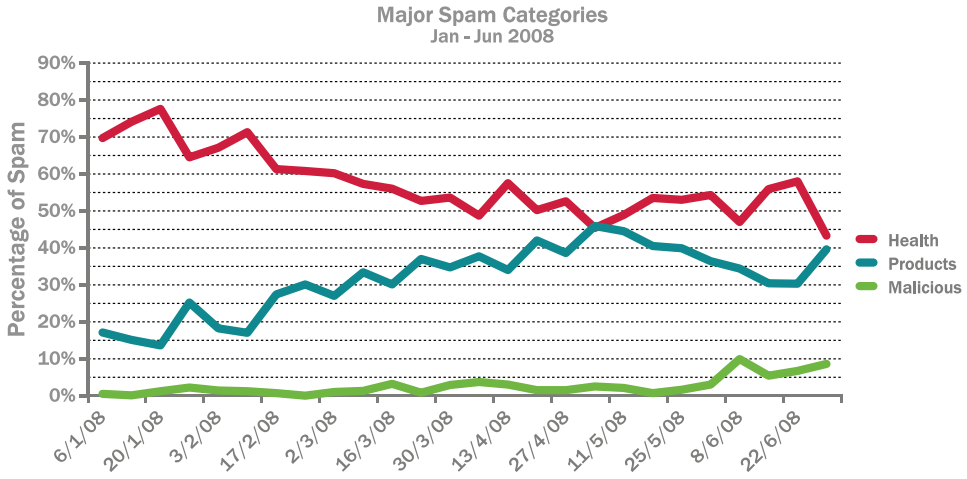


Figure 6: Rise in Product and Malicious spam

Stock spam remains insignificant

In 2007 stock spam was popular with Bot-herders and reached nearly 50% of all spam at one stage. However, as we noted in our prior report, stock spam dwindled to less than 1% in late 2007. Stock spam activity has remained at this low level for the first 7 months of 2008. Lower returns and successful law enforcement probably contributed to this decline.

Spam Message Structure

In contrast to the extensive experimentation of 2006 and 2007 with image, obfuscation and randomization techniques, spam in the first half of 2008 is relatively "normal" looking. There is roughly a 70:30 split between HTML formatted spam and plain text spam. Image spam has dropped away and now represents less than 1% of all spam (Figure 7). 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.

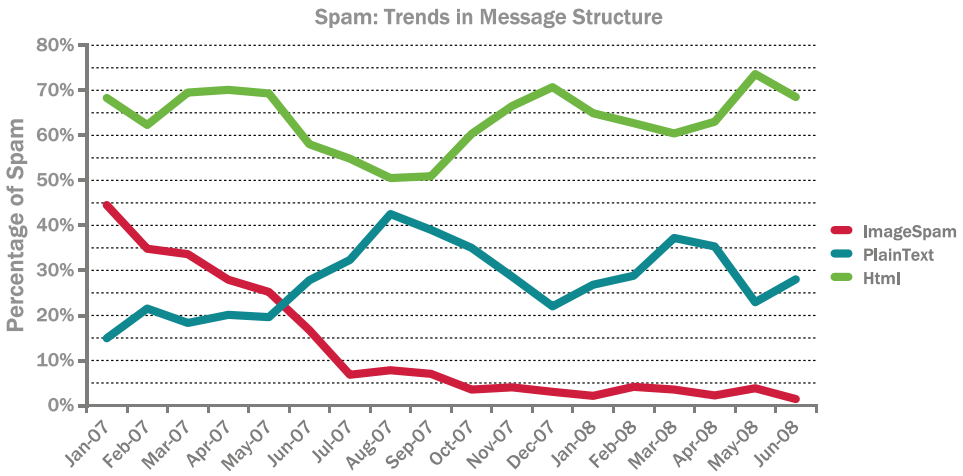


Figure 7: Trends in Spam Message Structure

Webmail Spam

A relatively new development is Webmail spam. There is currently a small amount of spam that originates from real Webmail service providers, such as Hotmail and Yahoo. What has happened is that spammers have automated the creation of user accounts at these services by various Captcha-breaking methods. Bots are then used to log into these accounts and send messages[7]. This spam distribution method is relatively small in overall spam terms – less than 1%. Nevertheless, the practice is a concerning development because it effectively sidesteps some common anti-spam defenses. For example, IP reputation and message header inspection are rendered useless as the source and header are completely legitimate.

Phishing

Phishing maintains a small but constant presence, representing on average just 0.5% of all spam over the last six months (Figure 8).

7 http://www.marshal.com/trace/traceitem.asp?article=280&thesection=trace

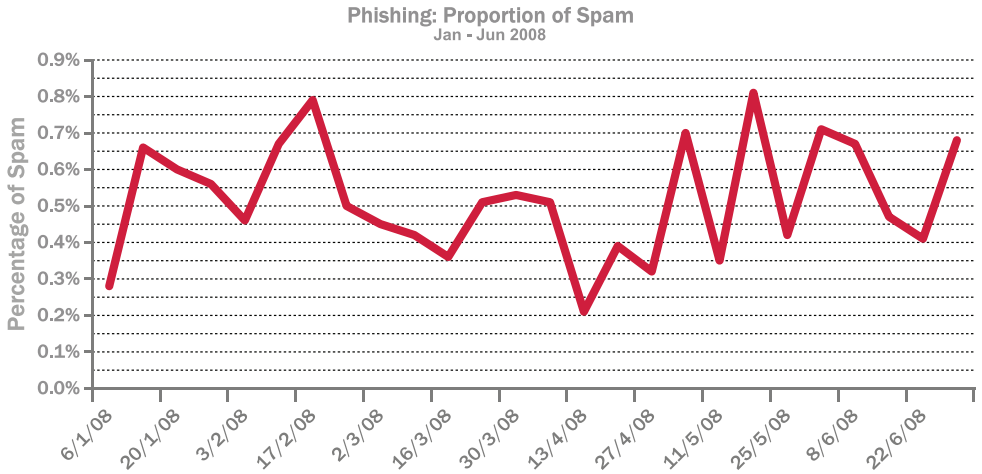


Figure 8: Phishing as a Proportion of Spam

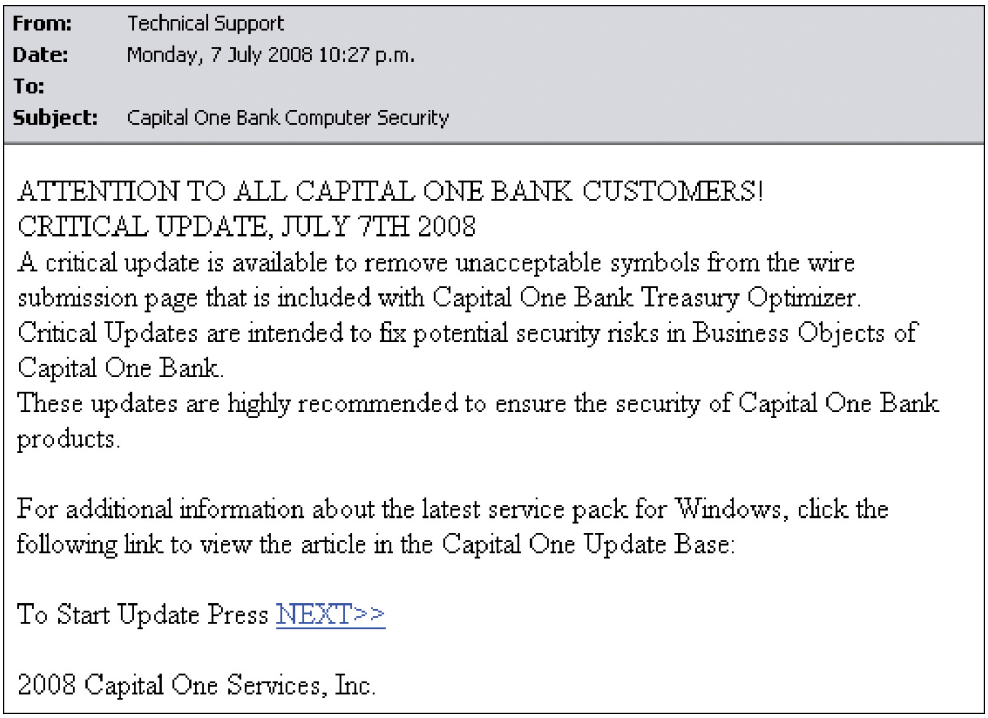
Its format is formulaic. Essentially, phishing spam looks like legitimate email that asks you to confirm your login security details. You link to what you think is the bank's website and use your login name and password. However, the link to the bank website that the phishing email provides, in fact, points to a false website that looks authentic but is controlled by the phishers. As a result, the cyber criminals gain access to your bank account credentials which they can use to steal your money 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 in the US, are targeted. Figure 9 shows the major US phishing targets as at the end of June 2008.

Figure 9: Major Phishing Targets, June 2008

Some of the major spam botnets are getting in on the phishing act, notably the ubiquitous Srizbi. Figure 10 shows a recent example from Srizbi that uses a very long domain in the URL – a good reason to be suspicious if you weren't so already:

http://top.capitalonebank.compub.login.htmlbank.serv.manager.cgipage.showshow.380367535.type.activex.comprj.gbh5d.com/login.html



From: Technical Support
Date: Monday, 7 July 2008 10:27 p.m.
To:
Subject: Capital One Bank Computer Security

ATTENTION TO ALL CAPITAL ONE BANK CUSTOMERS!
CRITICAL UPDATE, JULY 7TH 2008
A critical update is available to remove unacceptable symbols from the wire submission page that is included with Capital One Bank Treasury Optimizer.
Critical Updates are intended to fix potential security risks in Business Objects of Capital One Bank.
These updates are highly recommended to ensure the security of Capital One Bank products.

For additional information about the latest service pack for Windows, click the following link to view the article in the Capital One Update Base:

To Start Update Press NEXT>>

2008 Capital One Services, Inc.

Figure 10: Phishing email from Srizbi botnet

WEB THREATS

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

Browser Vulnerabilities

The browser itself is a key attack vector. Web browser vulnerabilities are commonly exploited when users visit malicious Web sites. Several off-the-shelf attack toolkits, such as Mpack or Icepack, simply query the browser and version, and serve up an appropriate exploit for that specific version.

Recent research indicates that some 45% of Internet users are at risk from simply running old or un-patched browsers[8].

If this wasn't serious enough, the myriad of vulnerabilities in browser plug-ins, like Flash Player, Java and QuickTime, means the actual number of users at risk is much higher. In May 2008, there was a widespread attack targeting a vulnerability in Adobe's Flash Player plug-in[9].

Mass Website Hacks

Remaining safe is no longer a question of avoiding shady or lesser-known websites. It is abundantly clear that many websites hosting malicious code are legitimate sites that have been hacked, as opposed to specific sites that have been set up by the criminals. This is a huge problem because, naturally, we tend to trust well known, legitimate websites. The advantage for attackers is that they do not have to entice users to compromised sites - users are going to browse to their favorite sites anyway.

In March 2008 there was a massive attack involving iFrame injections and SEO (Search Engine Optimization) poisoning that affected many high profile websites, including USAToday.com, News.com, Walmart.com and many others. The attack used the practice of caching search queries by injecting common search terms along with a simple iFrame script that loaded malicious code from other sites[10].

Soon after, in May 2008, there was a sophisticated, mass attack on many legitimate websites. The attack itself was carried out 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 website pages (Figure 11). The JavaScript itself directed users automatically to websites hosting various exploits[11]. Over 1.5 million legitimate websites were affected.

In our view, this style of mass website attack is the most concerning issue to arise so far 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 months to come.

---

8 http://www.marshal.com/trace/traceitem.asp?article=701&thesection=trace

9 http://www.marshal.com/trace/alertsitem.asp?article=673

10 SEO poisoning attacks growing - http://www.securityfocus.com/brief/701

11 http://www.marshal.com/trace/traceitem.asp?article=661&thesection=trace

Figure 11: Google search result showing JavaScript insertion from SQL Injection attack, May 2008.

Blended Threats

Today, many attacks are called "blended" threats because they involve multiple technologies and attack vectors. The typical example goes as follows. A botnet pushes out spam with links to websites hosting malicious code. Users following the link may be subjected to browser exploits and, in case that fails, may also be presented with a fake video or codec to "install." Once compromised, the victim's computer will download further malicious components including spambots, and the cycle then repeats itself.

In June 2008, we noticed a widespread malicious spam campaign from both the Srizbi and Rustock botnets. The links pointed to compromised Web servers hosting a file called "r.html" which showed as a "PornTube" page (Figure 12). The images on the page were links to the file video.exe. And if JavaScript was enabled a message box would pop up asking the user to install a "missing video ActiveX object" which is also the video.exe file[12].

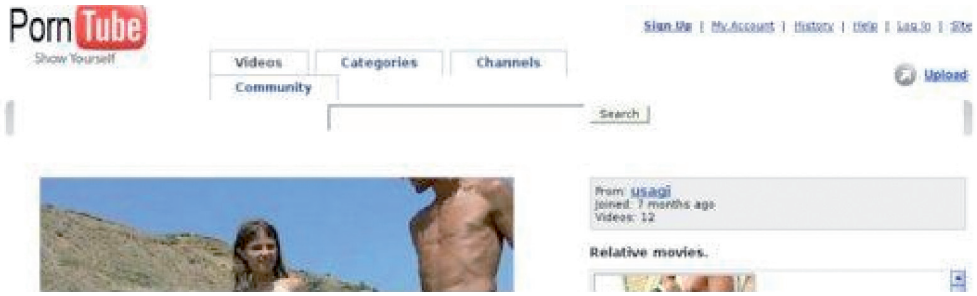


Figure 12: Fake "PornTube" site that installs a malicious file

12 http://www.marshal.com/trace/traceitem.asp?article=681

PREDICTIONS

Simply browsing will become ever more risky. The botnet-driven mass website attacks we have seen in the last few months will continue to attack legitimate websites.

Browser vulnerabilities continue to be targeted and, increasingly, third-party plug-ins will be targeted as there is even less chance these will be up to date.

Social engineering will remain a key theme for attackers. The effectiveness of malicious spam campaigns over last six months has shown us that simple social engineering ploys still work.

Recommendations

Receiving email and browsing the Web now pose more risks than ever before. Attacks are increasingly stealthy. The best advice we can provide is to encourage organizations to review their current Email and Web security strategies and products to ensure they have protection in place that meets today's rapidly evolving threat landscape.

- With a rise in malicious spam, good anti-spam protection is imperative; ensure spam filtering systems employ defense-in-depth by using multiple technologies for maximum accuracy and resiliency

- Take steps to secure Web browsing at the gateway, including URL filtering and the restriction of executable and other content that can be downloaded by users, ideally deploying a Secure Web Gateway technology that is able to actively scan and filter the content users are actually accessing and posting

- Keep Web browsers, plug-ins and other desktop software meticulously up-to-date as many malicious websites target old versions and known vulnerabilities

- Educate users about the new dangers of email and browsing, and advise them to avoid following links in unsolicited email and be suspicious of unexpected download prompts when browsing

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.

CONTACT MARSHAL

Europe Middle East & Africa
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.