M86 SECURITY

Security Labs Report

Jul 2009-Dec 2009 Recap

CONTENTS

INTRODUCTION

This report has been prepared by the M86 Security Labs team. It covers key trends and developments in Internet security over the last six months, as observed by the security analysts at M86 Security Labs.

M86 Security Labs is a group of security analysts specializing in Email and Web threats, from spam to malware. They continuously monitor and respond to Internet security threats. The Security Labs' primary purpose is to provide a service to M86 customers as part of standard product maintenance and support. This service includes updates to M86's unique, proprietary anti-spam technology, SpamCensor and Web threat and vulnerability updates to the M86 Secure Web Gateway products that are able to pro-actively detect and block new and emerging exploits and threats and the malware they serve.

M86 Security Labs analyzes spam, phishing, malware, follows Internet security trends, and is well recognized in the industry for being among the first to study the effect of the emerging Botnets as well as reporting on the in-the-wild use of newly discovered vulnerabilities and the exploits using them. Every day, the Security Labs analyzes over 7 million distinct Email messages. Looking for patterns and emerging trends, and correlating that with the Web exploit and vulnerability research provides M86 with a very complete Internet threat vantage point.

Data and analysis from M86 Security Labs is continuously updated and always accessible online at our website located at: http://www.m86security.com/labs

You can find us on Twitter at: http://twitter.com/m86labs

KEY POINTS OF THIS REPORT

- Spam volumes increased dramatically in 2009, to over 200 billion per day with the vast majority sent through Botnets of infected computers. In the second half of 2009, 78% of all spam originated from the top 5 botnets alone by volume.

- Malicious spam dramatically increased in volume, reaching 3 billion messages per day, compared to 600 million messages per day in the first half of 2009.

- Even with adequate protection from Antivirus software, Zero Day Vulnerabilities left users vulnerable to potential attacks 40% of the time **(in the 2nd half of 2009)**.

- Twitter attacks are increasing, benefiting from the use of shortened URLs. The use of shortened URLs has grown significantly, especially with the growing adoption of Twitter. They have become a new darling for attackers, making it easy to obscure malicious links and exploit end users' trust through social engineering.

SPAM

Spam continues to be a massive problem. Not only does spam consume valuable network resources, it remains a popular conduit for the distribution of malware, phishing and scams by cyber criminals. Spam therefore remains a significant threat to businesses. M86 Security Labs estimates that global spam volume is about 200 billion messages per day. Spam typically represents around 80-90% of all inbound Email to organizations.

SPAM REBOUNDS WITH VENGEANCE

2009 will be remembered as the year spam came back with a vengeance. The volume of spam rebounded in the first half of 2009, as the spamming botnets recovered ground from the shutdown of the McColo network in November 2008, which nearly halved spam volumes overnight. Our proxy for spam volume movements is the M86 Security Labs Spam Volume Index (SVI), which tracks changes in the volume of spam received by a representative bundle of domains. By the end of 2009 the SVI had grown by 50%, eclipsing pre-McColo levels.

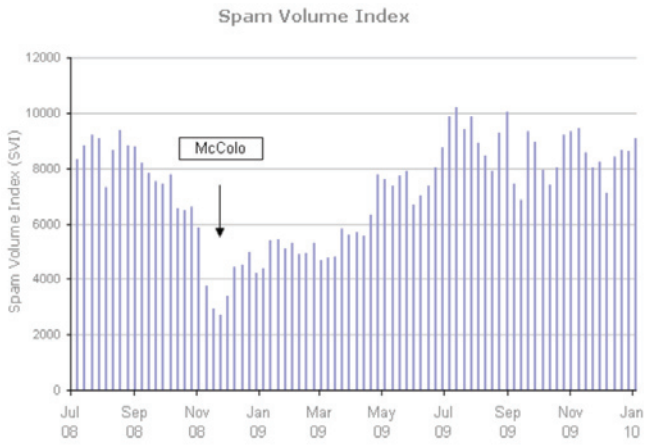

Figure 1: M86 Security Spam Volume Index (SVI)

BOTNET SOURCES OF SPAM

The vast majority of spam originates from botnets. M86 Security Labs monitors the spam output from major spam botnets by purposely running infected machines in a closed environment, tracking what is being sent and comparing that back with the main spam feeds to gauge the activity levels of each Bot network. Similar to the first six months of 2009, the last six months saw five botnets that were responsible for 78% of spam output, with the top nine responsible for 90% (Figure 2).

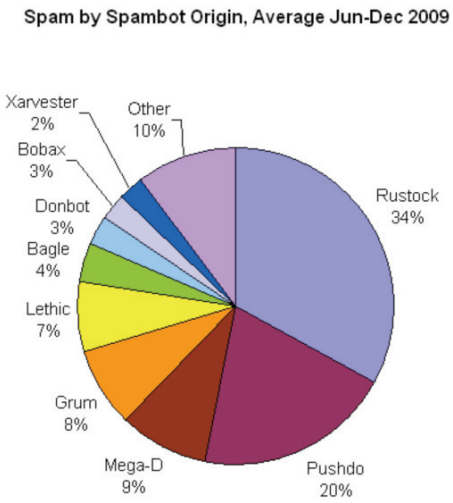

Figure 2: Spam by Botnet Origin, Average Jun-Dec 2009

The major spam botnets such as Rustock and Pushdo (or Cutwail) continue to dominate spam output, supported by second-tier botnets such as Mega-D, Grum, and Lethic, and Donbot. The spamming botnets are constantly in flux, waxing and waning, morphing, becoming obsolete, being replaced, taken down, and upgraded. It is important to identify the major contributors to the volume of spam, so the industry can take action against them, such as the botnet takedowns that have already occurred. Consider the impact on Spam levels if the top 2 or 3 botnets were disabled.

For the latest statistics on botnet spam output and detailed information about the botnets including how they work, refer to the M86 Security Labs site[1].

BOTNET DISRUPTION

On the back of the success of the McColo shutdown in late 2008, this last year saw several spamming botnets disrupted through their control servers being shutdown. In June 2009, a 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 and its shutdown temporarily affected spam output, mainly from the Pushdo botnet[2]. In November 2009, Mega-D's control servers were taken down disabling this botnet's spam output[3]. And in January 2010, Lethic's control servers were taken down, completely bringing its spam output to a halt[4].

[1] http://www.m86security.com/labs/bot_statistics.asp
[2] http://www.m86security.com/labs/i/FTC-Shuts-Down-Rogue-ISP,trace.1003~.asp
[3] http://www.m86security.com/labs/i/Mega-D-botnet-takes-a-hit,trace.1161~.asp
[4] http://www.m86security.com/labs/i/Lethic-botnet--The-Takedown,trace.1216~.asp

While these measures are useful efforts to control botnets, their long term effectiveness in stemming overall spam output has been negligible. As we have seen in Figure 1 on the previous page, spam volumes are impacted by botnet disruptions or takedowns, but tend to rebound strongly as botnet operators simply regroup and come back with newer and more sophisticated creations. In particular, the bot authors have built in more sophisticated location and recovery mechanisms to counter any sudden loss of their control servers, such as:

- Using a list of domains, instead of hardcoded IP addresses - if one domain fails it moves to the next one
- Having hard-coded DNS servers to resolve domain names
- Using domain generation algorithms in case everything else fails
- Using alternative communication protocols for command and control architecture

What we are dealing with here are organized, professional gangs with major businesses and significant revenues at stake. Therefore, they will not relinquish without a fight.

SPAM TYPES

Throughout the year, we've seen a consistent trend amongst the various spam types in our lab environment. 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 16%, while all the other categories come at under 4% (Figure 3). A number of categories recorded increases over the first half of the year, including Education which largely promotes online diplomas, Gambling promoting online casinos, Malicious spam and Phishing.

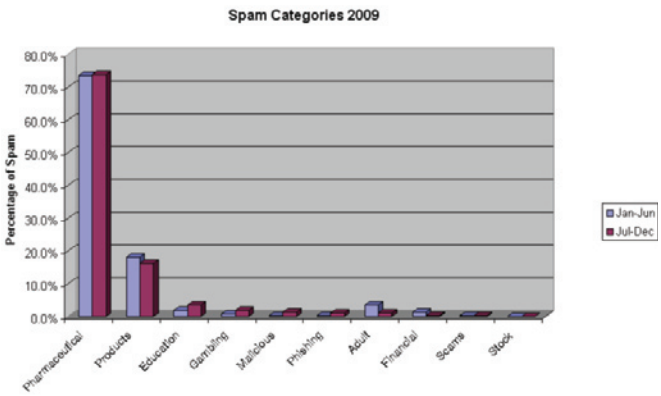

Figure 3: Spam Categories 2009

AFFILIATE PROGRAMS

Botnet operators or herders make money out of the products that are sold through their spam messages. This works by the online retailer tracking how the sale came to their website, from which spam campaign and then paying the creator of that spam campaign a commission on any sales made as a direct result of their spam campaign. This is called an affiliate program. The programs can provide many resources for affiliate members. Depending on the affiliate program, these can include pre-registered domains, web landing pages, undetectable executables and daily stats on how many users are visiting their sites[5]. Affiliates attract visitors to their sites through spam, search engine optimization, forum spam and social networks. The affiliates are either using their own botnets to send spam, or purchase spamming time from botnet owners. The affiliate members make a commission on each successful sale. Often affiliate programs have several different 'brands' from which members can choose to promote.

The most prominent affiliate program is run by a company called Glavmed and the notorious 'Canadian Pharmacy' is one of the brands linked to their organization that appears overwhelmingly in spam. The Glavmed website (www.glavmed.com) claims a 30-40% revenue share for referrals leading to sales. At any one time, multiple botnets can be seen spamming links leading to 'Canadian Pharmacy' websites. In September 2009, M86 Security Labs took a random sampling of spam, and automatically followed the links to determine the affiliate program being promoted. The 'Canadian Pharmacy' program was promoted in 67% of spam, with Prestige Replicas a distant second at 8%[6].

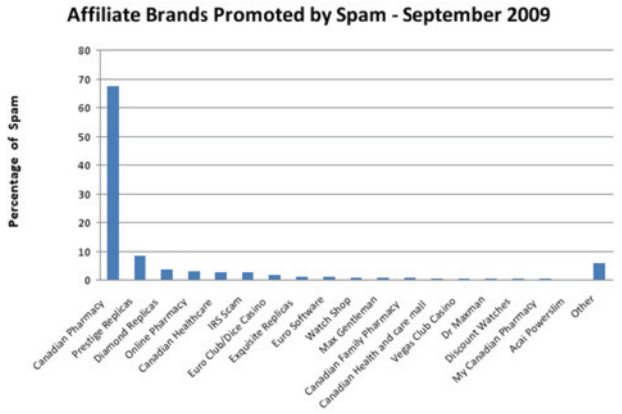

Figure 4: Spam Affiliate Programs

[5] http://www.m86security.com/labs/i/Ya-Bucks-Malware-Affiliate-Program,trace.1060~.asp
[6] http://www.m86security.com/labs/i/Top-Spam-Affiliate-Programs,trace.1070~.asp

Figure 5: 'Canadian Pharmacy' website

MALICIOUS SPAM

Malicious spam is categorized as Email that has a malicious attachment or an embedded URL that leads to a malicious website (also known as a blended threat). The latter half of 2009 saw an overall increase in the levels of malicious spam to 3 billion messages per day, compared with 600 million messages per day in the first half of the year. There were two main factors driving this increase

- Malicious executables being spammed out, typically with DHL or UPS 'Get your parcel' type subject lines (Figure 6), but also other themes like "Facebook update". The executable payload of these campaigns varies, often it was a downloader called Bredolab, which has been observed downloading a wide variety of malware including scareware, password stealers, and spambots such as Pushdo.

Figure 6: UPS Malicious spam with Bredolab downloader

- Blended threat campaigns, which are e-mail messages containing no attachments, instead contain a link that leads to web pages hosting malicious code. Therefore, the infection happens through the web browser, not through the e-mail client, hence the name 'blended threat.' The malware of choice distributed through most of these campaigns was Zeus, an information stealer (see Figure 7).

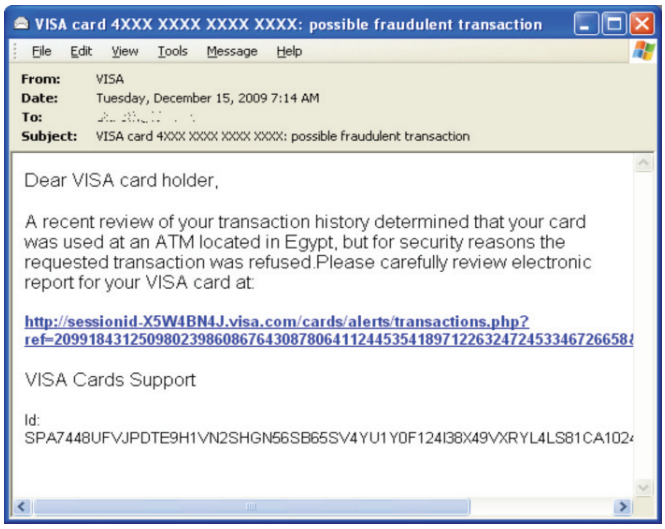

Figure 7: Blended threat attack from the Pushdo botnet that leads to the Zeus malware.

ZEUS CAMPAIGNS FROM PUSHDO

Over the last six months, we have seen numerous, large scale Zeus blended threat campaigns. These attacks use the combination of massive amounts of spam from the Pushdo botnet, well designed web pages, social engineering, thousands of random looking domain names hosted on a fast-flux network and exploit kits, all to install the Zeus (or Zbot) Trojan horse.

The social engineering aspect used well-known brands or trusted organizations. The websites were well designed, using the same look and feel of the targeted brand, good English and grammar, and offered a plausible reason for downloading and running an executable from the web site. The user's email, obtained from the spam link, was often included in the page to add credibility. Some sites have subtle features to add further credibility such as the VISA site showing the first number of a user's VISA card as '4' (all VISA cards start with '4') or stating that an executable is a self-extracting PDF file. A few of these sites, such as the Facebook and MySpace examples, even asked the user to login first (although the credentials were not verified at the time), giving the criminals login credentials, before users were asked to download and run a file.

If the user was suspicious enough to not download the executable file after clicking on the spam link, there was a chance they could get infected anyway if they were vulnerable to browser or application exploits incorporated in the web sites.

Each separate campaign used several hundred random looking domain names, often with the recipient's domain or the domain of a targeted brand as a sub-domain. For example:

cgi.ebay.com.<DOMAIN>.ne.kr/ws/ebayisapi.dll

<DOMAIN>.yhuttte.or.kr/owa/service_directory/settings.php

www.facebook.com.<DOMAIN>.org.uk/usersdirectory/loginfacebook.php

The directory structure on the malicious web server is also often similar to the web site it is trying to impersonate. Among the brands and organizations we have seen are VISA, Paypal, Ebay, Facebook, MySpace, American Express, CDC, Bank of America, HSBC, NACHA, IRS and FDIC.

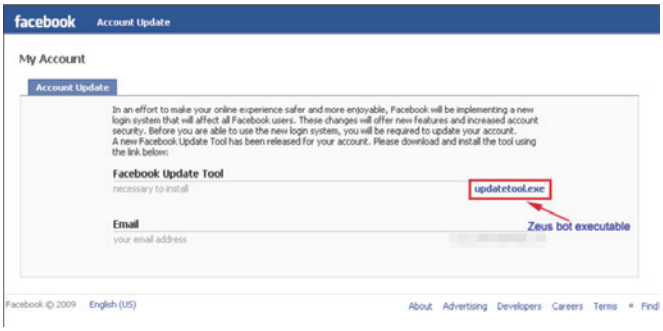

Figure 8: Facebook update scam leading to Zeus Trojan

VIRUT DISTRIBUTING SPAMBOTS

Over the past year, malware became more voluminous, sophisticated and complex. One piece of malware we encountered illustrates this complexity. A prevalent distribution vector for spambots and other attacks was a piece of malware called Virut, which is a file infecting virus that can download and install almost any type of malware on to an infected computer[7]. The Virut malware infects files with .exe and .scr file extensions. A user may encounter Virut by visiting malicious websites that contain exploits that download Virut as a payload.

Virut plays a part in distributing spamming Trojans such as Xarvester, Grum, Pushdo and Gheg. Virut also plays a role in distributing money mule and profit-driven malware that includes rogue anti-virus, keyloggers, password stealers and ad-clickers.

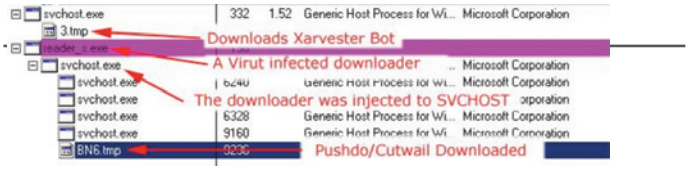

Figure 9: Virut infected machine also infected with two spambots.

WEB

Black Hat SEO

During 2009 a growing trend was the use of Search Engine Optimization (SEO) techniques to drive users to web pages hosting malicious code. Also known as SEO poisoning, the technique aims to elevate malicious landing pages up the search engine results ranking, thus ensuring a steady supply of victims. SEO poisoning is a particularly treacherous as users tend to implicitly trust search engine results.

The techniques vary, but many center on creating and posting web pages with keywords and phrases related to any hot trend, such as those derived from services like Google Trends, other celebrity news or popular topics. A good example of this technique in practice was seen in the number of malicious pages listed in search engine results immediately following the untimely passing of mega pop star, Michael Jackson. These 'enriched' web pages help to push up the search engine rankings for the criminals' malicious landing pages. The systems the criminals are using are sophisticated and highly automated, leading to a continuing supply of fresh search terms and 'loaded' web pages.

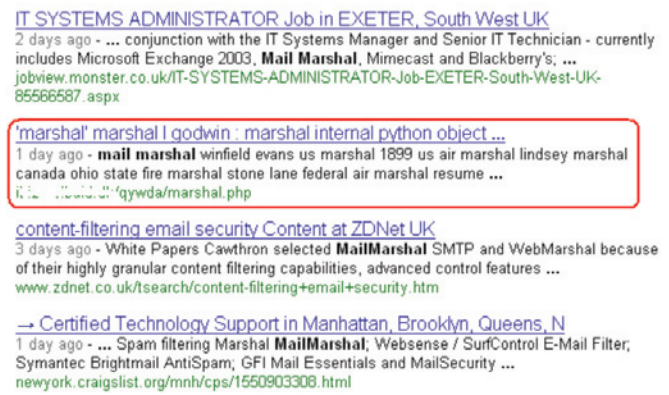

Figure 10: Bogus SEO result for 'MailMarshal

[7] http://www.m86security.com/labs/i/Virut-s-Not-So-Obvious-Motive,trace.873~.asp

SEO attacks involve the manipulation of a search engine's indexing algorithms using various techniques in order to place their websites higher up in the search results[8]. The size and scope of SEO poisoning is not immediately obvious because in order to find a SEO promoted malicious website you have to search for the specific search terms for which it was optimized. The following illustrates how widespread the problem is. We recently entered the term MailMarshal, M86 Security's email filtering product, into Google and chose the previous week's timeframe. As you can see in Figure 10 on the previous page, high up the list of results for 'Marshal' is a bogus result based off the term, which leads the end user to malware.

The whole success factor of SEO poisoning relies on the false website to be ranked high in search results. One way that search engines rank websites is by the number of 'backlinks', which are links on other websites that link back to the site in question. Attackers create thousands of backlinks to a web page they want to promote. When a search engine visits this page it sees legitimate content, but when a user visits they are redirected to a website of the attackers choosing.

Throughout 2009, the cyber criminals offering of fake anti-virus 'scareware', in particular, used SEO poisoning techniques to drive users to their landing pages. In many cases, we have seen end users being redirected to pages like the one featured in Figure 11.

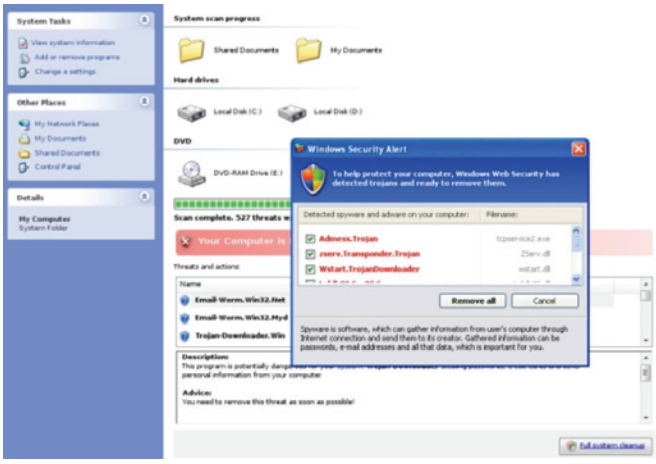

Figure 11: Scareware landing page from SEO campaign

ZERO-DAY VULNERABILITIES

During the last six months, we've observed an increase in the number of new zero-day vulnerabilities, with the most notable being discovered in Adobe and Microsoft products. We have seen close to a dozen zero-day vulnerabilities that were used by cyber criminals throughout 2009 (Figure 12).

Vulnerability CVE	Applications Affected
CVE-2009-0238	Microsoft Office
CVE-2009-0927	Adobe Reader/Acrobat
CVE-2009-1492	Adobe Reader/Acrobat
CVE-2009-1493	Adobe Reader
CVE-2009-1862	Adobe Reader/Acrobat/Flash
CVE-2009-2493	Adobe Flash Player/Internet Explorer
CVE-2009-2496	Microsoft Office
CVE-2009-3672	Microsoft Internet Explorer
CVE-2009-4324	Adobe Reader/Acrobat
CVE-2010-0249	Microsoft Internet Explorer

Figure 12: List of vulnerabilities used by cyber criminals throughout 2009

One of the major problems with zero-day vulnerabilities is the length of time during the "window of vulnerability," which is measured from the time the vulnerability is first discovered being used in-the-wild until the time when a patch is released by the application vendor.

In the past there have been cases where this window has remained "open" for months or even years. Even now, as bigger software companies become more cognizant of security, the time interval from zero-day vulnerability detection to the release of a patch could be very significant and take from several days (best case scenario) to several weeks or even months. It should be noted, of course, that even after the closure of a vulnerability, exploitation continues to be used everywhere in-the-wild because users are typically lax in applying necessarily updates for their applications and the latest security patches. A current example of this would be MDAC, which was patched in 2006, but is still widely used by cyber criminals.

The chart over the page illustrates the issue with the length of the window of vulnerability over the last six months. This example uses just 7 reported vulnerabilities.

[8] http://www.m86security.com/labs/i/Be-Careful-What-You-Search-For,trace.884~.asp

Figure 13: Window of Vulnerability

A cursory glance at Figure 13 shows that even though the window of vulnerability might be short at times, it is the overlapping time intervals that pose a real problem. It is during these overlapping time intervals that end users are completely vulnerable to attack with very little they can do about it. As indicated in red, within a six month period alone, Internet users/consumers not protected by true pro-active real-time on-premise security technology were completely exposed to potential attacks close to 40% of the time. This means that no protection was provided by application vendors during this timeframe and even the desktop AV scanners that need to react to these attacks provided little protection and as such, cyber criminals used this to their advantage by exploiting these zero-day vulnerabilities.

THE DUMMIES GUIDE TO ATTACK TOOLKITS

Attack toolkits are used to build the actual cyber attacks themselves. The increasingly professional nature of these tools being used, such as Web attack toolkits, shows us that the provision of software to the cybercrime industry has become a serious business in and of itself. One such example is the recent attack toolkits that closely resemble professional application packages.

As with any other professional software product, attack toolkits may include:

- An official website
- Version management
- Overviews of technical characteristics (present and future)
- Support
- Pricing lists
- Multi-lingual translations

Just a few years ago, the attack toolkit market was mostly comprised of WebAttacker, followed by the GPack and MPack toolkits. Newer attack toolkits such as Yes, LuckySploit, Eleonore and Fragus have helped to expand the market and increase the demand for these packages. Within the last six months, we've observed a significant increase in the number of new and different attack toolkits, such as SEO, MAX, Shaman's Dream, Siberia, and CleanPack.

Developers of modern attack toolkits advertise their products as easily configurable and manageable. Indeed, they do not require a deep knowledge of hacking and have made the process much more simple for cyber criminals. Combined with frequently updated versions that include the latest exploits, an attack toolkit is an effective weapon in the hands of any cyber criminal.

The following are examples of attack toolkit sites and products:

Figure 14: Yes Exploit Toolkit Website

Figure 15: Fragus Attack Toolkit

Figure 16: Eleonore Exp Attack Toolkit

ADOBE PDF ATTACKS

Adobe products remain one of the most targeted applications for vulnerabilities. In 2009 alone, there were several notable Adobe PDF vulnerabilities that were discovered and widely exploited: CVE-2009-0927, CVE-2009-1492, CVE-2009-1493, CVE-2009-1862. CVE-2009-4324 is the most recent vulnerability in an Adobe product[9]. In this example, attackers were able to package malicious code into a PDF file, which would go undetected by most desktop AV scanners. As soon as the end user opened the blank PDF file, the malicious code would be executed and their systems would be compromised. More information on this particular example can be found in one of our recent webinars[10].

From an attacker's perspective, the advantages are quite simple: PDF files are not browser dependent, and Adobe Reader and Acrobat are immensely popular products with highly visibility in the marketplace. Finally, the other boon for attackers is the fact that PDF's offer the ability to include dynamic content within a file.

Considering these advantages, PDF exploits are frequently used in attack toolkits, along with flash files and more recently, java (jar) exploits. In some cases, a set of PDF exploits is the only mode of attack needed by a cyber criminal to attack via a Web page.

Ultimately, PDF attacks tend to be very effective, with some achieving as high as 50% success rate. The following figure shows the success rate of a PDF exploit:

Figure 17: PDF Exploitation Rate

The end user often has a false sense of security, even if they are up to date with all the latest security updates, they mistakenly believe that permanent browser updates offer enough protection. However, the real situation is decidedly different. Multiple zero-day attacks, combined with limited capabilities[11] of anti-virus products in preventing the spread of malware through PDF files, leaves the consumer exposed to malware and unprotected against cyber attacks.

RISE IN TWITTER ATTACKS

As Twitter began surging in popularity through the first half of 2009, we warned users about the pitfalls of the service in our first half report. The trifecta of spam, malware and phishing problems on Twitter have continued to increase, highlighting the fact that cyber criminals love to target areas of the Web where the user base is large and growing, making it easier to see their attacks reap big rewards.

In August of 2009, we wrote about the rise of a weight loss spam campaign[12] and how its impact was seen in thousands of 'tweets' sent out across the service (Figure 18).

Figure 18: Spam campaign seen on Twitter in August of 2009

This spam campaign was one of many that we observed in the last half of 2009. These kinds of spam campaigns originate from dummy accounts or accounts that have been compromised through phishing campaigns.

Figure 19: Direct message spam from a phished account.

In addition to the mass tweets about weight loss spam, these phished accounts were also used to send out mass direct messages (commonly referred to as DM's) to followers pushing out links for games or services (Figure 19).

Twitter is also no stranger to being used as a medium to spread malware. One of the most high profile instances of this included well known venture capitalist, Guy Kawaski's Twitter account in late June of 2009. His account was set up to automatically update using a service called NowPublic. It tweeted out an update about a sex tape, which led to a piece of malware. The biggest issue with this is that, Mr.Kawasaki's Twitter account is followed by thousands upon thousands of users, and he is known to share links.

[9] http://www.m86security.com/labs/i/Adobe-PDF-Zero-Day,alerts.1210~.asp
[10] https://m86security.webex.com/m86security/lsr.php?AT=pb&SP=EC&rID=7091157&rKey=4beda2b0b3bbef14
[11] http://isc.sans.org/diary.html?storyid=7906
[12] http://www.m86security.com/labs/i/Twitter-Weight-Loss-Spam,trace.1057~.asp

Figure 20: Guy Kawasaki tweet leading to a Trojan attacking both Mac and PC users

The most interesting usage of Twitter in a spam campaign was observed[13] in November of 2009. It involved using a link to a tweet in a spam message to direct a user to the spam via Twitter (Figure 21). This was likely used to evade certain spam filters.

Figure 21: New technique to evade spam filters, linking out to Twitter with a spam domain being pushed in a tweet.

What it ultimately boils down to is the whole concept of trust, which is what is being taken advantage of by these cyber criminals on social networking services like Twitter. Users will naturally trust their friends, making it more likely that they will in fact click on a link shared with them on Twitter or any other social networking site. The exploitation of trust is one of the primary reasons why attacks on Twitter and other social networks succeed so well.

ABUSE OF URL SHORTENERS

The sheer growth of URL shortening services throughout 2009 was apparent. The usage of these services was a byproduct of the popularity of Twitter, which caps the number of characters that can be used in each update to 140. The problem with link sharing is that often times, URLs can be quite lengthy, often surpassing the 140 character limit with ease.

By masking the source URL behind a shortened URL, it is hard for an end user to determine what kind of content will be provided to them when they click through. This uncertainty is often put to the side when the content comes from a friend, once again highlighting the abuse of trust in social networks.

It comes as no surprise then that the majority of malicious links that we've observed on social networking sites throughout 2009 were of the shortened URL variety. And while this phenomenon remains prevalent on services like Twitter and Facebook, we have observed them being distributed in spam messages[14] as well (Figure 22).

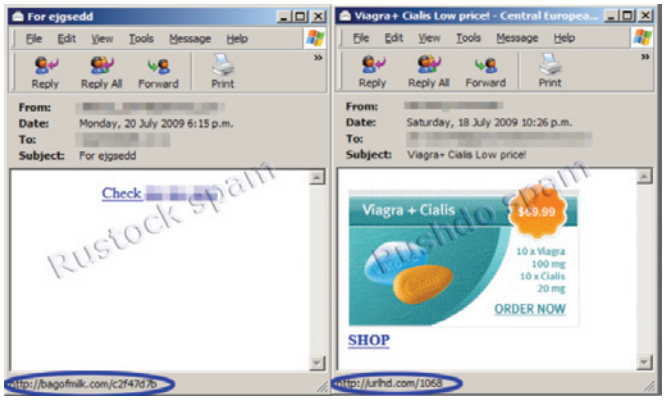

Figure 22: Example of shortened URLs included in spam messages

There are major players in the space, such as TinyURL and Bit.ly. However, the biggest concern lies not with the leaders, rather the hundreds of lesser known services that are up and running today and being used by cyber criminals. They remain unchecked, and do not have any safeguards in place to prevent malicious content from being spread through their services.

[13] http://www.m86security.com/labs/i/Twitter-Facebook-and-Bebo-used-in-spam-campaign,trace.1168~.asp
[14] http://www.m86security.com/labs/i/Spammers-Try-URL-Shortening-Services,trace.1038~.asp

RECOMMENDATIONS

- **Education is paramount.** Teaching users the importance of best practices for their every day Internet usage is vital. Show them examples of Scareware applications, explain how easy it is for them to get infected. Give them a Phishing test, and see if they can pick the false sites from the real. Above all else, the number 1 rule is to be wary about clicking on any links in email or on web pages. (Rule number 2: See rule 1).

- **Review your current Security Products.** Armed with the latest threat information, re-evaluate the security products that are being used in your organization or at home. Ask your incumbent vendors the tough questions about exactly what they do to detect and block these threats. Look to test products against each other and ensure the vendors are investing in threat research.

- **Be wary of links, even from trusted sources.** It cannot be emphasized enough that even if the source of a link is someone you trust, they themselves may have had their accounts compromised or someone might be spoofing their identity. Sending email to look as though it is from someone else's email account, for example is pretty straight-forward.

- **Stay up to date.** Keep Web browsers, add-ons/extensions, desktop applications up to date to their latest versions. We have seen that time and time again, many attacks target vulnerabilities found in old versions of Web browsers, applications or organizations are not blocking the latest spam and Web threats simply because their products are not up to date. While being completely up to date with the latest patches help to protect you and your end users from patched vulnerabilities, you will still need to remain on guard for the un-patched, zero day vulnerabilities.

- **Consider using browser add-ons/extensions to add an additional layer of security.** We recommend using the NoScript extension for Mozilla Firefox, which limits the execution of JavaScript code. We also suggest using extensions that will display shortened URLs as their full URLs, making it easier to know what the destination URL actually is. Many security vendors such as M86 have free tools for users to install on their personal or home computers, typically the most vulnerable. Tools such as SecureBrowsing[15], which analyzes links from search engine results or on web pages to gauge their malicious nature, it also works with shortened URL's such as those found in twitter.

[15] http://securebrowsing.finjan.com/

GLOSSARY OF TERMS

Affiliate Programs – A method by which spammers make money. By signing up for an affiliate program, spammers are provided with templates and a unique identifier, for which they will use to track referrals. If they drive back traffic that leads to a sale, they are rewarded with a commission. 'Canadian Pharmacy' is the most popular affiliate program today.

Attack Toolkit – A hacker kit that exploits several client side vulnerabilities to execute arbitrary code.

Black Hat SEO – The way cyber criminals utilize SEO ("black hat") to increase the search engine rankings for their own web sites, so that their malicious landing pages end up higher in search engine rankings, driving more end users to their sites.

Blended Threats - An attack that combines both e-mail and web as the attack vector. Foregoing traditional methods of attaching a virus directly to an e-mail message, a blended threat contains a link to a web site, which will either push malware to the end user or hosting malicious code.

Botnets (or Bot networks) – A botnet is a network of compromised computers (known as drones or zombies) that are used by cyber criminals to send out spam messages, spread malware, and other criminal activity.

Bot herder (or Bot owner) – The individual responsible for commanding the botnet to perform tasks by way of command & control.

Command and Control (or C&C) – The method by which the bot herder commands the various zombies in the botnet. Historically, botnets were controlled by way of Internet Relay Chat (IRC) and more recently, over HTTP (Hypertext Transfer Protocol). Bot herders have also started experimenting with other ways to implement command and control, such as through Twitter, Google Groups, and Facebook Notes.

CVE (or Common Vulnerabilities and Exposures) – A common identifier for publicly-known information security vulnerabilities.

Direct Message (or DM) – A private message that is sent between users of the social networking/micro-blogging service, Twitter.

Malicious spam - Spam messages that contain a malicious attachment, such as an executable or PDF file or containing a link that leads the end user to malware (known as a Blended Threat).

Scareware - A type of scam used by cyber criminals to convince an end user that their computers have been infected with malware. Usually delivered in the form of a pop-up or through a Black Hat SEO campaign, by scaring the end user, they trick the end user by convincing them that they are downloading a proper Anti-Virus solution, when they are instead downloading malware.

SEO (or Search Engine Optmization) – A method to increase the volume of traffic to a web site via search engines through "organic" search results, intended to move a web site up in the search engine rankings.

SEO Poisoning – A method employed by cyber criminals to poison search engine results for popular news items, trending topics, and overall hype. Common instances of this have been seen in deaths of celebrities, natural disasters, and product releases (such as Apple's iPad and Google Wave).

Spambots - Botnets that are primarily used to send out spam messages. Spambots can be rented out to cyber criminals for various campaigns.

Spam Categories - (See definition of Spam types)

Spam Types (or Spam Categories) – The different types of spam being sent out by various botnets. The most common spam type seen today is Pharmaceutical spam.

Tweet – A term used to describe the messages posted to the social networking/micro-blogging service, where messages are limited to 140 characters.

Zero-Day Vulnerabilities – A vulnerability that is unknown to others, undisclosed to the software developer, or for which no security fix is available.

M86 SECURITY™

Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

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

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

Asia-Pacific
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720