

Security Labs Report

July - December 2010 Recap

M86[®]
SECURITY

CONTENTS

Introduction	3
Review of Second Half (July through December) 2010	3
Key Points.....	3
Security Lab Statistics	4
Web Statistics.....	4
Spam Statistics.....	5
Events and Trends from July through December 2010	8
Stuxnet: A Defining Point in the Evolution of Malware?	8
Notable Botnet Disruptions and Takedowns	8
Spamit.com Closes Its Doors and Takes Spam with It.....	9
Zeus/SpyEye versus Traditional Phishing	10
How to Phish Regional Banks via Third Parties	10
Exploit Kits Becoming A “One-Stop Shop”.....	12
Mimicking Legitimate Social Networking Communications	13
Zeus/SpyEye Merger.....	14
Combined Attacks: Flash and Acrobat	14
Java Attacks Soar Into The New Year.....	15
Social Networks: Cybercrime Utopia	16
Conclusion	18
Recommendations	19

INTRODUCTION

The M86 Security Labs team prepared this report, which covers key trends and developments in Internet security over the last six months.

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 value-added service to M86 customers as part of product maintenance and support. This service includes frequent updates to M86's unique, proprietary anti-spam technology, SpamCensor, as well as Web threat and vulnerability updates to the M86 Secure Web Gateway products. The updates allow M86 customers to proactively detect and block new and emerging exploits, threats and malware.

M86 Security Labs analyzes spam, phishing and malware activity, and follows Internet security trends. The team is recognized in the industry and regularly reports on these issues, including newly-discovered vulnerabilities and the exploits using them "in the wild." Every day, the Security Labs team analyzes millions of distinct email messages, infected websites and malware reports. The results of these analyses, correlated with Web exploit and vulnerability research, provide M86 with a unique vantage point on Internet threats.

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

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

REVIEW OF SECOND HALF (JULY TO DECEMBER) 2010

During this period, web-based threats continued to grow more sophisticated. However, email threats such as spam decreased markedly following the takedown of major spam operations.

Key Points

- Patched vulnerabilities in software applications that are not updated promptly continue to be targeted as the point of infection in malicious attacks. This underscores the fact that many users have yet to update their browsers and other third-party applications.
- Botnet disruptions and the closure of the spam affiliate program, Spमित.com, contributed to significant spam reductions in the second half.
- The discovery of the Stuxnet worm in the second half of the year signals an evolution of malware and its potential for causing more than just financial losses.
- Traditional phishing attacks have declined as a result of more efficient methods for capturing banking credentials and credit card numbers through malware like ZeuS and SpyEye.
- Phishers are more successful in targeting end users by posing as third-party agencies (such as tax officials) instead of individual banking institutions.
- Exploit kits are continuously refined, adding robust features that makes them more attractive to kit users, and easier to craft attacks against end users.
- Since the author of the SpyEye Trojan received the source code to the ZeuS Trojan, the security community anticipates a more sophisticated version of the Trojan to appear in the coming year.
- Cybercriminals explore new ways to combat proactive security technologies through the use of combined and cross-component attacks. In the first half of 2010 they targeted Flash and Javascript; in the second half of 2010, Flash and Adobe PDF were the focus.
- Social networks remain a developing area for cybercriminals looking to exploit end users, both through vulnerabilities in the sites themselves and through various scams that net the criminals money via affiliate programs.

SECURITY LAB STATISTICS

Web Statistics

World Malware Map

Where is most malicious code being hosted in the world?

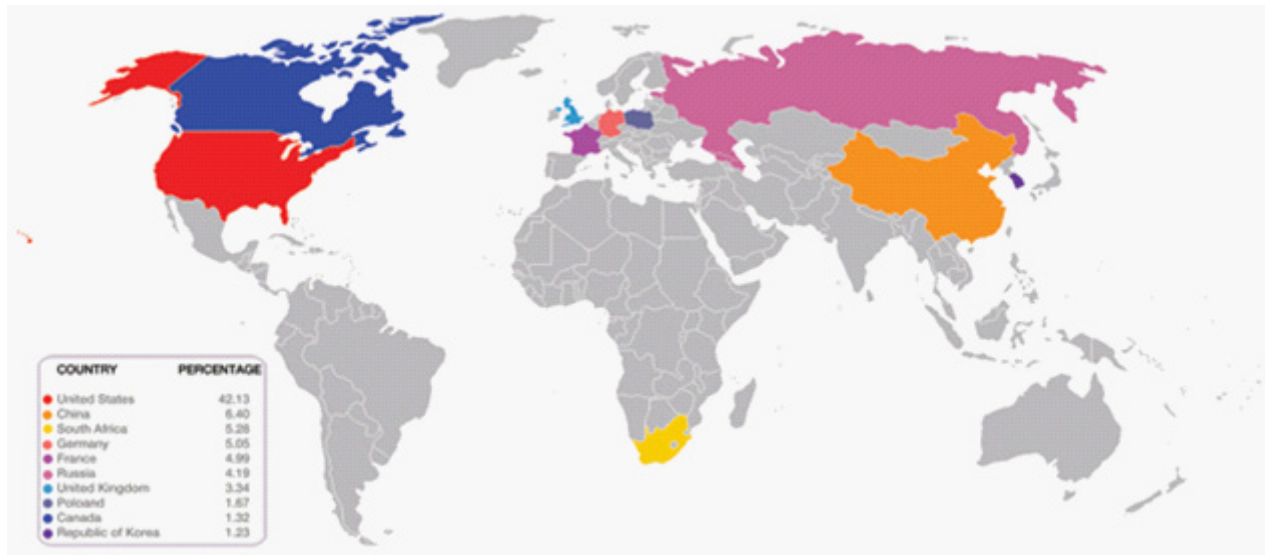


Figure 1: Geo-location of Malicious Code Hosted on Servers in the Second Half of 2010

The U.S. continues to host the majority of malicious code. This often comes as a surprise, considering that other countries on this list are typically associated with malicious attacks. The number and popularity of U.S. websites make them attractive targets. In our first half 2010 report, the U.S. led the way, hosting 43% of malicious code. This percentage remains unchanged.

Percentages in China and Korea decreased by 7.7% and 1.7%, respectively, while other countries like Germany, France and the United Kingdom experienced increases. Canada broke into our top 10, entering at 1.32%.

In addition, South Africa saw its share of infected websites increase from 2.25% in the first half to over 5% in the second half, taking over the third place spot. This increase could be attributed to South Africa hosting the 2010 FIFA World Cup.

Top 15 Most Observed Vulnerabilities

During the first half of 2010, anonymous feedback from M86 filtering installations showed most observed threats were based on the following vulnerabilities:

VULNERABILITY	DISCLOSED	PATCHED
1. Microsoft Internet Explorer RDS ActiveX	2006	2006
2. Office Web Components Active Script Execution	2002	2002
3. Microsoft Video Streaming (DirectShow) ActiveX Vulnerability	2007	2009
4. Real Player IERPCTI Remote Code Execution	2007	2007
5. Adobe Acrobat and Adobe Reader CollectEmailInfo	2007	2008
6. Adobe Reader GetIcon JavaScript Method Buffer Overflow	2009	2009
7. Adobe Reader util.printf() JavaScript Func() Stack Overflow	2008	2008
8. Microsoft Internet Explorer Deleted Object Event Handling	2010	2010
9. Microsoft Access Snapshot Viewer ActiveX Control	2008	2008
10. Adobe Reader media.newPlayer	2009	2009
11. Microsoft Internet Explorer (IE) iepeers.dll	2010	2010
12. BaoFeng StormPlayer Buffer Overflow	2009	2009
13. JVM Buffer Overflow Vulnerabilities	2009	2009
14. Microsoft IE STYLE Object Invalid Pointer Reference	2009	2009
15. Java WebStart Arbitrary Command Line Injection	2010	2010

Reviewing this data leads to conclusions similar to those of our first half of 2010 report: Microsoft and Adobe products remain popular point-of-infection targets for cybercriminals.

Despite the fact that these vulnerabilities were patched years ago, many of them are still targeted today. This is likely a result of their success rates, and it reinforces the importance of updating software applications, from browsers to PDF readers. It is critical to ensure that system and software patches are being applied as soon as they become available.

Most Popular Exploit Kits

In addition to tracking the most observed vulnerabilities in the wild, we track the most popular exploit kits observed in the wild:

EXPLOIT/TOOLKITS
1. Eleonore
2. Phoenix
3. Nuclear Pack
4. Unique Pack
5. Adpack Advance
6. Fragus
7. Neosploit
8. SEO
9. Sploit25
10. Fiesta

Of note, the Neosploit kit has made a return to the top 10. This is discussed in depth later in this report. Based on our data, we concluded that the popularity of an exploit toolkit is based on the same factors as most software applications. There is a direct correlation between the toolkit's popularity and the number of releases throughout the year and support available to toolkit customers. The media exposure for each toolkit and pricing also contribute to its popularity. Some kits sell for as low as \$150, while others such as the Phoenix exploit kit can be purchased for \$2,000.

Spam Statistics

Spam Volume Index

The volume of spam dipped sharply towards the end of 2010 due to botnet disruptions and affiliate program closures.

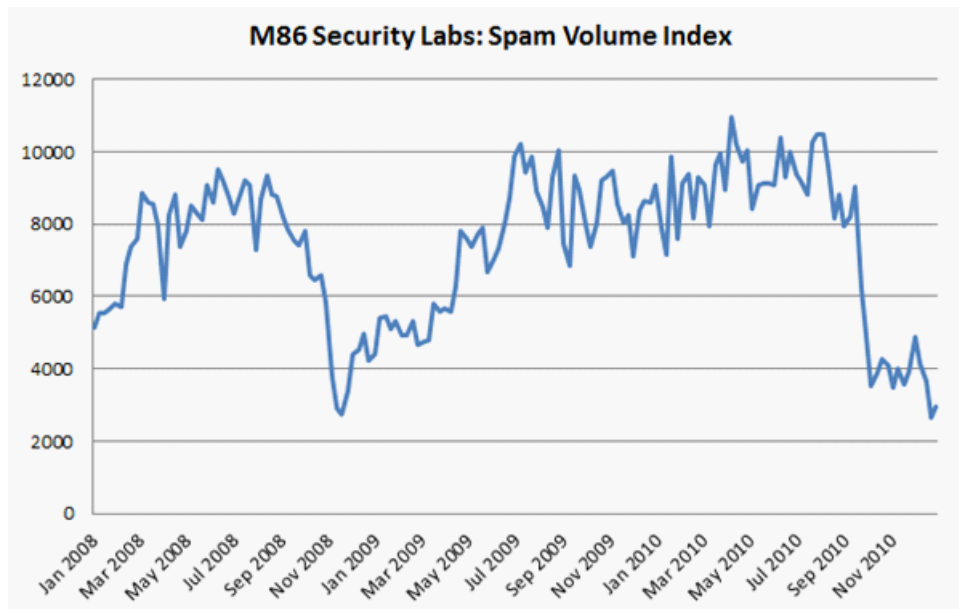


Figure 2: Spam Volume Index

Our proxy for spam volume movements is the M86 Security Labs Spam Volume Index (SVI, Figure 2), which tracks changes in the volume of spam received by a representative bundle of domains. By year end, the SVI was approximately 3,000—only one third of what it was at end of June 2010. These low spam volume levels have not been seen since the end of November 2008, when the rogue hosting provider McColo was taken offline.

We attribute the drop in spam to a number of notable events that occurred in the second half of 2010. Most significantly, Spamit.com, an underground affiliate program used by several spamming botnets, was shut down in late September. Spamit.com was linked closely to Glavmed and the “Canadian Pharmacy” brand of bogus online pharmacies. The Rustock botnet was most affected, with its spam output drastically reduced. Other events include:

- Control servers for the Pushdo botnet (and its Cutwall spamming component) were disrupted in August 2010
- The Mega-D botnet slowly ground to a halt as law enforcement authorities closed in on the operator
- The Bredolab botnet, which often installed spamming malware, was disrupted in October 2010

What does this mean for spam volume going forward? As we have seen in the past with the takedown of McColo, spam tends to rebound from these lulls. Therefore, we fully expect spam volumes to return to previous levels sometime in 2011. As always, we will continue to monitor these statistics and publish new spam charts and graphs on our [Spam Statistics page](#).

Spam Botnets

Where the Spam Comes From

The bulk of spam is emitted from botnets, which are networks of computers compromised by malware. M86 Security Labs monitors the output from major spam botnets by observing infected machines in a closed environment, and then comparing behavior with incoming spam feeds to gauge the activity levels of each botnet.

Prior to the massive changes in the spam ecosystem, the Rustock botnet was the predominant spam botnet, accounting for 50% of the spam M86 Security Labs observed in June 2010. However, by year end, Rustock had all but disappeared, leaving the second-tier botnets, Lethic and Grum, among the top spam senders.

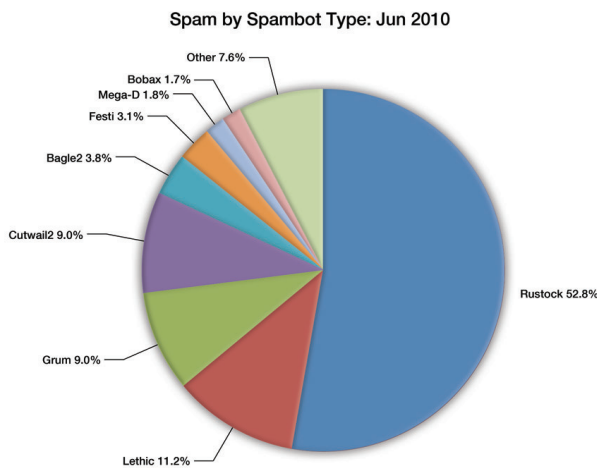


Figure 3: Spam by Spambot Type for June

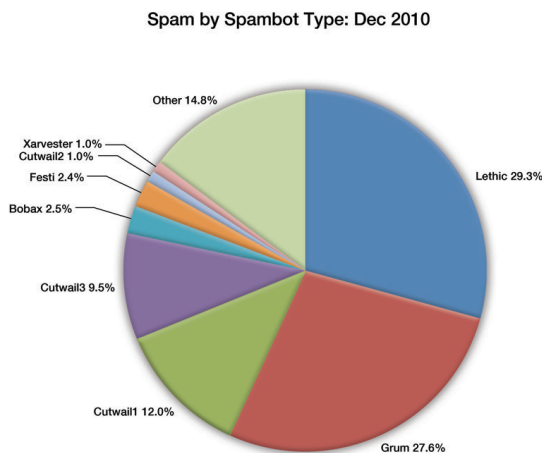


Figure 4: Spam by Spambot Type for December

Spam Categories

Pharmaceutical Spam Dominates

During the second half of 2010, pharmaceutical (“pharma”) spam remained the top spam category at 86.2% of all spam. This result reflects the number and predominance of the pharma affiliate programs that the botnet operators sign up with. Spam touting replica watches was second at 5.4%, with fake diplomas and cheap software at 3.2% and 2.3 % respectively. All the other categories were below the 1% mark.

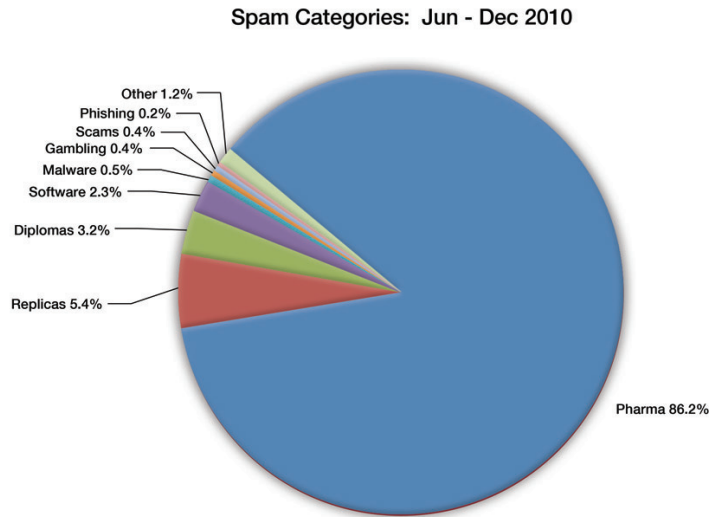


Figure 5: Spam Categories

Following the Spamit.com closure in September, some of the major spamming botnets were forced to search for alternative affiliate programs. In particular, after a brief lull period, Grum swapped to a Replica program, which led to a rise in Replica spam in November and December. However, Grum has recently moved back to Pharma-based programs.

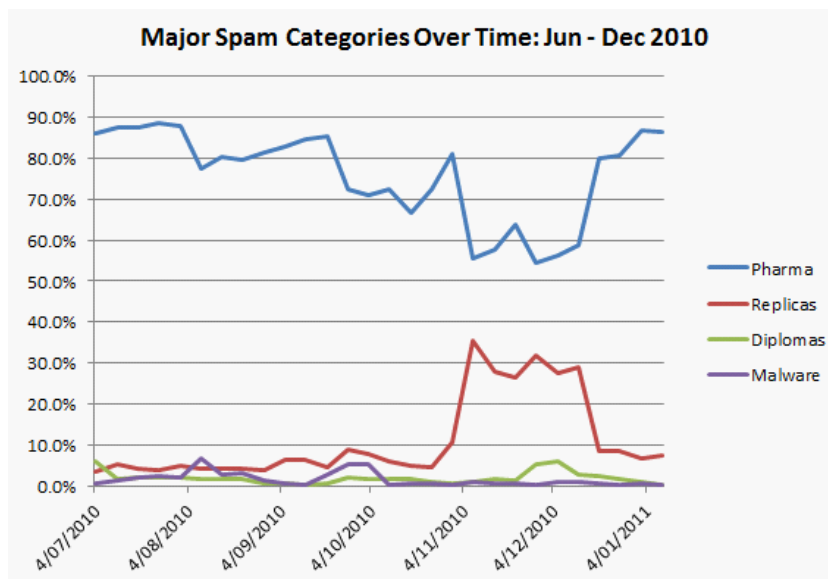


Figure 6: Spam Categories

Another interesting point illustrated in the chart is the overall decline in the proportion of malicious spam. In the third quarter 2010, malicious spam averaged 2.4% of total spam and peaked at more than 5% of all spam. With the disruption of the Bredolab botnet and the reduction in spam bearing the Bredolab malware, this number dwindled to an average of just 0.6% in the last quarter.

EVENTS AND TRENDS FROM JULY THROUGH DECEMBER 2010

Stuxnet: A Defining Point in the Evolution of Malware?

Game-changing Malware Targets Industrial Control Systems

The Stuxnet worm generated considerable news and raised several questions: Who was its intended target? Who wrote this sophisticated piece of malware? Most security professionals are primarily interested in what it portends for the future of malware. Stuxnet was not the first malware crafted to target industrial control equipment, but it was the first confirmed case of malware that attempted to re-program the equipment for disruptive purposes.

Stuxnet was first reported in July 2010 by VirusBlokAda, a security company based in Belarus. They noted in their findings that Stuxnet was designed to affect only certain Siemens industrial control equipment connected to PCs, highlighting the fact that this malware had completely different goals than most malware targeted at companies and individual users. Unlike most targeted attacks, this infection did not spread via the Internet, because the controller computers that connect to these systems are not usually connected to the Internet. Instead, the malware reached these PCs through social engineering attacks that convinced users to plug a USB memory device into the systems. Once connected, the malware then spread to other PCs on the private network using other exploits and P2P RPC techniques. The objective was to re-program the control equipment and cause critical failures in the processes controlled.

It has been suggested that Stuxnet malware is akin to a weapon, which can be used as part of a complex cyber warfare attack.

We now realize that through malware, any system is open for attack, including safety systems. This particular attack was aimed at nuclear facilities, and was apparently designed to delay the development of arms. But what if a similar attack was used to disable critical warning systems or cause a reactor meltdown? An attacker using a victim's own infrastructure to cause damage is far cheaper than flying a bomber overhead or launching a missile. Then too, missiles can be traced back to the attacking party easily, whereas in this case, we still do not have concrete evidence as to who was behind Stuxnet.

The use of malware for disruption and financial gain is one thing. Stuxnet has opened the door to a whole new set of possibilities, evolving to serious new levels.

Notable Botnet Disruptions and Takedowns

A Year Full Of Disruptions

Among the notable botnets disrupted or disabled in the second half of 2010 were the Pushdo/Cutwail and Mega-D botnets. In late August, our spam data showed a complete stop to spam coming from the Pushdo/Cutwail botnet. Cutwail is the spamming component of the Pushdo botnet.

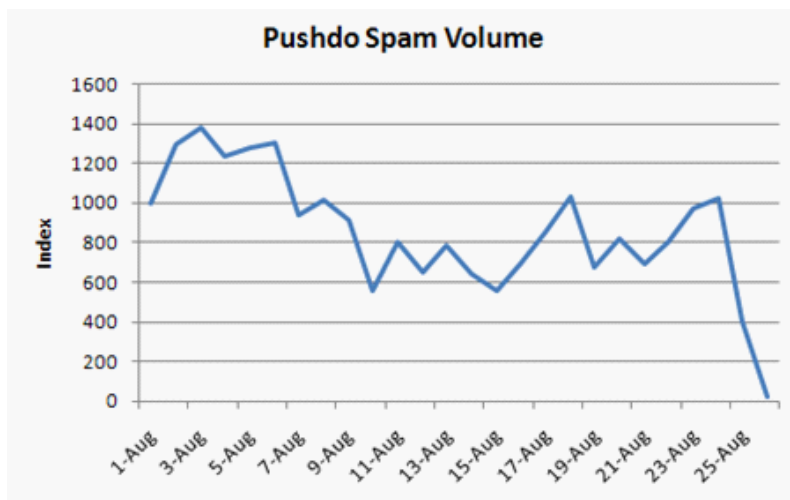


Figure 7: Pushdo Spam Volume Declines Following Takedown Attempt

This event was the result of a coordinated takedown attempted by researchers at The Last Line of Defense (TLLoD). As we cautioned in our [blog post](#) regarding the crippling of the botnet, these types of efforts are typically short lived. Time and again, efforts to take down a botnet have a visible impact, but the botnets are revived and return to their normal activities.

Another botnet, Mega-D, has been taken down multiple times, only to return again to continue its spamming operations. The FBI identified the man behind the botnet, a Russian named Oleg Nikolaenko. He was apprehended in Las Vegas in November of 2010 and the Mega-D botnet ceased to exist.

The lesson? To impact spam volumes and botnet activity long term, it is necessary to target the people behind the botnets. Although we have previously suggested that targeting the affiliate networks may also help to cripple botnets, in reality the botnets find a way to move on to the next program. If Pharmacy spam is off the table, then they migrate to Replica watch spam.

Spamit.com Closes Its Doors and Takes Spam with It

One of the Most Popular Affiliate Programs Disbands, Greatly Impacts Spam Volume

One of the biggest stories to hit the spam world in 2010 was the sudden shutdown of Spamit.com, one of the most popular affiliate programs. It was linked to GlavMed, the company behind one of the largest and oldest affiliate program brands, 'Canadian Pharmacy'.

Spamit.com announced on its website that it was shutting down operations on October 10.

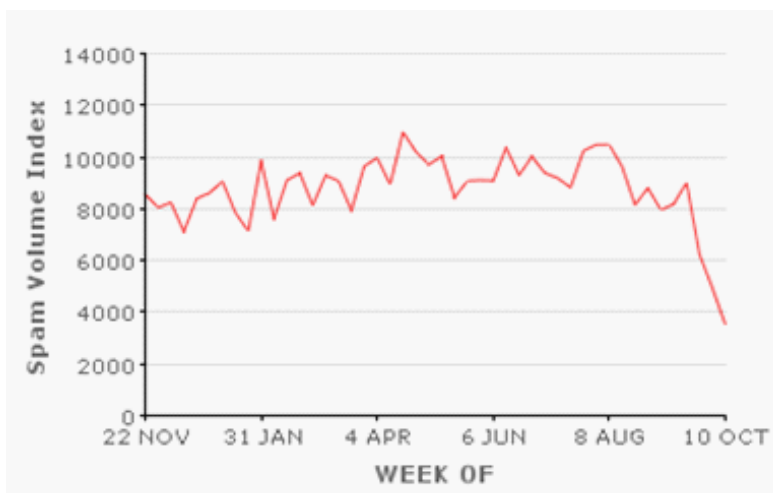


Figure 8: Spam Volume Index Decrease Following The Spamit.Com Closure

The Spamit shutdown coincided with a two-week drop-off in overall spam volume, which we track using our Spam Volume index (Figure 8).

The shutdown hindered the spam operations of the Rustock botnet, which saw a decrease in its spam activity. Another spambot, Grum, also recorded a sharp decline following the shutdown.

Many botnet operators were forced to look for competing affiliate programs. For instance, the Xarvester botnet, which has been linked to Spamit.com, changed its affiliate program of choice from Canadian Pharmacy to Ultimate Replicas, which promotes replica watches.

ZeuS/SpyEye versus Traditional Phishing

Why Traditional Phishing Attacks Have Declined in Favor of More Effective Methods

Over the last few years, we have monitored the volume of phishing campaigns that rely on e-mail. The volume of these campaigns has become so small that we no longer report it on our spam statistics page. The reason? Today, there are more effective ways to harvest banking credentials.

Traditional phishing attacks involve crafting legitimate-looking e-mail that appear to come from a bank. The goal was to trick users into clicking a link leading to a website that appears to represent the bank in question. The attackers hope that the user will be fooled by this page and submit their banking credentials.

This scenario faces a number of challenges. First, the attacker must successfully guess the user's banking institution. Even if that is accomplished, users have become more aware of these types of attacks.

A more effective method for stealing banking credentials comes in the form of malware. Trojans like SpyEye and ZeuS have become popular in the last few years, and for good reason: they are successful at stealing confidential data off a user's system.

Instead of relying on a fake bank login page, the Trojans monitor traffic to the banks the victim visits, capturing the data submitted into the forms on these legitimate pages for submission to the command and control server.

Malware like ZeuS and SpyEye can also perform a Man-in-the-Browser attack. In this form of attack they inject additional forms onto pages from a legitimate banking website, requesting additional information like Social Security numbers. Another benefit of this approach is that the malware can also tamper with the transaction pages returned from the bank, showing the user that no malicious activity has occurred, when in reality, there is money being siphoned behind the scenes.

Cybercriminals tend to move their activities towards the most effective solutions. This is why we have seen Trojans become the method of choice for stealing banking credentials.

How to Phish Regional Banks via Third Parties

Why Target a Specific Bank When You Can Target Them All?

In addition to the shift away from traditional phishing methods, we observed two separate attacks involving impersonation of a third party institution. The examples we have seen involve a fake notice of a tax refund, which is tempting to the user and also presents an apparently legitimate reason for seeking your banking credentials: to send you a tax refund.

The first campaign we observed involved e-mail claiming to be from the New Zealand Department of Inland Revenue (IRD), which informs the user that they are eligible for a tax refund. When the user clicks the link in the spam message, they are directed to a web page that looks like the New Zealand IRD site. However, what's different about this page is that there is a section regarding an "Annual Refund Policy" which highlights various banking institutions in New Zealand. The user is asked to click the appropriate bank logo in order to begin the refund procedure.

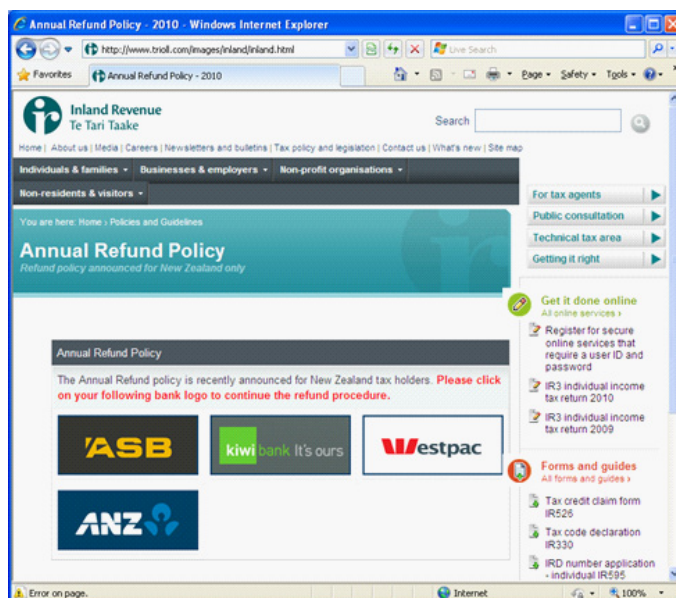


Figure 9: New Zealand's Inland Revenue Site Spoofed to Target Users of Regional Banks

This is a clever take on phishing. Instead of guessing which institution a user banks at, the phishing website prompts the user to select their own bank, making it that much easier for the criminals.

Once the user clicks the link to their bank, they are redirected to a fake version of the bank website, where they will submit their banking credentials, not realizing they are being phished.

After discovering the New Zealand version of this phishing scam, we located files on a server that indicated that this tax scam template was part of some sort of phishing kit. We confirmed this to be true when we discovered a similar campaign.

In December, we observed the same type of phishing campaign—this time targeting UK banking customers. Users received e-mail claiming to be from HM Revenue and Customs, once again offering a tax refund.

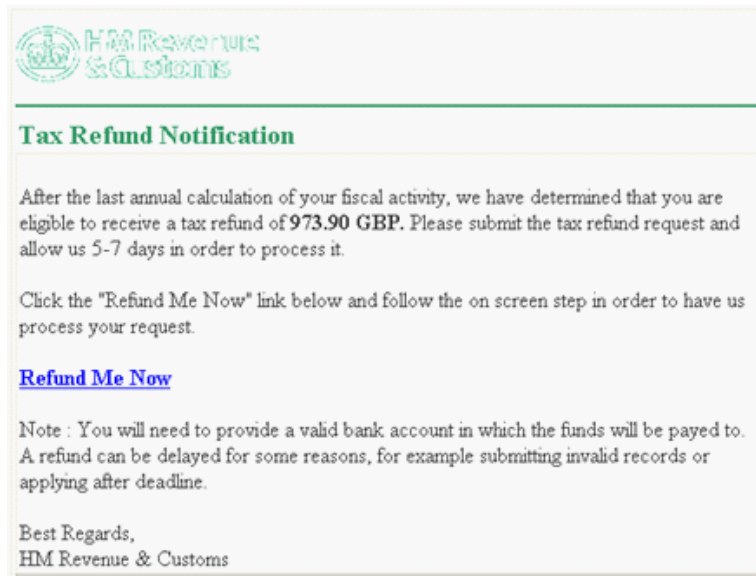


Figure 10: Fake E-Mail from UK's HM Revenue and Customs Regarding a Tax Refund

When the user clicks the "Refund Me Now" link, they are redirected to a fake HM Revenue and Customs page, which shows logos for various banks in the UK.

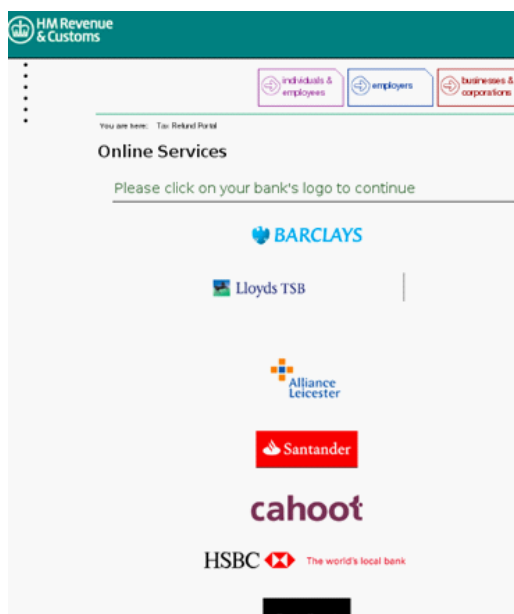


Figure 11: Similar to Figure 9, a Spoofed Version of the HM Revenue & Customs Site

This trend shows that despite the decline in traditional phishing methods targeting individual banks, cybercriminals are finding new ways to trick unsuspecting users into giving up their banking information.

Exploit Kits Becoming A “One-Stop Shop” Making Life Easier for Cybercriminals, One New Feature at a Time

In 2010, the trend was to make cybercrime easier by adding additional features to exploit kits. Though not new in the cybercrime world, the inclusion of an antivirus scanner within the Siberia exploit kit underscores this trend.

Scanner	Scan result
AVG Free	-
ArcaVir	-
Avast	-
Avast 5	-
AntiVir (Avira)	TR/Dldr.Java.Agent.CW
BitDefender	-
VirusBuster Internet Security	-
Clam Antivirus	-
COMODO Internet Security	TrojWare.Java.TrojanDownloader.Agent@105702274
Dr.Web	-
eTrust-Vet	-
F-PROT Antivirus	-
F-Secure Internet Security	-
G Data	-
IKARUS Security	Trojan-Downloader.Java.Agent
Kaspersky Antivirus	Trojan-Downloader.Java.Agent.cw
McAfee	-
MS Security Essentials	-
ESET NOD32	-
Norman	-
Norton Antivirus	-
Panda Security	-
A-Squared	Trojan-Downloader.Java.Agent!IK
Quick Heal Antivirus	-
Rising Antivirus	-
Solo Antivirus	-
Sophos	-
Trend Micro Internet Security	-
VBA32 Antivirus	-
Vexira Antivirus	-
Webroot Internet Security	-

Figure 12: Virus Scan Results From a Virustotal Clone that Is Now Being Used in Exploit Kits

The image shows results of a scan of a malware executable. Although it looks similar to the results from a scan at virustotal.com, this particular tool uses an underground virus scanning service. Use of an underground service is necessary, since uploading a piece of malware to virustotal would allow antivirus vendors to observe the sample and update their signatures to stop it from infecting users.

The scanning service is not new, its inclusion within the exploit kits themselves is new. We have already seen exploit kits that include modules to check the site rating on services like McAfee’s Site Advisor and Norton’s Safe Web. The inclusion of virus scanning within the kits themselves is all part of the natural progression.

Neosploit Exploit Kit Returns, Ushers in Simple to Use Malware-as-a-Service

The return of the Neosploit exploit kit has brought more than just enhancements to obfuscation techniques. It is now being offered to customers as Malware-as-a-Service. The people behind Neosploit are responsible for its activation and for providing access to their customers.

Offering up the exploit kit as a service provides a number of benefits:

1. There is no need to install a kit on a server. Users only need to redirect the request to the backend server.
2. It is harder to expose the people behind the exploit kit
3. Updating the toolkit is simple, since it is continually maintained by the team

These enhancements further reduce the barrier to entry for would-be cybercriminals.

Mimicking Legitimate Social Networking Communications Messages Fool Even Savvy Users

E-mail spam purporting to be from a legitimate organization has been a common theme amongst spam and phishing messages. More often than not, these attempts are done halfheartedly.

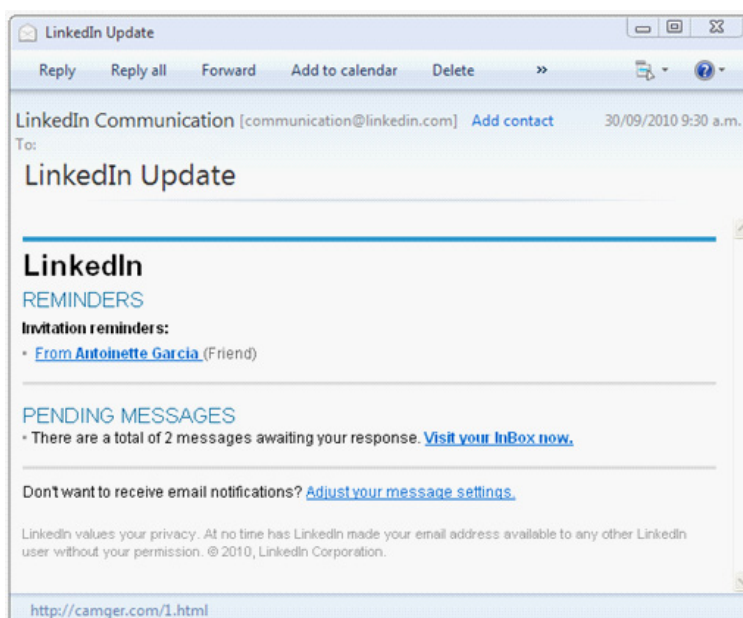


Figure 13: Spoofed Message from LinkedIn

In September of 2010, we encountered a series of spam messages claiming to be from LinkedIn, the social networking site used by professionals and businesses. These messages looked similar to genuine LinkedIn messages.

Spam messages were sent as “reminders” of pending connection requests from LinkedIn users. The messages themselves contained little information, requiring the user to click a link and visit LinkedIn to read more. [This spam campaign](#) was slicker than usual and easily fooled many users into clicking on the link, which led to the Phoenix exploit kit infection page.

Those behind this type of spam campaign recognize that users are becoming more aware of the types of scams targeting them. They see the need to craft messages that look as legitimate as possible in order to maximize the possibility of success. Social networking messages, as seen in this campaign, make it easier to target end users.

Zeus/SpyEye Merger

The Shape of Things to Come?

In the second half of 2010, M86 Security Labs reported on a ZeuS attack that targeted the customers of a global financial institution, recording 3,000 victims and stealing \$889,000 USD from their accounts. (more about the [ZeuS report](#)).

A few months after this report was released, the US Federal Bureau of Investigation (FBI), with the help of various police forces around the world, began to make criminal charges against individuals who were associated with the ZeuS botnet. Shining the light on the millions of dollars that these individuals had stolen brought about mainstream attention to the cybercriminal activity associated with the ZeuS botnet.

In late October, [Brian Krebs reported](#) that the author of the ZeuS botnet was planning to stop maintaining the ZeuS Trojan. According to Krebs, the source code for ZeuS was being handed over to the developer of SpyEye, known as a rival to the ZeuS Trojan.

Despite this announcement, it is believed that the ZeuS Trojan will continue to thrive due to its significant user base. However, with the source code now transferred to the creator of SpyEye, the community at large is waiting to see just how sophisticated the next variant of SpyEye will become.

Combined Attacks: Flash and Acrobat

Flash and Acrobat Sitting in a Tree: e-x-p-l-o-i-t

In our first half 2010 report, we showcased the concept of combined cross-component attacks. In that case, we described a combined attack using Java and Adobe Flash ActionScript to bypass security technologies, which have become more savvy in blocking obfuscated code.

Another form of combined attacks emerged in 2009 and has since been exploited in the wild. This involves Adobe's flagship products like Acrobat, used to view PDF files. In this case, the method of attack involves a vulnerability in Adobe Flash.

```
20 30 20 52 20 5D 20 3E 3E 0A 65 6E 64 6F 62 6A 0 R ] >>.endobj
0A 31 32 20 30 20 6F 62 6A 0A 3C 3C 20 2F 45 46 ..12 0 obj.<< /EF
20 3C 3C 2F 46 20 31 34 20 30 20 52 20 3E 3E 20 <</F 14 0 R >>
2F 54 79 70 65 20 2F 46 69 6C 65 73 70 65 63 20 /Type /Filespec
2F 46 20 28 70 6F 63 2E 73 77 66 29 20 3E 3E 0A /F (poc.swf) >>.
65 6E 64 6F 62 6A 0A 31 33 20 30 20 6F 62 6A 0A endobj.13 0 obj.
3C 3C 20 2F 53 75 62 79 70 65 20 2F 46 6C 61 73 << /Subtype /Flas
68 20 2F 50 61 72 61 6D 73 20 31 35 20 30 20 52 h /Params 15 0 R
20 2F 54 79 70 65 20 2F 52 69 63 68 4D 65 64 69 /Type /RichMedi
61 49 6E 73 74 61 6E 63 65 20 2F 41 73 73 65 74 aInstance /Asset
20 31 32 20 30 20 52 20 3E 3E 0A 65 6E 64 6F 62 12 0 R >>.endob
6A 0A 31 34 20 30 20 6F 62 6A 0A 3C 3C 20 20 2F j.14 0 obj.<< /
54 79 70 65 20 2F 45 6D 62 65 64 64 65 64 46 69 Type /EmbeddedFi
6C 65 20 20 2F 50 61 72 61 6D 73 20 3C 3C 20 2F le /Params << /
53 69 7A 65 20 36 34 36 20 3E 3E 20 2F 44 4C 20 Size 646 >> /DL
36 34 36 20 2F 4C 65 6E 67 74 68 20 36 34 36 20 646 /Length 646
3E 3E 0A 73 74 72 65 61 6D 0A 46 57 53 09 80 02 >>.stream.FWS!E.
00 00 78 00 05 5F 00 00 0F A0 00 00 0C 01 00 44 ...x.....D
11 08 00 00 00 43 02 FF FF FF BF 15 0B 00 00 00 .....C.yyy.....
01 00 53 63 65 6E 65 20 31 00 00 BF 14 34 02 00 ..Scene 1...4..
00 01 00 00 00 00 10 00 2E 00 00 00 00 13 00 04 .....
76 6F 69 64 16 63 6F 6D 2E 62 65 61 76 65 72 63 void.com.beaverc
6F 72 65 2E 65 66 66 65 63 74 73 0D 54 65 78 74 ore.effects.Text
41 6E 69 6D 61 74 69 6F 6E 06 4F 62 6A 65 63 74 Animation.Object
24 63 6F 6D 2E 62 65 61 76 65 72 63 6F 72 65 2E Scum.beavercore.
65 66 66 65 63 74 73 3A 54 65 78 74 41 6E 69 6D effects:TextAnim
61 74 69 6F 6E 05 73 74 61 72 74 06 42 61 72 6B ation.start.Bark
79 73 0D 66 6C 61 73 68 2E 64 69 73 70 6C 61 79 ys.flash.display
06 53 70 72 69 74 65 05 74 72 61 63 65 29 49 6D .Sprite.trace)Im
61 67 69 6E 65 20 61 20 74 65 78 74 20 65 66 66 agine a text eff
65 63 74 20 77 69 74 68 20 67 72 65 61 74 20 6D ect with great m
61 6A 65 73 74 79 2E 14 45 66 66 65 63 74 20 6E ajesty..Effect n
6F 77 20 73 74 61 72 74 69 6E 67 2E 0C 66 6C 61 ow starting..fla
```

Figure 14: Screenshot of a Flash File Embedded in a PDF File Targeting CVE-2010-2168

The connection between the two Adobe products is that Acrobat has a built-in flash player (authplay.dll). The vulnerability to malicious Flash code is present for all Acrobat installations, even for clients that do not have Adobe Flash installed. When a user opens a malicious PDF file, it will drop and execute a malicious binary. In the case of the combined attack, the vulnerability being exploited is within Adobe Flash, not Adobe Acrobat.

This method is also a good way to evade antivirus scanning. It makes detection more complex, as PDF streams can be compressed and encoded.

This new attack is the latest in a trend of combined cross-component attacks that have begun to appear over the last few years. Attacks are no longer simple. They are becoming more sophisticated and more complex. As security technologies that are intended to protect businesses and users grow and mature, so do the attacks in the wild.

Java Attacks Soar Into The New Year

Early Reports on the Rise of Java Attacks Become the Attack Method of Choice

In our first half 2010 report, we highlighted the rise in Java-related exploits. Our research at the time showed it to be the method of choice, proving to be most successful in achieving successful exploitation of end-user systems.

In the second half of 2010, we found that Java-based attacks rose to higher levels than anticipated.

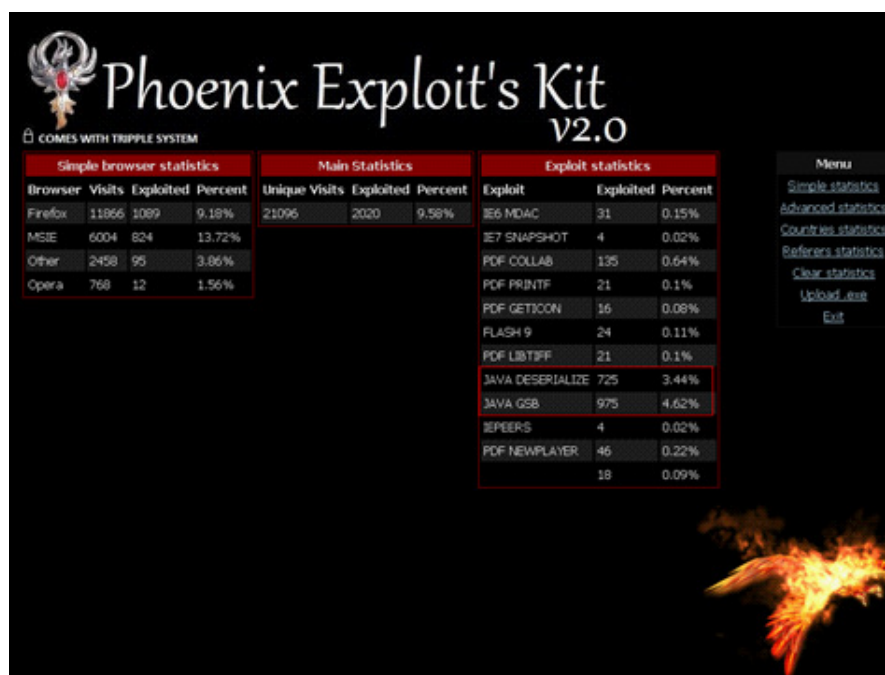


Figure 15: Phoenix Exploit Kit Admin Page Showing the Domination of Java-based Exploits

Data from exploit kits such as Phoenix (in Figure 15 above) shows a continuation of this trend. These types of attacks are most successful because Java versions on end-user systems are not being updated regularly. Vulnerabilities such as [Java GSB](#) have been patched, yet these vulnerabilities can still be exploited in the wild.

A contributing factor is that users are deterred by the Java update process, and therefore continue to delay the updates needed to address critical vulnerabilities.

Social Networks: Cybercrime Utopia

The Ideal Pool of Users

In the past, we have cautioned that the rise of social networks would lead to an increase of attacks targeting these websites and their users.

Twitter Hit by Multiple XSS Vulnerabilities

In the second half of the year, Twitter was the victim of multiple cross-site scripting (XSS) vulnerabilities. The most notable incident affected thousands of users of the site, including Sarah Brown, the wife of the former British Prime Minister Gordon Brown.

This vulnerability took advantage of a flaw in Twitter, which allowed users to post javascript code within a tweet (the update functionality of Twitter). This code was not properly sanitized, allowing the code to be executed within the Twitter.com site when a user would mouse over a tweet containing the onMouseOver code.

Twitter deserves credit for responding to this and other security-related issues, as they have been making a concerted effort to mitigate various possible attacks on the site.

Survey Scams Increase

One of the reasons social networks are targeted by cybercriminals is that many users trust that links and content are from legitimate sources.

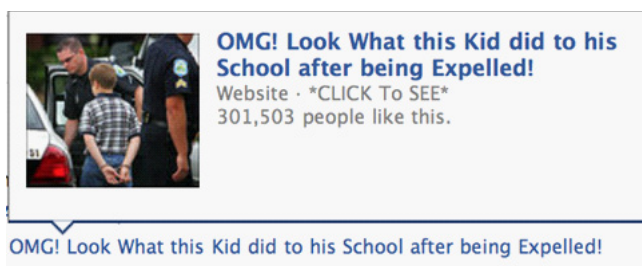


Figure 16: Example of Outrageous Headlines Used in Facebook Scams

On both Twitter and Facebook, M86 Security Labs has identified a growing number of scams that lead users to bogus online surveys. Some of the most popular survey scams in the second half of 2010 used outrageous news stories and shocking headlines to lure the user into installing a rogue Facebook application, which presents a survey. Additionally, we continue to see scams pitching free iPhone 4's and free iPads, attractive consumer-oriented products, as well as an age-old social networking scam that offers users the ability to "see who viewed your profile," a feature not provided to users of most social networks.

The benefit for the scammers is the money that can be earned through affiliate programs that pay for the successful completions of surveys or the completion of offers for services like Netflix and GameFly. As we have seen with spam, affiliate programs earn big bucks for spammers. It's no surprise to see similar tactics being used on social networks, which offer the potential for additional profits.

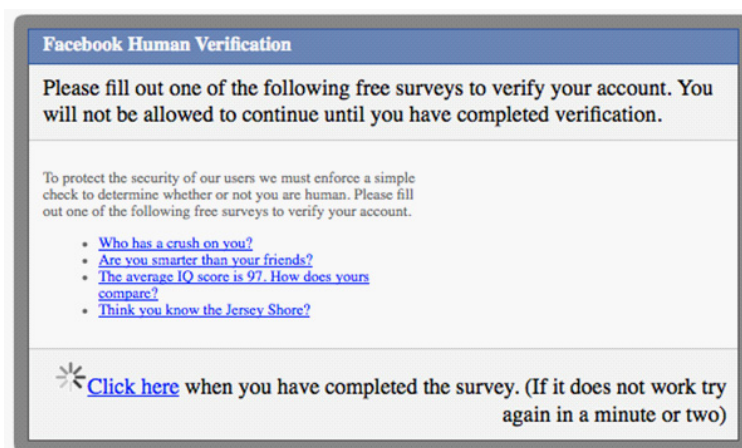


Figure 17: One Bogus Facebook Application Tries to Convince Users to Fill Out One of Four Surveys



Figure 18: Free iPad Offer Scam. The Ad Explicitly States in Fine Print That It Is Not Endorsed by Apple and May Require More than Just Filling Out the Survey to Obtain the “Free iPad”

The fake surveys typically request personally-identifiable information. As the user progresses through the survey, they are asked more questions about their household income, shopping habits, and so forth. Once the questions are completed, the users are presented with offers from various companies.

Step 2 Complete The Survey

TV & Phone

My TV service is: Cable Satellite (Dish/Direct TV) None

What type of cell phone plan do you have? Pre-Paid Contract No cell phone

Education & Career

If you could go back to school to get a better job and make more money, would you? Yes No

Highest level of education:

My employment status: Full-Time Part-Time Unemployed Stay at home parent Retired

Have you or your spouse served in the Military/Armed Services? Yes No

Home, Finance & Auto

My household status: Own my own home Rent Live with parents Live with significant other

My marital status: Single Married

Do you have children under 18? Yes No

My household income: Over \$75,000 \$50,000 - \$75,000 \$25,000 - \$49,999 Under \$25,000

My debt status: Over \$15,000 \$10,000 - \$15,000 \$5,000 - \$10,000 Under \$5,000 None

Do you owe \$10,000 or more in Tax Debt? Yes No

My credit status: Excellent Good Fair Poor

Do you have an active checking account? Yes No

Do you have an active credit or debit card? Credit card Debit card Both None

Is your car under warranty? Yes No I don't have a car

Do you plan to move within the next 3 months? Yes No

Health

Are you diabetic? Yes No

Figure 19: Example of a Survey Scam That Requests Large Amounts of Personal Information

On Twitter, the users are led directly to the scam survey page. On Facebook, however, the users are sent to a Facebook Application Installation page. If the user agrees to install the application, they are allowing the author of the application access to their profile information as well as the ability to post updates to their Facebook page.



Figure 20: False Facebook Applications Spam News Feeds With Messages Like These to Convince a User's "Friends" to Visit the Rogue Application and Install It

By gaining access to the user's page, the application is able to spread further, reaching the news feed of users that were inaccessible before. With the built-in trust that social networks create, users are also more likely to visit a link posted by a friend than they would if the link came in an unsolicited e-mail.

Despite best efforts by both Twitter and Facebook, these scams continue to occur. Since they remain a successful avenue for generating money for cybercriminals, we expect them to continue to appear in different forms and gain momentum in the coming year.

CONCLUSION

In comparing the first half of 2010 to the second half, we see new trends emerging and many of the old tactics still working. So for cybercriminals, an old adage holds true: "If it ain't broke, don't fix it."

We continue to see the most popular exploits targeting older vulnerabilities that have already been patched, with Adobe Reader/ Acrobat and Internet Explorer remaining a consistent choice for attackers. Our research suggested that Java-based vulnerabilities would increase significantly, and they did. We continue to caution users that the best way to avoid becoming a victim is to ensure that all of their applications are updated to the most recent versions.

We saw a dramatic decrease in the volume of spam, following the closure of a notable affiliate program as well as various takedown efforts conducted by security researchers. Despite these events, we still believe that spam will rebound to its previous levels. While we cannot know when it will happen, we do know for certain that cybercriminal operations see spam playing an important role in their activities. Until those behind the spam botnets are apprehended, we expect that spam volume will continue to recover from any setbacks.

The race between cybercriminals and security companies continues, as the authors of malware seek new ways to bypass security technologies that prevent their successful attacks against organizations and end users.

The prolific ZeuS botnet was tracked by law enforcement, as serious efforts were made to hunt down those responsible for attacks that led to significant financial losses for businesses. With other data-stealing Trojans in the wild and SpyEye receiving its rival's source code, we expect to see a new flavor of SpyEye emerge and other rival banking Trojans become more sophisticated, allowing their clients to continue their operations.

Social networks remain a prime target for cybercriminals who want to take advantage of user trust. Adding security controls plays a role in preventing these attacks from succeeding, but user education must play a bigger role in the future.

Cybercrime is a profitable venture. As new technologies are developed and more people use the Internet, cybercriminals will find ways to extend their reach. Criminals see dollar signs attached to the profile pages of users today, and they have found many ways to cash in. We encourage you to follow our recommendations below to help ensure that you do not become a victim.

RECOMMENDATIONS

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 current vendors the tough questions about exactly what they do to detect and block these threats. The solutions you use should have a solid base of reactive controls in anti-virus and URL scanning, along with proactive technologies such as real time code analysis. Consider testing products against each other, and ensure the vendors are investing in threat research.

Education is paramount. Teaching users about best practices for their everyday Internet usage is a key part of a security policy. Show them examples of social networking scams. Explain how easy it is for a computer to get infected. Encourage them to keep their applications up to date (see below). Above all else, they should be wary about clicking on any links in email, and pay close attention to the links found in search engine results and those posted by contacts on social networks.

Stay up to date. Keep Web browsers, add-ons/extensions, and desktop applications up to date with their latest versions. We have seen time and again that attacks target vulnerabilities found in old versions of Web browsers or applications. 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 helps 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 for 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 the actual destination URL. M86 Security and other security vendors provide free tools for users to install on their personal or home computers—typically the most vulnerable. One such tool is SecureBrowsing, which analyzes links from search engine results or on Web pages to gauge their malicious nature. It also works with shortened URLs such as those found in Twitter.

Review and familiarize yourself with privacy settings. As noted earlier, education is paramount and often users do not realize the type of information they are sharing through their social networks. Review your privacy settings on the various social networks on which you participate. For example, Facebook's privacy settings are now located at <http://facebook.com/privacy>.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

8845 Irvine Center Drive
Irvine, CA 92618
United States

Phone: +1 (949) 932-1000
Fax: +1 (949) 932-1086

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 3, Level 7, 100 Walker St
North Sydney NSW 2060
Australia

Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899

Version 02/02/11