Symantec Intelligence

Symantec Intelligence Report: May 2012

Flamer; Olympic Scams; Macs Under Attack; Mobile Threats Continue to Rise and Android Malware Increases

Welcome to the May edition of the Symantec Intelligence report, which provides the latest analysis of cyber security threats, trends, and insights from the Symantec Intelligence team concerning malware, spam, and other potentially harmful business risks. The information used to compile the analysis for this report includes data from April and May 2012.

Report highlights

- Spam – 67.8 percent (an increase of 3.3 percentage points since April): page 11
- Phishing – One in 568.3 emails identified as phishing (a decrease of 0.03 percentage points since April): page 14
- Malware – One in 365.1 emails contained malware (an increase of 0.03 percentage points since April): page 16
- Malicious Web sites – 4,359 Web sites blocked per day (an increase of 48.7 percent since April): page 17
- Targeted Attacks, Cyber Espionage and W32.Flamer: page 2
- London 2012 Olympic Games – Spammers Aiming for the Gold: page 3
- Flashback—The day of the Mac threat has arrived: page 5

Introduction

The threat landscape is continually shifting and changing. For years attackers focused on Windows PCs because of the widespread prevalence of the Windows platform, the return on investment was much greater. However, in 2012 there has been a shift in the attentions of the attackers. This shift was clearly underway in 2011 as we reported in the latest Symantec Internet Security Threat Report[1] (ISTR) for 2011, where Android threats moved from something that was more a novelty, to become a regular occurrence, such as Opfake, which covers a wide range of device OSes, from Symbian, to Windows Mobile, to Android, and even targeting iOS devices. Not only has the growth in mobile threats continued into 2012, but the pace has quickened significantly. By the end of May 2011, we had seen 11 new Android threat families and twelve months on, the number will have passed 30; that's almost a threefold increase, year on year. There was also a month-by-month average increase of 42.5% in the number of new threat families.

It's not just mobile devices that are being targeted either. While Apple's Macintosh computers have been attacked in the past, the idea that this computing platform would be targeted en mass is something Internet security experts have warned about for years. That day has finally arrived. A trojan by the name of Flashback, which first appeared last year, had a breakout performance in April, successfully infecting approximately 600,000 Macs.

The recent discovery of W32/Flamer, uncovers a highly sophisticated and targeted threat primarily targeting a few hundred organizations and individuals located in the Middle East. Based on the latest Symantec analysis, Flamer appears to act as a general-purpose spying too. In order to shed some light, we thought we would provide a quick round-up of what we know so far. This month we're also highlighting the first few signs of Olympic related spam[2]. Finally, for the first time this year, spam levels have begun to climb, with two-thirds of email traffic now identified as spam, 3.3 percentage points higher than in April; still lower than the 75% annual average for 2011.

I hope you enjoy reading this month's report, and feel free to contact me directly with any comments or feedback.

Paul Wood, Cyber Security Intelligence Manager
paul_wood@symantec.com
@paulowoody

[1] *http://www.symantec.com/threatreport/*

[2] *NB: The Symantec Intelligence Report is not sponsored or endorsed by the London 2012 Olympics.*

Report analysis

Targeted Attacks, Cyber Espionage and W32.Flamer

By Benjamin Nahorney

The recent discovery of W32/Flamer, uncovers a highly sophisticated and targeted threat primarily targeting a few hundred organizations and individuals located in the Middle East. Based on the latest Symantec analysis, Flamer appears to act as a general-purpose spying too, ideally designed for cyber espionage and stealing all types of information from compromised machines. In order to shed some light, we thought we would provide a quick round-up of what we know so far.

W32.Flamer: The story so far

The news first broke when the Iranian Oil Ministry began disconnecting their oil facilities from the Internet last month. The state's oil production was reportedly under attack from a virus called 'wiper', according to the Iranian Students' News Agency. A few weeks later, the Iran National CERT, Budapest University of Technology and Economics' CrySyS lab, released details on the threat.

It seemed as though another case of digital espionage in the Middle East had been discovered. Flamer (a.k.a. Flame or Skywiper) appeared to have been in existence since 2010, maybe even earlier. The threat seemed to be the epitome of covert malware, hiding in systems undetected for years and quietly siphoning off information, sending it to the malware's authors in ways not easily picked up by standard network analysis.

The news generated a great deal of media interest; it was almost as if a prize jewel-thief had been caught red-handed. Comparisons to Stuxnet and Duqu were made. The finger was pointed at the political opponents of Iran. Flamer was called the most complex piece of malware found to date. But how many of these claims are true? As with most statements like these, there is a grain of truth in most of them. Let's separate the wheat from the chaff.

What does Flamer do?

There has been a lot of speculation that Flamer is a type of cyber-weapon. At this point we have not seen any evidence to support this. A more accurate description of Flamer is a cyber-espionage tool used to gather data from the compromised computers.

Who made Flamer?

In short, we don't know. As was the case with Stuxnet and Duqu, the finger has been pointed at nation states in political opposition with Iran. However, there is no smoking gun that leads us to anyone in particular. All evidence that has come to light so far is purely circumstantial, and any attempts to pin down the culprits are simply based on conjecture.

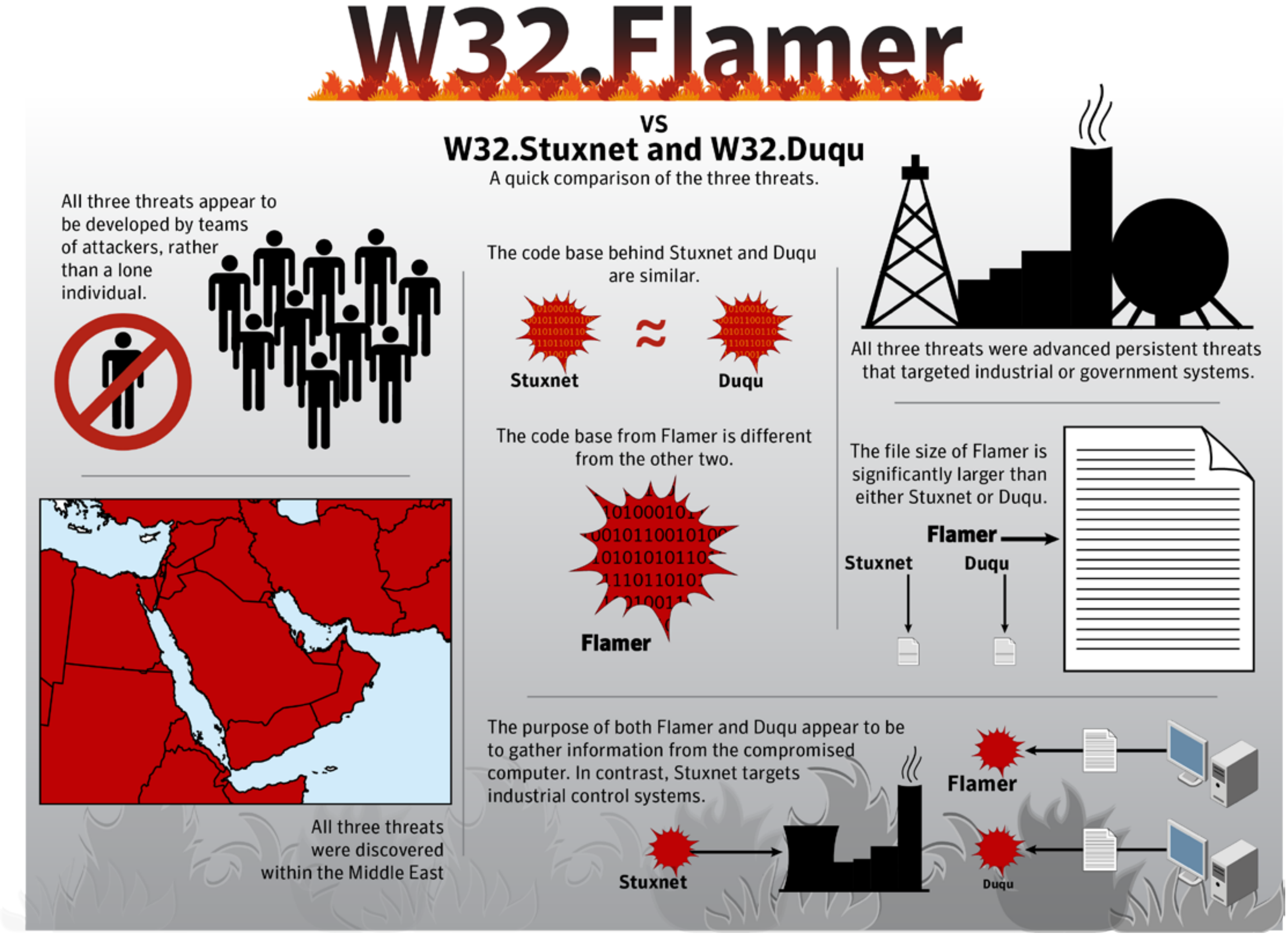
Catching Flamer isn't like catching a jewel thief. It's like finding the tools left behind after the thief has already made off with the prize diamond.

Flamer is the most complex piece of malware, ever.

Flamer is huge. Weighing in at 20 megabytes, it's many times larger than Stuxnet or Duqu. The complexity in analyzing Flamer lies with this fact. It's easily on par with Stuxnet and Duqu in terms of complexity, but vastly larger.

What is interesting in terms of Flamer is that it appears to have been developed by professional software developers. The code is very clean, and has an advanced architectural design. For instance, it makes use of a highly customizable scripting language called *Lua*, which allows the attackers to create custom modules for the threat. It also contains a SQLite database which it uses to collect and store information.

Is Flamer related to Stuxnet and Duqu?


W32.Flamer
vs
W32.Stuxnet and W32.Duqu
A quick comparison of the three threats.
All three threats appear to be developed by teams of attackers, rather than a lone individual.
The code base behind Stuxnet and Duqu are similar.
≈
Stuxnet
Duqu
All three threats were advanced persistent threats that targeted industrial or government systems.
The code base from Flamer is different from the other two.
Flamer
The file size of Flamer is significantly larger than either Stuxnet or Duqu.
Flamer
Stuxnet
Duqu
All three threats were discovered within the Middle East
The purpose of both Flamer and Duqu appear to be to gather information from the compromised computer. In contrast, Stuxnet targets industrial control systems.
Flamer
Stuxnet
Duqu

No. However, there are certain factors that all share in common. For example, Flamer has appeared in the Middle East, in particular in Iran, just as Stuxnet and Duqu did. It also appears to be politically motivated, as were Stuxnet and Duqu. However, while Stuxnet and Duqu shared similar code bases, at this point we have yet to find an overlap with Flamer. It seems as though Flamer could have been written by an entirely different team of programmers.

How come it hasn't been detected before?

Flamer could be looked at as a textbook model for a targeted attack. Its entire purpose is to quietly compromise a computer and remain hidden on that system. It did just that for a long period of time. It seems as though Flamer was discovered when it stopped behaving covertly. Given how the Iranian Oil Ministry rapidly unplugged its computers from the Internet, and dubbed the threat 'wiper', it seems that, albeit circumstantially, Flamer began behaving in a manner that drew attention to it.

The details surrounding Flamer and its overall capabilities are still being researched and uncovered. We hope to have more info on the larger picture in next month's report.

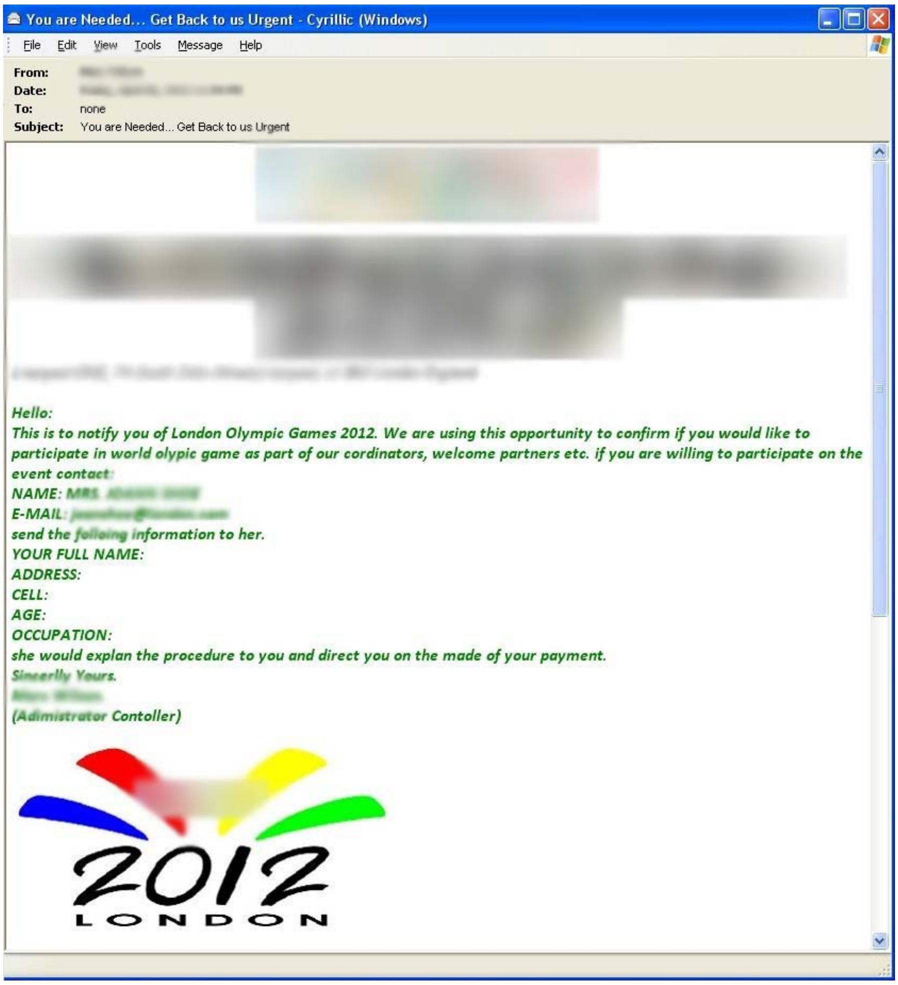
For the latest information on W32.Flamer, please follow the Symantec Security Response team on Twitter: @ThreatIntel; here you will find links to the latest blogs and deeper analysis of this cutting-edge targeted attack.

London 2012 Olympic Games – Spammers Aiming for the Gold

By Samir Patil

With the excitement of the 2012 Summer Olympic Games building, consumers and Internet users need to be on the lookout for scammers trying to cash in on the event. Symantec has kept its eye on the ball and reported on malicious, phishing and 419-spam campaigns associated with major global sporting events in the past, and this year's Olympics will be no different.

We have already seen lottery scams related to London Olympics. However we have uncovered a new scam where spammers are asking for participation in the event in the form of co-coordinators, welcome partners, and more. To participate, the reader is asked to provide a large amount of personal data up front—a red flag for any sort of promotion like this. The presence of the official logo of the event in the email is to possibly deceive users of its legitimacy.



You are Needed… Get Back to us Urgent - Cyrillic (Windows)
File Edit View Tools Message Help

From: [redacted]
Date: [redacted]
To: none
Subject: You are Needed... Get Back to us Urgent

[redacted]

Hello:
This is to notify you of London Olympic Games 2012. We are using this opportunity to confirm if you would like to participate in world olypic game as part of our cordinators, welcome partners etc. if you are willing to participate on the event contact
NAME: [redacted]
E-MAIL [redacted]
send the [redacted] *information to her.*
YOUR FULL NAME:
ADDRESS:
CELL:
AGE:
OCCUPATION:
she would explan the procedure to you and direct you on the made of your payment.
[redacted]
([redacted] *Contoller)*

Figure 1 – Spam asking for Olympic participation

As the 2012 London Olympics draws nearer, we are expecting this type of threat to proliferate. Users should make it a habit to check the legitimacy of any message before downloading the attachment and avoid clicking on any links so as not to provide any personal and sensitive information such as account numbers.

Symantec will continue to monitor these attacks and keep users informed. Users are advised not to click on URLs from unsolicited emails. We recommend avoiding communication using phone numbers or email addresses provided in scam emails.

To ensure that spammers don't take away gold at the Olympics, deploy effective spam filters and make it a priority to educate email users against such scam emails.

Here are a few handy tips:

- You can't win a lottery without buying a lottery ticket
- People with millions of dollars in hand can usually spell and punctuate correctly
- THEY KNOW HOW TO TURN OFF CAPS LOCK TOO!!!

Thanks to Senthilnath Kesavelu for contribution to this story.

Flashback—The Day of the Mac Threat has Arrived

By and large, Mac users historically have had a pretty easy time in the threat landscape. While the occasional virus or Trojan has appeared, the platform has been largely ignored by attackers. This led many to believe the platform was simply more secure than Windows, leading the occasional Mac user to claim "I don't need antivirus protection, I have a Mac."

Whether such claims are true or not, that all changed last April. A new variant of the Flashback Trojan, called OSX.Flashback.K, appeared and spread like wildfire. The threat ultimately infected around 600,000 Macs, leading to a series of copycat threats, and proving to attackers that the platform was a viable alternative to Windows. So what is it about Flashback.K that made it so much more successful than most Mac malware to-date?

Flashback was first discovered in September of 2011[3]. At the time the threat masqueraded as an Adobe Flash Player installation package, which is where the name originates. Since Apple does not provide Flash updates, it's easy to see how some users may have been duped by a phony install package.

The attackers tried a few more variations of Flashback, with limited success, until they hit upon a well-known Java vulnerability. The Oracle Java SE Remote Java Runtime Environment Denial Of Service Vulnerability[4] (CVE-2012-0507) had been publically disclosed in February, and subsequently patched by Oracle. However, Apple was slower to patch the Java versions that they look after within their OSX operating system. This left Mac users exposed and attackers pounced.

The exploit was added to a version of the popular Blackhole exploit kit and seeded out to compromised websites throughout the Internet. If a Mac user happened to come across one of these websites, the kit attempted to exploit the Java platform and install Flashback. The result was more than half a million compromised Macs.

Once the word spread, Apple was quick to release a patch for the vulnerable version of Java and distribute it to users of OSX version 10.6 and 10.7. The company, in an uncharacteristic move, would release a patch for the no-longer-supported OSX 10.5 a few weeks later.

Other malware authors sat up and took notice. In the following days and weeks, other new OSX threats appeared, such as OSX.Sabpab and OSX.Olyx.B, hoping to cash in on the newly discovered susceptibility of the Apple operating system.

It is entirely possible that the success of this botnet even caught its authors by surprise. One of the payloads of the threat was to generate pay-per-click revenue. When taking into account similar threats in the past, a botnet of this size could easily generate tens of thousands of dollars in revenue per day from ad clicks. However, only around 10,000 of the 600,000 compromised computers managed to download and install the ad-clicking component. By our estimates, this only resulted in about $14,000 (USD) total in three weeks[5], and it's unclear if they were even able to collect the revenue earned. In all, this falls far short of the botnet's potential.

So how did we find ourselves in this position? Why now, after all these years, are Macs suddenly being compromised to a significant extent? It could be that, in many ways, Mac security is currently in a position that Windows was in eight to ten years ago. There are a number of factors potentially at play here:

[3] *http://www.symantec.com/security_response/writeup.jsp?docid=2011-093016-1216-99*

[4] *http://www.securityfocus.com/bid/52161*

[5] *http://www.symantec.com/connect/blogs/osxflashback-how-turn-your-botnet*

- It could be that many Mac users aren't concerned about security because they haven't encountered a serious security issue. As a result they aren't as vigilant in their security practices, either because they don't think they have to be or they just don't know they're vulnerable.
- It's also possible that many Mac users have made OSX their operating system of choice based on positive experiences with the walled garden that is iOS—the mobile version of the operating system found on the iPhone and iPod Touch—and think that a Mac is just as secure.
- Apple's time-to-patch track record is also a factor. There was roughly a six week gap between Oracle's announcement of the patch and Apple pushing it out on their platform.
- Another critical factor is the rapid growth in the adoption of OSX as an operating system of choice as a home PC. The Macintosh now makes up over 10% of the US market share[6], according to the analyst firm, Gartner (Worldwide numbers are harder to determine, but may even be greater). Perhaps the Mac has reached a critical mass that has made it a viable target.
- There is also the factor of what attackers would consider a "quality" target. Given how Apple computers are generally more expensive than PCs, the owners may have more disposable income on average, perhaps adding to the interest of attackers.

Regardless of the reasons, it looks like Mac malware is here to stay. It is a good time for Mac users to sit up, take notice, and ensure they adhere to the standard security practices that have been used in the Windows world for years.

Delving into Android.Opfake

By Masaki Suenaga

Pre-dating many of the mobile platforms it currently targets and outlasting several of the mobile platforms where it originated from, Android.Opfake has a tendency for survival on the mobile threat landscape not unlike roaches in the aftermath of a nuclear holocaust. Combing business savvy through a strong black market affiliate network and quick reaction time to adapt itself to thwart efforts by security vendors, Opfake has not only managed to stay in business for several years, the Opfake family has come to define the evolution of mobile malware.

Like many traditional Trojan horses, on the surface Android.Opfake purports to be a legitimate application. In fact, we have observed several variants of the Trojan masquerading as various apps and content, including an installer for the Opera Web browser and a pornographic movie. Analysis of the code behind the malicious program, as ever, reveals a truer sense of its nature. Numerous suspicious functions exist in its functionality that would have no reasonable place in any legitimate application. For example, encryption of its own configuration files—doubtless an attempt to prevent its behavior from becoming too obvious. It also contains functionality to collect contact details from the device—behavior that immediately raises concerns about information-stealing.

These suspicious activities and more are discussed in greater detail in a recent white paper, entitled Android.Opfake In-Depth.

Opfake - Additional Analysis

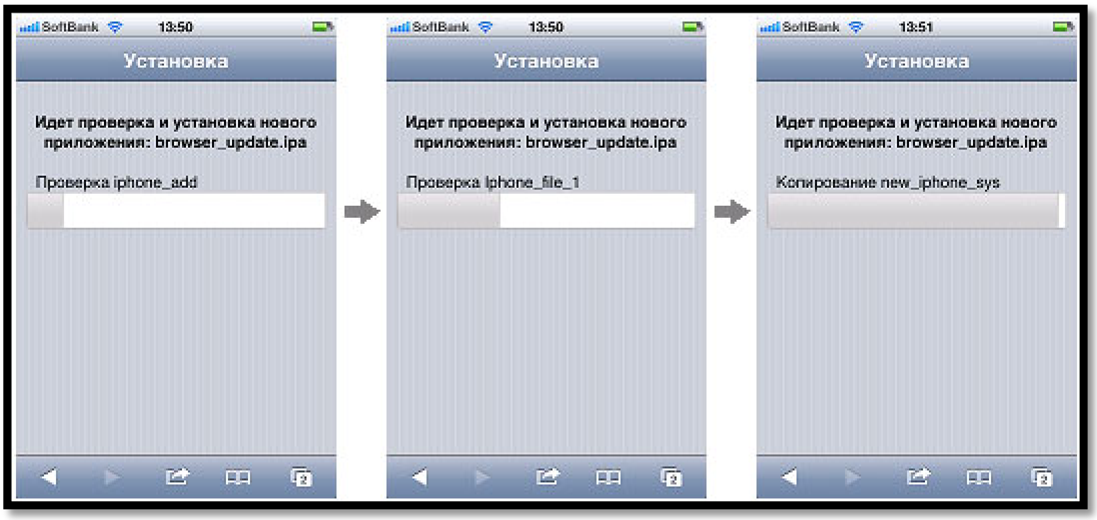
Opfake is more than just an Android threat. It had its "humble" beginning on the Symbian operating system. Before too long it appeared on the Windows Mobile platform. It seems that where there's a mobile platform, the Opfake gang isn't above attempting to exploit it—they've even made an attempt at targeting the iPhone[7], albeit through an indirect method. Rather than using an app, the Opfake gang laid out an elaborate online scam to trick iPhone users.

Given how applications can only be installed on an iPhone through the official App Store (unless the phone is jailbroken), an attacker cannot easily trick an ordinary user into installing malicious software. What the Opfake gang attempted to do was trick the user into simply *thinking* they were installing software. After trying one of a variety of social engineering tricks (e.g. telling the user their browser is out-of-date), they present the user with what looks like an installation screen. However, the screen is fake, being nothing more than a webpage with a graphic that appears to install something. When the "process" completes, the user is asked to input their phone number, under the guise that

[6] *http://www.gartner.com/it/page.jsp?id=1981717*

[7] *http://www.symantec.com/connect/blogs/opfake-scam-targets-iphone-users*

this will protect the user from unauthorized copying of the application, or some other similar reason. If the user complies, they most likely end up being the victim of a premium SMS scam.



Идет проверка и установка нового приложения: browser_update.ipa

Проверка iphone_add

Идет проверка и установка нового приложения: browser_update.ipa

Проверка Iphone_file_1

Идет проверка и установка нового приложения: browser_update.ipa

Копирование new_iphone_sys

Figure 2 – Fake installation progress shown on mobile screen

This may not seem like much, given that no application was actually installed. It's just an increased phone bill at worst, right? This is true to some extent, but a charge here or there on a number of phone bills could turn into something quite lucrative.

To get a rough idea just how profitable Opfake could be, let's go back to the Android side of things. It's tough to get the full scope, without exact numbers on a threat. We can only really count cases where our detection technology flags a threat. This can indicate one of two things: either our software has blocked a threat from installing, or it has picked up a threat when our software is installed on a device that has previously been compromised.

So how much money could the samples we've seen have garnered for the attackers? Based on the default costs outlined in Suenaga's whitepaper and the number of detections we've seen, the potential income could have been around 2,086,560 Rubles, or more than $53,000 (USD) over the last 90 days. Again, this only takes into account the devices that have Symantec technologies installed. But it's also worth noting that this threat is largely localized to phones that can send premium SMS messages to Russian numbers. If this is just a fraction of the overall infection, this can add up to quite a bit of money for the attackers.

Premium-rate number threats may not seem all that sophisticated, but they seem to be lucrative, if the numbers of threats that utilize this method are any indication. It's also recalls a time of Dialer threats of the late 90s, where attackers would compromise a computer's modem and make it call a premium-rate number. In time attackers moved on to other, more sophisticated threats, mainly because modems went the way of the dinosaurs. But since mobile devices generally include phones, threats like Opfake will likely continue to include such features, so long as it remains profitable to them.

Playing Cops & Robbers with Banks & Browsers

By Nino Fred P. Gutierrez

The following is an excerpt from a blog that provides an overview of Gutierrez's whitepaper on Trojan.Neloweg. The full paper is available on the Symantec Security Response website[8].

We are tracking a banking Trojan called Trojan.Neloweg. Looking at attempted infections blocked in figure 3 below, a small number of users were being targeted in the UK and the Netherlands.

[8] *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Trojan_Neloweg_Bank_Robbing_Bot_in_the_Browser.pdf*

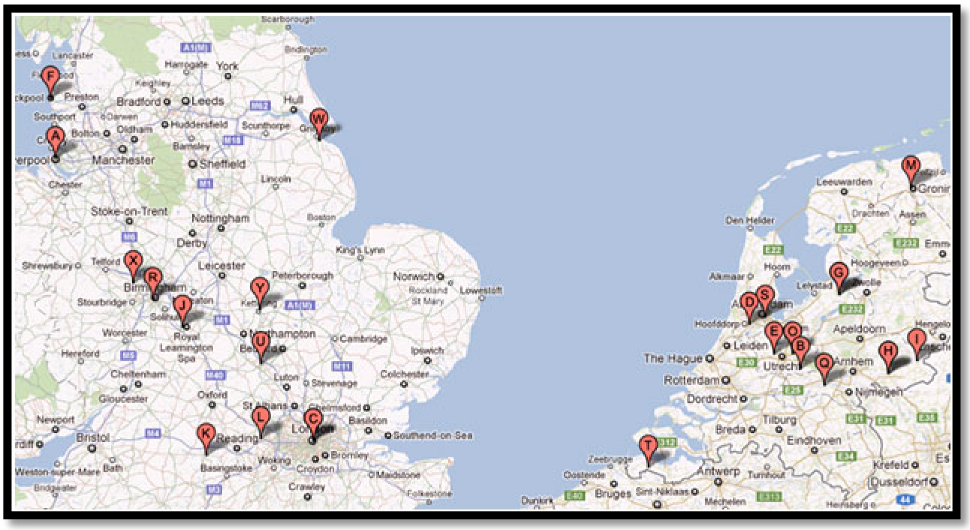


Figure 3 – Location of attempted infections

Digging into the threat, we saw that the login credentials of these users (including banking credentials) may have been stolen.

Trojan.Neloweg operates similar to another banking Trojan known as Zeus[9]. Like Zeus, Trojan.Neloweg can detect which site it is on and add custom JavaScript. But while Zeus uses an included configuration file, Trojan.Neloweg stores this on a malicious webserver.

Once a particular banking page has been matched, Trojan.Neloweg will cover part of the page in white, using a hidden DIV tag, and execute custom JavaScript located on the malicious server. We are currently monitoring the threat to see what changes it is making to the banking pages that a compromised users visits.

In terms of popularity, Firefox and Internet Explorer combined make up over 50% of the usage statistics. It is no surprise that Trojan.Neloweg would target these two giants. Interestingly, it also specifically targets a handful of browsers that utilize the Trident (Internet Explorer), Gecko (Firefox), and WebKit (Chrome/Safari) browser engines. There are a few reasons why a range of browsers may be targeted. The most obvious one is to ensure that the bot infects as many targets as possible. The second reason is that some people use less well-known browsers for online banking in order to achieve security through obscurity. Targeting those less well-known browsers may mean that the attacker is more likely to infect a browser used for online banking.

Not only does it attempt to steal banking credentials, but also any other login credentials. To achieve this, the malware authors give the browsers added bot functionality. The browser can function like a bot and accept commands. It can process the content of the current page that it is on, redirect the user, halt the loading of particular pages, steal passwords, run executables, and even kill itself.

The full entry can be found on the Security Response Blog[10].

Phishers Offer Fake Storage Upgrades

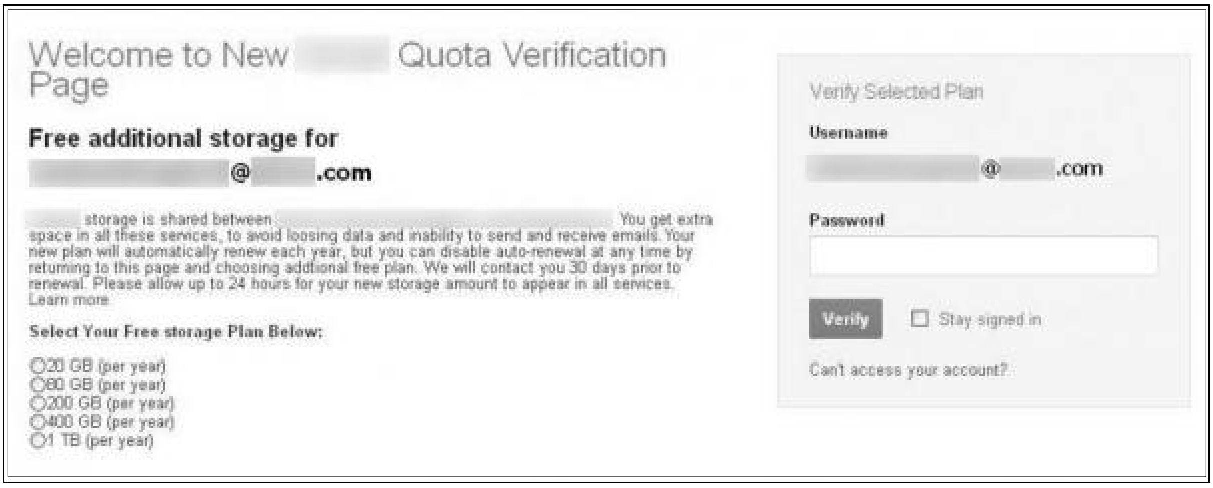
By Mathew Maniyara

Customers of popular email service providers have been a common target for phishers for identity theft purposes. Phishers are constantly devising new phishing bait strategies in the hope of stealing user email addresses and passwords. In April 2012, Symantec observed phishing pages that mimicked popular email services in an attempt to dupe users with attractive storage plans.

[9] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99*

[10] *http://www.symantec.com/connect/blogs/playing-cops-robbers-banks-browsers*

Customers were flooded with fake offers of free additional storage space for services such as email, online photo albums, and documents. In the first example shown in figure 4, the phishing site was titled "Welcome to New [BRAND NAME] Quota Verification Page". According to the bogus offer, the additional storage plan ranged from 20 GB to 1 TB per year, at no extra cost. The phishing page boasted that the free additional storage plan will help customers prevent loss of data and the inability to send and receive emails due to exhausted storage space. It also stated that the plan will auto-renew each year and the customer can choose to cancel at any time by returning to the same page:



Welcome to New [redacted] Quota Verification Page

Free additional storage for [redacted]@[redacted].com

[redacted] storage is shared between [redacted] You get extra space in all these services, to avoid loosing data and inability to send and receive emails. Your new plan will automatically renew each year, but you can disable auto-renewal at any time by returning to this page and choosing addtional free plan. We will contact you 30 days prior to renewal. Please allow up to 24 hours for your new storage amount to appear in all services. Learn more

Select Your Free storage Plan Below:

○20 GB (per year)
○80 GB (per year)
○200 GB (per year)
○400 GB (per year)
○1 TB (per year)

Verify Selected Plan

Username: [redacted]@[redacted].com

Password:

□ Stay signed in

Can't access your account?

Figure 4 – Example of fake verification page

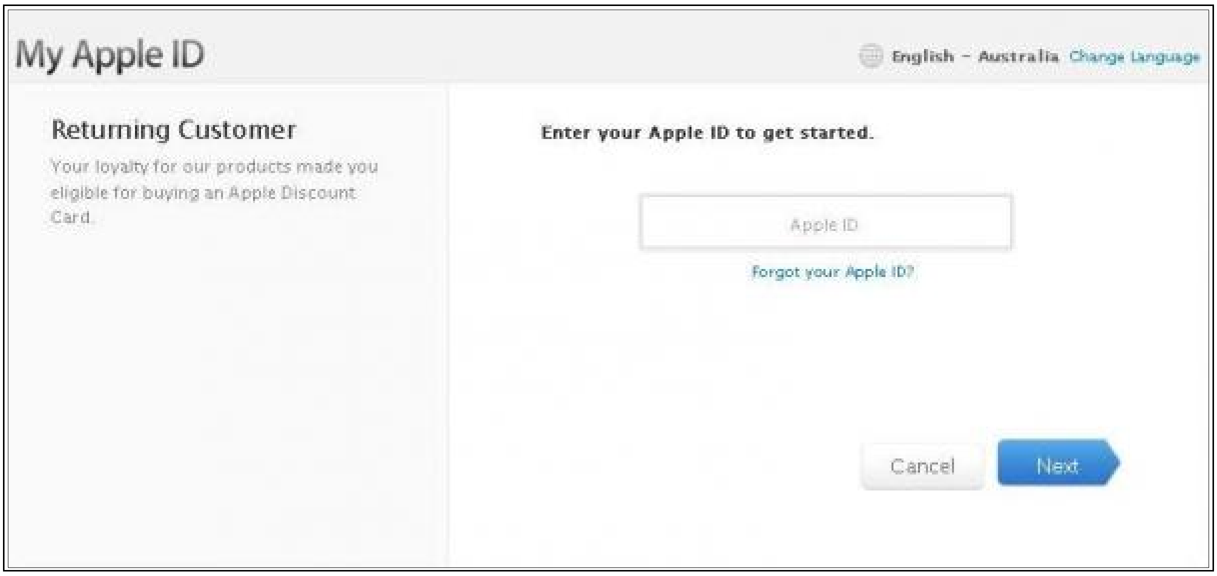
To avoid customer suspicion when the bogus offer doesn't materialize, phishers used a time-buying strategy. They indicated that customers would be contacted 30 days prior to renewal and also that the upgrade process will take effect in a 24-hour time span. After user credentials are entered, the phishing page redirected to a page which confirmed the upgrade was initiated and complete.

The full entry can be found on the Security Response Blog[11].

Phishing for Fake Discount Cards

By Mathew Maniyara

Phishers are constantly developing new strategies in an effort to trick end users. In April 2012, phishers created sites spoofing the Apple brand with fake offers for Apple discount cards. In this phishing attack, customers were targeted by region: namely, the UK and Australia.



My Apple ID

Returning Customer

Your loyalty for our products made you eligible for buying an Apple Discount Card.

Enter your Apple ID to get started.

Apple ID

[11] *http://www.symantec.com/connect/blogs/phishers-offer-fake-storage-upgrades*

Figure 5 – Phishing site spoofing Apple brand name

The phishing sites mimicked the webpage of Apple and prompted customers for their Apple ID. The phishing page stated the customer's long-term loyalty toward the brand gave them eligibility for an Apple discount card as a reward. Upon entering an Apple ID and clicking the "Next" button, the customer was redirected to a page that asked for more confidential information:

Here, the phisher explained that, with a discount card worth nine Australian dollars (rewarded to the customer), they can receive credit for $100 (AUD) at any Australian Apple store or on Apple's Australian website. To accept the offer, customers were asked to provide their personal and credit card information. Personal information included full name, address, date of birth, and driver's license number.

Credit card information included credit card number, expiration date, 3 digit security code, and secure-code password. After clicking the button titled "Submit and get your $100 (AUD) Apple Discount Card", the phishing page redirected to the legitimate Apple website.

The full entry can be found on the Security Response Blog[12].

[12] *http://www.symantec.com/connect/blogs/fake-discount-cards*

Global Trends & Content Analysis

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 64.6 million attack sensors and records thousands of events per second. This network monitors attack activity in more than 200 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, and other third-party data sources.

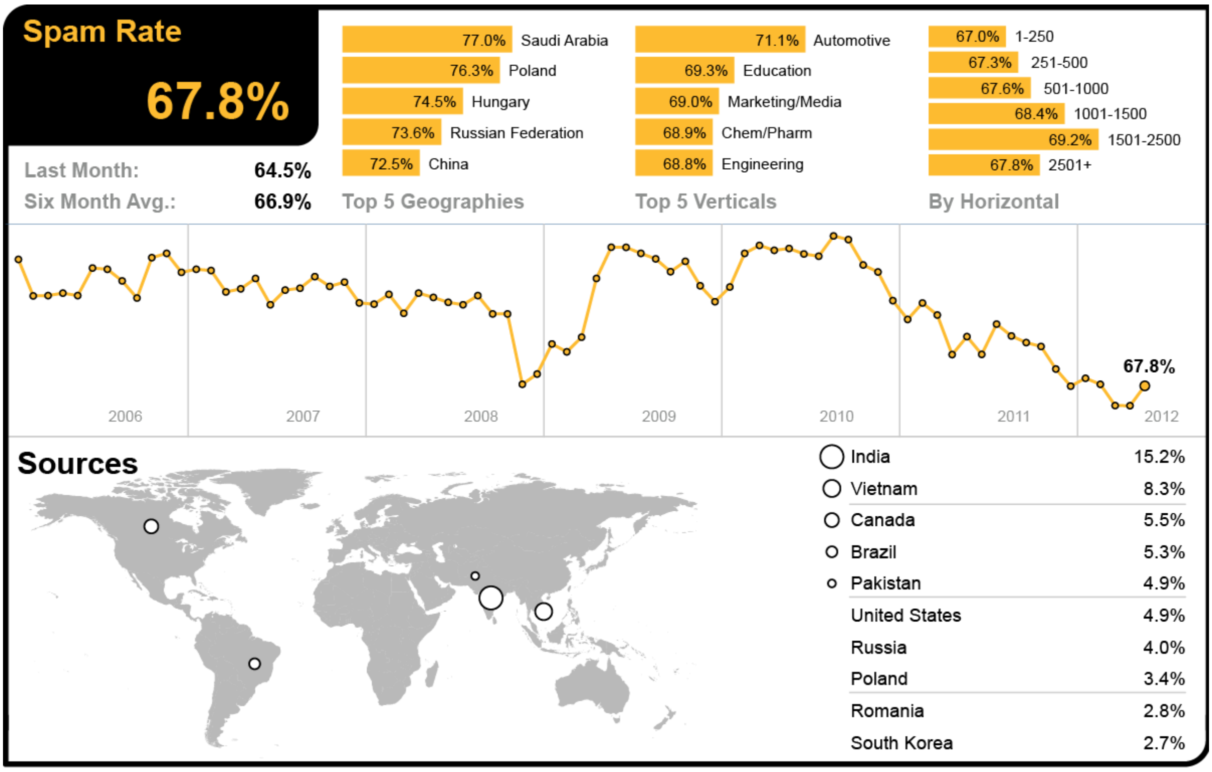
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

Spam, phishing and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is able to detect new and sophisticated targeted threats before reaching customers' networks. Over 8 billion email messages and more than 1.4 billion Web requests are processed each day across 15 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises and consumers the essential information to secure their systems effectively now and into the future.

Spam Analysis

In May, the global ratio of spam in email traffic rose by 3.3 percentage points since April, to 67.8 percent (1 in 1.48 emails). This represents the first increase in spam levels since the end of 2011.



Spam Rate

67.8%

Last Month:	64.5%
Six Month Avg.:	66.9%

Top 5 Geographies

77.0%	Saudi Arabia
76.3%	Poland
74.5%	Hungary
73.6%	Russian Federation
72.5%	China

Top 5 Verticals

71.1%	Automotive
69.3%	Education
69.0%	Marketing/Media
68.9%	Chem/Pharm
68.8%	Engineering

By Horizontal

67.0%	1-250
67.3%	251-500
67.6%	501-1000
68.4%	1001-1500
69.2%	1501-2500
67.8%	2501+

Sources

India	15.2%
Vietnam	8.3%
Canada	5.5%
Brazil	5.3%
Pakistan	4.9%
United States	4.9%
Russia	4.0%
Poland	3.4%
Romania	2.8%
South Korea	2.7%

May 2012

As the global spam rate rose, Saudi Arabia remained the most spammed geography in May; with a spam rate of 77.0 percent.

In the US, 67.8 percent of email was spam and 67.6 percent in Canada. The spam level in the UK was 68.0 percent. In The Netherlands, spam accounted for 69.6 percent of email traffic, 67.3 percent in Germany, 67.1 percent in Denmark and 67.1 percent in Australia. In Hong Kong, 67.2 percent of email was blocked as spam and 66.9 percent in Singapore, compared with 64.5 percent in Japan. Spam accounted for 67.7 percent of email traffic in South Africa and 72.0 percent in Brazil.

The Automotive sector was the most spammed industry sector in May, with a spam rate of 71.1 percent; the spam rate for the Education sector was 69.3 percent and 68.9 percent in the Chemical & Pharmaceutical sector. The spam rate in the IT Services sector was 67.8 percent, 67.1 percent for Retail, 67.6 percent for Public Sector, and 67.2 percent for Finance.

The spam rate for small to medium-sized businesses (1-250) was 67.0 percent, compared with 67.8 percent for large enterprises (2500+).

Global Spam Categories

The most common category of spam in May related to the Adult/Sex/Dating category, down slightly from April, but still making up the vast majority of spam for the month.

Category Name	May 2012	April 2012
Adult/Sex/Dating	70.16%	79.46%
Pharma	19.22%	13.97%
Jobs	3.47%	2.32%
Watches	3.45%	1.99%
Software	1.78%	1.07%
Casino	0.88%	0.37%
Degrees	0.57%	0.37%
Mobile	0.14%	0.20%
419/Scam/Lotto	0.13%	0.12%
Weight Loss	0.08%	0.01%
Newsletters	0.03%	0.03%

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .ru top-level domain increased by 7.5 percentage points in May, with the .br top-level domain joining the top-four for the first time, as highlighted in the table below.

TLD	May 2012	April 2012
.com	66.6%	66.2%
.ru	7.5%	7.1%
.net	5.8%	6.3%
.br	3.4%	N/A

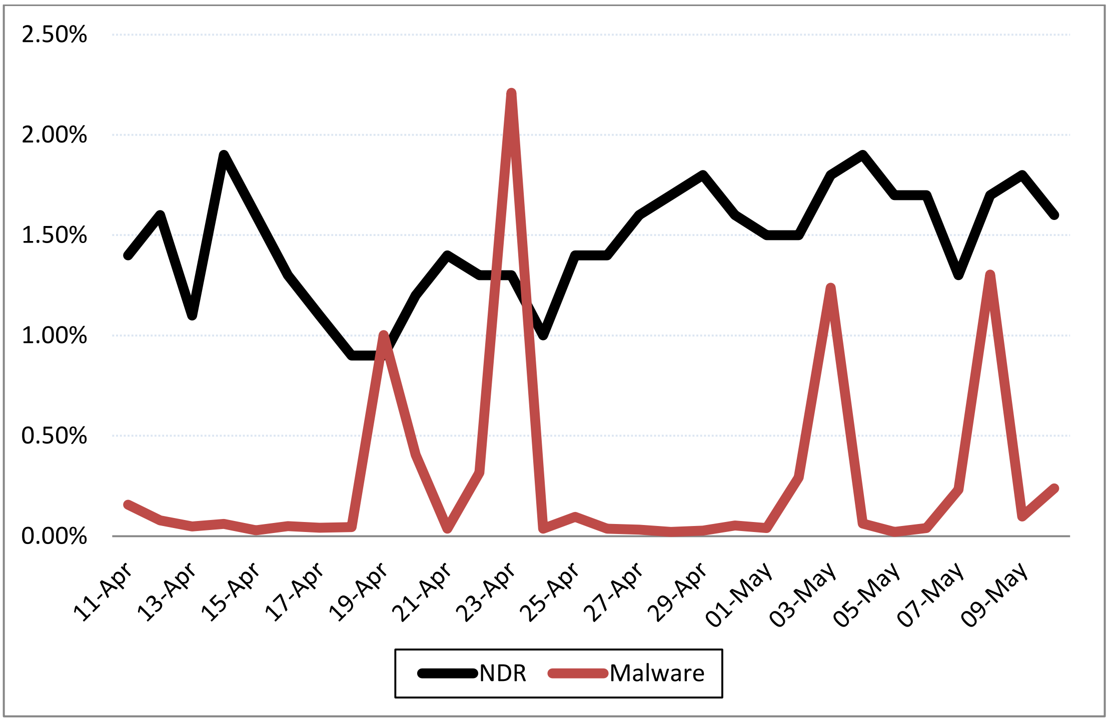
Average Spam Message Size

In May, the proportion of spam emails that were 5Kb in size or less increased by 6.6 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size decreased by 8.0 percentage points, as can be seen in the following table. This suggests spam campaigns are moving to very short message sizes; the larger spam file sizes can often relate to malware with malicious file attachments.

Message Size	May 2012	April 2012
0Kb – 5Kb	51.1%	44.5%
5Kb – 10Kb	29.1%	37.2%
>10Kb	19.8%	18.3%

Spam Attack Vectors

The proportion of spam that contained a malicious attachment or link increased toward the end of the previous month, with four major spikes of spam activity during the period, as shown in the chart below. Many of these larger attachments were related to generic polymorphic malware variants, such as Bredolab, as discussed in previous[13] Symantec Intelligence reports.



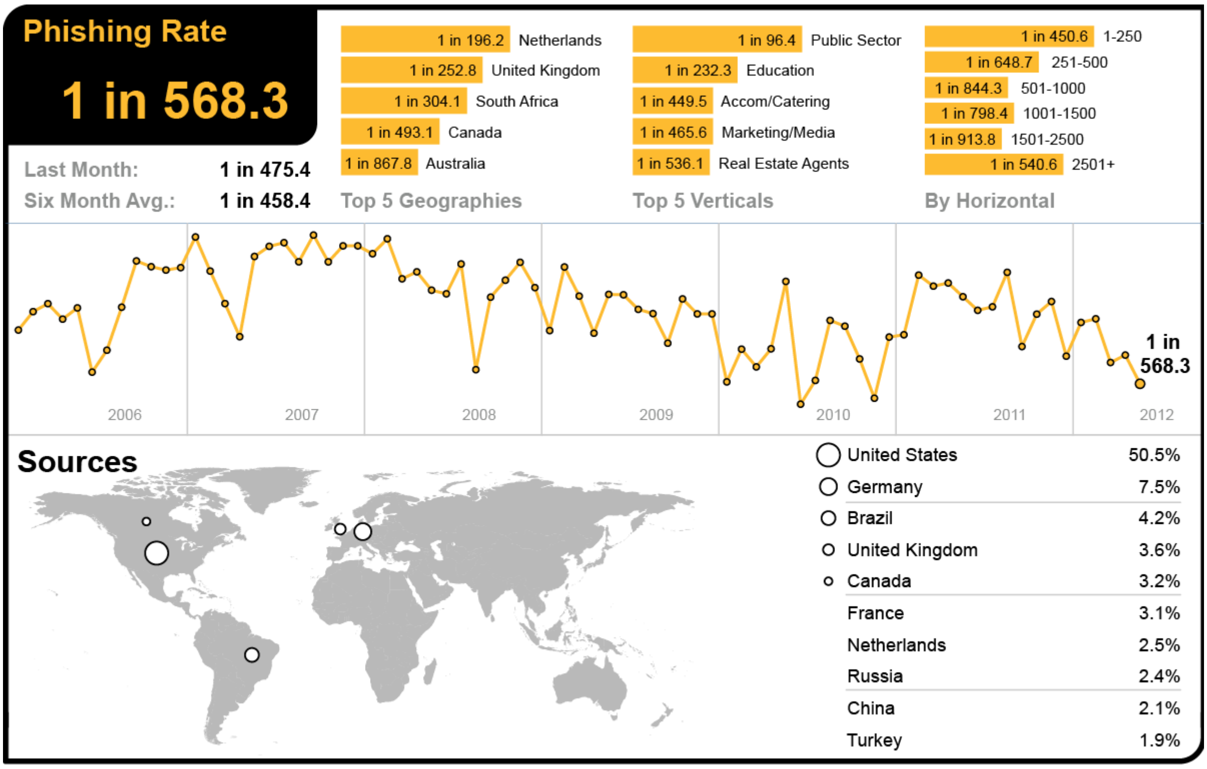
Between April and May, the number of spam emails resulting in NDRs (spam related non-delivery reports), has increased, and sometimes follow the profile of malware attacks. In these cases, the recipient email addresses are often invalid or are bounced by their service provider; however, with lower volumes of spam in circulation than in previous years, more spam is using more targeted approaches, to minimize the number of NDRs.

NDR spam, as shown in the chart above, is often as a result of widespread dictionary attacks during spam campaigns, where spammers make use of databases of first and last names and combine them to generate random email addresses. A lower-level of activity is indicative of spammers that are seeking to maintain their distribution lists in order to minimize bounce-backs; IP addresses are more likely to appear on anti-spam block-lists if they become associated with a high volume of invalid recipient emails.

[13] *http://www.symanteccloud.com/intelligence*

Phishing Analysis

In May, the global phishing rate decreased by 0.03 percentage points, taking the global average rate to one in 568.3 emails (0.18 percent) that comprised some form of phishing attack.



May 2012

The Netherlands remained the country most targeted for phishing attacks in May, with one in 196.2 emails identified as phishing.

Phishing levels for the US reached one in 1,702 and one in 493.1 for Canada. In Germany phishing levels were one in 884.3, one in 930.9 in Denmark. In Australia, phishing activity accounted for one in 867.8 emails and one in 2,310 in Hong Kong; for Japan it was one in 5,525 and one in 2,072 for Singapore. In Brazil one in 1,502 emails was blocked as phishing.

The Public Sector remained the most targeted by phishing activity in May, with one in 96.4 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 1,326 and one in 1,170 for the IT Services sector, one in 990.1 for Retail, one in 232.3 for Education and one in 631.8 for Finance.

Phishing attacks targeting small to medium-sized businesses (1-250) accounted for one in 450.6 emails, compared with one in 540.6 for large enterprises (2500+).

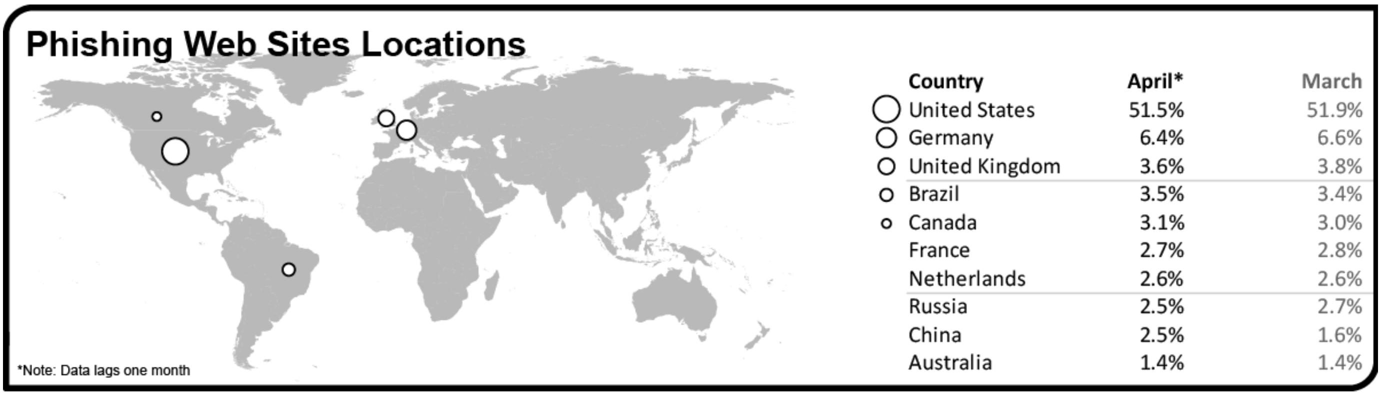
Analysis of Phishing Web sites

Overall, the number of phishing Web sites increased by 16.3 percent in May compared with the previous month. The number of phishing Web sites created by automated toolkits jumped by 62.5 percent, accounting for approximately 65.9 percent of phishing Web sites, including attacks against well-known social networking Web sites and social networking apps.

The number of unique phishing domains decreased by 24.9 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), increased threefold by 228.3 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 3.3 percent of all phishing Web sites, an increase of 5.9 percent compared with the previous month. The number of non-English phishing Web sites increased by 7.5 percent.

Of the non-English phishing Web Portuguese, French, Italian, and German were among the highest in May.

Geographic Location of Phishing Web Sites



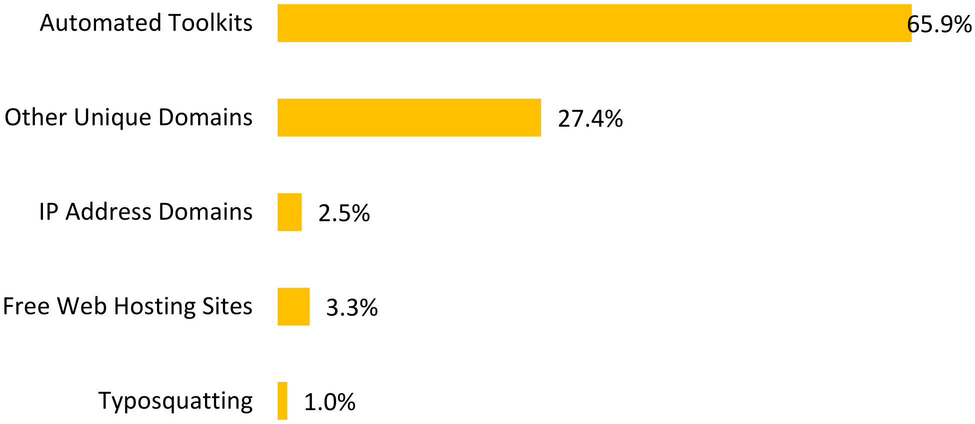
Phishing Web Sites Locations

Country	April*	March
○ United States	51.5%	51.9%
○ Germany	6.4%	6.6%
○ United Kingdom	3.6%	3.8%
○ Brazil	3.5%	3.4%
○ Canada	3.1%	3.0%
France	2.7%	2.8%
Netherlands	2.6%	2.6%
Russia	2.5%	2.7%
China	2.5%	1.6%
Australia	1.4%	1.4%

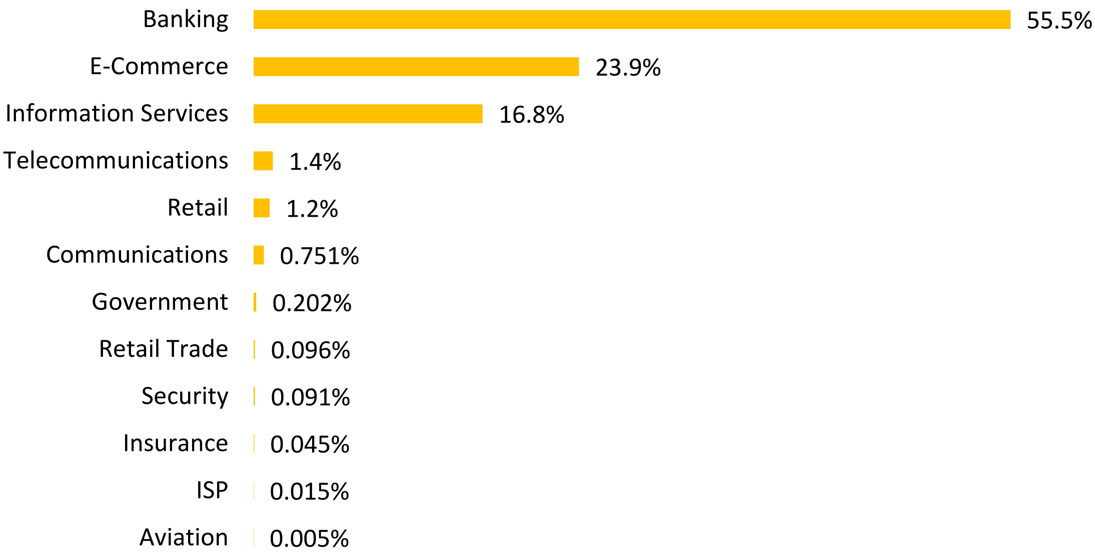
*Note: Data lags one month

May 2011

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry

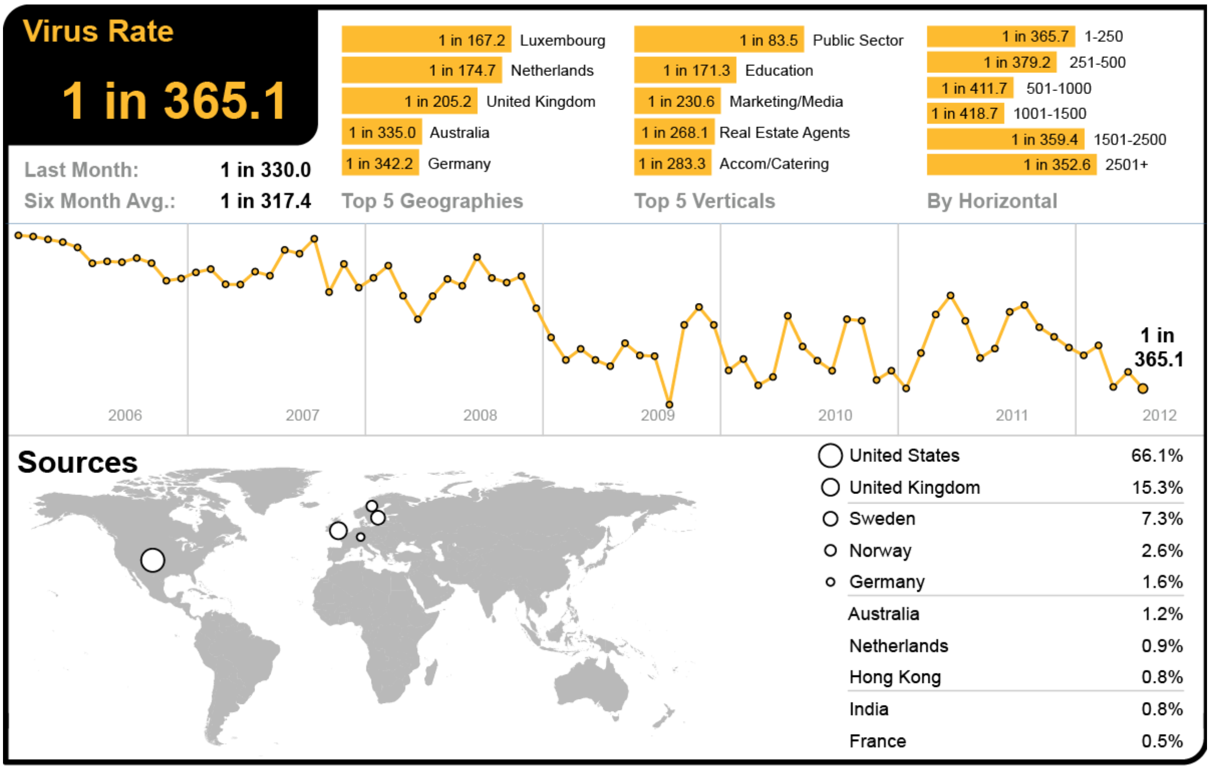


Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 365.1 emails (0.27 percent) in May, a decrease of 0.03 percentage points since April.

In May, 26.2 percent of email-borne malware contained links to malicious Web sites, 16.9 percentage points higher than the previous month.



May 2012

Luxembourg was the geography with the highest ratio of malicious email activity in May, with one in 167.2 emails identified as malicious.

In the UK, one in 205.2 emails was identified as malicious, compared with South Africa, where one in 731.2 emails were blocked as malicious. The virus rate for email-borne malware in the US was one in 640.3 and one in 343.2 in Canada. In Germany virus activity reached one in 342.2 and one in 654.2 in Denmark. In Australia, one in 335.0 emails was malicious. For Japan the rate was one in 2,036, compared with one in 709.7 in Singapore. In Brazil, one in 599.1 emails in contained malicious content.

With one in 83.5 emails being blocked as malicious, the Public Sector remained the most targeted industry in May. The virus rate for the Chemical & Pharmaceutical sector reached one in 427.7 and one in 521.5 for the IT Services sector; one in 507.6 for Retail, one in 171.3 for Education and one in 457.0 for Finance.

Malicious email-borne attacks destined for small to medium-sized businesses (1-250) accounted for one in 365.7 emails, compared with one in 352.6 for large enterprises (2500+).

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for May, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 28.7 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically, including aggressive strains of polymorphic malware such as Bredolab, accounted for 18.4 percent of all email-borne malware blocked in May.

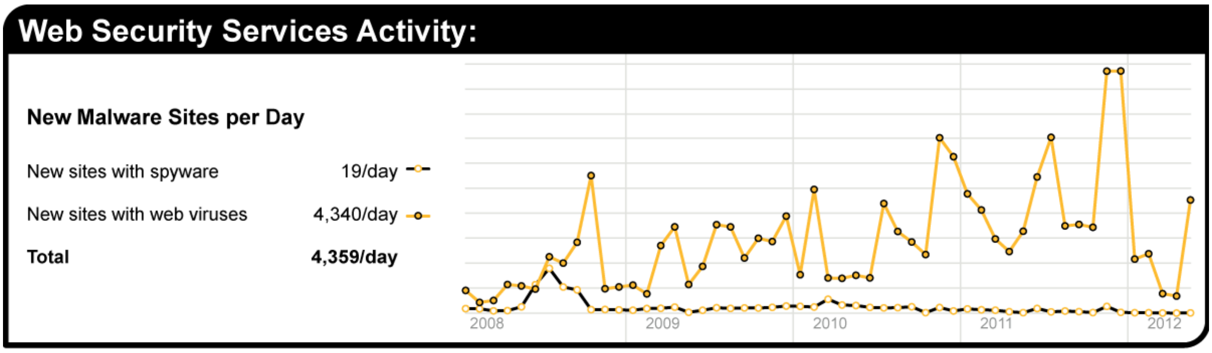
Malware Name	% Malware
Suspicious.JIT.a	11.63%
Exploit/SuspLink	8.90%
W32/Bredolab.gen!eml.j	7.32%
HTML/JS-Encrypted.gen	4.35%
W32/Packed.MalProtector-5927-205c	4.09%
W32/Bredolab.gen!eml.k	4.01%
Exploit/Link-generic-ee68	2.71%
Gen:Variant.Graftor.20106	2.18%
W32/Packed.Generic-6663-2579	2.03%
Exploit/Link-ce71	1.69%

The top-ten list of the most frequently blocked malware accounted for approximately 48.9% of all email-borne malware blocked in May.

Web-Based Malware Threats

In May, Symantec Intelligence identified an average of 4,359 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware—an increase of 48.7 percent since April. This reflects the rate at which websites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when Web-based malware is in circulation for a longer period of time to widen its potential spread and increase its longevity.

As detection for Web-based malware increases, the number of new Web sites blocked decreases and the proportion of new malware begins to rise, but initially on fewer Web sites.



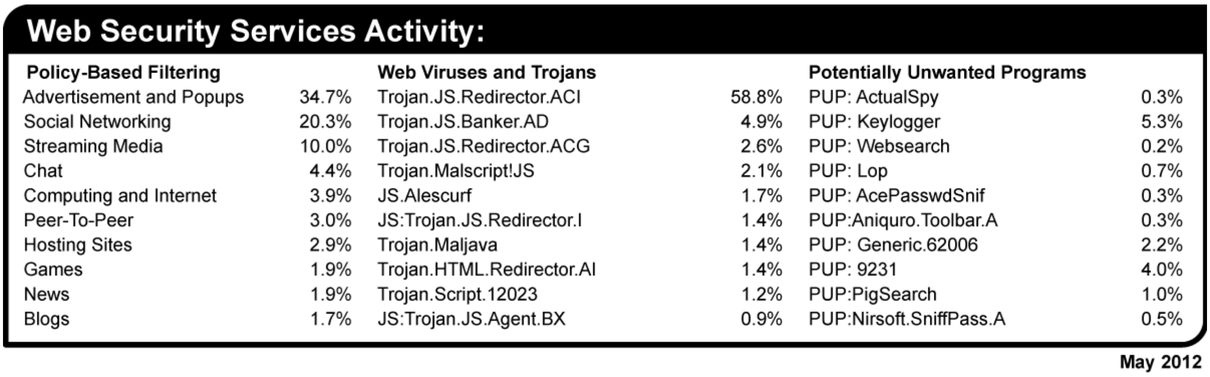
The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during May, compared with the equivalent number of Web-based malware Web sites blocked each day.

Web Policy Risks from Inappropriate Use

The most common trigger for policy-based filtering applied by Symantec Web Security.cloud for its business clients was the “Advertisements & Popups” category, which accounted for 34.7 percent of blocked Web activity in May. Web-based advertisements pose a potential risk though the use of “malvertisements,” or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless Web site.

The second-most frequently blocked traffic was categorized as Social Networking, accounting for 20.3 percent of URL-based filtering activity blocked, equivalent to approximately one in every 5 Web sites blocked. Many organizations allow access to social networking Web sites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.

Activity related to streaming media policies resulted in 10.0 percent of the URL-based filtering blocks in May. Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes. This rate is equivalent to one in every 10 Web sites blocked.



Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	34.7%	Trojan.JS.Redirector.ACI	58.8%	PUP: ActualSpy	0.3%
Social Networking	20.3%	Trojan.JS.Banker.AD	4.9%	PUP: Keylogger	5.3%
Streaming Media	10.0%	Trojan.JS.Redirector.ACG	2.6%	PUP: Websearch	0.2%
Chat	4.4%	Trojan.Malscript!JS	2.1%	PUP: Lop	0.7%
Computing and Internet	3.9%	JS.Alescurf	1.7%	PUP: AcePasswdSnif	0.3%
Peer-To-Peer	3.0%	JS:Trojan.JS.Redirector.I	1.4%	PUP:Aniquro.Toolbar.A	0.3%
Hosting Sites	2.9%	Trojan.Maljava	1.4%	PUP: Generic.62006	2.2%
Games	1.9%	Trojan.HTML.Redirector.AI	1.4%	PUP: 9231	4.0%
News	1.9%	Trojan.Script.12023	1.2%	PUP:PigSearch	1.0%
Blogs	1.7%	JS:Trojan.JS.Agent.BX	0.9%	PUP:Nirsoft.SniffPass.A	0.5%

May 2012

Endpoint Security Threats

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway filtering.

The table below shows the malware most frequently blocked that was targeting endpoint devices for the last month. This includes data from endpoint devices protected by Symantec technology around the world, including data from clients which may not be using other layers of protection, such as Symantec Web Security.cloud or Symantec Email AntiVirus.cloud.

Malware Name[14]	% Malware
W32.Sality.AE	5.76%
W32.Ramnit!html	4.82%
W32.Ramnit.B	4.33%
W32.Downadup.B	3.38%
W32.Ramnit.B!inf	3.29%
Trojan.Maljava	2.47%
W32.Virut.CF	1.69%
W32.Almanahe.B!inf	1.59%
W32.SillyFDC	1.45%
W32.SillyFDC.BDP!lnk	1.10%

[14] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*

While W32.Sality.AE[15] holds the top spot this month, Ramnit detections came in second, third, and fifth, making it the most prevalent family. Variants of Ramnit were recently implicated in the theft of identities from major social networking websites, and many of these stolen credentials were used to distribute malicious links via the profile pages of the affected users, heightening the risk for those users who shared the same password for several online accounts, potentially providing the attackers with a springboard into corporate networks.

Approximately 44.8 percent of the most frequently blocked malware last month was identified and blocked using generic detection. Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked.

By deploying techniques, such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware family, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.

[15] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99*

About Symantec Intelligence

Symantec Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. Symantec.cloud Intelligence publishes a range of information on global security threats based on data captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary technology uses predictive analysis to detect new and sophisticated targeted threats, protecting more than 11 million end users at more than 55,000 organizations ranging from small businesses to the Fortune 500.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

NO WARRANTY. The information contained in this report is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This report may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043.