# THREAT REPORT

## H1 2012

F-Secure

## F-Secure Labs

At the F-Secure Response Labs in Helsinki, Finland, and Kuala Lumpur, Malaysia, security experts work around the clock to ensure our customers are protected from the latest online threats.

Round-the-clock response work takes place in three shifts, one of which is handled in Helsinki, and two in Kuala Lumpur. At any given moment, F-Secure Response Labs staff is on top of the worldwide security situation, ensuring that sudden virus and malware outbreaks are dealt with promptly and effectively.

## Protection around the clock

Response Labs' work is assisted by a host of automatic systems that track worldwide threat occurences in real time, collecting and analyzing hundreds of thousands of data samples per day. Criminals who make use of virus and malware to profit from these attacks are constantly at work on new threats. This situation demands around the clock vigilance on our part to ensure that our customers are protected.

# FOREWORD

MIKKO HYPPONEN
CHIEF RESEARCH OFFICER

Over the last 25 years, we've seen a massive change in how we think about information. In the 1980s, information was mostly still analog. It was stored on paper, in binders, on shelves and in safes. Today, of course, almost all information has gone digital. It is created and stored on computers, and transmitted over computer networks.

From security viewpoint, secret information can now potentially be reached from anywhere in the world; you no longer have to be in the same physical location as the information. This means that espionage has gone digital. And while we've seen several cases of nation-state espionage done with backdoors and trojans, we've seen only one documented case of a nation-state doing cyber sabotage with malware. That case is Stuxnet.

During my years in this industry, I've seen multiple mysteries. But few of them have been as interesting as the case of Stuxnet[1]. F-Secure Labs estimates that it took more than 10 man years of work to develop Stuxnet. Related attacks like Duqu and Flame might have taken even more.

Stuxnet is a good example of the thinking behind these new kinds of offensive attacks: If you want to disrupt the secret nuclear program of a foreign nation, what can you do? Well, you have a couple of options. You can try international pressure and boycotts. But if that doesn't work, then what? You can try a conventional military attack and bomb their facilities. However, attribution back to you as an attacker is a problem. So is the fact that you can attack only the facilities you know about.

Using a digital attack like Stuxnet has several advantages, especially in providing deniability. If the United States officials had not leaked[2] the information that Stuxnet was created by the US government together with the Israeli government, we would have never known it for sure. Stuxnet was obviously a game changer.

> Just like modern hi-tech research revolutionized military operations over the last 50 years, we are going to see a new revolution, focusing on information operations and cyber warfare. This revolution is underway and it's happening right now.

But what does it mean in the long term? I think we are now seeing the very first step of a new arms race: the cyber arms race.

We haven't seen real online warfare yet, of course, because we haven't seen wars between technically advanced nations lately. But any future crisis is likely to have a cyber component as well.

> It's important to understand that cyber warfare does not necessarily have anything to do with the Internet.

Many of the more devastating cyber attacks cannot be launched remotely, as the most critical networks are not connected to public network. Think along the lines of a Special Forces unit going deep into enemy territory with embedded geeks in the team, to dig up fiber optic cables to be able to reach the systems that were supposed to be unreachable.

The main point of any arms race is to let your adversaries know about your capabilities so that they don't even think about starting a fight. We're not yet at this stage in the cyber arms race. Almost all of the developments in this area are secret and classified.

However, it will eventually become as public as any other defense technology. Maybe we'll eventually see public cyber war exercises where a country will demonstrate their attack capabilities. Maybe we'll eventually see cyber disarmament programs.

Defending against military-strength malware is a real challenge for the computer security industry. Furthermore, the security industry is not global. It is highly focused in just a handful of countries. The rest of the countries rely on foreign security labs to provide their everyday digital security for them. For example, there are only around 10 security labs in all of Europe; the vast majority of countries have no labs of their own.

> On the Internet, borders don't really matter. But in time of crisis, they do.

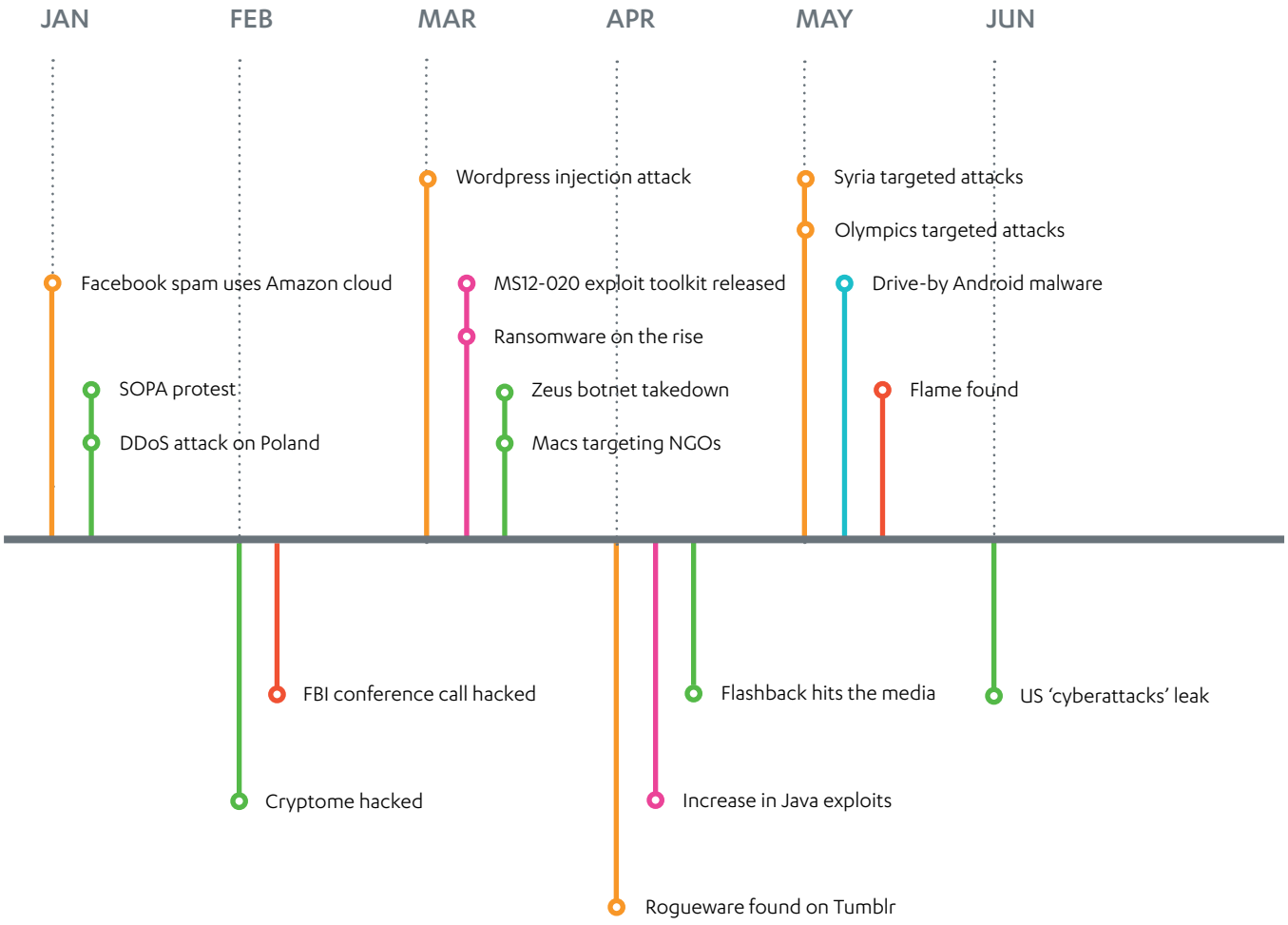
# CONTENTS

THIS THREAT REPORT HIGHLIGHTS TRENDS AND NEW DEVELOPMENTS SEEN IN THE MALWARE THREAT LANDSCAPE BY ANALYSTS IN F-SECURE LABS DURING THE FIRST HALF OF 2012. ALSO INCLUDED ARE CASE STUDIES COVERING SELECTED NOTEWORTHY, HIGHLY-PREVALENT THREATS FROM THIS PERIOD.


CONTRIBUTING AUTHORS

Broderick Aquilino
Karmina Aquino
Alia Hilyati
Timo Hirvonen
Mikko Hypponen
Mikko Hyykoski
Sarah Jamaludin
Mikko Suominen
Zimry Ong
Paolo Palumbo
Chin Yick Low
Sean Sullivan
Juha Ylipekkala

## 2012 INCIDENTS CALENDAR*




*Source: Labs Weblog (see page 37).

# EXECUTIVE SUMMARY

## CHANGES IN THE THREAT LANDSCAPE

One of the most pervasive trends we saw in the computer threat landscape in the first half of 2012 was the expanding usage of vulnerability exploitation for malware distribution. This phemonenon is directly tied to the recent improvement in *exploit kits* - toolkits that allow malware operators to automatically create exploit code. The most common way users come across exploit kits is on malicious or compromised legitimate websites, where they silently probe and exploit any vulnerabilities present on a site visitor's machine.

Like software developers in any other field, the authors of these exploit kits have been steadily improving their products and product support. The result of their efforts is a tool that greatly simplifies vulnerability exploitation, giving even technically unskilled users the ability to attack multiple vulnerabilities with little effort.

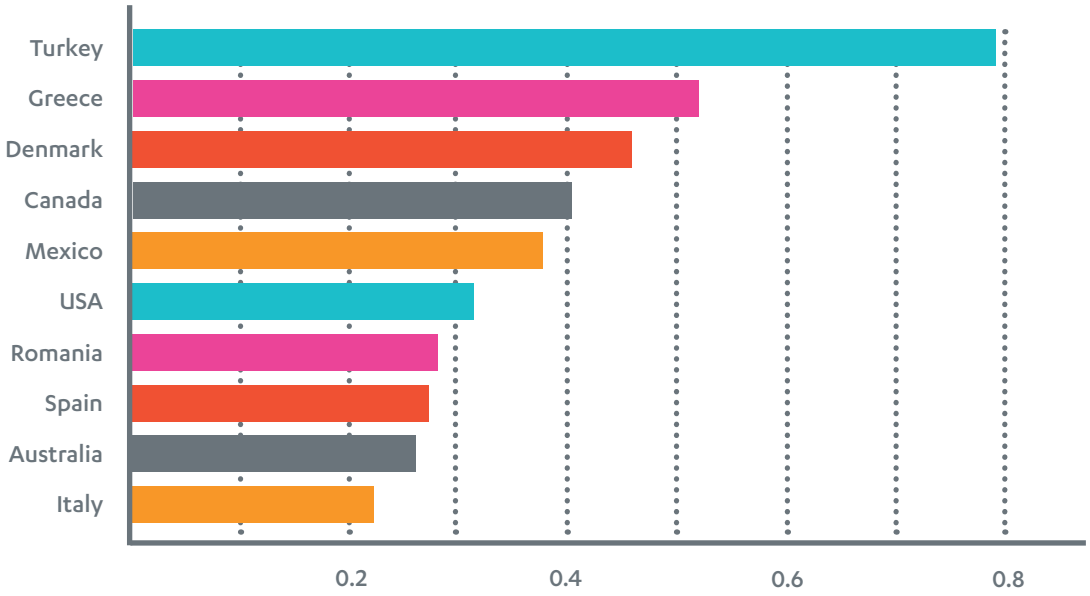
Malware authors and distributors have not been slow to take advantage of the benefits offered by exploit kits, as they allow even the most basic malware distribution operations to incorporate exploit attacks into their infection strategies. For example, rudimentary drive-by downloads or phishing runs that typically depend only on social engineering tricks to infect a machine (essentially, by duping the user into voluntarily downloading a malicious file), may now also attempt to exploit vulnerabilities on the user's machine at the same time, increasing the effectiveness of the attack and potentially gaining more victims.

Of these exploit kits, the most significant is undoubtedly Blackhole, which first emerged in 2010 and has rapidly become the leading exploit kit in use today. With over a hundred reported variants and a constantly updated exploit database, it's no wonder Blackhole exploit kits have been widely taken into use by malware distributors.

Vulnerability exploitation also played a part in the Flashback trojan 'outbreak', one of the most notable incidences to occur in 2012. This malware exploited a vulnerability in Java to gain control of Mac OS X machines. Early variants of the trojan had actually been discovered in late 2011, but the malware had been highly successful at keeping its infections hidden from the users - at least, until a buggy variant was released that triggered security alerts on the affected machines. The subsequent media coverage and response, from both users and security vendors, did result in positive remedial actions, as Apple took a number of steps to assist clean-up of infected systems and introduced a number of new features on subsequent versions of the operating system to prevent recurrence of a similar attack.

Vulnerability exploitation was also part of the Zeroaccess rootkit's infection strategy. Also known as Sirefef, this sophisticated, continuously changing[3] malware has become one of the most prevalent threats of its kind, accounting for 9% of all malware-related detection queries to F-Secure's cloud lookup systems in the second

ZEROACCESS DETECTION QUERIES PER MILLE IN Q2 2012*,
TOP 10 COUNTRIES




* Detections queries per mille: Measures the number of times queries were made for every 1000 clients to F-Secure's cloud lookup systems for the given time period.

quarter (Q2) of 2012. In some countries, Zeroaccess alone makes up a notable percentage of the detection queries from that country (see above). The rootkit is not only prolific but multi-faceted, as variants have differing capabilities. Machines infected with Zeroaccess are roped into a peer-to-peer botnet, which reportedly has been used for rogueware and spam distribution, click-fraud and various other undesirable or criminal activities. The consequences of a Zeroaccess infection mean that the malware could also be considered 'crimeware'.

Other crimeware that continue to make an impact in the first half of 2012 are Zeus and Spyeye, two families of banking trojans that specialize in stealing online banking credentials. In recent years, these trojans have metamorphosized into 'malware frameworks', with modular components that can be added on for customized functionality. While development of the Spyeye trojan framework itself has all but halted, malware derived from leaked source code for version 2 of the Zeus trojan still continues to proliferate, even with the takedown of the Zeus botnet in March[12]. Unsurprisingly, Europe continues to be the main theatre of operations for these malware, with over 72% of all Zeus and Spyeye-related infections identified by F-Secure's cloud lookup systems in Q2 being detected in various West European countries; India, the United States and Canada account for the rest.

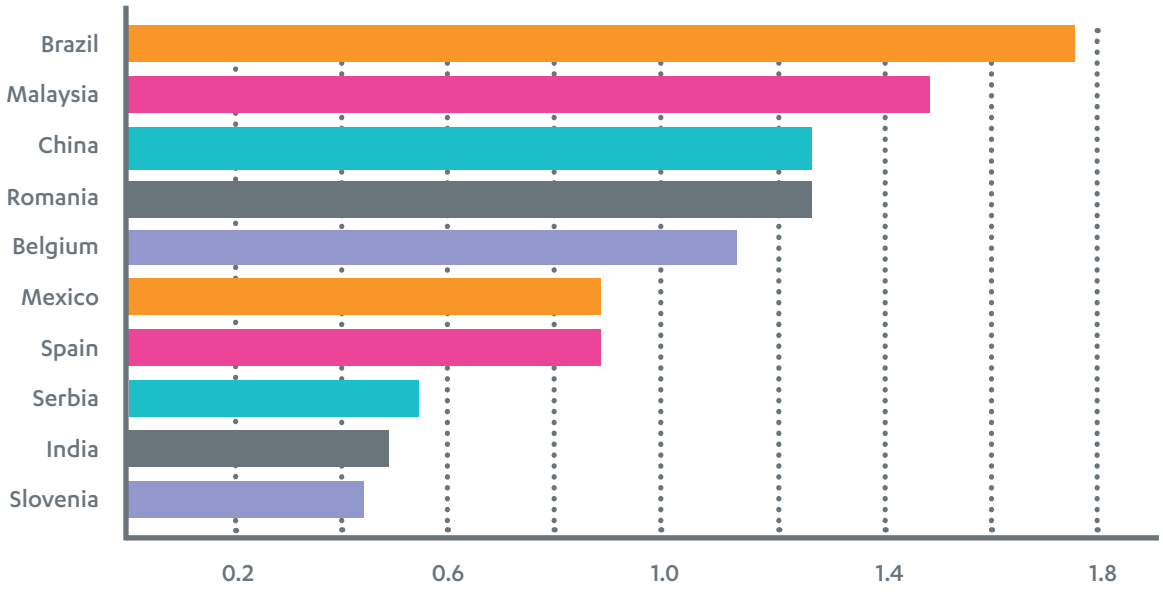
Another profit-making form of malware is ransomware, which saw a resurgence in the first half of 2012 when the Reveton family emerged, targeting users in Europe and the United States in particular. A notable trend in the samples we saw this year were a number of shared characteristics, most obviously in using a 'police-based' theme to disguise their demands. In almost all cases, the ransoms were to be paid using disposable cash cards or online payment channels - methods that are irreversible and untraceable.

Fake antivirus programs, known as rogueware, are another type of profit-making malware that continues to plague users. These products have seen little technical change in the past few years; what has been changing recently has been their distribution methods, as we now see rogueware being spread via Search Engine Optimization (SEO) poisoning and spam emails - routes that were once more associated with malware distribution than with rogueware.

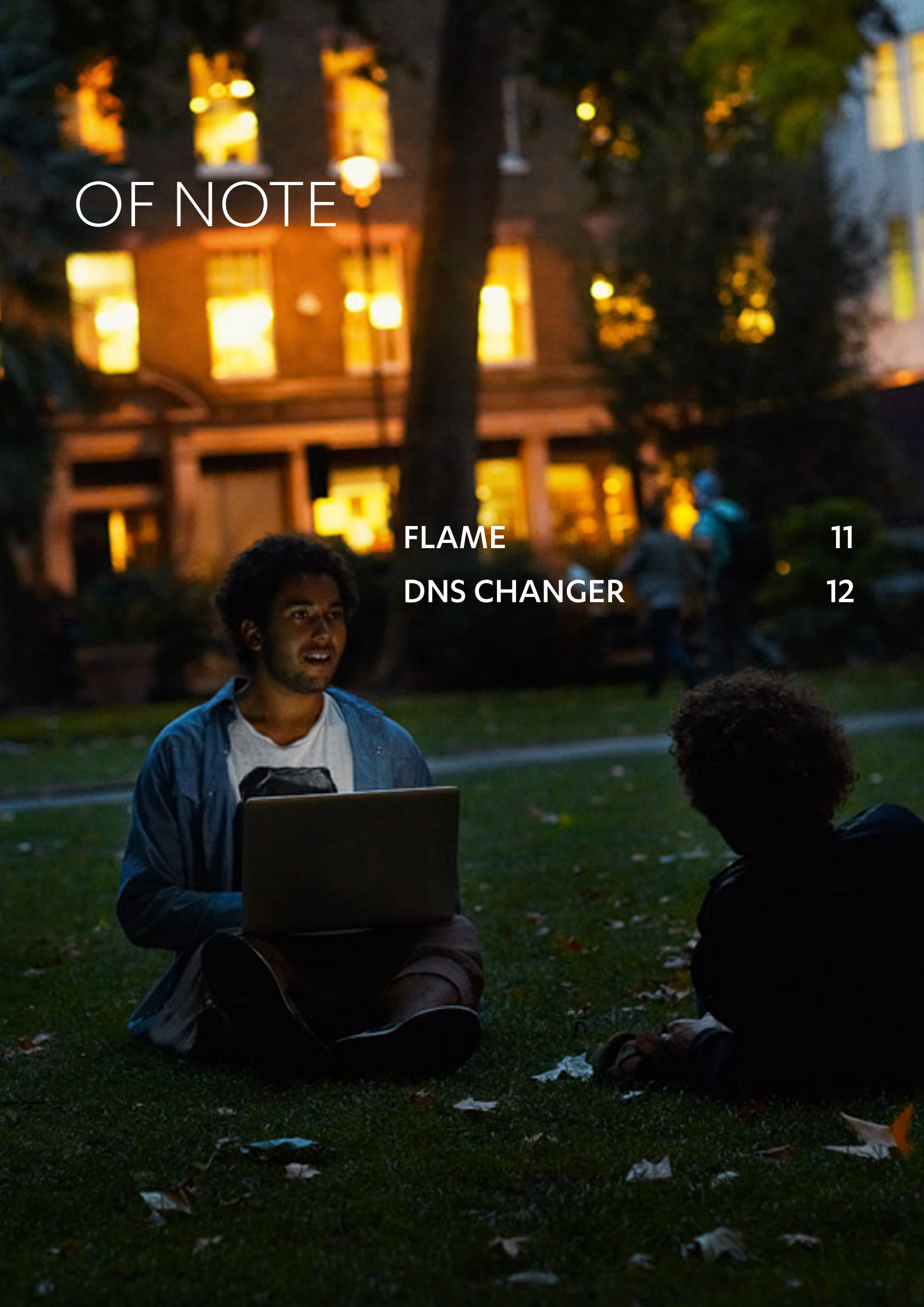
On the mobile front, Android continues to hold the dubious honor of being the platform with the most threats. In Q2 2012 alone, we saw a 65% increase in malicious file samples detected, and identified 19 new malware families. This year also saw some technical developments, with the appearance of the first drive-by Android malware and the use of Twitter as a bot control mechanism. Despite the precipitous decline in the total number of Symbian users over the last few years, threats on this platform still continue to be detected. Based on our Q2 cloud lookup statistics for mobile threats detected on Windows desktops, almost 80% of all Symbian-related detections came from three threats, *Trojan:SymbOS/SrvSender*, *Worm:SymbOS/Beselo.A* and *Worm:SymbOS/Commwarrior.C*, with the most infections recorded in Egypt, Malaysia and India, in that order. We also identified one new threat on this platform, Trojan:SymbOS/Monlater, during the this period.

And last but not least, despite three years having past since the Downadup (aka Conficker) outbreak, the worm remains one of the most persistent threats around. In Q2 alone, Downadup accounted for almost 13% of all malware-related detection queries to F-Secure's cloud lookup systems. In some countries, a significant percentage of the detection queries made from these locations were related to this single threat (see below).

DOWNADUP DETECTION QUERIES PER MILLE IN Q2 2012*, TOP 10 COUNTRIES




* See Detection queries per mille note on previous page.



# OF NOTE

# FLAME

The Flame malware was found in May 2012[21]. While this malware is definitely important, it is not widespread. We believe Flame has been used as an espionage attack by a Western intelligence agency, targeting a limited number of computers in the Middle East.

Here are 10 interesting facts about Flame:

1. Flame has a keylogger and a screengrabber.

2. Flame has built-in SSH, SSL and LUA libraries.

3. Flame searches for all Office documents, PDF files, Autodesk files and text files on the local drives and on the network drives. Since there would easily be too much information to steal, it uses IFilters to extract text excerpts from the documents. These are stored in a local SQLite database and sent to the malware operators. This way, they can instruct the malware to hone in on the really interesting material.

4. Flame can turn on the microphone of the infected computer to record discussions spoken near the machine. These discussions are saved as audio files and sent back to the malware operators.

5. Flame searches the infected computer and the network for image files taken with digital cameras. It extracts the GPS location from these images and sends it back to the malware operators.

6. Flame checks if there are any mobile phones paired with the infected computer via Bluetooth. If so, it connects to the phone (iPhone, Android, Nokia etc), collects the Address Book from the phone and sends it to the malware operators.

7. The stolen info is sent out by infecting USB sticks that are used in an infected machine and copying an encrypted SQLite database to the sticks, to be sent when they are used outside of the closed environment. This way data can be exfiltrated even from a high-security environment with no network connectivity.

8. Flame creates a local proxy which it uses to intercept traffic to Microsoft Update and drop a fake update onto the machine. This is used to spread Flame to other machines in a local area network. The fake update was signed with a certificate linking up to Microsoft root, as the attackers found a way to repurpose Microsoft Terminal Server license certificates. Even this wasn't enough to spoof newer Windows versions, so they did some cutting-edge cryptographic research and came up with a completely new way to create hash collisions, enabling them to spoof the certificate. They still needed a supercomputer though. And they've been doing this silently since 2010.

9. When Flame was finally busted, the attackers got busy destroying all evidence and actively removing the infections from the affected machines.

10. Latest research proves that Flame is indeed linked to Stuxnet. And just one week after Flame was discovered, US Government admitted that they had developed Stuxnet together with the Israeli Armed Forces[2].

# DNS CHANGER

On July 2nd, one week before the F.B.I.'s substitute DNS servers were scheduled to be shut down, we asked "News from the Lab" readers (our F-Secure Labs' blog) the following question:


Somewhat surprisingly, 87% of the nearly 500 respondents voted a resounding "no".

And just why is that such a surprise? Well... these computers were victims after all. Clearly the F.B.I. did the right thing in November 2011 when they arranged to have substitute servers put into place. Not to have done so would have been an undue (and very sudden) shock to possibly millions of people — and all at once. That would have been costly and it would have undone the public good that was served by the arrests that were made. Public sentiment also seemed to support reauthorization on March 8th. But by July, it seems that among our blog's security minded readers, enough was enough. It was time to pull the plug and let the victims sink or swim. Was that the right thing to do? It seems to have been so.

Most of the press coverage the week prior to July 9th was quite reasonably measured. It simply noted that there were up to 300,000 unique IP addresses still affected and that on July 9th they were at risk of being cut off from "the Internet" (due to lack of DNS).

### OPERATION 'GHOST CLICK' [22]

On Nov 8 2011, the United States Federal Bureau of Investigations (FBI) disabled a large network of rogue Domain Name System (DNS) servers and arrested the individuals operating it. This network was used to manipulate computers infected with a DNSChanger trojan, which are forced to connect to the rogue network rather than to legitimate Internet Service Providers (ISPs). Users surfing the Web on infected computers would be redirected from legitimate sites to fraudulent or malicious ones.

During the operation, the FBI did not entirely shut down the rogue DNS network, as doing so would have adversely affected many users. Instead, the FBI established a temporary, clean network of DNS servers as part of its efforts to assist affected users and ISPs. This grace period has since expired and the FBI-supported DNS network was finally shut down on 9 July 2012.

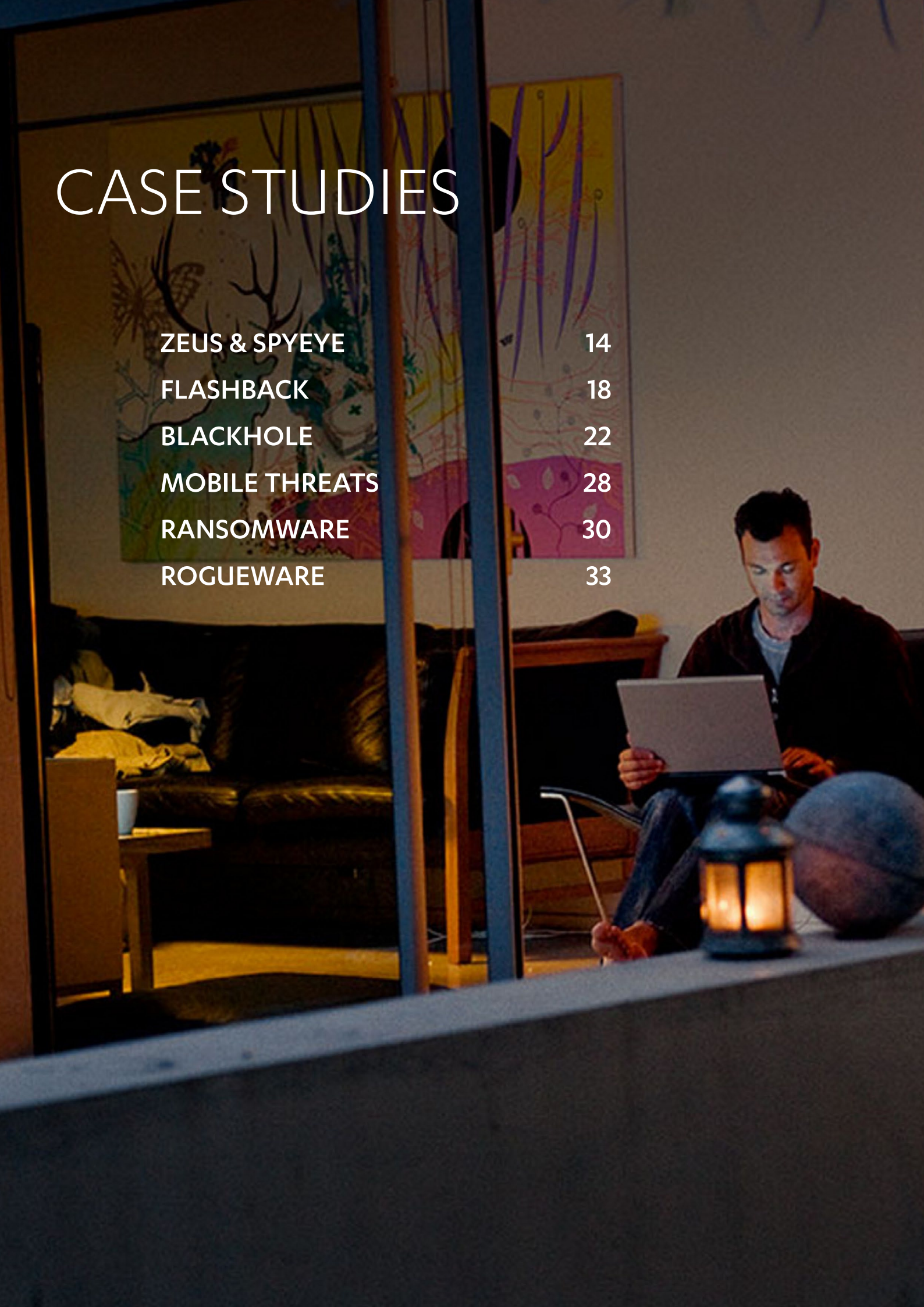
Even many of the headlines were matter of fact. However, there is something very compelling about an antivirus story that has an associated calendar date and so the coverage rapidly went from measured to hype and it soon made its way to television. At which point it was the next big thing. Then on July 9th... nothing happened — which is of course a good thing. But having been hyped, many then asked why nothing had happened. Was it a case of Chicken Little? Had antivirus companies just made the whole thing up? Why wasn't there a disaster?

Because ISPs stepped into the F.B.I.'s place and set up their own "substitute" servers. And the press coverage likely helped make it enough of a PR issue that network administrators within the ISPs could justify the time and effort to their bosses. So by making it an issue... it transformed it into a non-issue. Success!


But perhaps the next time that law enforcement goes through this process it would be wiser to stagger the shutdown dates among different regions in order to limit the amount of hype that inevitably latches onto calendar dates. Non-tech examples are readily available as well. Consider the London 2012 Olympics. In the run-up to the event, London's public officials broadcasted numerous warnings advising citizens of the extra traffic that was due. Then during the actual Olympics... nothing happened and reports began calling the center of London a "ghost town". Of course it wasn't really, statistics showed a considerable amount of extra traffic on public transportation, but it was spread out during the entire day rather than rush hours and it wasn't focused on the center of London.

Broadcasting warnings of known future events turns out to be a real challenge in today's world but we shouldn't let that stop us. Overall, it's beneficial in the end. On a final note, Nicole Kobie of PC Pro deemed the DNS Changer process a success. Here's an amusing quote of hers regarding some of the press coverage:

*"I haven't seen a single report of a PC dramatically refusing to access the internet, leaving confused users struggling to get back online — I've seen more journalists posting their email addresses on Twitter, begging for stories from people cut-off from the web, hilariously looking in the absolutely wrong place for someone stuck offline."*



# CASE STUDIES

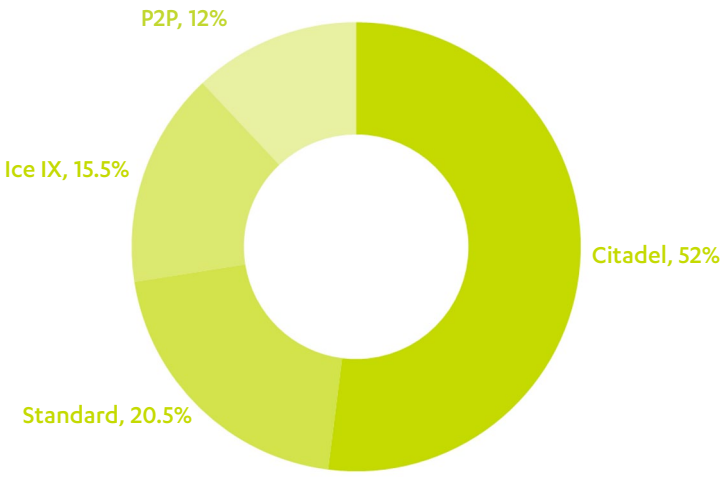
# ZEUS & SPYEYE

Two of the most notable information-theft trojans of recent years have been Zeus and Spyeye - advanced crimeware which, among other functionalities, are capable of injecting content into specific web pages as the victim accesses targeted websites in their web browser. This makes them well suited for use as banking trojans, which is their typical use case.

Crimeware such as Zeus and Spyeye are the products of development tools known as *malware creation kits*, which are developed and maintained like any other software project. The kit author(s) then sell the products to the actual attackers for use.

In the last year, we saw the two families move from being competitors to undergoing a limited merging; this then changed again last fall, with an influx of new Zeus variants. In contrast, development of the Spyeye trojan has largely halted, with most of the development effort now focused on producing modular plug-ins to supplement the basic Spyeye trojan functionality.

DISTRIBUTION OF ZEUS 2-BASED VARIANTS, APRIL-MAY 2012




* Based on 862 analyzed samples from between 1 April and 15 May 2012.

## ZEUS: DERIVATIVES MAKE THEIR MARK

The sizeable Zeus family has been around since at least 2007, when Version 1 of the malware was first found. Today, Zeus Version 1 represents a very small minority of Zeus-based threats; Version 2, which appeared in 2010, and its many sub-versions, are the most prevalent Zeus variants in the current threat landscape, due to one particular event. In May of 2011, the source code for version 2.0.8.9 was leaked onto the Internet and inevitably resulted in other authors creating new versions, or derivatives, based on the leaked code. So far, three major derivatives have appeared:

- Ice IX
- Peer-to-peer (P2P) version
- Citadel

There are also custom versions that have various new functionalities, but they appear in much more limited numbers and are not sufficiently unique to be considered more than just Zeus 2 variants.

Ice IX was the first Zeus 2 derivative to appear on the market in August 2011. Despite the author's grandiose claims of a "redesigned and enhanced" core, this variant included only one significant change, and that was an ineffectual attempt to allow only Ice IX trojans to fetch the key component of Zeus's operations from the trojan's command

and control (C&C) server - a configuration file which defines the targeted websites, and the URLs where stolen data is sent. Preventing anyone else from retrieving this file would hinder attempts to warn the intended targets, as well as preventing other variants from contacting updated versions of the malware or sending stolen data forward.

The second Zeus derivative uses a peer-to-peer (P2P) network to fetch configuration files and updates from other infected computers. The extensive changes incorporated into the derivative (see graphic at right) focus almost exclusively on the configuration file, and appear to be aimed at hindering retrieval and analysis of the configuration file. Many of the changes are to code sections that have been unaltered for years, such as the binary structure and compression method, which has not changed since 2008 (version 1.2).

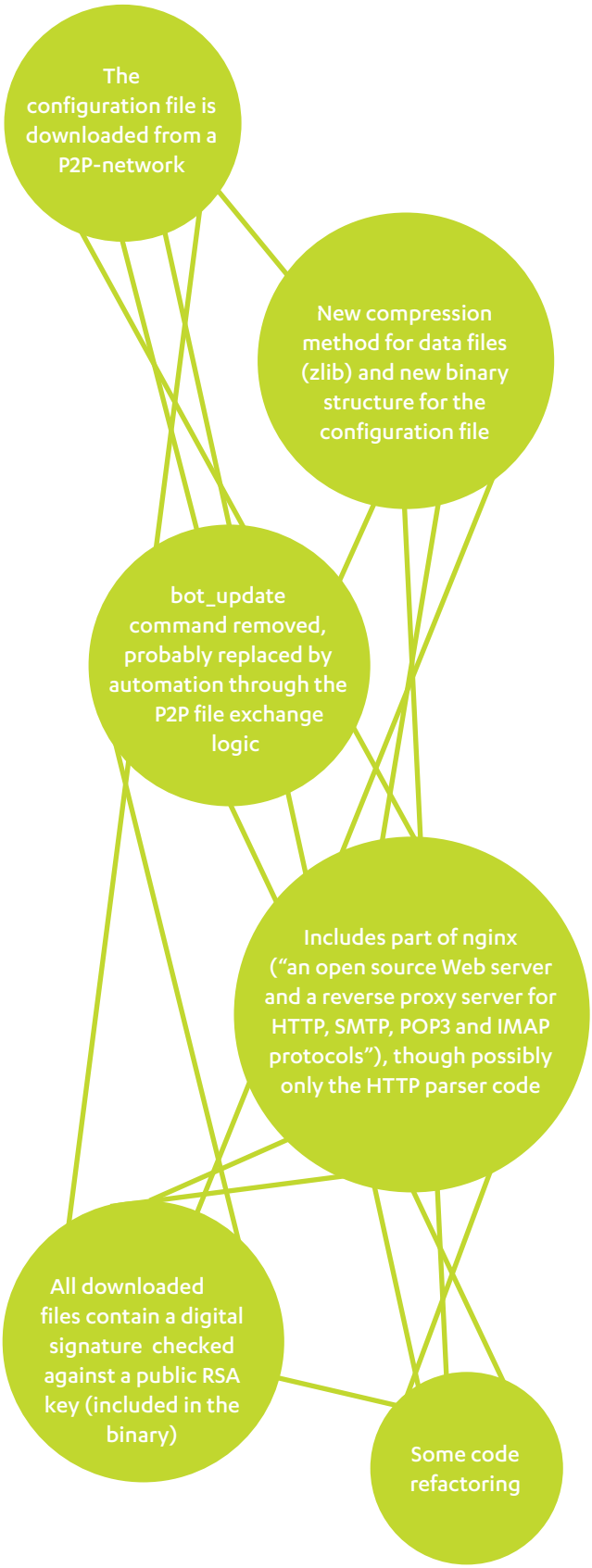
The date this version was released to the public can be estimated from the registration data for the domains created by its Domain Generation Algorithm (DGA). The trojan uses these domains as 'backup servers' if it cannot connect to other machines on the P2P network. As the first domain registration occurred on September 5th 2011, the trojan was likely let loose close to that date. These backup servers only host another list of infected machines from which the trojan could retrieve the actual configuration file. This backup system means that the configuration file is never stored on an external web server, but is handled entirely within the botnet itself.

All analyzed P2P samples have contained the same RSA public key used to check the digital signatures of incoming files. Other botnet-specific encryption keys have also been the same. We conclude that the P2P version must therefore be a private one and the kit used to create the trojans has not been resold further. This also means that all of these trojans link to the same botnet, which is controlled by a single entity.

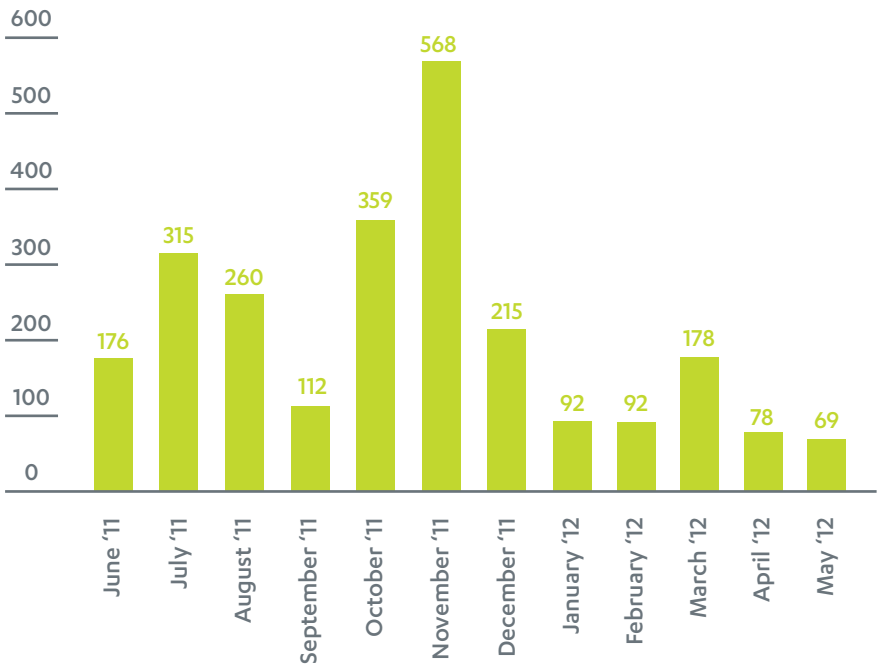
Based on the extensive changes and relatively short time it took for this version to appear after the source code leak, it is probable that the P2P version was not created by an outsider working from the leaked code. It is a logical, carefully crafted evolution of the Zeus code and could perhaps even be called Zeus 3. While there is no way to identify its author, it is certainly plausible that it is the same person who was behind the original Zeus 2.

In January 2012, the third Zeus derivative, Citadel, appeared in underground markets. Since then, Citadel has undergone rapid development, as the malware's users (that is, attackers) report bugs and request the addition of new features, such as video capture, new backdoor commands, and a modular plug-in architecture that allows new functionalities to be added via downloadable modules, rather than by modifying the trojan itself (a feature already in use by SpyEye). Citadel's active

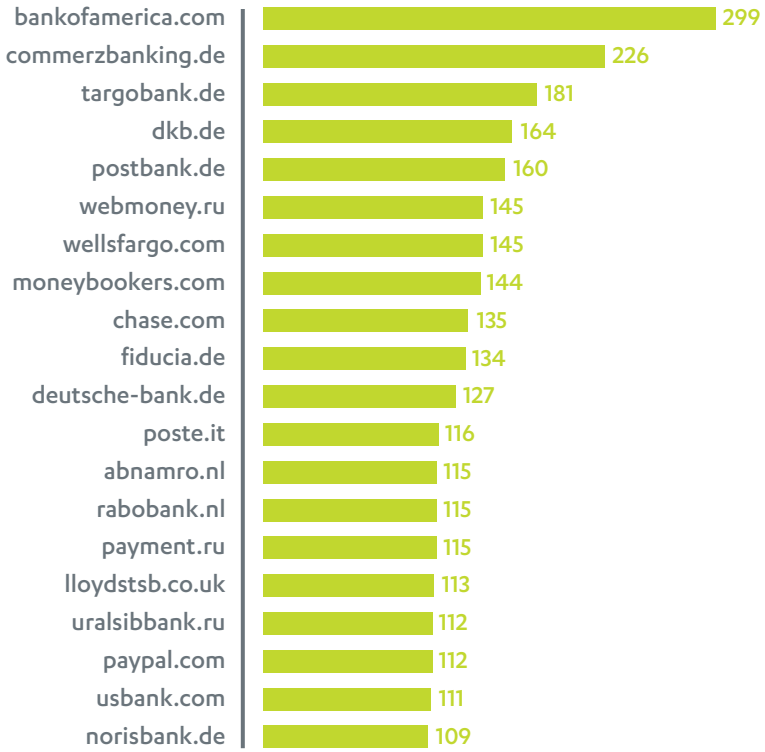
ZEUS PEER-TO-PEER VERSION CHANGES



SPYEYE SAMPLES RECEIVED PER MONTH, JUNE 2011-MAY 2012




TOP-20 BANKS TARGETED BY SPYEYE TROJAN




development means it will probably evolve into its own separate family over time as it grows more and more distant from its Zeus origins.

Of the three derivatives, Citadel has thus far been the market leader, followed by the standard Zeus version 2 variant and the other variants maintaining roughly equal shares. Interestingly, the Citadel samples detected were all version 1.1 or newer; the first Citadel version has already all but disappeared. This is probably a result of Citadel's active development.

One consideration is that that due to the way F-Secure gathers samples, the number of P2P variants gathered may not be directly comparable to the other variants. The statistics do make it clear however that it does form a significant percentage of Zeus infections, and is possibly the single largest Zeus botnet.

## SPYEYE: THE PAST YEAR IN NUMBERS

Unlike Zeus, Spyeye usage and development appears to have become less popular with the malware's target market in the last few months. This market shift is reflected in the statistics derived from samples we have gathered in the past year.

From June 2011 to May 2012, we received 2,514 Spyeye samples. The graph on the top left shows the number of samples received each month. The sample collection saw a noticeable peak in November 2011, which may be due to a Spyeye update that was made at the beginning of October. Since that time, the average number of monthly samples collected has decreased.

In total, the collection of samples contained 736 different domains, mainly related to banks and online finance-related companies. The chart at bottom left indicates how often a particular bank was referenced in those samples.

The graph at right shows SpyEye's so-called "campaign codes", which are used to identify particular attacks launched against targeted sites. Out of 137 campaign codes recorded, the top 10 codes accounted for 50 percent of all attacks. The relatively small number of campaign codes responsible for such a large percentage of attacks indicates that quite a small number of groups are using Spyeye.

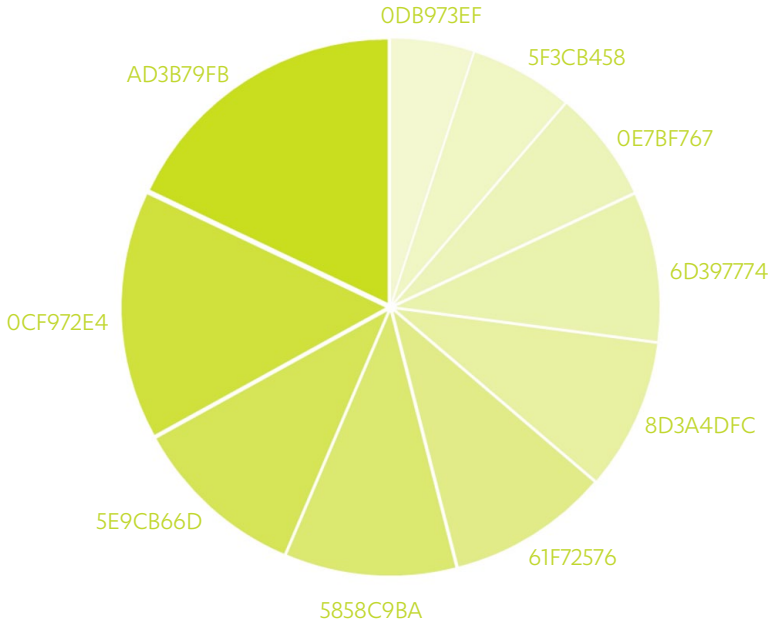
Unlike Zeus, we have not seen any significant code changes in the Spyeye trojan itself for some time. Even though development of the Spyeye trojan seems to be ending however, it doesn't mean that there isn't new plug-in development.

In the same way that the P2P version of Zeus was modified to use modular components, Spyeye uses plug-ins to allow a single malware to perform different actions on victim machines - for example, target a specific bank. As such, the standard Spyeye trojan becomes a malware 'framework' that authors can tailor by adding the desired plug-in.

The higher level of activity going into plug-in development is however somewhat misleading, for although we recorded 64 plug-ins, some of these are duplicates of existing plug-ins that were simply renamed. The list of Spyeye plug-ins at right includes more than 10 instances of this duplication. To illustrate, the plug-ins "c.dll", "customconnector.dll" and "f.dll" are all renamed copies of "ftpgrabber.dll".

Looking forward, we do not expect to see any major development of the Spyeye framework in the future; Spyeye toolkit users will however continue developing new plug-ins to expand the usability and effectiveness of the trojan.

### TOP-10 SPYEYE CAMPAIGN CODES




### SPYEYE PLUG-INS

| | | | |
|---|---|---|---|
| zuchek4_0.dll | win_sound.dll | webinjects.txt | webfakes.dll |
| w3check_3_6.dll | w2chek4_6.dll | w2chek4_4.dll | USBSpread.dll |
| update.dll | tst1.dll | tom_v_5.dll | terminate.dll |
| stb_3_5.dll | stb_3_4.dll | spySpread.dll | socks5.dll |
| socks.dll | skdv_0_7b.dll | skdv_0_7.dll | SecureConnect.dll |
| screenshots.txt | rt_3_5.dll | rt_3_1.dll | rt_2_4.dll |
| rst_3_5.dll | rst_2_0.dll | rst_1_1.dll | redetrf1_3_7.dll |
| rdp.dll | Plugin_USBSpread.dll | muie.dll | mngr1_1.dll |
| mch_3_5.dll | maincps.txt | keylog.dll | jazz_3_2.dll |
| jabbernotifier.dll | hookspy.dll | hntr_1_0.dll | ftpgrabber.dll |
| ftpbc.dll | flashcamcontrol.dll | ffcertgrabber.dll | f.dll |
| emailgrabber.dll | doberman_v_4_7.dll | dns.txt | dev_3_6all.dll |
| dev_3_5.dll | dev_3_1.dll | dev_3_0.dll | ddos.dll |
| customconnector.dll | customconector.dll | creditgrab.dll | connector2.dll |
| collectors.txt | ccgrabber.dll | cc grabber.dll | c.dll |
| bugreport.dll | brgr_1_2.dll | block.dll | billinghammer.dll |

# FLASHBACK

In the first half of 2012, we encountered the first massive malware outbreak on the Mac OS X platform. This malware, dubbed Flashback, reportedly infected more than 600,000 Macs around the world[23]. By a simple rough estimate, if we assume there are approximately 45 million Macs out there, Flashback would thus have infected more than 1% of the available machines, making it as widespread on Macs as the 2009 Conficker worm outbreak was on Windows.

The Flashback trojan affected a wide swath of the computer-using community, but given the popularity of Mac desktops and laptops among students, it's not surprising that the malware seems to have hit university campus populations the hardest. The extent and repercussions of the outbreak's impact on campus systems was remarked on by OxCERT, the Oxford University Computing Services' network security team[24].

Flashback was distributed by a classic online redirect mechanism - users visiting legitimate but compromised websites were forcibly redirected to a malicious site hosting the Flashback malware.

"...PROBABLY THE BIGGEST OUTBREAK SINCE BLASTER STRUCK THE WINDOWS WORLD ALL THE WAY BACK IN THE SUMMER OF 2003."

— Oxford University Computing Services' network security team (aka OxCERT)

The trojan exploited the then-unpatched CVE-2012-0507 vulnerability in Java. At the time the Flashback outbreak first became public news, this vulnerability had already been patched by Oracle, Java's developer, in February 2012, closing the loophole for Windows users. Unfortunately, Apple, who maintained the Java updates for OS X at the time, had not yet released an equivalent patch, inadvertently leaving thousands of OS X Java users vulnerable to an attack targeting the loophole.

Overall, the Flashback trojan itself is a complex piece of malware. It has features which are commonly found in Windows malware, like 'locking' itself to the infected host, dynamic API loading during runtime, encrypted communication with command and control (C&C) servers, and so on. The trojan also has features to avoid detection by the system or user, including avoiding installing itself on machines with known security software, and in early variants at least, attempting to disable updates for XProtect, OS X's security component. The level of sophistication in the malware indicates it was not created by amateurs but by professional cyber syndicates who have several years of experience in writing malware.

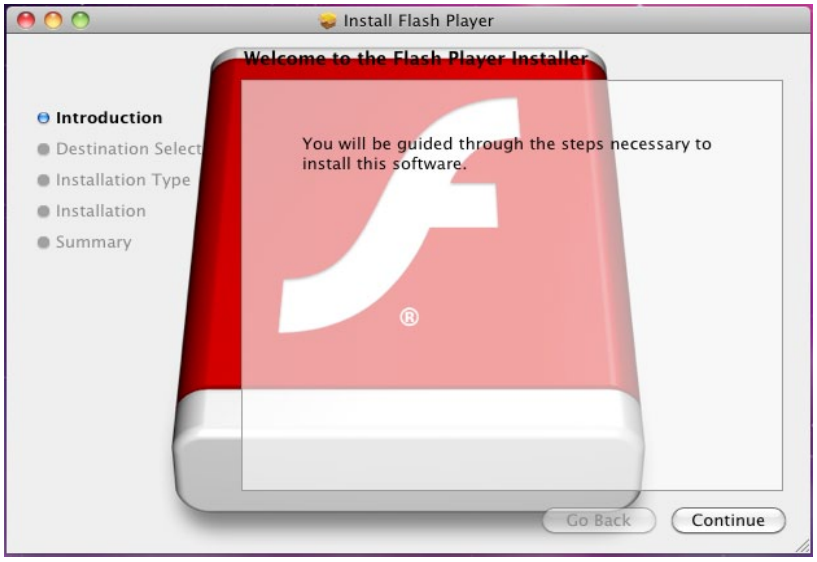
Early Flashback variants had been identified by security researchers as early as September 2011. At the time however, it was mostly only security-conscious and technically-aware Mac users who considered the trojan an issue. Given Mac's much

vaunted 'immunity' to malware, most users simply did not have an antivirus product installed to give them warning. This was compounded by the fact that XProtect is unable to detect the trojan - a fact noted by later Flashback variants, which no longer bothered to disable XProtect updates.

In the months following, the malware's author(s) introduced new variants of the Flashback malware, including one with a modification that unintentionally allowed it to infect machines with the Little Snitch firewall installed, triggering a warning message and rousing suspicions in alert users, who subsequently raised the alarm in Apple forums[25]. News of the trojan infections subsequently reached a more mainstream audience.

Response to the escalating number of reported infections was swift, as samples poured in for analysis and various antivirus vendors quickly produced removal tools for disinfecting affected machines[26]. On 3 April, Apple released a software update that closed the security vulnerability. In June, Apple finally implemented its long-standing plan of allowing Oracle to handle Java updates for the OS X platform, so that its users will in future receive Java updates simultaneously with other major platforms[27]. F-Secure still however continues to advise users to disable or remove Java from general use, due to the multiple exploits against it in recent years (see page 21).

There are a few positive things that resulted from the Flashback outbreak. The incident has raised user awareness that Macs are not immune to malware. After all, malware are just malicious programs, therefore any system that can run software has the potential to be affected. The incident has also lead Apple to introduce innovative solutions that made OS X a bit more secure. In OS X Lion 10.7.4 and Snow Leopard Security Update 2012-002, Apple disabled the global launch variables that are typically used only by developers for testing and are not usually found in a normal user's system[28]. This, in effect, disabled some types of Flashback infections. The move also narrowed down possible launch points for future malware, for if other malware authors intended to copy the approach used by Flashback, they can now only use an attack method that requires the user to manually enter their administrator password.




Early Flashback variant posing as a Flash Player installer

And finally, one brilliant feature was introduced after the Flashback outbreak. One of the best practices for computer security is to remove software that you do not use - and now, for OS X Lion 2012-003, the Java browser plugin and Java Web Start are automatically deactivated after 35 days of inactivity[29]!

## QUIET DEVELOPMENT AND SPREAD

Flashback had actually been quietly infecting Mac machines for months, before a buggy variant was released at the end of March 2012 and triggered alarms that drew major attention to it.

The trojan had been spotted as early as September 2011, but at the time it disguised itself as a Flash Player installer to dupe users into installing it (this is where the malware got its name). Later Flashback variants changed to simply exploiting Java, but at that time chose to target the CVE-2008-5353 and CVE-2011-3544 vulnerabilities, which were already patched by Apple.

However, there was no reason why the malware couldn't be updated to target an unpatched vulnerability - which is exactly what occurred.

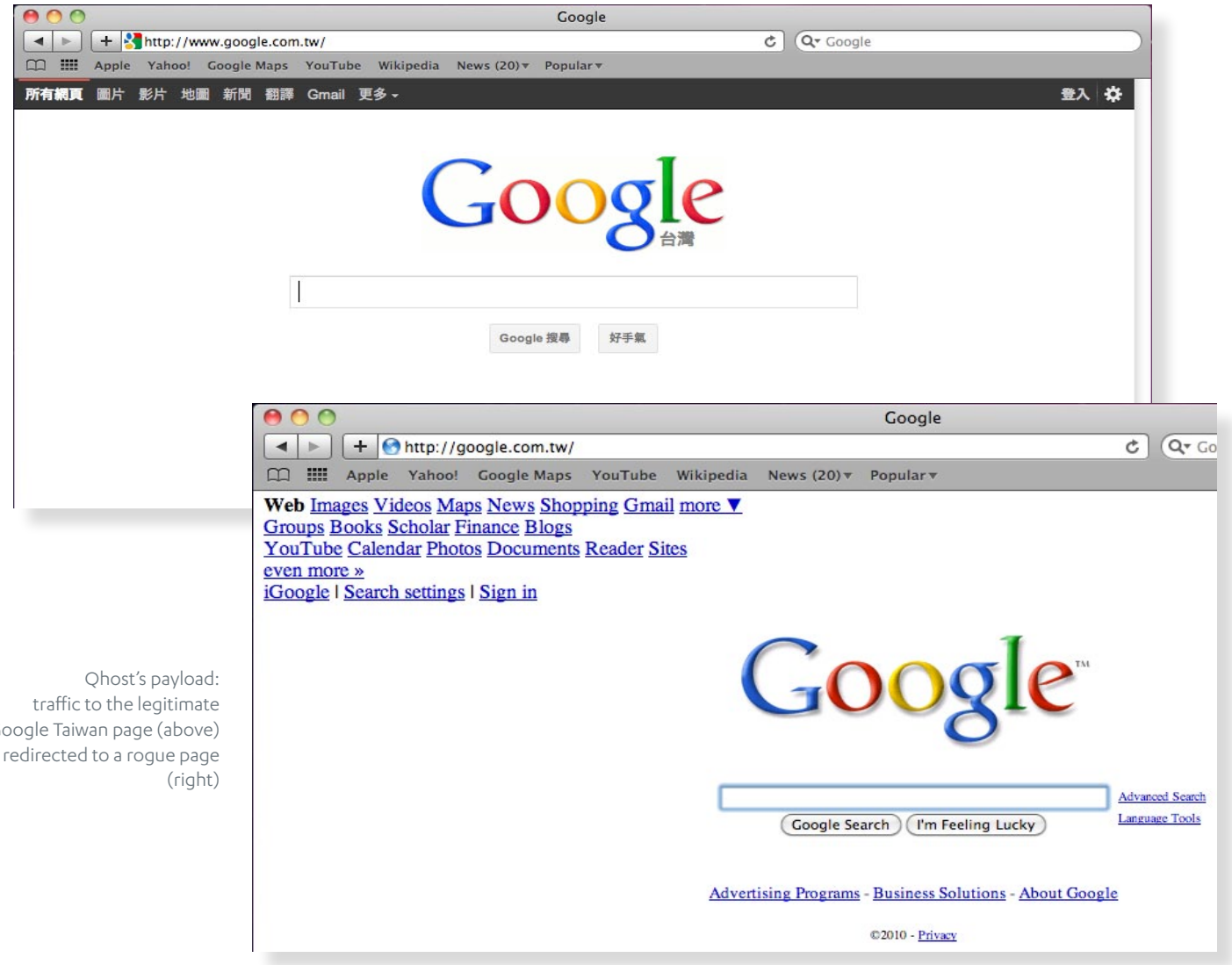
Interestingly, in August 2011 we found another malware using exactly the same social engineering tactic. This malware was dubbed Mac Qhost as a reference to an existing Windows-based malware, because like its counterpart, the malware adds entries to the hosts file to hijack web traffic.

The Mac Qhost malware redirected Google visitors to a rogue webpage posing as a Google page and serving fake search results. When users clicked a link, they were redirected again to a third-party webpage displaying unsolicited advertisements.

## MAC QHOST AND FLASHBACK

So how does Mac Qhost relate to Flashback? Well for one, it has exactly the same payload. In all the samples we analyzed, Flashback targeted Google-related sites and redirected the site visitors to a third-party page that presumably displays advertisement-related links. Based on the malware's behavior, we believe Flashback is the next incarnation of the Mac Qhost malware.

The major difference between Flashback and Qhost is that the former doesn't modify the hosts file as the latter does, but instead infects browsers and hijacks visitors to specific websites. Early Flashback variants checked if a webpage displayed in an infected web browser belongs to a targeted website; if so, it injected JavaScript into the page,




Qhost's payload: traffic to the legitimate Google Taiwan page (above) is redirected to a rogue page (right)

which executes another JavaScript hosted on a remote server. We presume that the JavaScript from the remote server either renders a fake webpage mimicking the destination page, or outrightly redirects the user to an unsolicited webpage.

The targeted website and the injected content are specified in configuration data retrieved from a remote site during the trojan's installation. Theoretically, Flashback's configuration file could be modified for other usages, such as phishing, though we have yet to see samples targeting non-Google sites.

In newer variants, the payload is no longer dependent on retrieved configuration data; instead, the payload routine is hardcoded in the malware binary and is no longer configurable. In addition, the trojan now only targets Google search results. When these are displayed in an infected browser and the user clicks on one of the links, the malware communicates with a remote server to determine when and where users are to be redirected. This development gave us concrete proof that the gang behind Flashback is only interested in targeting Google-related traffic.

Flashback's malware author(s) continue to tinker with their product, sometimes with unintended results. One of the latest trojan variants included a bug which led to the malware failing to loaded to the correct process and caused the payload to fail. Though a buggy variant that fails to deliver its payload may sound like good news, on a cautionary note, Flashback includes functionality that may allow it to do more than just redirect Google results. The malware also has a built-in 'virtual machine'-like feature that can interpret a set of instructions given by a remote server. This particular feature is what has lead some security researchers and IT reporters to dub the network of Flashback-infected machines a 'botnet'. Although the characteristics of the malware suggest that the remote command feature is most likely only used to update or remove itself from a machine, the possibility remains that it can be used to do something more nasty. This feature is still present in all variants; therefore we would like to remind users of the risk that remains even with the buggy variant.



**VULNERABLE JAVA**

Since December 2010[30], the Java development platform has been the most targeted or exploited commonly-used application, surpassing the previous target of choice, Adobe Reader.

Java is designed to be cross-platform, making it suitable for use across multiple operating systems. Unfortunately, this feature can be exploited by malware authors, who can take exploits for patched Windows-based Java vulnerabilities in Windows and port them to other platforms, such as OS X.

Due to the escalating incidences of vulnerability exploits against Java, we have been advising users to disable Java, or at the very least, diligently keep it up-to-date. Based on our surveys, most users don't really need Java when browsing the Web.

If for some reason you do need Java, turn it on only when you need it. And then turn it off again after you're done. Another option is to use a two-browser approach: use a separate browser with Java enabled solely for accessing sites that need them.

# BLACKHOLE

In the last few years, we've seen vulnerability exploitation become the popular, if not preferred, way for attackers to gain access to and infect a computer. To facilitate and simplify their operations, more and more malware distributors are taking advantage of the simple automation and convenience offered by exploit kits, which can automatically generate multiple exploits.

The most successful and most popular of these kits is Blackhole, as it is ideal for an attacker's purposes: it can be easily found and purchased from various underground forums; the kit's developers constantly update it with the latest and most effective exploits; and using it allows the attackers to increase the scope and speed of their operations at little cost.

Blackhole exploit kits are hosted on a live webpage (referred to here as the *landing page*). Attackers then use various strategies or methods, most commonly compromised sites, SEO poisoning and social engineering schemes, to draw users onto the landing page, where the kit then generates the various exploits used to probe the visitor's web browser and machine for vulnerabilities.

If the user's browser or machine includes an exploitable vulnerability, it is infected and open to manipulation. The eventual payload delivered via the exploits can be as creative as the attackers want to be, but the most common payloads we've seen this year involve dropping various forms of malware onto the affected machine. So far, we've seen the following malware types or families delivered with Blackhole's assistance:

- **Rogueware**: Fake or fraudulent programs designed to appear to be legitimate antivirus software.
- **Ransomware**: Programs that encrypt the user's documents or 'lock' the computer system and demand payment to restore normal access.
- **Zeus**: Crimeware used to intercept online banking transactions
- **ZeroAccess**: Programs that display unsolicited advertisements and redirects the web browser to unsolicited sites.
- **Sinowal**: Data-stealing trojans mainly targeting details related to online banking portals; may also monitor user activity and download additional components.
- **TDSS**: Backdoor programs that silently control the system to facilitate installation/actions performed by other malware.

## INFECTION VECTORS

There are multiple vectors or pathways in which users can be diverted to these malicious pages. Based on statistics, samples, emails and other resources gathered in the first half of 2012, the most common methods users are encountering Blackhole exploit kits so far are i) through compromised websites, ii) Search Engine Optimization (SEO) poisoning and iii) email spam.

### Compromised sites

This occurs when an attacker gains unauthorized access to a legitimate site and either plants the exploit kit directly onto the site so it can infect the site's visitors, or redirects site visitors to a landing page containing the exploit kit.

### Search Engine Optimization (SEO) Poisoning

Users may be redirected to a Blackhole landing page via poisoned Google image search results. For example, in the Google Image search result example shown at top right, the user is shown the image referred by the link in imgurl, but in the background their browser is redirected to the location referred to by imgrefurl, which eventually redirects to the actual Blackhole exploit kit landing page (at the location in the inset).


Poisoned image search result

### Email Spam

Another common way to get users to the exploit kit landing page is with spam emails containing links to the landing page.

The spam emails used can vary greatly, as seen in the examples at right (middle). As with most spam, Blackhole emails appear to be from known companies and institutions. In the table below are some of the misappropriated sender names


Blackhole's spam emails

| FEBRUARY | MARCH | APRIL | MAY | JUNE |
|---|---|---|---|---|
| BETTER BUSINESS BUREAU | | | AT&T | AMAZON |
| INTERNAL REVENUE SERVICE | | | BEST BUY | FEDERAL TAX PAYMENT SYSTEM |
| INTUIT | LINKED IN | | | |
| NACHA | AICPA | BILL ME LATER | | PAYPAL/EBAY |
| FDIC | SEC | EMEDIA | CITIGROUP | CRAIGSLIST |
| XEROX | | US AIRWAYS | TAXSLAYER.COM | UPS |
| | | FEDERAL RESERVE WIRE NETWORK | USPS | FEDERAL RESERVE WIRE NETWORK |
| | | | | VERIZON |
| | | | | VISA |
| | | | | TWITTER |
| | | | | XANGA |
| | | | | NY AIRLINES |
| | | | | HABBO HOTEL |

Blackhole's fake email senders

used in Blackhole spam emails for the first half of 2012.

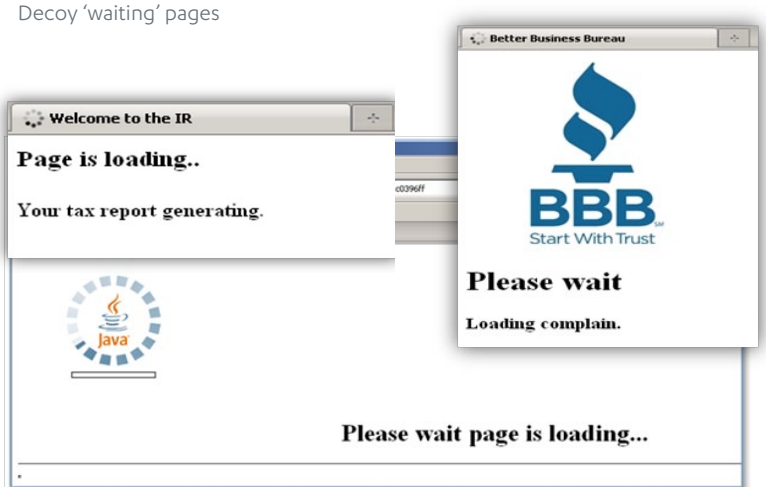
Though the specific characteristics of the spam emails vary, they do all share broadly similar characteristics in the way the malicious link formatting and redirections are performed.

### Redirections and URL Formats

The malicious links in Blackhole spam emails follow a small number of particular formats or structures, which can be summarized as:

- [domain]/[7 or 8 random alphanumeric characters]/index.html
- [domain]/[Wordpress directory]/[filename].html
- [domain]/[filename].html

Decoy 'waiting' pages




```
<script type="text/javascript" src="http://blueminded.co/TKdj1FCP/js.js"></script>
<script type="text/javascript" src="http://rijplatenverhuur.be/7EVyFpqb/js.js"></script>
<script type="text/javascript" src="http://ibimakeup.com/KgdpwCpx/js.js"></script>
<script type="text/javascript" src="http://jaffnavoice.com/AJFajPtY/js.js"></script>
```

Redirect script

Common Wordpress directories used are: wp-content, wp-admin, wp-includes and themes (especially the twentyten theme), while common filenames used include avo.html, info.html, usp.html, page.html, conf.html, zone.html, palco.html, enoz.html, ozon.html and post.html.

If the user clicks on the link in the spam email, they are redirected to a page that essentially asks them to wait while the infection happens, as in the sample images at left.

Some of these pages contain scripts (with the format [domain]/[8 random alphanumeric characters]/js.js) that redirect to the Blackhole Exploit Kit landing page; others redirect directly to the landing page.



## BLACKHOLE EXPLOIT KIT LANDING PAGE

The location of the Blackhole landing page varies, but the URL usually follows this format:

[IP/domain]/[optional directory]/[PHP script].php? [parameter name]=[16 alphanumeric characters]

The filename for the PHP script can be specified in the exploit kit; some filenames we've seen so far include: showthread.php, page.php, src.php, google.php and index.php. Some examples of landing page formats we've encountered so far:

- [IP/domain]/main.php?page=[16 alphanumeric characters]
- [IP/domain]/google.php?gmpid=[16 random alphanumeric characters]
- [IP/domain]/showthread.php?t=[16 alphanumeric characters]
- [IP/domain]/indexi.php?pagexxi=[16 random alphanumeric characters]
- [IP/domain]/catalog.php?rio=[16 random alphanumeric characters]

# BLACK HOLE in SPAM

RECEIVED FROM

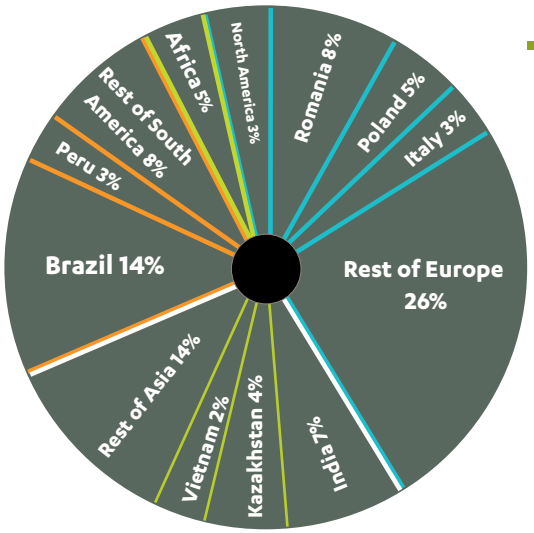
Europe
**42%**

North America
**3%**

South America
**23%**

Africa
**5%**

Asia
**27%**




## SOCIAL ENGINEERING: EMAIL SPAM THEMES

Bill Statements
Account Notification
Document Scan
Social Media Notification
Purchase Notification
Tax Notification
Product Offers
Complaint Report
Account Verification

**1:25**

Spamlinks received are Blackhole Exploit Kit URLs

SPAMMED DOMAINS HOSTED IN

USA **51.8%**

GER **6.3%**

UK **4%**

ITA **3.5%**

BRA **2.6%**

**30%** of the domains used in the spam are running WordPress

Based on data from February to June 2012.

```
document.write('<center><h1>Please wait page is loading...</h1></center><hr>');
function end_redirect(){
    window.location.href='http://173.208.196.246/jdb/inf.php?id=25bb45ac9fa3055
}
try{
    var PluginDetect={
        version:"0.7.8",name:"PluginDetect",handler:function(c,b,a){
            return function(){
                c(b,a)
```

PluginDetect script

## BLACKHOLE EXPLOITS

Once the user has been diverted onto the landing page, the actual system compromise can begin. This involves executing a series of exploits in succession to ensure infection from various possible vulnerable points. Blackhole exploits vulnerable browser plug-ins such as Java, Adobe Reader and Adobe Flash Player.

To avoid reinventing the wheel, Blackhole makes use of a legitimate third-party script called PluginDetect to determine the versions of the plug-ins installed on the system. The PluginDetect script version used by Blackhole earlier this year was 0.7.6 (later updated to 0.7.8).

### 1st Exploit: Java

In the first half of this year, the kit's developers updated the targeted Java exploit from the Oracle Java Applet Rhino Script Engine vulnerability (CVE-2011-3544) to the Java AtomicReferenceArray Type Violation vulnerability (CVE-2012-0507).

**NOTE**
[BED] stands for *Blackhole Exploit directory* and refers to the location [IP/domain]/[content or data]

The malicious Java packages are usually delivered by a URL with the following format: [BED]/[filename].jar. The JAR filenames can be specified by the attacker; common names used include: GPlugin.jar, Jas.jar , Qai.jar, sp30.jar or Pol.jar.

**NOTE**
[file number] represents a series of alphanumeric characters

If the exploitation is successful, Java will download a binary from a URL formatted as [BED]/[1 alphabetical character].php?f=[file number]&e=0. The filenames usually follow a distinct format, for example: [random floating number]g8j8.exe, [random floating number].exe, soap[number]_pack.exe or kb[number].exe. Once downloaded, the file is executed using the command: regsvr32 –s TEMP\filename.

**NOTE**
'TEMP' refers to the system's Temporary folder

### 2nd Exploit: Microsoft Data Access Components (MDAC)

If the browser is vulnerable to MDAC (CVE-2006-0003), Blackhole exploits it and downloads a binary from [BED]/[1 character].php?f=[file number]&e=2. This file is saved using a filename with 7 random alphanumeric characters.

### 3rd Exploit: Help and Support Center

If a Media Player plug-in is present, Blackhole attempts to exploit the HCP protocol vulnerability (CVE-2010-1885). If the browser is Internet Explorer, it checks for the version of the installed Media Player plug-in. For versions earlier than 10, it visits one specific Blackhole exploit URL; for versions 10 or later, another location is visited instead. If the browser is anything other than Internet Explorer, yet another location is visited.

Successful exploitation will lead to a binary download from [BED]/[1 alphabet character].php?f=[file number]&e=5. The downloaded binary is executed from either TEMP\exe.exe or TEMP\file.exe.

### 4th Exploit: Adobe Reader

Blackhole uses different exploits based on which version of the Adobe Reader plug-in is running. For Adobe Reader plug-in versions 1 to 7, it opens a malicious PDF file from [BED]/ap1.php?f=[file number] that exploits CVE-2007-5659 and CVE-2008-2992, whereas for versions 8 to 9.3, a PDF from [BED]/ap2.php is used to exploit vulnerability CVE-2010-0188.

If the exploits are successful, a binary file is downloaded from a remote site and executed using the command "regsvr32 –s TEMP\wpbt[number].dll".

**NOTE**
[number] starts with '0' and increments with each additional binary download

### 5th Exploit: Adobe Flash

To exploit any Adobe Flash plug-ins present, different exploits are used depending on the plug-in version:

- *CVE-2011-0559*: versions 10 or earlier, 10.0.x (where x is greater than 40) or 10.1
- *CVE-2011-0611*: versions 10.2.x (where x is less than 159) or 10.x (where x is less than 2)
- *CVE-2011-2110*: versions earlier than 10.3 and 10.3.181.x (where x is less than 24)

The first two vulnerabilities are exploited using the Flash files from [BED]/field.swf and [BED]/score.swf, while the third uses a Flash file from [BED]/flash.swf. Like the Adobe Reader exploit, if successful a binary file is downloaded from a remote site and installed using the command "regsvr32 –s TEMP\wpbt[number].dll".

### 6th exploit: Microsoft XML Core Services

In June, the Microsoft XML Core Services vulnerability (CVE-2012-1889) was reported. Just days after a Metasploit module was published targeting this vulnerability, the Blackhole exploit kit was updated to include it. Successful exploitation leads to a binary download from [BED]/[1 alphabet character].php?f=[file number]&e=7. As with the Adobe exploits, the downloaded file is executed using the command "regsvr32 –s TEMP\wpbt[number].dll".

```
HTTP/1.1 200 OK
Server: nginx/0.8.55
Date: Thu, 14 Jun 2012 06:57:04 GMT
Content-Type: application/x-msdownload
Connection: keep-alive
Content-Length: 166400
Pragma: public
Expires: Thu, 14 Jun 2012 08:57:41 GMT
Cache-Control: must-revalidate, post-check=0, pre-check=0
Cache-Control: private
Content-Disposition: attachment; filename="calc.exe"
Content-Transfer-Encoding: binary

MZP@@@@ !@L!This program must be run under Win32
$7
```

HTTP header with binary filename

This vulnerability was highly exploited during the 'zero-day' period before a patch was released. In response, Microsoft quickly released a separate 'fix it' patch to close the vulnerability, and later included the patch in the July MS12-043 bulletin.

### PAYLOAD

In addition to the various files the preceding exploits drop on the system, we also observed that the filename specified in the HTTP header of the binary payloads are the same - calc.exe, readme.exe, info.exe, about.exe or contacts.exe. These files are usually found in the Internet Cache, as filename[1].exe (e.g. calc[1].exe).



## INFECTION CLEANUP AND PREVENTIVE MEASURES

The Blackhole exploit kit is only a means to deliver any kind of payload, including but not limited to the malware families mentioned earlier. Thus, manual cleanup steps differ depending on the installed payload. Automatic cleanup of the payload can be done by your F-Secure security product.

In order to avoid getting infected through Blackhole, the user must be wary of any unsolicited emails of the same types mentioned earlier. They may also want to check the links within the emails and verify if they appear to be coming from domains not related to the supposed sender, or if they have a similar URL format to those used by Blackhole.

Moreover, it is best that the user keeps their system up-to-date with the latest patches, especially for programs or components targeted by Blackhole, to deter vulnerability exploitation.

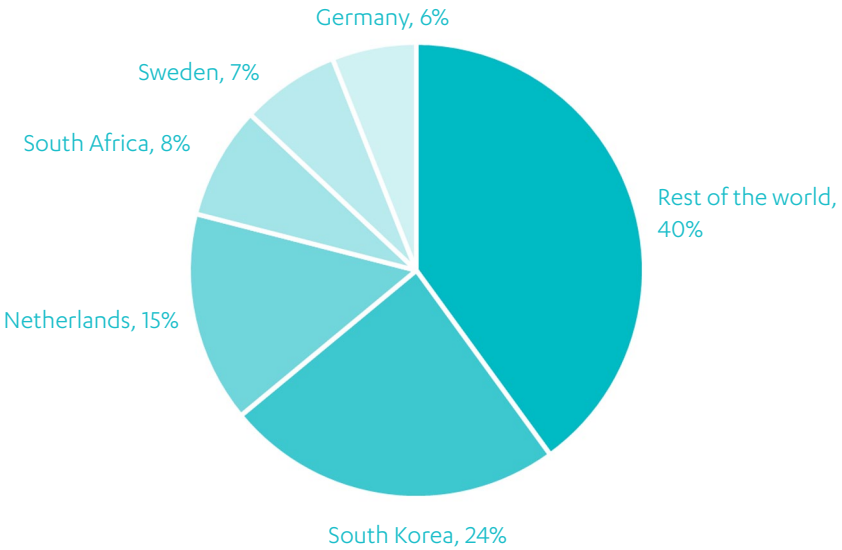
# MOBILE THREATS

Continuing the trend of constant growth in Android malware that began last year, in the second quarter of 2012 we received and identified 5333 unique malicious applications, a 64% increase compared to the previous quarter. As usual, these malicious or unwanted applications are mostly from third-party markets.

In Q2 of 2012, we added 19 new Android malware families, as well as 21 new variants of known families. A high percentage of these new variants come from the FakeInst and OpFake Families. These two families are in fact closely related and in some instances, can be classified as one family. Despite the multiple variants, the general behavior of these families remains the same, with most of the new variants modified only to help them evade anti-virus technology.

In this quarter, we saw further evolution in Android malware development, with the introduction of two new major techniques, namely the usage of drive-by download for distribution and the utilization of the micro-blogging service Twitter as a bot mechanism. An interesting detail we've previously noted is that Android malwares tend to be regionally-focused attacks; we saw another example of that this quarter, with a report from Spain of an Android-based, banking-related attack.

**ANDROID THREATS BY COUNTRIES, Q2 2012**




*Based on data from F-Secure's cloud lookup systems for the period April to June 2012

## DRIVE-BY DOWNLOAD ON ANDROID

Drive-by downloads have long been a standard infection vector for PC-based threats, but until now we had not seen it used by mobile threats. This changed in the middle of May, when we reported that the first drive-by download malware for Android had been spotted in the wild. The malware was detected as *Trojan-Proxy:Android/NotCompatible.A*.

Unlike other Android trojans seen thus far, this malware does not appear to steal data or send premium-rate SMS messages. Instead, it forces the device to act as a proxy, potentially making it part of a bot network if it can connect to a specified control server that can issue commands to it.

For NotCompatible.A to be installed, the device must be configured to accept installation of programs from unknown (i.e., non-Play Store) sources. If so, when the user visits a compromised website in the device browser, the trojan-proxy is automatically downloaded onto the device and appears in the notification tray, waiting for the user to install it. The malware uses the filename "Update.Apk" and the program name is shown as "com.Security.Update" - both names chosen as a social engineering trick to dupe users into thinking the downloaded file is innocuous.

## TWITTER CONTROLLED

Another new technique that emerged this quarter was the use of Twitter as a bot controller. This was seen in the case of *Trojan:Android/Cawitt.A*, which was designed to access a Twitter account (possibly set up by malware) to obtain its server addresses. Via the Twitter account, the trojan is able to receive a command with the variables needed to send an SMS. It also sends the International Mobile Equipment Identity (IMEI) number, the device's phone number and the Android ID to the server.

## REGIONAL-TARGETED ATTACKS

We've noticed before that Android malwares appear to have region-specific characteristics. For example, Android trojans in China have mainly been premium-SMS sending programs, while Spanish Android malwares are mostly banking related.

In Q1 2012, we saw *Trojan:Android/FakeToken.A* appear in Spain. In Q2, we discovered *Trojan:Android/SmsSpy.F*, a malware known to be related to the PC-based banking-trojan Zitmo (SmsSpy is also sometimes referred to by this name).

As the malware arrives via a link in a message sent to the device, it appears this particular Android trojan specifically targets device owners who perform online banking transactions and receive the Mobile Transaction Authorization Number (mTan) confirmation code. The message sent informs the user that they should download and install the application available from an included link, purportedly as a 'security measure'. Needless to say, users who do so unwittingly compromise their online banking transactions.

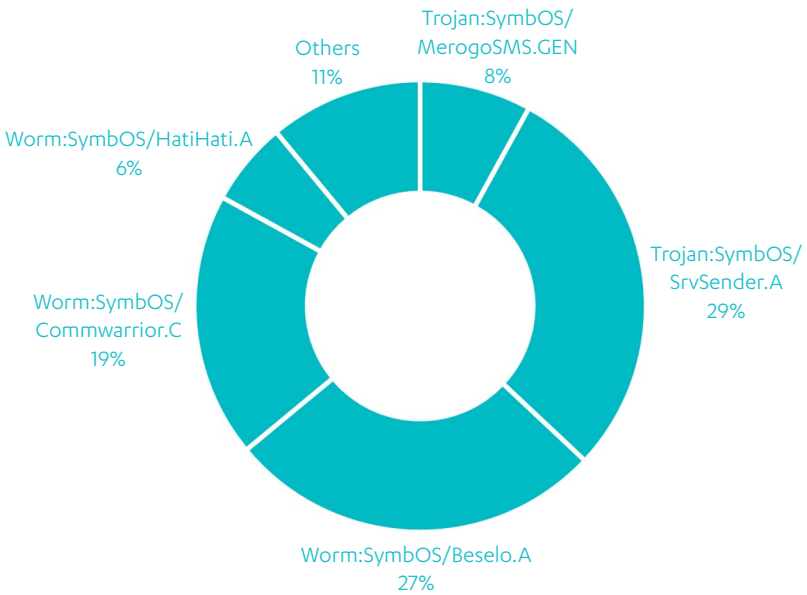
## SYMBIAN: BANKING-TROJANS AND MONLATER

On the Symbian platform, infections continue to be recorded despite a drastically reduced number of total infections over the last few months. Almost 80% of the detections seen come from 3 families, as seen in the chart below.

This quarter also saw the appearance of a new Symbian malware family, *Trojan:SymbOS/Monlater*. Variants from this family appear to be closely related to the large *Trojan:SymbOS/Monsoon* family, which generates revenue for its author(s) by using premium and WAP services. Monsoon variants are also able to communicate with a command and control (C&C server), which may issue instructions or download and install new components on the malware.

The Monlater variants are likely downloaded from the same C&C server that Monsoon variants contact for further instructions. As the structure is sound and active, there is no reason to doubt that this same channel would not be used to push new versions of the malware, as well as new components designed to hide the existing variants from detection.

TOP SYMBIAN THREATS, Q2 2012




*Based on data from F-Secure's cloud lookup systems for the period April to June 2012

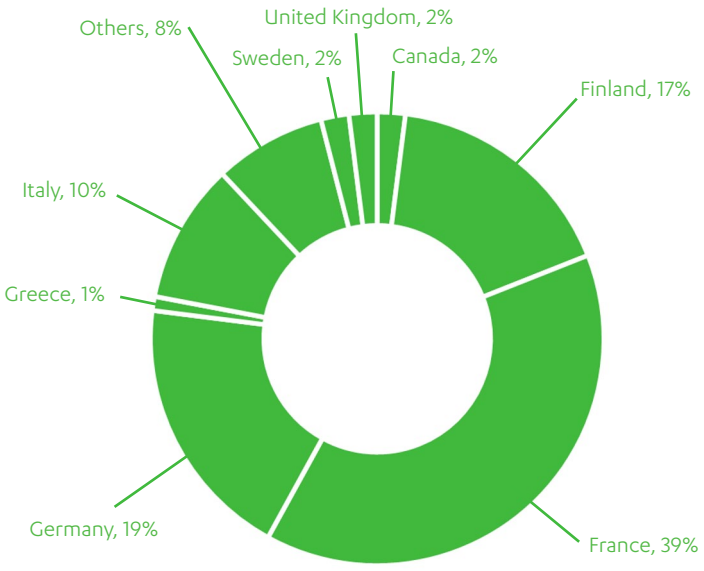
# RANSOMWARE

Throughout Q2 2012, we saw a return of malware employing extortion techniques to make money out of their victims. Typically, this kind of malware (usually referred to as 'ransomware') will take control of the user's own computer and/or their files and documents, then leverages the victim's surprise, embarrassment and fear to push them into paying the ransom demanded in order to regain control.

Ransomware has been a longstanding but low prevalence threat in computer security. In 2012 however, we saw not only a surge in the number of ransomware infections but also a number of changes in the ransomware threat landscape, mainly in the distribution methods and geographical locations of the victims, as well as the techniques used to gain control of the user's system or data and the payment methods preferred by the ransomware operators.

Most of these changes originated in the Reveton ransomware family, which has been the most active or dominant group in the last few months. On a technical note, an interesting case we saw this year was a new variant in the Zeus malware family which included ransomware features.

REVETON RANSOMWARE BY COUNTRY




**Based on statistics for May 2012, taken from F-Secure's cloud lookup systems.

## DISTRIBUTION

In the past, we saw ransomware arriving on a victim's computer mainly through social engineering schemes or as part of a malware payload.

### Driveby downloads and Blackhole

From late 2011 all the way through the first half of 2012 however, we've seen a steady increase in ransomware being delivered via drive-by downloads, particularly those using Blackhole exploits.

### Shift in targeted countries

The geographical distribution of ransomware victims have also changed. While previously we mostly saw ransomware in the Russian market, in Q2 2012 we observed a wave of attacks specifically targeted at users in various European countries, followed by a similar wave against users in the USA in the second half of May.

To illustrate, if we look at the distribution of Reveton's infections for May 2012 (left), we can see that most of the infection reports are coming from European countries, mostly France, Germany, Finland and Italy.

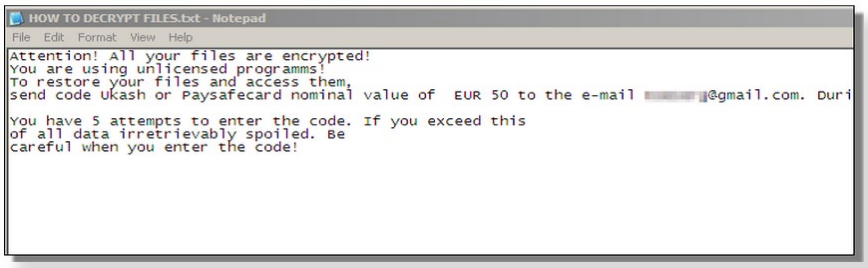
## EMBARRASSMENT AND ENCRYPTION

In the past, we saw numerous examples of ransomware that locked the desktop and even replaced the desktop background with very explicit pornographic images to create embarrassment, until payment was made.

More recently, we've seen ransomware, particularly from the Ransomcrypt and GPCode families, resorting to encrypting the user's documents, denying them access to the files unless payment is made. The ransom amount demanded varies depending on the variant/country in question. Some samples reportedly also threatened that if the demand is not met, the trojan will 'erase the hard disk' or worse, the user will be taken to court.

In some cases, the encryption used has been so strong that decryption and recovery of the affected files was not possible; either the ransom had to be paid or the files had to be restored from a backup.


Screenshots of Ransomware demands




Ransomcrypt's demand

## THEMATIC CHANGE AND LOCALIZATION

Another change we have noticed is a 'standardization' of themes used by this year's ransomware. Previous ransomware we've seen presented their demands in various ways, ranging from supposed 'data corruption requiring repair software' schemes to bald-faced extortionist demands. In Q2 2012 however, almost all ransomware we've seen are 'police themed', or designed to appear to be from an actual law enforcement authority.

In the samples we've seen, the ransomware 'locks' the screen and displays a message, allegedly from the national police force. Depending on the variant, the message may claim that the user's computer has been logged as visiting sites related to terrorism or abuse, and a 'fine' must be paid to release the computer again.

The ransomware authors have put in some effort to identify plausible organizations that might conceivably enforce compliance and punishment of the alleged "crime", and (mis) appropriate the names of existing law enforcement organizations in each country to use in their ransomware for added effect. The effort extends to using email links that appear very similar to official contact points from the actual authorities.

The authors have also gone to some trouble to localize their messages, with variants being reported in at least six languages: Dutch, English, French, Finnish, German and Spanish. The localized variant is displayed to the user based on their geographical location.

## PAYMENT OPTIONS

In previous ransomware cases, we saw a wide variety of payment methods being used. This year however, ransomware payment demands are almost exclusively outside traditional credit card circuits. Instead, the ransomware authors now prefer to use online payment methods or disposable cash cards, such as Ukash andPaysafecard. Unlike credit card transactions, payments made using these methods are both irreversible and anonymous, making them ideal for the ransomware operator's purposes.

## RANSOMWARE FAMILIES

Most of the ransomware we have seen so far this year fall into three distinct families, two of them new and one old with a new, updated variant.

### Trojan:W32/Reveton

Most of the police-themed ransomware targeting users in Europe have been from this family. Variants in the family will display an alarming, official-looking notification message on the user's desktop that falsely claims to be from a local law enforcement authority - the specific organization named will change depending on the user's location. The ransomware then 'locks' the desktop, making the computer mostly unusable and demands payment (supposedly a 'fine') through Paysafecard and/or Ukash, to restore normal access to the computer. Additional information, including removal instructions, are available in the Labs Weblog post, Police themed ransomware[31] and threat description Trojan:W32/Reveton[32].

### Trojan:W32/Ransomcrypt

Variants in this family encrypt files on the affected computer, supposedly because the user is "using unlicensed programs". When encrypting the files, Ransomcrypt also appends the extension, '. EnCiPhErEd'. The ransomware then displays a text file demanding payment in return for a password to decrypt the affected files. Users attempting to enter a password are only permitted 5 tries; after that, the ransomware deletes itself from the system, leaving the files encrypted. Additional analysis and a decryption script for affected files is available in the Labs Weblog post, Trojan:W32/Ransomcrypt[33].

### Zeus with Ransomware features

The Zeus malware family is more known for being involved in botnets and online banking transaction hijacking, but a new variant includes a backdoor command called *win_unlock*. When this particular variant is executed, it opens a specific webpage in the Internet Explorer web browser. The page presumably shows some type of extortion message, but at the time of the writing, is no longer available. The malware then prevents the user from doing anything with the infected system, effectively 'locking' it like other ransomware. Fortunately, this particular variant includes its unlock information in the registry of the affected machine, which can be modified - and the computer unlocked - with a few simple steps in a registry editor. Additional information and repair instructions are available in the Labs Weblog post, ZeuS Ransomware Feature: win_unlock[34].

## RECOMMENDATIONS

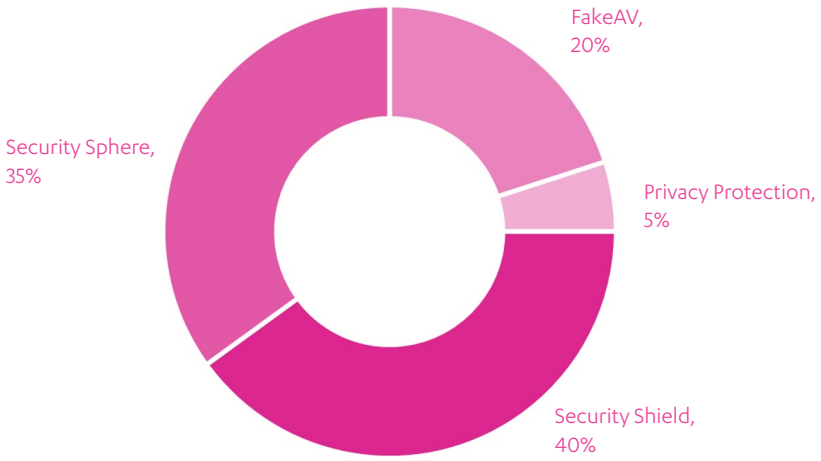
- **Back up your important files frequently**
  If an infection occurs, you can restore encrypted files from backup
- **Contact your ISP/antivirus vendor's Support for available assistance**
  In some cases, a tool may be available to recover the affected file
- **Update all your programs**
  This prevents driveby downloads from silently installing ransomware on the system
- **Consider reformatting**
  If the computer system itself is affected, consider reformatting it rather than paying the demand

# ROGUEWARE

Fake antivirus and antispyware programs have been a longstanding nuisance to computer users. These programs, which are also known as 'rogueware' or 'scareware', are designed to appear to be legitimate security software, but use misleading, high-pressure or fraudulent means to convince the user to download and install a 'trial' version of the product, and subsequently to purchase a 'full' version of it.

Rogueware deliberately imitates the graphical user interface and branding of established, legitimate antivirus or antispyware programs, in some cases even outrightly copying the actual logos or designs with only a few minor modifications. This imitation is a form of social engineering, in that the rogueware exploits the user's unconscious trust in a familiar brand or professional appearance, to gain legitimacy. This appearance of respectability convinces many users to purchase the product.

MOST POPULAR ROGUWARE, APRIL-MAY 2012



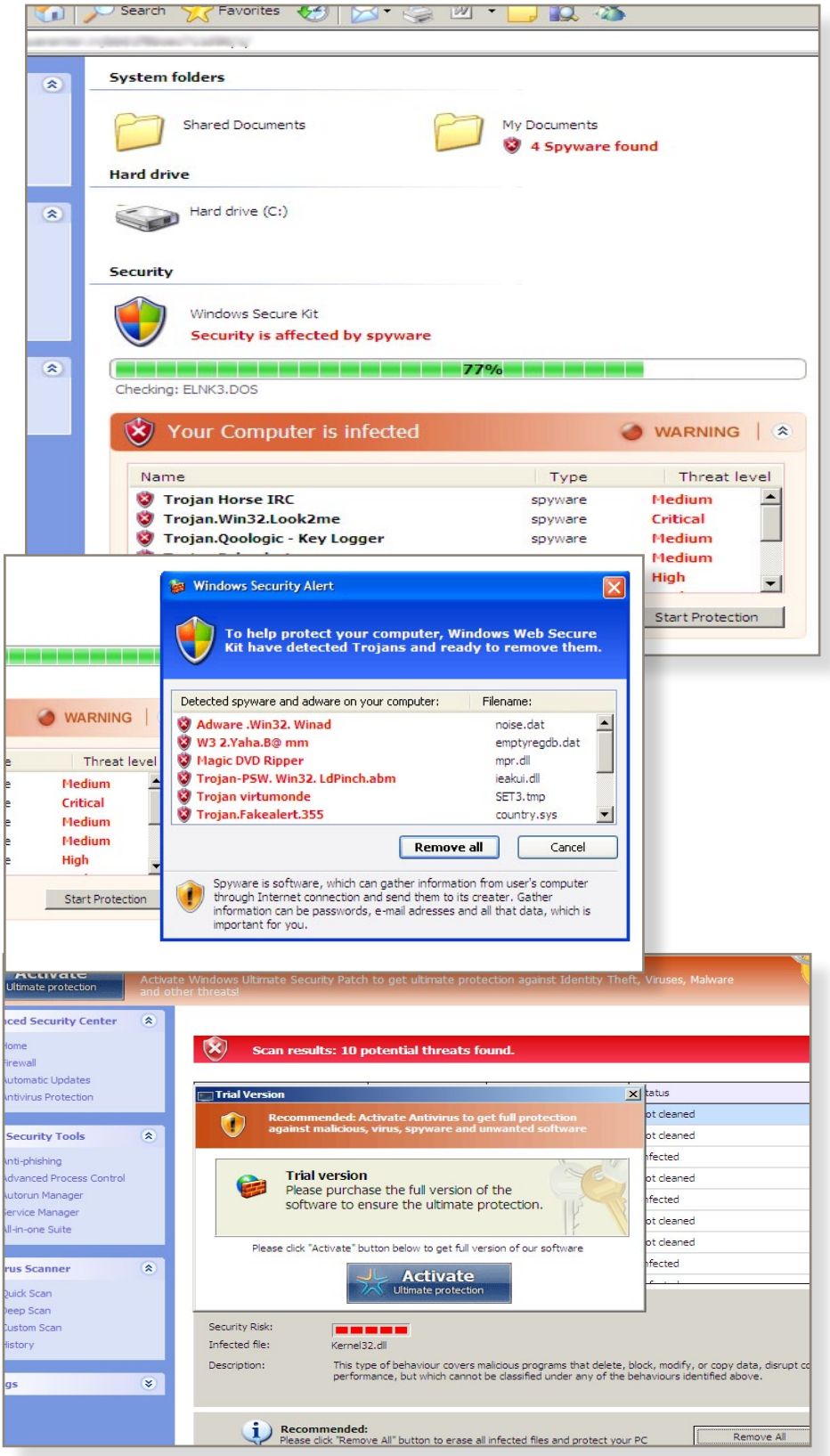

## A TYPICAL CASE

The most typical scenario for a rogueware infection starts with the user being shown a fake system scan warning. This may be either on the computer desktop or during a visit to a (compromised) website. Usually, no actual scan is performed; instead, a screenshot of a generic system folder is displayed with the alarming scan result posted in front. The scan appears to show infections present on the system and urges the user to 'download and install a trial antivirus' to remove the infections.

If the 'trial' is downloaded, installed and run, multiple infections are typically shown to be present, even on a clean machine. In the more malicious cases, no scan is performed even when the trial is run - a screenshot of a scan dialogue is simply displayed, with the same scan results image displayed after. No removal is attempted; the user is instead urged to purchase the 'full' version of the product to clean the machine. If the user does purchase the upgraded version, it may or may not have scanning and removal capabilities. In extreme cases, the product may actively harm the user's system.

## DISTRIBUTION

Historically (that is, five years or so ago), rogueware was most commonly spread by affiliate sites targeting their own website visitors. In the last few years however, rogue distribution schemes have begun incorporating techniques and social engineering strategies once more commonly seen in malware distribution, including the use of exploits on compromised sites, malicious spam emails and drive-by downloads.




Rogueware pretending to scan the system (top); fake scan results (middle) and request to purchase 'full version' (bottom). Note the misuse of legitimate Windows icons.

### Social Engineering

Copying a tactic previously seen used by trojan-downloaders, some rogues are also distributed using social engineering techniques that entice users into attempting to view a 'video clip' hosted on a compromised site. When the video is loaded, the user instead sees a request to download a file, supposedly additional software needed to watch the video; in reality, the user unknowingly downloads the rogue product installer.

### Search Engine Optimization (SEO) Poisoning

This distribution method begins when the user performs a search using a popular search engine, such as Google, and is returned a list of search results. Unbeknownst to the user, a legitimate site that appears in the search results has previously been compromised and now contains a malicious script, iframe or exploit kit designed to exploit a vulnerability in the user's system. If the user visits the site using a browser or system with a vulnerability, the site is able to inject the malicious script, iframe or object into the user's system and redirect the web browser to a page or site promoting the rogue.

A fake scan result is displayed on this page or site, claiming that the user's system 'may be infected'. Unlike earlier rogues, which often used more extreme language ('Your system is infected with XYZ'!), some particularly sophisticated rogues now tailor their language to sound more cautious, most likely as a way to evade legal issues.

If the user believes the scan results, they may then download and install the rogue product. After the installer is executed, a legitimate-looking antivirus program interface is displayed, pretending to run a system scan. Fake scan results are subsequently displayed that appear to show the machine infected with multiple malware. The program then informs the user a 'full' version must be purchased before the product can clean the system.

## ROGUEWARE FAMILIES

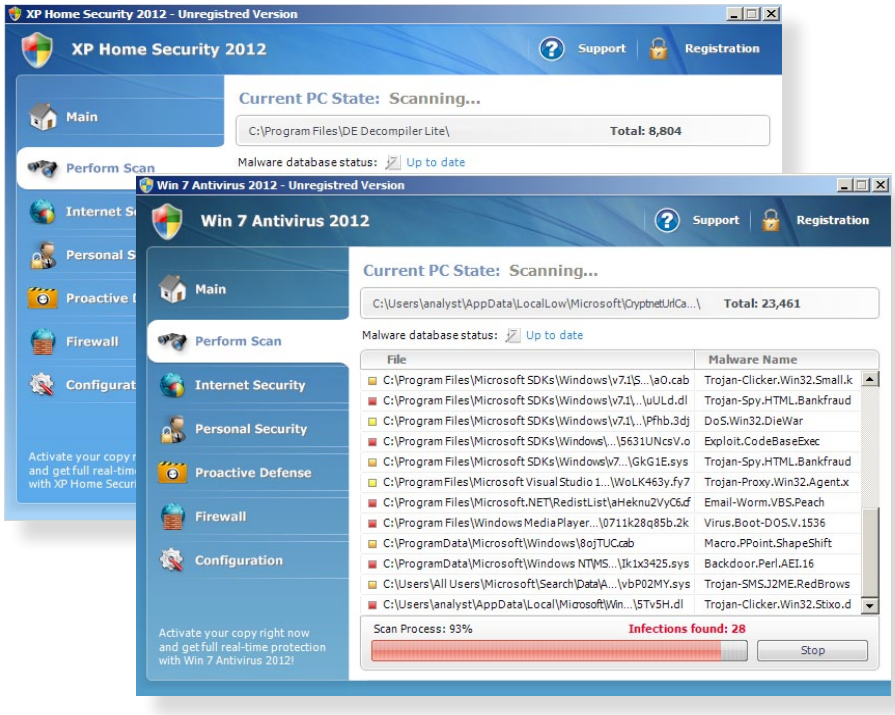
### FakeAV

The family of rogue programs that we detect with the name FakeAV is large and varied. A particular characteristic of this family is that the products typically randomize the branding design used for the program, depending on the machine on which it is installed. Despite the randomized choice of branding however, the actual branding designs are relatively static. Some of the designs we've seen are pictured at right.

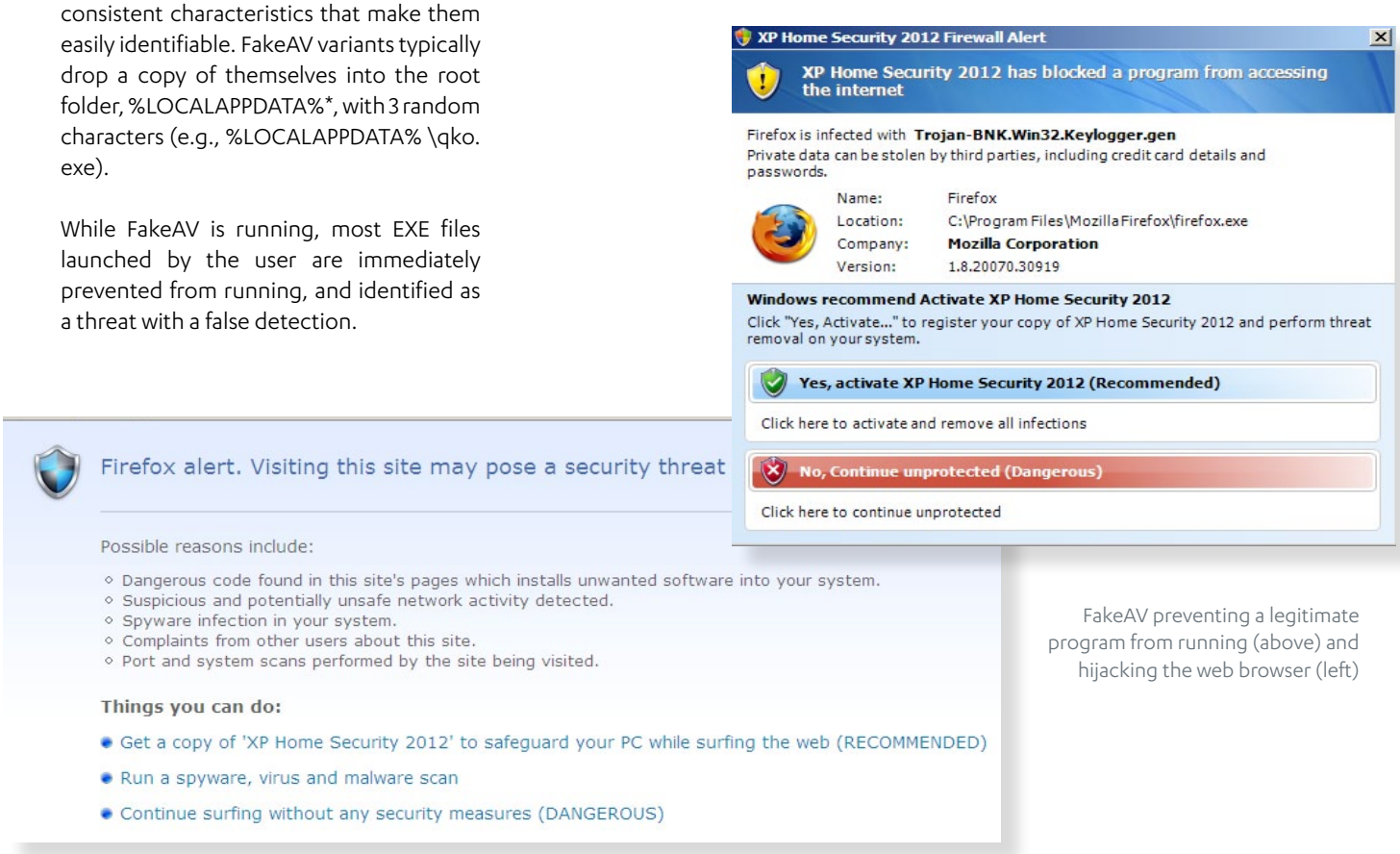
In the rogueware landscape, though FakeAV has not been one of the most prevalent threats, it has been a consistent, longstanding one. In November 2011, the number of infections actually spiked for a short time, but since January 2012, the rate of infections has been gradually decreasing.

FakeAV variants have a number of consistent characteristics that make them easily identifiable. FakeAV variants typically drop a copy of themselves into the root folder, %LOCALAPPDATA%*, with 3 random characters (e.g., %LOCALAPPDATA% \qko.exe).

While FakeAV is running, most EXE files launched by the user are immediately prevented from running, and identified as a threat with a false detection.




Various FakeAV 'designs'




FakeAV preventing a legitimate program from running (above) and hijacking the web browser (left)

* On Windows 7, *%LOCALAPPDATA%* refers to: C:\Users\username\AppData\Local, while on Windows XP, it refers to C:\Documents and Settings\username\Local Settings\Application Data

The rogue will however allow web browsers such as Mozilla Firefox to run - but will hijack the browser's pages to prevent the user from accessing known sites related to antivirus or security program vendors.

### Security Shield

We first saw Security Shield rogues in 2010 and over time, have observed numerous changes made to the product. Unlike other rogue families, the operators behind Security Shield have been very active, constantly modifying its interface and branding. The only consistent element of this family has been the name, which has been maintained as Security Shield in all the time it has been detected.

Unlike other rogue families, which have seen a gradual decline in infection rates over the last few months, Security Shield variants are still both prolific and active, possibly due to the constant effort by its operators to keep the products 'new and improved'. This family accounts for almost 40% of the rogue infections we detected in the first few months of 2012.


Security Shield

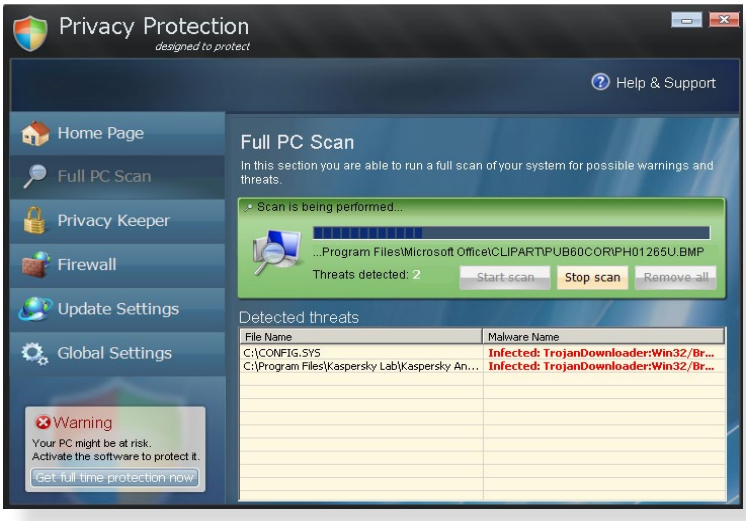
### Security Sphere

Apart from using different icons and images, Security Sphere rogues are pretty much identical to Security Shield products, and may possibly even be from the same author.

The first Security Sphere variant was found in March 2011, and coincided with a steep drop in Security Shield detections, at least until April 2011. Since June 2011, the situation has been reversed and Security Sphere now ranks as the 2nd most prevalent rogue family, after Security Shield.

### Privacy Protection

In the first quarter of 2012, Privacy Protection had the least number of detected samples. Like FakeAV, Privacy Protection uses a static design for its graphic user interface that makes the product easily identifiable. In addition, it makes consistent, identifiable system changes, including adding "Privacy Protection" in the registry entry.




Privacy Protection

# SOURCES


**FOREWORD**

1. Stuxnet Redux:Questions and Answers
   http://www.f-secure.com/weblog/archives/00002066.html
2. US 'cyberattacks' leak
   http://www.f-secure.com/weblog/archives/00002374.html

**EXECUTIVE SUMMARY**

3. ZeroAccess's Way of Deletion
   http://www.f-secure.com/weblog/archives/00002385.html

**2012 INCIDENTS CALENDAR**

4. Facebook spam uses Amazon cloud
   http://www.f-secure.com/weblog/archives/00002304.html
5. SOPA protests
   http://www.f-secure.com/weblog/archives/00002301.html
6. DDoS attack on Poland
   http://www.f-secure.com/weblog/archives/00002302.html
7. Cryptome hacked
   http://www.f-secure.com/weblog/archives/00002313.html
8. FBI conference call hacked
   http://www.f-secure.com/weblog/archives/00002309.html
9. Wordpress injection attack
   http://www.f-secure.com/weblog/archives/00002328..html
10. MS12-020 exploit toolkit released
    http://www.f-secure.com/weblog/archives/00002338.html
11. Ransomware on the rise
    http://www.f-secure.com/weblog/archives/00002344.html
12. Zeus botnet takedown
    http://www.f-secure.com/weblog/archives/00002337.html
13. Macs targeting NGOs
    http://www.f-secure.com/weblog/archives/00002339.html
14. Flashback outbreak
    http://www.f-secure.com/weblog/archives/00002346.html
15. Increase in Java exploits
    http://www.f-secure.com/weblog/archives/00002285..html
16. Rogueware found on Tumblr
    http://www.f-secure.com/weblog/archives/00002352.html
17. Syria targeted attacks
    http://www.f-secure.com/weblog/archives/00002356.html
18. Olympics targeted attacks
    http://www.f-secure.com/weblog/archives/00002370.html
19. Drive-by Android malware
    http://www.f-secure.com/weblog/archives/00002366.html
20. Flame found
    http://www.f-secure.com/weblog/archives/00002371.html

**OF NOTE**

21. Labs Weblog; *Flame-bait Questions*; published 30 May 2012;
    http://www.f-secure.com/weblog/archives/00002372.html
22. Labs Weblog; *FBI: Operation Ghost Click*; published 10 November 2012;
    http://www.f-secure.com/weblog/archives/00002268.html

**CASE STUDIES**

23. Labs Weblog; *Mac Flashback Infections*; published 5 Apr 2012;
    http://www.f-secure.com/weblog/archives/00002345.html
24. Labs Weblog; *Oxford Muses on Mac Flashback: Worst Outbreak Since Blaster;* published May 2, 2012;
    http://www.f-secure.com/weblog/archives/00002355.html
25. Apple Support Communities; *.rserv wants to connect to cuojshtbohnt.com*; https://discussions.apple.com/thread/3844172?start=135&tstart=0
26. CNET; Topher Kessler; *Flashback malware removal tool roundup*; published April 13, 2012;
    http://reviews.cnet.com/8301-13727_7-57413811-263/flashback-malware-removal-tool-roundup/
27. Ars Technica; *Forget Apple: Oracle to bring Java security fixes directly to Mac users*; published Apr 27, 2012;
    http://arstechnica.com/apple/2012/04/oracle-updates-java-to-se-7-for-os-x-brings-full-jdk-support/
28. Apple Support; *OS X Lion v10.7.4, Security Update 2012-002: Global DYLD launch variables no longer loaded;*
    http://support.apple.com/kb/TS4267
29. Apple Support; *About the security content of Java for OS X 2012-003 and Java for Mac OS X 10.6 Update 8;*
    http://support.apple.com/kb/HT5247
30. Microsoft Security Intelligence Report; *SIR Volume 10*;
    http://www.microsoft.com/security/sir/archive/default.aspx
31. Labs Weblog: *Police themed ransomware*; published Apr 4, 2012;
    http://www.f-secure.com/weblog/archives/00002344.html
32. Threat Description*: Trojan:W32/Reveton;*
    http://www.f-secure.com/v-descs/trojan_w32_reveton.shtml
33. Labs Weblog post: *Trojan:W32/Ransomcrypt;* published Apr 12, 2012; http://www.f-secure.com/weblog/archives/00002347.html
34. Labs Weblog post: *ZeuS Ransomware Feature: win_unlock*; published May 21, 2012;
    http://www.f-secure.com/weblog/archives/00002367.html

# F-SECURE IN BRIEF

F-Secure has been protecting the digital lives of consumers and businesses for over 20 years. Our Internet security and content cloud services are available through over 200 operators in more than 40 countries around the world and are trusted in millions of homes and businesses.

In 2011, the company's revenues were EUR 146 million and it has over 900 employees inmore than 20 offices worldwide. F-Secure Corporation is listed on the NASDAQ OMX Helsinki Ltd. since 1999.

# Protecting the Irreplaceable





F-Secure