

THREAT REPORT

H2 2013



Protection around the clock

Response Labs' work is assisted by a host of automatic systems that track worldwide threat occurrences 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.

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.

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.



FOREWORD

Our enemies keep changing. We used to fight the online hackers. Then the online criminals. Nowadays we worry more and more about governmental action.

MIKKO HYPPÖNEN
CRO, F-SECURE LABS
<http://twitter.com/mikko>

But is governmental surveillance a real problem in a world where everybody seems to be sharing everything about their life with no worries? People tweet their breakfasts, foursquare their location, facebook their dating patterns and instagram their friends and family. For some, this is not a problem - at least it's not a problem at the moment. And this is what all these services encourage you to do, as that's how they make all their money.

Sharing pictures of your drunken partying might not matter much if you are nobody in particular. It might matter more a decade later, if you've become a public figure, a teacher or a politician. And then it might be too late to take anything back. In fact, it's going to be interesting to watch presidential elections in around 2040, as the teenage angst pics and posts of all candidates will be dug out from old social media and discussion forum archives for everyone to see.

But governmental surveillance is not about governments collecting the information you're sharing publicly and willingly. It's about collecting the information you don't think you're sharing at all - information such as the online searches you do with search engines. Or private e-mails or text messages. Or the location of your mobile phone at any time. Surveillance like this has only been possible for a couple of years. The Internet and mobile phones made it possible. And now it's being done for that exact reason: because it can be done.

But just because it can technically be done doesn't make it right.

“GOVERNMENTAL SURVEILLANCE IS NOT ABOUT GOVERNMENTS COLLECTING THE INFORMATION YOU'RE SHARING PUBLICLY AND WILLINGLY.

IT'S ABOUT COLLECTING THE INFORMATION YOU DON'T THINK YOU'RE SHARING AT ALL.”

EXECUTIVE SUMMARY

In 2013, the world in general - and the computer security industry in particular - was inundated with news of the alleged foreign surveillance and hacking activities conducted by the United States' National Security Agency (NSA), revealed in disclosures from whistleblower Edward Snowden. The barrage of revelations left many concerned, to say the least, and has led some to examine more closely the mechanics of web browsing as it is performed today by most users, to understand how it may be vulnerable to online surveillance and datagathering. In our article on web privacy we cover some of the ways a user may unwittingly have their browsing activities or personal information captured and collected online, even while visiting legitimate, clean sites.

The general unease created by news has led to, among other actions, public companies being questioned about the steps they take to protect their client's privacy. In the computer security industry, vendors were challenged on their stand against governmental malware. At F-Secure, respect for privacy is one of our core values and is reflected in how our products are designed. In addition, it is and always has been our stand to detect any malware regardless of its source, up to and including those produced by state entities, such as the R2D2 backdoor we began detecting in 2011 ^[1] that was allegedly used by the German government.

Besides governmental malware engaged in datagathering or monitoring, there are always opportunistic threats out for monetary gains. A good example seen in H2 2013 is the reported targeted attack on a professional poker player's laptop, which had a Remote Access Trojan (RAT) planted on it in order to view his hand during online poker tournaments. Such attacks on players colloquially known as card sharks are, appropriately enough, known as *sharking*.

On a larger scale, we look more closely at the Mevade botnet, which appears on our list of top 10 reported detections for this period. We examine the most prevalent variants of the botnet and the C&C servers it uses, as well as its usage of the TOR network and its ability to share files on the Kad peer-to-peer (P2P) network.

One notable incident in H2 2013 involved the arrest of the alleged creator and distributor of the Blackhole and Cool exploit kits. As detection reports for these exploit kits decline, we look into how other rivals are scrambling to fill the void they left, notably the Angler exploit kit with its exploits for Java, Flash and Silverlight.

On the mobile threats front, we find that of the top 10 countries reporting Android malware, Saudi Arabia and India topped the charts. We note some trends in the kinds of apps being targeted for repackaging or trojanizing, and highlight characteristic features of such modified packages. We examine third-party app stores to see how likely users are to encounter malicious packages on such sites, and examine how vulnerabilities are likely to be introduced into an Android device.

We profile the most common vectors used to deliver malware to a user's device and find that unsurprisingly, web-based channels are most often used, with a strong emphasis on exploits targeting the Java development platform. This also coincides with the topmost threat type in our top 10 detections for this period – web-based attacks.

And finally, on the Mac platform, we saw slight but steady growth of new threats emerging in H2 2013, though this is a very miniscule amount compared to Windows or even Android.

SOURCE

1. F-Secure Weblog; Mikko Hypponen; *Possible Governmental Backdoor Found ("Case R2D2")*; published 8 October 2011; <http://www.f-secure.com/weblog/archives/00002249.html>

CONTENTS

THIS THREAT REPORT HIGHLIGHTS TRENDS AND NEW DEVELOPMENTS SEEN IN THE MALWARE THREAT LANDSCAPE BY ANALYSTS IN F-SECURE LABS DURING THE SECOND HALF OF 2013. ALSO INCLUDED ARE CASE STUDIES COVERING SELECTED NOTEWORTHY, HIGHLY-PREVALENT THREATS FROM THIS PERIOD.

CONTRIBUTING AUTHORS	FOREWORD	3
BRODERICK AQUILINO	EXECUTIVE SUMMARY	4
KARMINA AQUINO	CONTENTS	5
CHRISTINE BEJERASCO	H2 2013 INCIDENTS CALENDAR	6
EDILBERTO CAJUCOM	IN REVIEW	8
SU GIM GOH	OF NOTE	11
ALIA HILYATI	GOVERNMENTAL TROJANS	12
MIKKO HYYKOSKI	THE END IS HIGH?	13
TIMO HIRVONEN	SHARKING	14
MIKKO HYPPONEN	CASE STUDIES	15
SARAH JAMALUDIN	FOCUS ON ASIA	16
CHOON HONG LIM	MORE ON MEVADE	17
ZIMRY ONG	EXPLOIT KITS	20
MIKKO SUOMINEN	ALL ABOUT ANDROID	22
SEAN SULLIVAN	THE STATE OF WEB PRIVACY	30
MARKO THURE	PROFILING INFECTION VECTORS	33
JUHA YLIPEKKALA	MAC MALWARE	35
	SOURCES	36

H2 2013 INCIDENTS CALENDAR

HACKS & ESPIONAGE

NSA

Sep

Lawsuits lead to publication of FISC court order

Secret court order authorized 'novel use' of existing tech for NSA data trawling

Oct

NSA reportedly collects e-mail & IM contacts lists

Contacts from e-mail and IM services intercepted during transit over global data links

Oct

Reports of NSA snooping angers multiple countries

France, Germany and other countries protest excessive surveillance of their citizens

Nov

NSA said to intercept intra-data center traffic

'Muscular' program intercepted unencrypted traffic between tech giant's data centers

Sep

GCHQ allegedly hacked into Belgian telco

Report of hack in Germany's *Das Spiegel* prompts inquiry into incident in Brussels

Oct

Source code & passwords stolen in Adobe site breach

Source code for multiple Adobe products stolen, as well as login details for Adobe site users

Oct

vBulletin site breach exposes customer details

Breach of forum software makers' site exposes customer info, including passwords

Nov

Massive internet traffic diversions spotted

Rerouting sends data through Belarus or Iceland, researchers uncertain who, how or why

SECURITY & ENFORCEMENT

Jul

FBI charges 5 for 'top US cyber hacks in last 7 years'

5 charged for massive thefts of credit card details from US retailers and banks

Aug

Russia jails ChronoPay owner for hiring botnet

Judge hands 2.5 years in penal colony to Pavel Vrublevsky for cyber-attack attempt on rival

Oct

Silk Road drug site closed, operator arrested

FBI charges US defendant with drug trafficking and money laundering

Oct

BlackHole & Cool exploit kits creator arrested

Russia arrests 'Paunch', creator/operator behind two most prevalent exploit kits in the wild

Aug

M'soft patches bugs detailed at CanSecWest

Sep

iOS7 launches with new security features

Nov

M'soft issues Fix-it for 0-day CVE-2013-3906

Sep

EU Civil Liberties committee debates US surveillance

Committee begins examining issues surrounding US surveillance of EU citizens

Sep

RSA drops 'NSA-related' encryption algorithm

RSA Security warns customers to drop encryption suspected of being compromised by NSA

Oct

EU passes amendment to data protection laws

Lawmakers increase protection for online privacy; finalization from 28 member states pending

Nov

Microsoft increases bug bounty to USD 100,000

Hopes increased bounty encourages more voluntary submission of bug reports

MALWARE & VULNERABILITIES

July

Janicab backdoor uses RLO twist to disguise itself

Malware uses right-to-left override (RLO) to pretend it's a Word file instead of a program

Aug

Browlock ransomware expands to new countries

Police-themed malware moves from US, UK & Canada into Germany, Italy, and France

Sep

Mevade botnet using TOR to spread adware, malware

C&C commands for widespread botnet leads to spike in traffic on anonymizing network

Oct

CVE-2013-3893 exploited in targeted attacks

Targeted attacks exploit flaw in Internet Explorer; Metasploit module for exploit also released

Jul

Vulnerability similar to 'Masterkey' reported

Chinese researchers report loophole allowing malicious code to be added in file header

Jul

Mobile trojan uses Google Cloud Messaging (GCM)

GCM used by data-harvesting Tramp trojan receive remote commands

Jul

Rogue mobile AV pushed in third-party ads

Fake mobile AV seen being advertised in-app and in ads on mobile browsers

Aug

FinFisher docs claim support for Windows Phone

Mobile spy software claims it runs on multiple platforms, including Windows Phone

The H2 2013 Incidents Calendar lists interesting developments in the field of information security that occurred during the second half of 2013, as reported in various technology news portals, security research publications or sites, major newspapers and the F-Secure Weblog. The source for each item in the calendar is listed on page 36.

Nov NSA allegedly infected 50,000 systems globally Planted software intended to 'enable intelligence collection' from infected systems	Dec NSA reportedly tracking millions of phone calls Data used to track associates travelling with known targets under 'Co-Traveller' program	Dec NSA said to 'piggyback' on Google's cookies NSA & GCHQ reportedly used tracking cookies on Google sites to locate targets	Dec US federal judge rules PRISM 'unconstitutional' Program said to violate 4th Amendment ban on unreasonable search and seizure
Nov Data from Cupid Media hack found on server Data from dating site hack in January found on same server as data from Adobe hack	Nov Bitcoin exchanges become targets for cyberheists Skyrocketing prices for Bitcoin prompt targeted attacks on online Bitcoin wallets	Dec Server storing data stolen by botnet found Pony botnet harvested login details for popular sites from infected systems	Dec Target reports breach of customer data Attackers reported infected POS systems to gather customer details
Nov FBI arrests two brothers for cyberheists Two US brothers charged with theft of millions from accounts in US banks and brokerages	Nov UK gives 10 years to Stratfor hacker UK jails Jeremy Hammond for theft of credit card info from hack of intelligence firm	Nov ICANN shuts down 'Dynamic Dolphin' Domain registration industry's governing body revokes license for spammer-friendly registrar	Dec 13 plead guilty to DoS attack on Paypal Attack launched as protest against Paypal's decision to cut ties with WikiLeaks
Dec Adobe patches Flash & Shockwave issues	Dec M'soft patches 0-day CVE-2013-3906, others		
Nov Tech giants up defenses against NSA snooping Yahoo!, Google, Facebook and others harden systems to block potential NSA intrusions	Nov Facebook notifies users affected by Adobe breach Social networking site asks users with same login details on both sites to change password	Nov EU demands more rights for EU data handled in US EU demands right to redress under US law for EU citizens affected by US surveillance	Dec Microsoft, FBI & others disrupt ZeroAccess botnet Action disrupts contact between US-based infected systems and C&C IP addresses
Nov CryptoLocker ransomware alert issued in US & UK CERT bodies in US and UK issue alert to citizens after seeing increase in ransomware reports	Nov CVE-2013-3906 exploited in targeted attacks Specially crafted Word files exploit flaw in attacks reported in Middle East and South Asia	Dec Rogue 'trusted' certs for Google domains found Fake SSL certificates said to be used by French security agency to spy on private network	Dec Trojan tailored to target poker players reported Malware silently installed on machine shows user's cards during online poker games
Aug Android 'Masterkey' presented at BlackHat Loophole allows editing of app code without affecting cryptographic signature	Aug Masterkey exploit found in multiple apps Apps with exploit targeting recently published 'Masterkey' flaw found in China markets	Sep iOS fingerprint lock bypass reported Hacker group publishes low-tech bypass of iPhone 5S fingerprint scanner	Oct Google pulls apps with aggressive ad library Apps with ad library code-named 'Ad Vulna' pulled from store if library not updated

IN REVIEW

UPDATES IN THE THREAT LANDSCAPE

As we grow more and more accustomed to and dependent on the Internet and its services, the threats to our “connected community” inevitably grow in tandem. According to the statistics we compiled for H2 2013 (based on the anonymized data sent to our cloud-based telemetry systems from our desktop and mobile clients), **web-based attacks** - which typically involve techniques or malware that redirects the web browser to malicious sites - doubled in number during this six-month period, as compared to the first half of the year. Web-based attacks were actually the most commonly reported type of attack, based on our list of Top 10 Detections for H2 2013 (next page). When breaking down these threats to the countries reporting these detections, we saw web-based attacks being reported more frequently in Sweden, France, Finland and Germany.

Though **exploits** are often used to facilitate web-based attacks, we categorize this particular threat type separately due to its significant presence in the top threats. The three most prominent exploit-related detections we observed in H2 2013 were Majava and those that targeted the CVE-2013-2471 and CVE-2013-1493 vulnerabilities. Not coincidentally, all three of these involve vulnerabilities in the Java development platform, which has attained enough popularity among businesses and developers to have also become the defacto target for attackers. This is exemplified by a new entry in our top detections list - the detections identifying exploits targeting the CVE-2013-2471 vulnerability found in certain sandboxed Java Web Start applications and sandboxed Java applet versions.

If we combine the percentages of these three (19%, 4% and 3%, respectively), Java-related exploits make up the second-most reported threat type in H2 2013, with most reports coming in from the USA, France, Germany and Finland. This is however actually a decline in the amount of Java-related exploits compared to the previous half of 2013, which may be attributed to the October arrest of “Paunch”^[1], the alleged creator of the BlackHole & Cool exploit kits which were responsible for enabling a sizeable portion of the attacks against Java. Since the arrest, the number of reported detections we’ve seen for BlackHole and Cool have sharply declined. Unfortunately, this seems to have simply left a void that new contenders are now squabbling to fill, with other exploit kits such as the **Angler exploit kit** rapidly gaining momentum and market share.

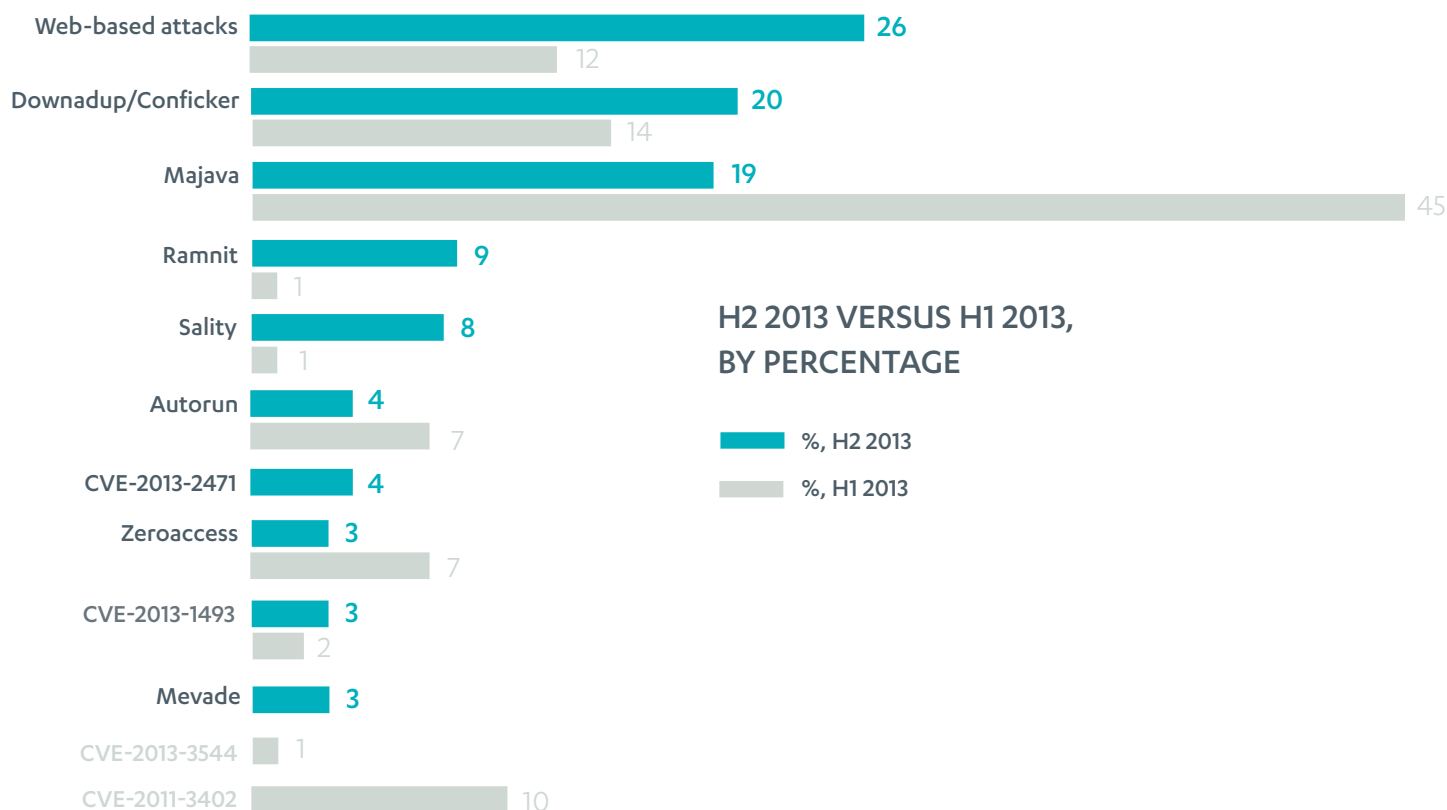
A familiar, still active threat is the worm we identify as **Downadup** (also known in the media as Conficker). Though the worm is fairly long in the tooth, having been first reported in 2008, it still has a tenacious grip on its spot in our Top 10 Detections chart, with very active detection rates being seen in Brazil, followed closely by the United Arab Emirates, and trailed not far behind by Italy.

Downadup’s continued presence may be attributed to ‘environmental factors’: a large number of networks or systems still running old, unpatched Windows operating systems which gives the worm a reservoir of viable habitats, as it were, in which to linger and continue infecting; and possibly the unavailability of skilled, meticulous technical support to completely remove this malware from an infected network, which if not properly performed leads to a chance of reinfection. Machines and networks running older versions of operating systems and business-critical software are, sadly, still not a rarity today, even in most developed countries. This state of affairs is even more widespread in regions such as **Asia**, which as a general rule tends to see far more of the older threats which no longer work against newer or more regularly updated systems.

Other longstanding threats that continue to be active are **Ramnit** (a worm with file infector abilities that was first detected in 2010) and **Salinity** (a polymorphic file infector first seen in 2003). Unlike Downadup, over time these two threats have evolved as other malware authors

TOP 10 DETECTIONS

H2 2013



TOP COUNTRIES FOR TOP 10 DETECTIONS IN H2 2013, BY PERCENTAGE

	France	United States	Sweden	Brazil	Finland	Germany	Netherlands	Italy	Great Britain	Poland	Denmark	Malaysia	Tunisia	India	Turkey	Vietnam	Belgium	Egypt	Pakistan	Romania	Japan	Taiwan	Bulgaria	Canada	Colombia	Indonesia	Mexico	Slovenia	Norway	United Arab Emirates	All other countries
	%																														
Web-based attacks	12	7	18		9	9	6	4	3		4						3													25	
Downadup/Conficker	6			18				7				6								3	2	4		3				4		16	32
Majava	12	20	9		10	9	7	3	5	3	3																				17
Ramnit				3								4	6	12	7	19		6	4	3						4					33
Sality				13						3		9	3	13	12	8		4	2	2											30
Autorun	12			7						4		10	3	8	5						4	3					4				41
CVE-2013-2471	9	10	13		15	11	7	3	4	5	5																				17
Zeroaccess	22	23	6		4	4	3	3	7		3												3								22
CVE-2013-1493	10	17	13		9	14	7		4		4					3															27
Mevade	32	3	6	5	5	4	6	4	3	5																			4		16

modified and released variants for their own nefarious purposes, so that their persistent presence in our statistics is mainly due to continuous, active targeting by attackers. In H2 2013, both Ramnit and Sality surged up from accounting for only 1% of the top 10 reported detections in the period, to 9% and 8%, respectively. These threats were most active in Vietnam, India, Turkey and Brazil.

Trending in the opposite direction are detections related to the **ZeroAccess** botnet, which went down 4% from H1 to account for only 3% of the top 10 reported detections. This was a precipitous drop from the second half of 2012, when ZeroAccess accounted for fully 27% of the detections reported to our systems. The steep decline of this botnet may be attributable to the disruption exercise conducted by Microsoft's Digital Crimes Unit, the United States Federal Bureau of Investigations and industry partners, which blocked network traffic from and to computer systems based in the United States to 18 known ZeroAccess command and control (C&C) servers - though later research indicates the action may have had less impact than first thought ^[2]. Still, subsequent observation of the botnet's activities ^[3] indicate that it is no longer being actively pushed by its operators, leading to its current shriveled state. The small trickle of ZeroAccess detections we still see are mostly in France, the United States and the United Kingdom.

Another newcomer to the Top 10 Detections list is **Mevade**. Though the threat itself is not new (it was first seen in late 2012), this is the first time it has featured in the top threats list, accounting for 3% of reported detections and most active in France, followed by Sweden and Netherlands. This botnet is noted for being the first to extensively utilize the Tor anonymizer network to hide its traffic. This means that a tactic like *sinkholing*, where network traffic is routed to an IP address controlled by a system administrator, security researcher or other benevolent party to trace and counter botnets, is ineffective. It also makes taking down the botnet really difficult, if not impossible.

The most common **infection vector** for malware to reach users continues to be the Internet, which includes such channels as malware forcibly downloaded on a visitor's machine by an exploit kit, malicious advertising (malvertising), tainted software bundles from share sites and of course, from malicious sites. In addition, for those concerned about **web privacy**, the widespread use of tracking cookies, scripts and other user-tracking techniques means that even successfully preventing a malicious download may not be enough to prevent loss of their personal data.

For mobile platforms, the continued dominance of the **Android** operating system makes it almost the exclusive target for mobile threats we've seen this period. Though the relatively low number of vulnerabilities found in Android makes the operating system itself difficult to attack, this security is largely circumvented by the relative ease with which malware authors can provide their 'products' and dupe users into installing it on their own devices, with the necessary permissions to straightforwardly use the device (and the user's data) for the attacker's own benefit. Of the top 10 Android malware detections reported to our systems in H2 2013, more than 75% of the reports originated from Saudi Arabia and India. The Android malware families most commonly reported in that period were GinMaster, Fakeinst and SmsSend, which either harvest data from the device or send premium-rate SMS messages.

And finally, when it comes to threats on the **Mac** platform, we saw slight but steady growth with 18 new threats emerging in H2 2013, though this is a very miniscule amount in comparison to Windows or even Android. 83% or the majority of these new entrants are backdoors, with rootkits and trojans making up the remaining percentage.

SOURCES

1. Krebs on Security; Brian Krebs; *Meet Paunch: The Accused Author of the BlackHole Exploit Kit*; published 6 December 2013; <http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/>
2. Arstechnica; Sean Gallagher; *Microsoft disrupts botnet that generated \$2.7M per month for operators*; published 7 December 2013; <http://arstechnica.com/security/2013/12/microsoft-disrupts-botnet-that-generated-2-7m-per-month-for-operators/>
3. Naked Security by Sophos; James Wyke; *Have we seen the end of the ZeroAccess botnet?* published 7 January, 2014; <http://nakedsecurity.sophos.com/2014/01/07/have-we-seen-the-end-of-the-zeroaccess-botnet/>

OF NOTE

GOVERNMENTAL TROJANS

12

THE END IS NIGH?

13

SHARKING

14



GOVERNMENTAL TROJANS

WE WILL DETECT IT

In late October 2013, F-Secure, along with many other antivirus companies, received a letter from Dutch digital rights organization Bits of Freedom, who together with a coalition of other similar bodies and interested academics requested a formal clarification on company policy related to detecting programs created and distributed by governments, law enforcement agencies and other state entities. Below is an excerpt of the original information request and the full text of the reply sent by F-Secure CEO Christian Fredrikson on 1 November 2013.

EXCERPT OF REQUEST

“Several governments are planning to grant or have granted law enforcement with the authority to remotely break into computers, both foreign and domestic, in order to conduct surveillance in the course of investigations. In order to adequately breach the security of users' personal computers, law enforcement agencies must exploit vulnerabilities in users' software and install malware that will collect data from the targeted computers.

As a manufacturer of anti virus software, your company has a vital position in providing security and maintaining the trust of internet users as they engage in sensitive activities such as electronic banking. Consequently, there should be no doubt that your company's software provides the security needed to maintain this trust.

The consumers and companies whose systems you protect should be able to rely on the detection and removal of viruses and malware, regardless of their origin. Therefore, we would like to ask you to clarify your policy on this subject. More precisely we would appreciate a response to the following questions:

1. Have you ever detected the use of software by any government (or state actor) for the purpose of surveillance?
2. Have you ever been approached with a request by a government, requesting that the presence of specific software is not detected, or if detected, not notified to the user of your software? And if so, could you provide information on the legal basis of this request, the specific kind of software you were supposed to allow and the period of time which you were supposed to allow this use?
3. Have you ever granted such a request? If so, could you provide the same information as in the point mentioned above and the considerations which led to the decision to comply with the request from the government?
4. Could you clarify how you would respond to such a request in the future?

F-SECURE'S RESPONSE

F-Secure Corporation is happy to see that Bits of Freedom (and the rest of the parties behind this information request) are raising awareness on this very important topic. Furthermore, F-Secure is proud to answer these questions, as we have held a very strong position on these issues.

Our answers are:

1. **Yes, we have detected governmental malware used by law enforcement (such as the R2D2 trojan used by German government).**
2. **No**
3. **No**
4. **If we would be approached by a government asking us not to detect a specific piece of malware, we would not comply with their request. To us, the source of the malware does not come into play when deciding whether to detect malware. If it's malware, we will protect our customers from it. Our decision-making boils down to a simple question: would our customers want to run this program on their system or not. Obviously the answer for governmental trojans would be "No".**

We would also like to point out that our policy on this has not changed since we announced it in 2001. It can be viewed at http://www.f-secure.com/en/web/labs_global/policies.

SOURCE

1. F-Secure Weblog; Mikko Hypponen; *F-Secure Corporation's Answer to Bits of Freedom*; published 6 November 2013; <http://www.f-secure.com/weblog/archives/00002636.html>

THE END IS NIGH?

Microsoft's Windows XP operating system reaches its end of extended support period on April 8th of this year. And after that? No more public system updates. No more public security updates. Users will be on their own. But XP is still a very popular OS – or at least it is prevalent (see other sections of this report for details).

Elsewhere in this report are detection statistics which highlight two very serious threats to Windows users: web-based attacks and Java-based attacks. And Windows XP is particularly an issue because once compromised – it is much more difficult to repair than its siblings. An ounce of prevention is really worth more than a cure in the case of XP.



Prediction: the April 8th “deadline” will be picked up by the mainstream press as a type of “Y2K” apocalypse waiting to happen. And when nothing happens on April 9th? The press will again publicly question what all the fuss was about. Meanwhile, in the tech press... reporters will be patiently waiting for the first critical post-XP vulnerability. When (not if) a powerful zero-day exploit makes its way to market – that’s when the real concerns begin and important questions will be asked. Can XP be trusted?

But all is not lost. Patching XP is not the first line of defense. Or it really shouldn’t be.

Some businesses will continue to use Windows XP throughout 2014, either due to contractual obligation, or because their customers do so and they need XP to provide support. In those situations, IT managers have their work cut out for them. Air gapping systems or isolation to separate networks from critical intellectual property is recommended. Businesses should already be making moves such as this for “Bring Your Own Device” (BYOD) users. XP is just another resource to manage.

Folks that continue to use XP at home can do so with some reasonable amount of safety, for a while still, but they absolutely need to review their Internet (particularly web browsing) and computing habits:

1. Install Windows XP’s final update.
2. Install an alternative browser or browsers (they’re free!) — don’t rely solely on Internet Explorer. And don’t use Internet Explorer as the default.
3. If installed, make sure Microsoft Office is fully patched. Note that older versions of Office will run things such as Flash by default if embedded in documents. If using an older version of Office, tighten up the security options. Don’t open documents from sources you don’t trust.
4. Review the third-party software you’ve installed and uninstall anything that isn’t needed. If you’re going to keep XP, do a “spring cleaning” and get rid of old software. Because old software very often equals vulnerable software.
5. For the third-party software that you keep – consider disabling or uninstalling the browser plugins. Set the browser to “always ask” what to do about things such as PDF files.
 - a. Do you need Java installed on your home laptop? Probably not.
 - b. Advanced browser features include “click to play” options. They’re worth the extra effort.
6. Have an up-to-date security product with antivirus and firewall installed.
7. Keep your XP computer connected to a NAT router, at home, which will act as a hardware firewall. (Practically speaking, this means you shouldn’t be roaming connecting your laptop to free Wi-Fi hotspots – keep your computer at home on a trusted network.)
8. And finally... consider upgrading your OS. If you don’t want Windows 8 – there’s always Windows 7. The OEM installation is still available from many fine online retailers.

SHARKING

HIGH-ROLLERS IN THE CROSSHAIRS

In the Labs, we get a lot of samples, with most of them being submitted online. Every now and then though, someone visits one of our Labs to bring their computer in for forensic analysis.

In early September last year, a guy in his early 20's pulled up and parked his Audi R8 just outside our Helsinki HQ. His name was **Jens Kyllönen**—a professional poker player both in real world tournaments and in the online poker world. He's a high-roller by any measure, with wins in the range of EUR2.5 million in the past year. So why would this poker star go out of his usual routine to drop by for a visit? This is his story.

Last September, Jens participated in a poker tournament held in a 5-star hotel in Barcelona. He spent the day at the tournament and during a break, went up to his room to find his laptop missing. On returning to the room after alerting the hotel, the laptop had 'reappeared'—but now wasn't booting right. He suspected something was amiss.

Thinking his laptop might have been compromised, Jens asked us to analyze it, so we made full forensic images and started digging. Soon, it was obvious his hunch was correct—the laptop was indeed infected, by a **Remote Access Trojan (RAT)** with timestamps coinciding with the time when the laptop had gone missing. An attacker had evidently installed the Trojan from a USB memory stick and configured it to start automatically at every reboot. The RAT allows an attacker to remotely view anything displayed on the laptop—including seeing the victim's hand in online poker games (see illustration at right). The malware uses obfuscation, but isn't all that complicated. Since it's written in Java, the RAT can run on any platform (MacOS, Windows, Linux). This kind of attack is very generic and works against any online poker site we know.

After analyzing Jens's laptop, we started looking for other victims. It turned out yet another professional player, **Henri Jaakkola**, who stayed in the same room as Jens at the event, had the exact same Trojan installed in his laptop.

This isn't the first time professional poker players have been targeted with tailor-made Trojans; we previously investigated several cases in which malware was used to steal hundreds of thousands of euros. What makes these cases noteworthy is that they were not online attacks—the attacker took the trouble of targeting the victims' systems on site. The phenomenon is now big enough to warrant its own name: **Sharking**—targeted attacks against professional poker players (colloquially known as 'poker sharks'). It's similar to *whaling attacks* which are targeted against upper business managers.

HOW IT WORKS



The normal view of the online poker game, as seen by the attacker (cards at the front of the screen).



The RAT shows the attacker the cards being held by the infected machine's user (in this case, two Queens). This gives the attacker a strategic advantage in the poker game.

So, what's the moral of the story? If you have a laptop that is used to handle large sums of money, **keep it secure**. This advice is true whether you're a poker pro using a laptop for online matches or a business controller in a large company wiring large funds around the world.

CASE STUDIES



FOCUS ON ASIA	16
MORE ON MEVADE	17
EXPLOIT KITS	20
ALL ABOUT ANDROID	22
THE STATE OF WEB PRIVACY	30
PROFILING INFECTION VECTORS	33
MAC MALWARE	35

FOCUS ON ASIA

As Asia develops by leaps and bounds, we've noticed a corresponding increase in malware detections being reported to our cloud-based systems from the region. In this report, we cover some trends seen in the statistics we compiled from malware detections reported in H2 2013 from Japan, Malaysia, Taiwan, Hong Kong, the Philippines and India.

DOWNADUP LINGERS ON

Of note is the worm we identify as Downadup (also known as Conficker in the media), which continues to be a stand-out presence in infections reported from this region, particularly in Malaysia, where the worm tops the charts. We also see a high number of Conficker infections reported in the Philippines and Taiwan. The malware's continued presence in our statistics for Asia is rather surprising, since Conficker is more than 5 years old. Microsoft warned users of the vulnerability the worm exploited in October 2008 and released an out-of-band security patch to close the loophole shortly thereafter. The continued prevalence of the worm in this region points to the possibility that in Asia at least, there are still many Windows XP systems running without these patches.

MAILCAB INFECTIONS

In Taiwan, an ancient macro virus we identify as X97M.Mailcab tops the charts as the most detected infection in that country in H2 2013. First seen in late 2012, Mailcab spreads in infected Microsoft Excel workbooks, which are distributed as e-mail file attachments. Once opened, the malicious file lowers the security settings for the Office suite, then mails copies of itself to contacts listed in messages in the Outlook e-mail client (a worm-like characteristic).

The continued presence of Mailcab in any significant number is rather surprising since macro viruses and worms (like Conficker), which were once more common, have in recent years become much reduced threats as software developers introduced security features that prevented them from infecting files or spreading as wildly as they once did. Mailcab's appearance in the statistics indicates that in Asia, older versions of business-critical programs are still in widespread use.

MOBILE

Meanwhile in India, with the availability of cheaper Android smartphones and wireless broadband, mobile detections have become particularly prominent in the statistics we see being reported from the subcontinent. Though the vast majority of the detections related to potentially unwanted applications (PUA), which are of relatively little concern, the most common malicious program we see being reported in the country is Trojan:Android/GinMaster. This malware is distributed in a trojanized app and when installed, uses an exploit to install additional applications on the device and steal information.

As with most Android apps we identify as malware, these programs are mainly distributed through third-party app stores.

More generally, India continues to report a wide range of detections that were once more common but have, in most countries, become almost extinct. Specifically, variants in the Salty, Ramnit and Autorun families (a polymorphic file infector, a worm with file infection capabilities and a worm, respectively) are prominently featured in the country's statistics. Again, these threats were addressed years ago by the developers of affected software, and their continued presence in the country points to an abundance of machines running older, un-updated software.

JAVA

As for Japan, in H2 2013 we noticed a decline in Java-targeted exploits which were prevalent in the first half of 2013, especially those identified by the Majava detection family. Most enterprises run Java, which powers many of their in-house applications and legacy systems. At the time, hackers were targeting unpatched Java environments, aided by a climate in which vulnerability after vulnerability was being announced in rapid succession by Oracle. With the recent drop in Java-related detections however, we are inclined to think that many of the environments using Java, or its plug-ins, have been patched by now.

WINDOWS XP

And finally, on the topic of desktop computers, Windows XP continues to be the software of choice amongst personal and business computer users, currently constituting about 30% of all PC users^[1]. The majority of these are in Asia, where piracy is still rampant. It is also noteworthy that according to Bloomberg BusinessWeek^[2], as many as 90% of all ATM machines are still running Windows XP.

Microsoft recently announced that Windows XP will reach its end of life (EOL) on April 8th, 2014. What that means to XP users is that there will be no new security updates, non-security hotfixes, no support options or online technical content updates available. To be protected, users are urged to upgrade their operating system to the latest Windows version, either 8.1 or at least Windows 7, both of which currently have far fewer known vulnerabilities and a better security framework than XP.

SOURCES

1. Net Applications; *Desktop Operating System Market Share (January, 2014)*; <http://www.netmarketshare.com/operating-system-market-share.aspx>
2. Bloomberg BusinessWeek; Nick Summers; *ATMs Face Deadline to Upgrade From Windows XP*; published 16 January 2014; <http://www.businessweek.com/articles/2014-01-16/atms-face-deadline-to-upgrade-from-windows-xp>

MORE ON MEVADE

Mevade was one of the most prevalent malware families in the second half of 2013, accounting for about 3% of our total malware detections during that period. However, Mevade is not exactly new to the malware scene. A variant formally bearing the family name was first seen by our systems back in December 2012, and researchers from Fox-IT have linked the malware to even earlier strains that dated back to as early as 2009 based on related detection names. They also attributed the sudden influx of Tor users seen at the end of August 2013 to this malware^[1].

Mevade has spawned several variants since then, each with varying functionalities. Our detection statistics show that the most prevalent variant is the downloader, which accounted for roughly 97% of all Mevade detections. Strings in this variant's

Figure 1: Module name in downloader component

sample (Figure 1) suggest that it is just an updater component that also serves as an installer rather than a stand-alone variant. This finding supports the number in our statistics as other components should not have been able to infect the system once the installer is blocked. The strings also match with the cover employed by the trojan, which is an update service for Adobe Flash Player (Figure 2).

The updater component continuously polls its command and control (C&C) server for installation instructions. The request can be seen in the following format:

- `http://{SERVER}/updater/{UUID}/{VERSION}`

{UUID} is a unique identifier for the infected host that is derived from the machine GUID (HKLM\Software\Microsoft\Cryptography) and the volume serial number, while {SERVER} is selected from a list of domain names that is hardcoded in the malware (Table 1).

Table 1: Domain names hardcoded in the downloader component

svcupd[dot]net	updsvc[dot]com
srvupd[dot]com	updsvc[dot]net
srvupd[dot]net	updsrv[dot]net

If this is only the updater component, then what about the actual payload? As of this analysis, none of the domains are resolving to a host. However, there is a feature in F-Secure

products that can see the history of a file in the system. From this, we saw that the component has installed other Mevade samples, specifically the variants that use Tor.

accounted for more than 80% of the remaining variants (Figure 3). The top-2 samples were both compiled on 1st September 2013, while the third sample was compiled on 23rd August 2013.

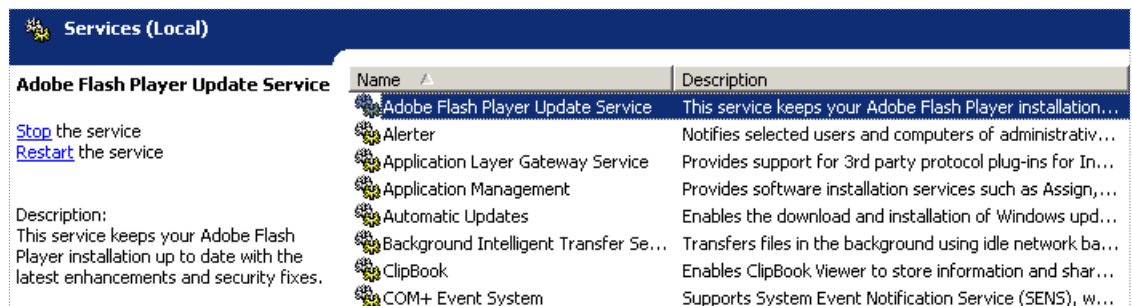


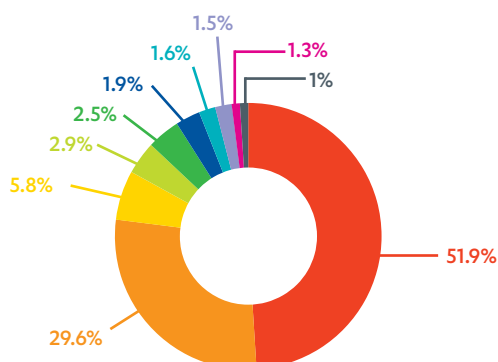
Figure 2: Mevade posing as a Flash Player update service

As mentioned earlier, these variants install a Tor client to the systems. For those unfamiliar with Tor, it is a virtual sub-network on the Internet where members are anonymous to one another. It is usually used as a transit network for users to anonymize themselves when visiting other servers on the Internet.

Another less popular usage of Tor is to host hidden servers inside the virtual network itself. Hidden here means that the servers are unreachable from the Internet without the Tor client. It also means that the servers would be physically untraceable, making it the perfect place for criminals operating illegal services to hide from law enforcers without needing to go offline. This is also where the authors of Mevade have chosen to host their C&C servers, hence the need to install a Tor client.

It is common for security researchers to work with domain name registrars to change records of domain names associated with botnets, and redirects them to servers controlled by the

MEVADE'S SAMPLE DISTRIBUTION



HASHES OF NON-DOWNLOADER SAMPLES

- 60e3e4227497ad83885e859903cb98d769ed9b9c
- 12df7f18c8b07e2fa955e58427c5a52ac3b785e6
- edc7a434f18424d73c1403a15ee417bd59eea95
- 86adb7af4d1a582dfd021c9521d0c2d50d5354f
- 014ace48897e81052b9552a5a7ab04d00a8e5227
- 85bd27ba64a150536fc42445df9efae775c52c8c
- 669c1e6857c541160906e8fb89a5f708b7fa2c50
- c79cef4ae59b5a304bfa0b05b8bf2d1a8f0b81b8
- 127cb991ca9908e71e231ab0be9318c1cde818bd
- 9c9c3a26f7876b9a7e633ea5c72ee57c52e82f5a

Figure 3: Non-Downloader Mevade Sample Distribution

MEVADE'S SETUP

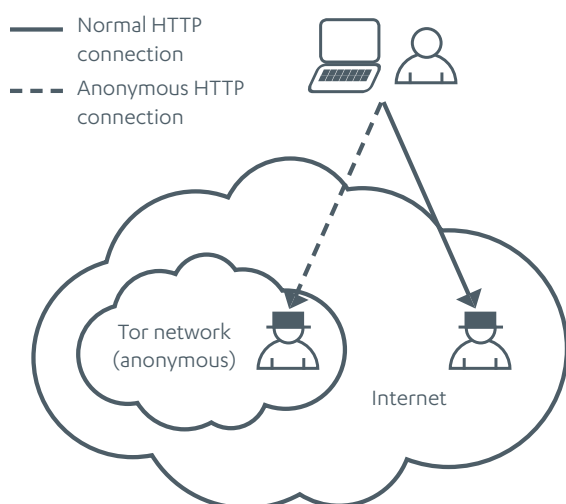


Figure 4: Mevade's command and control setup

researchers instead. This process is called *sinkholing*, and is done to study, measure and disrupt botnets. However, servers in the Tor network use domain names that are just pseudo names derived from secret keys that only the server operators have access to. These names are totally unrelated to the domain names on the Internet. Without the secret keys, it is impossible to operate these pseudo domain names. With that being said and given the anonymous nature of the Tor network, the botnet is theoretically immune to sinkholing and takedowns.

In addition to the servers in the Tor network, we found a couple of variants (compiled after 14th September 2013) that also use normal HTTP servers for their C&C servers^[2,3]. **Figure 4** summarizes the malware's command and control setup, while **Table 2** and **Table 3** list down the domain names hardcoded in the malware.

Table 2: Pseudo domain names of Mevade's C&C servers in the Tor network

pomyeasfnmtn544p[dot]onion	wsytsa2omakx655w[dot]onion
ijqqxydixp4qbzce[dot]onion	lqqth7gagyod22sc[dot]onion
7fyipi6vxyhpeouy[dot]onion	lorpzyxqscsmcx[dot]onion
onhiimfoqy4acjv4[dot]onion	mdyxc4g64gi6fk7b[dot]onion
6tlpoektc3gudt3[dot]onion	ye63peqbnm6vctar[dot]onion
qxc7mc24mj7m4e2o[dot]onion	7sc6xyn3rrxtknu6[dot]onion
lqqciuwa5yzxewc3[dot]onion	l77ukkijtdca2tsy[dot]onion

Table 3: Normal domain names of alternate Mevade's C&C servers

angelikajongedijk[dot]no-ip[dot]biz
stuartneilseidman[dot]dyndns[dot]pro

One feature of Mevade not usually found in other malware is its ability to share files across the Kad peer-to-peer network. This instance is not the first time where a malware makes use of the Kad network. The notorious TDL malware is known to send and receive commands through the Kad network^[4] for resiliency against takedowns. However, Mevade has not displayed a similar capability yet. For now it seems that the malware only communicates with its C&C servers via HTTP. This applies to both the servers located in the Tor network and those that are not. A summary of the malware's communication with the servers can be seen in **Table 4**.

Table 4: Command and control summary

LOCATION	DESCRIPTION
http://{SERVER}/data	Where the malware downloads the list of peers in the Kad network
http://{SERVER}/cache	Where the malware reports statistical data
http://{SERVER}/policy	Where the malware gets its commands

The days when malware was written by hobbyists have long passed. These days, malware is written with very specific motives. But in the case of Mevade, it is difficult to determine its purpose just by looking at the samples. None of the C&C servers in the Tor network are online as of this analysis; none of the normal HTTP C&C servers are returning a valid response. Based on the malware's supported commands (Table 5), the botnet operators can practically do anything they wanted on the infected system.

Table 5: Supported commands

update	execute
mirrors	share
update-config	

We could only speculate based on the strings found in the samples. The malware authors seem to have chosen “adw” (Figure 5) to name one of the main modules. The name sounds like “adware,” which may suggest that the malware was created with the intention to monetize through installations of third party adware. Or perhaps it was conceived for that purpose, but has since expanded to monetization through pay-per-install schemes.

The C&C servers are unusually quiet for a botnet of this size. It seems as if the operators are waiting for the right buyers as of the time of this analysis. Of course there is the possibility that

the servers have already been sinkholed or taken down, but as discussed earlier, this is unlikely since it would be very hard if not impossible to have achieved that, at least for those in the Tor network.

A more likely possibility is that the operators of the botnet have utilized or leased out the computing power of the infected machines by installing Bitcoin mining software. Researchers have discovered that some domains that are historically related to those used by Mevade are being used in Bitcoin mining activities^[5]. Bitcoin mining has become one of the favorite monetization techniques for malware since the value of Bitcoin shot up exponentially in 2013^[6]. It also provides a less intrusive approach to making money from botnets; therefore, less likely for infected users to notice and remove the malware.

Figure 5: Module name in main component

SOURCES

1. Fox-IT; ydklijnsma; *Large botnet cause of recent Tor network overload*; published 5 September 2013; <http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/>
2. Sample; sha1 hash: e17eeb872c12ce441ff29fc3ab21d74b008c70f5
3. Sample; sha1 hash: 8a5f79e405844ebbb41b417d8a2e0c9759d6a6dd
4. About.com, Mary Landesman; *TDSS aka TDL: A Botnet Framework*; <http://antivirus.about.com/od/virusdescriptions/p/Tdss-Aka-Tdl-A-Botnet-Framework.htm>
5. AnubisNetworks Blog, João Gouveia and Martijn Grooten; *UnknownDGA17: The Mevade connection*; published 7 November 2013; <http://www.anubisnetworks.com/unknowndga17-the-mevade-connection/>
6. Bloomberg, Olga Kharif; *Bitcoin Tops \$1,000 as Virtual Money Gains Popularity*; published 28 November 2013; <http://www.bloomberg.com/news/2013-11-27/bitcoin-surges-to-1-000-as-virtual-money-gains-wider-acceptance.html>

EXPLOIT KITS

THE NEW CONTENDER

In the second half of 2013, we were presented with the biggest news yet in the exploit kit threat landscape—the arrest of Paunch, the alleged creator and distributor of the Blackhole exploit kit^[1]. The effect of this news was evident in our telemetry. Paunch's arrest took place in October and in the same month, we saw a drop in both Cool and Blackhole infections (see Figure 1). However, we also witnessed the rise of three other kits—Angler, Styx, and Nuclear (see Figure 2)—which might be trying to capitalize on Paunch's arrest.

The Reveton gang, known to be using the Cool exploit kit, was noted to be quick to act and move on to a new kit. According to security researcher Kafeine, Reveton was being pushed by the Whitehole exploit kit just a few hours after the news broke. A day later, Kafeine noted that the Reveton gang had started using Angler. It seemed that a replacement for Cool has been found.

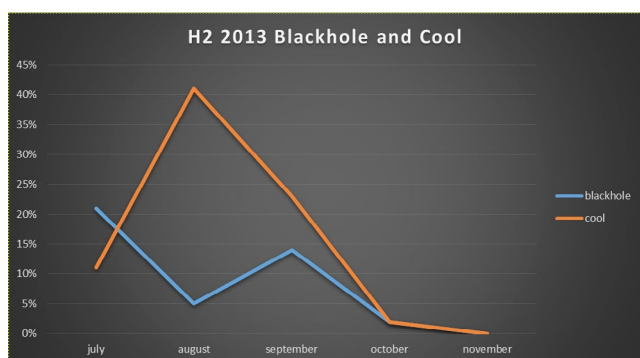


Figure 1: A drop in Blackhole and Cool infections

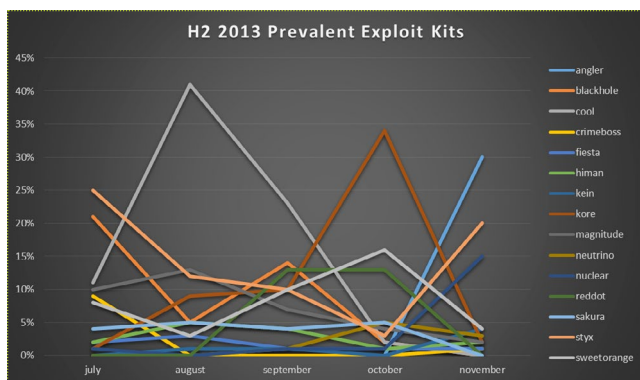


Figure 2: Angler, Styx and Nuclear infections rising

The Angler exploit kit was first seen in our telemetry during the last week of September. It is usually distributed via malvertising.

LANDING PAGE AND URL PATTERN

Angler's URLs have so far been following a rather straightforward format, making them identifiable. Some examples of the URLs include:

- [http://ku\[...\]va.da\[...\]in.ca/se2v9pa2gx](http://ku[...]va.da[...]in.ca/se2v9pa2gx)
- [http://tn\[...\]ig.pi\[...\]et.com/s6u9qe8qtk](http://tn[...]ig.pi[...]et.com/s6u9qe8qtk)
- [http://ha\[...\]an.na\[...\]lq.com/m2b3hvvvg2n](http://ha[...]an.na[...]lq.com/m2b3hvvvg2n)
- [http://je\[...\]ne.ma\[...\]ne.com/1gi0tjg36m](http://je[...]ne.ma[...]ne.com/1gi0tjg36m)
- [http://ve\[...\]at.xa\[...\]ls.com/gwxywna71f](http://ve[...]at.xa[...]ls.com/gwxywna71f)

The landing page has notable characteristics as well. Initially, the title of the landing page was "Gmail." Then, it was changed to "Microsoft apple.com." In December, the title was changed again to "Microsoft apple.com" (notice the missing "o") (see Figure 3).

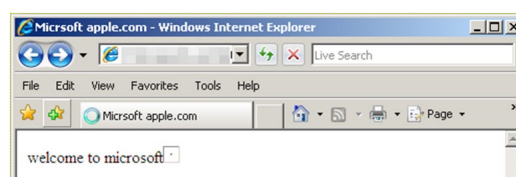


Figure 3: Landing page title changed to "Microsoft apple.com"

Another distinguishable characteristic in the landing page is the use of window object properties as flags for vulnerable plugins. All the properties have a common prefix that the kit authors updated every now and then. For example, in mid-November, the prefix was "sterling" and the properties were *window.sterlingj*, *window.sterlingf*, and *window.sterlings* to indicate the presence of a vulnerable version of Java, Flash, and Silverlight, respectively. At the end of December, the prefix was switched to "zitumba."

F-Secure detects the landing page as **Exploit:JS/AnglerEK.A**.

EXPLOITS

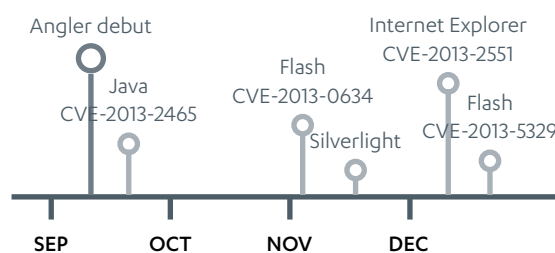


Figure 4: Angler vulnerability support

Internet Explorer

An Internet Explorer exploit against CVE-2013-2551 was added to Angler in December 2013. The vulnerability was demonstrated by VUPEN during the Pwn2Own competition in CanSecWest 2013 that took place in March 2013. Microsoft then patched the vulnerability in May 2013.

F-Secure detects the CVE-2013-2551 exploit in Angler as **Exploit:JS/AnglerEK.A**.

Java

When Angler first appeared in September 2013, it included just one exploit, which was targeting the Java vulnerability CVE-2013-2465. The vulnerability had been patched in the Java 7 update 25, released in June 2013.

In December 2013, Angler was found to be still exploiting the same Java vulnerability. There was, however, one interesting detail in how the exploit was served—the JAR is compressed using gzip and Pack200, a compression method specially optimized for JAR archives. Angler was the first (and currently the only) exploit kit to utilize Pack200.

F-Secure detects the Java exploits in Angler as **Exploit:Java/CVE-2013-2465.A** and **Exploit:Java/Majava.J**.

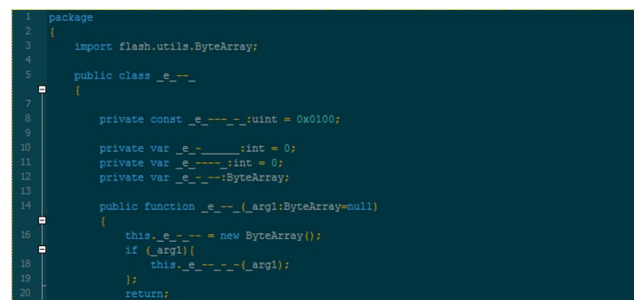
Flash

The first Flash exploit was added to Angler in November 2013. It exploited the vulnerability CVE-2013-0634 that had been patched in February 2013.

The Flash exploit utilizes encryption and obfuscation in various ways. The outer layer of the exploit decrypts an embedded Flash with a single-byte XOR key and loads it. Most of the method, class, and variable names of the inner Flash have been obfuscated to names such as `_e_----`, `_e_--_`, and `_e_--_` (see **Figure 5**). In addition, the most important strings have been encrypted with AES128. The strings are decrypted on-the-fly using the decryption key stored inside. For example, the regular expression string that would trigger the vulnerability is stored in AES128 encrypted form.

In December 2013, Angler added a support for the Flash vulnerability CVE-2013-5329 that was patched in November 2013. Angler was the first kit to exploit the said vulnerability. At the same time, the Flash file still includes the exploit for CVE-2013-0634.

The encryption of the outmost layer has been updated from single-byte XOR to RC4. Instead of simply storing the encryption key in Flash and then loading it, the key is set byte by



```

1 package
2 {
3     import flash.utils.ByteArray;
4
5     public class _e_----
6     {
7
8         private const _e_--_uint = 0x0100;
9
10        private var _e_--_int = 0;
11        private var _e_--_int = 0;
12        private var _e_--_:ByteArray;
13
14        public function _e_--_(_arg1:ByteArray=null)
15        {
16            this._e_-- = new ByteArray();
17            if (_arg1){
18                this._e_--_(_arg1);
19            }
20            return;
21        }
22    }
23 }

```

Figure 5: Obfuscated method, class, and variable names

byte in the ActionScript code at run-time. The exploit authors have also paid special attention to loading the embedded Flash object—they use `flash.system.WorkerDomain.createWorker` method instead of the well-known and more common `flash.display.Loader.loadBytes` method. Moreover, all strings related to loading the Flash object (i.e. class and method names) are protected with AES128 encryption that is decrypted on-the-fly. After the RC4 is decrypted, there are no further obfuscation or encryption layers, and the decrypted Flash contains strings like “attack,” “Shellcode,” and “DoExploit.”

F-Secure detects the Flash exploits in Angler as **Exploit:SWF/Salama.H**.

Silverlight

In November, Angler introduced an exploit against Silverlight, making it the first kit ever to exploit Silverlight. The exploit targeted two different vulnerabilities: CVE-2013-3896 and CVE-2013-0074. CVE-2013-3896 allows the attacker to disclose information about the process memory and use that information to bypass ASLR and DEP. The vulnerability was patched by Microsoft in October 2013. The other vulnerability, CVE-2013-0074 is exploited to run code in the security context of the current user. It was patched by Microsoft in March 2013.

Even though Flash and Java have a significantly higher market share than Silverlight, there are at least two likely reasons why Angler authors added the Silverlight exploit. Firstly, it was easy—a working exploit with full source code had been released on Packet Storm in October 2013. Secondly, there is at least one very popular website that requires Silverlight: Netflix. They have over 40 million subscribers, and they use Silverlight for video streaming.

F-Secure detects the Silverlight exploit as **Exploit:MSIL/CVE-2013-0074.E**.

SOURCE

1. Krebs on Security; Brian Krebs; *Meet Paunch: The Accused Author of the BlackHole Exploit Kit*; published 6 December 2013; <http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/>

ALL ABOUT ANDROID

To no one's surprise at this point, Android continues to be the most targeted mobile operating system, as threats against this platform accounted for 804 new families or variants, or 97% of the new threats we saw by the close of 2013. The remaining 23 new threats seen (3% of the year's total), were targeted against Symbian. No other platform saw any new threats emerge last year. Given the hugely disproportionate attention being directed at the Android platform, in this Threat Report when we consider mobile threats for the second half of last year, we will cover only our research into the threats targeting Android users.

Looking at the detections reported to our cloud-based systems from the users of our mobile security product in H2 2013, the top 10 countries combined saw a little over 140,000 Android malware detections - still a drop in the ocean compared to the number of desktop-related detections reported in the same period. Despite the relatively low total numbers, ongoing developments in the mobile threat landscape are worth noting, as they show how malware authors are busy refining their tactics in order to gain more victims and improve their profit-generating schemes.

Of the top 10 countries reporting Android malware detections to our systems in H2 2013, fully 75% of the reports originated from Saudi Arabia and India; in comparison, the five European countries in the list combined only accounted for a little over 15% of reported detections. Further analysis also gives us a sketchy map of the most common threats faced by users of our mobile product in particular regions or countries (next page). One notable pattern is the wide distribution of the GinMaster trojan family, which appears in the top 3 malware families across the

board in Europe, Asia and the Americas. Almost as prevalent is the large Fakeinst family, which has a near uniform presence in Europe, as does the SmsSend family.

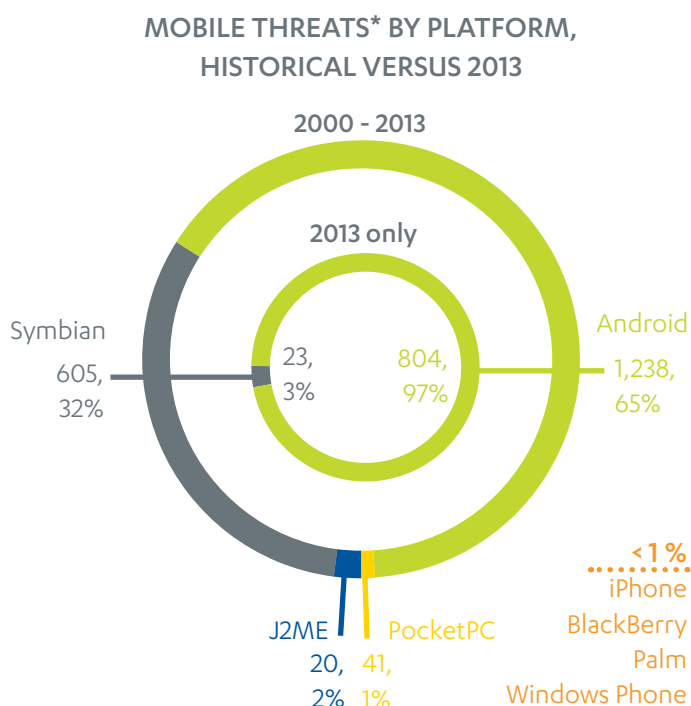
SECURITY ENHANCEMENTS

Despite the extreme focus of malware authors on the Android platform - or perhaps that should be because of - it would be incorrect to say that Google hasn't been actively making efforts to increase the security of the Android platform. Each new version released by the tech giant has included a number of security-related changes that help mitigate the effects of malware. For example, in Android 4.3 (Jellybean), a prompt was introduced to verify activity when the Messaging app sends a large amount of text messages in a short time, a useful measure against apps that silently send hundreds of SMS messages (though reportedly annoying to some users who regularly send group texts). The September release of Android 4.4 (Kit Kat) also included multiple security enhancements - though the removal of the hidden AppOps feature in this version may be interpreted as a step backwards by those who prefer to have greater control over the permissions used by the installed apps.

While the various enhancements released in each update incrementally improve the security of the platform itself, actual per-user security is highly variable, since the fragmented nature of the Android ecosystem between various device vendors makes it basically impossible to ensure a uniform security level across all users. For most users, this means their device security ends up being largely in their own hands - both figuratively and practically.

EXPLOITING THE USERS

Unlike desktop-targeted malware, to date only a handful of Android malware we've seen target actual vulnerabilities in the operating system, most notably the so-called Masterkey vulnerability that was publicly announced in early 2013 (more details on Android vulnerabilities are on page 28). Though a handful of programs were later found in third-party app sites which included an exploit for this vulnerability, they have so far been an exception to the rule. This may be simply because the Android platform has so far had relatively few vulnerabilities - only 7 were publicly announced^[1] in 2013, while the iOS platform has seen 90 vulnerabilities announced^[2] in the same time period. A more cynical hypothesis however would be that malware authors are unlikely to bother with finding complicated ways to exploit the device when they can simply trick the user into giving them access to the device to do their dirty work.

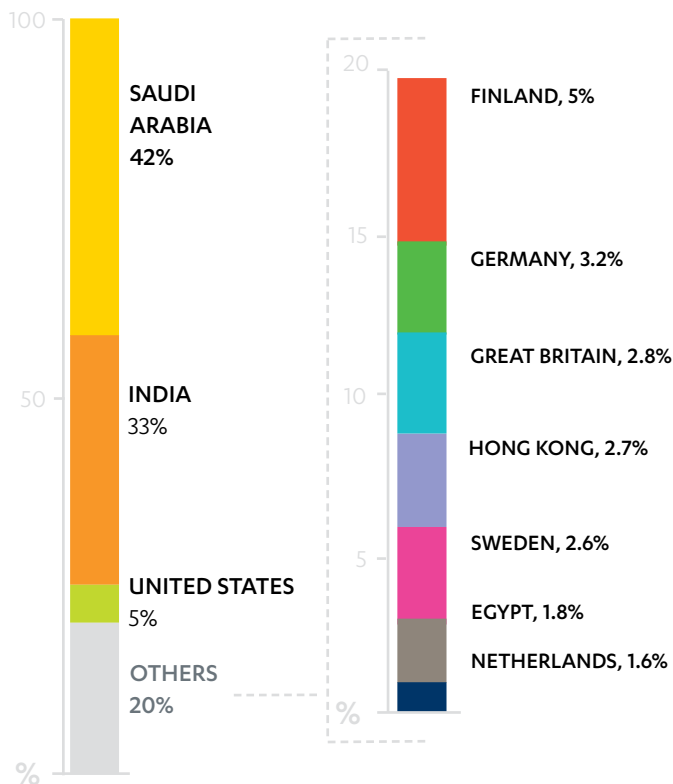


* Count of new families, or new variants of existing families, for all mobile platforms.

SOURCES

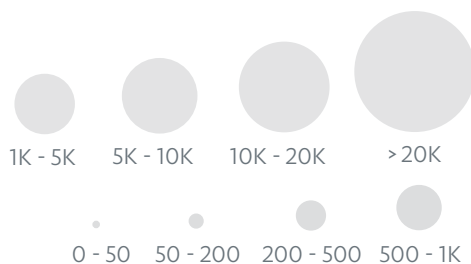
1. CVE Details; Google > Android > Vulnerability Statistics; <http://www.cvedetails.com/product/19997/Google-Android.html>
2. CVE Details; Apple > iPhone Os > Vulnerability Statistics; <http://www.cvedetails.com/product/15556/Apple-iPhone-Os.html>

TOP 10 COUNTRIES REPORTING ANDROID MALWARE DETECTIONS IN H2 2013, BY PERCENTAGE



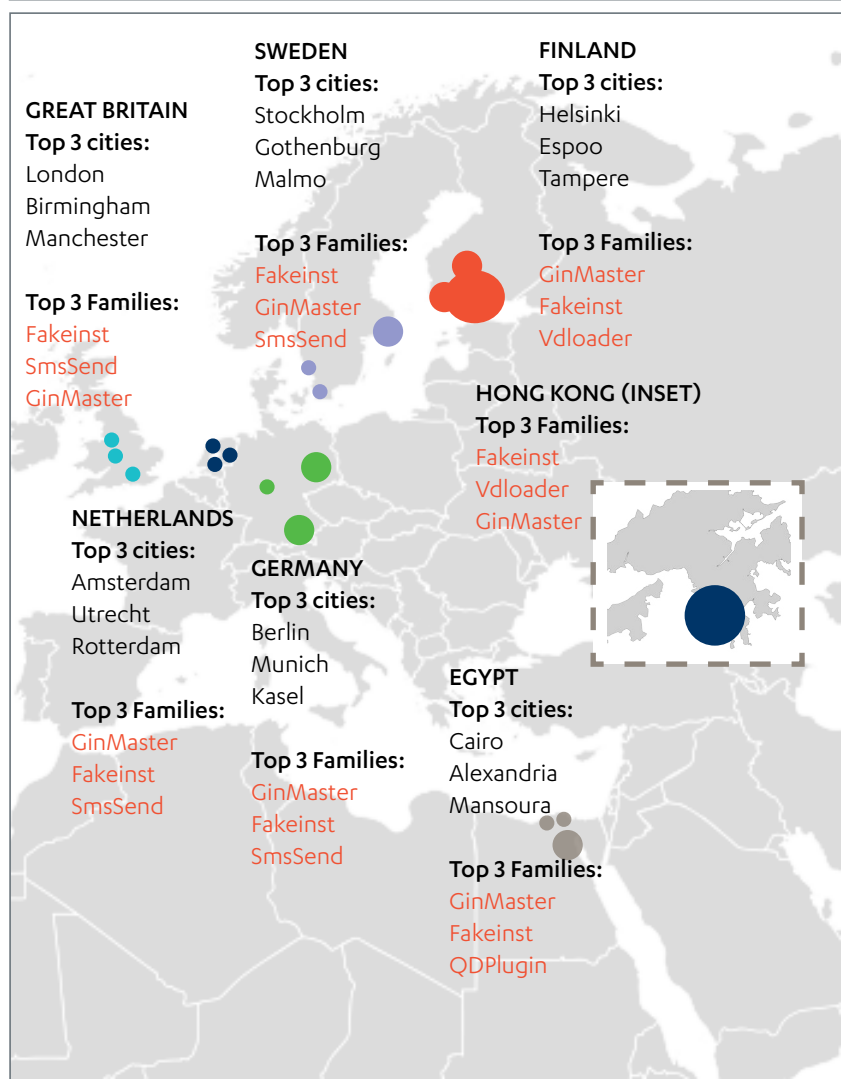
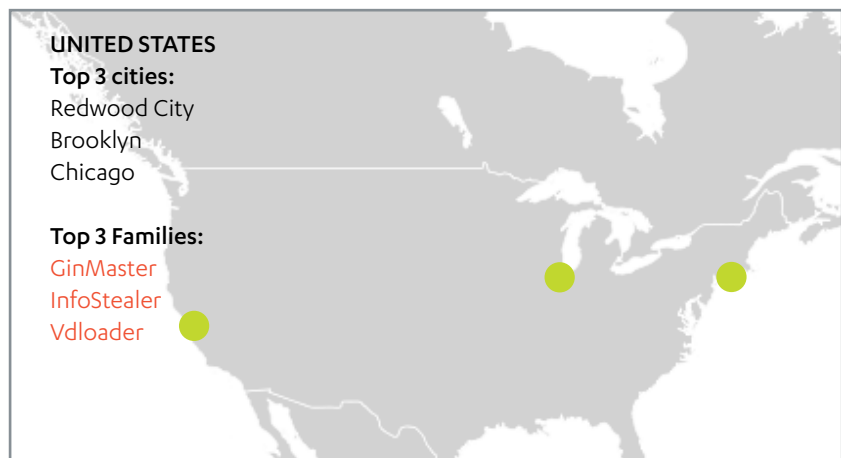
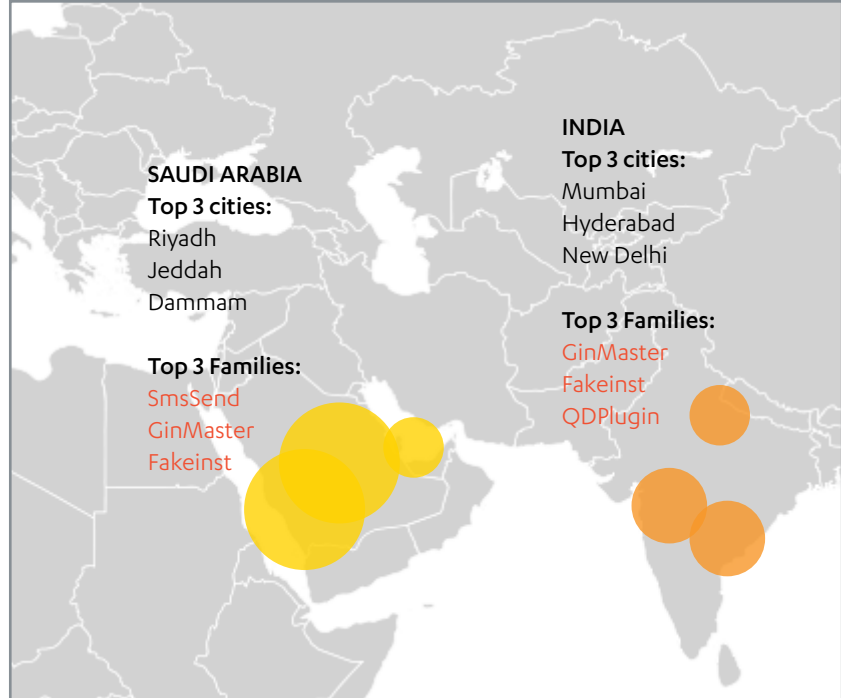
The top 10 countries combined reported a little over 140,000 Android malware detections to our cloud-based systems during H2 2013, with the majority of these detections being reported from Saudi Arabia and India. The remaining 25% of the detections were scattered through most of Europe, with the only other notable countries being Hong Kong and Egypt.

TOP 3 MALWARE FAMILIES & TOP 3 CITIES OF TOP 10 COUNTRIES IN H2 2013, BY DETECTION COUNT



The maps at right depict the top 3 cities for each of the top 10 detections (above), based on the count of detections for known Android malware families reported to our cloud-based systems.

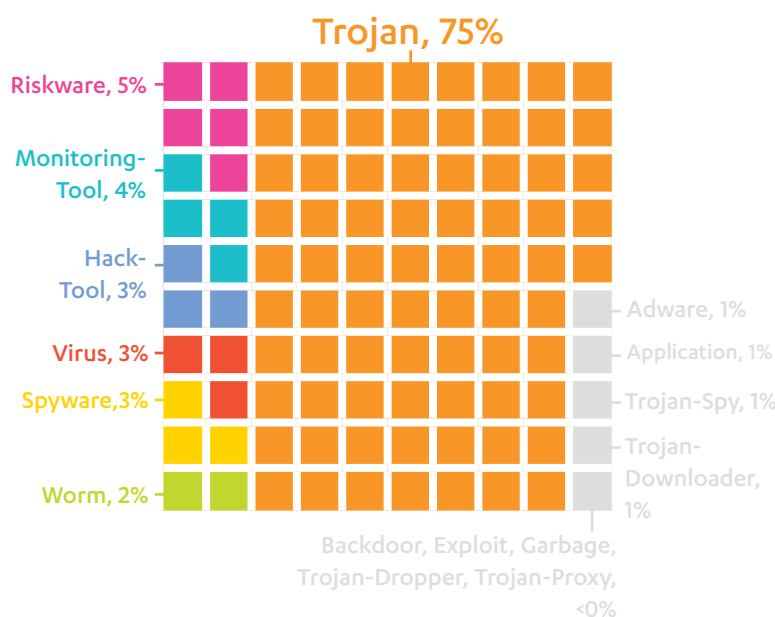
We also compare the top 3 Android malware families reported in each of the top 10 countries - except for the special administrative region of Hong Kong, which for illustrative purposes is treated here as one city.



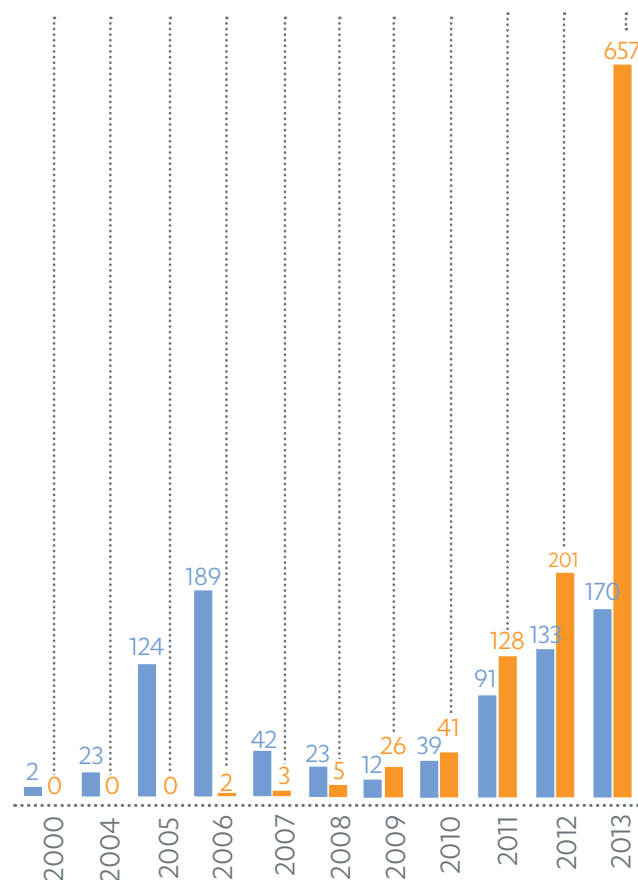
MOBILE THREATS* MOTIVATED BY PROFIT, 2000 - 2013

NOT PROFIT-MOTIVATED ■ PROFIT-MOTIVATED

MOBILE THREATS* BY TYPE, 2000 - 2013



*Based on count of unique samples for all mobile platforms.



PERMISSION TO BE MALICIOUS

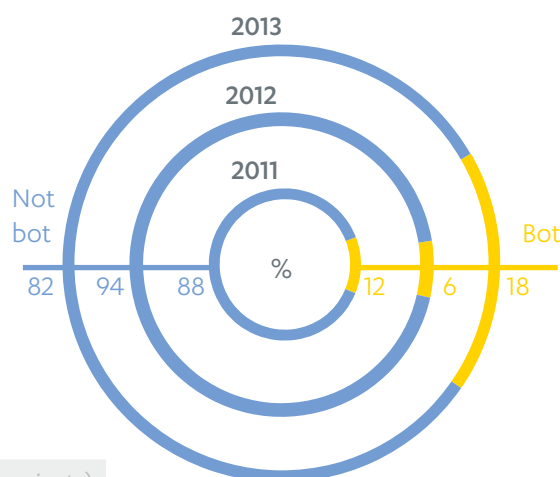
By and large, the majority of malicious apps we see targeting Android exploit the mechanics of the user's interactions with their device. The most common type of malware - Trojans (above) - has malicious routines injected into the packages of clean, legitimate programs (most commonly popular gaming or casino apps), which are then redistributed on various app stores, often with a new name that sounds reminiscent of the clean app. The repackaged app typically asks for more permissions than the original untrojanized program, which is the 'weak point' that allows it to carry out its malicious routines, whether that be sending SMS messages or connecting to a botnet of similarly-infected devices (bottom right). Repackaged apps are essentially an updated take on social engineering, since they take advantage of the user's overriding desire to install and use a popular app to gain the permissions needed to execute their malicious behavior.

In some cases, not only does the device user incur loss from the repackaged app's activities - either by paying for SMS messages sent by the malware or by paying for an app that should be free - but the developer of the original app may also lose revenue if the repackaged app is a paid program now being distributed for free, or for the repackager's profit. The majority of the mobile threats we saw in 2013 were motivated by profit (top). More details on trends we noted in the malicious apps we saw in this period are on page 25.

ADS FOR MOBILE MALWARE

On a final note, the most common distribution channel for mobile malware continues to be via third-party app sites, but in the last couple years there have been a number of incidents of malware being pushed by ads in mobile browsers that can be summarized as: "Warning! You're infected. Get this app now to disinfect your device". This is essentially a transplant of the way rogueware is distributed from desktop platforms to a mobile platform. More details on malware distribution channels are in the Profiling Infection Vectors case study on page 33.

ANDROID MOBILE BOTS †, 2011 - 2013



† Based on count of detections (families and variants) with bot capabilities in the respective years.

APPS AND APP STORE TRENDS

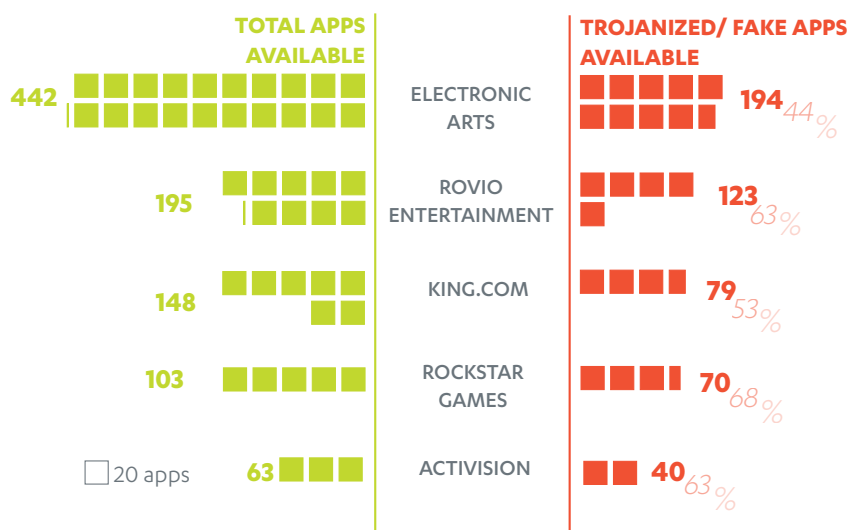
DURING THE H2 2013 PERIOD, WE FOUND OR RECEIVED AND CATEGORIZED 182,015 MOBILE APPS. THE FOLLOWING ARE SOME OBSERVATIONS BASED ON THE COLLECTED SAMPLES.

REPACKAGED OR FAKED APPS

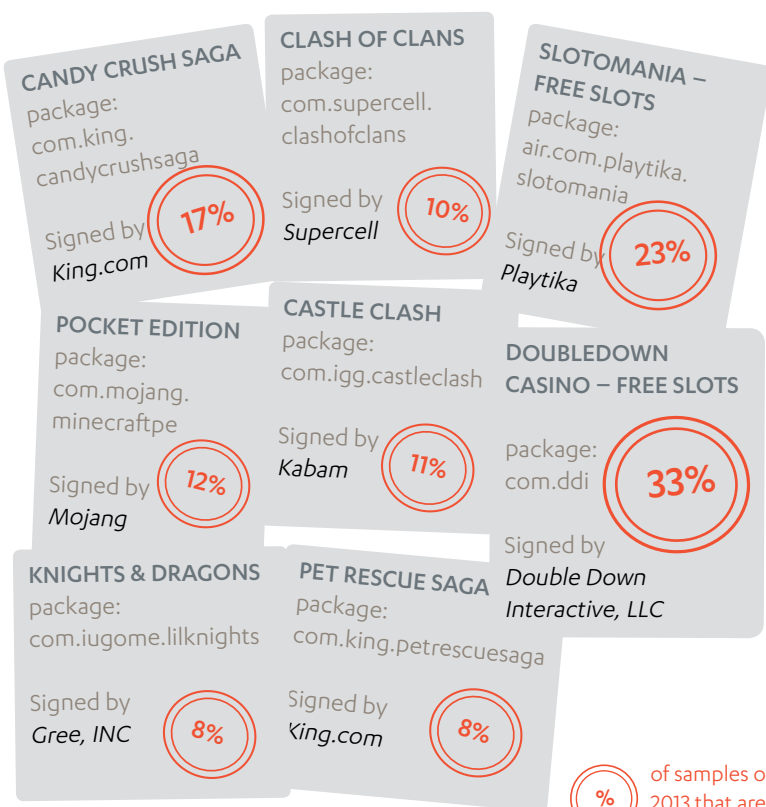
Malware authors looking to maximize the number of victims installing their 'products' will often take advantage of the interest in popular apps, especially games. A common tactic is to *repackage* or *trojanize* a clean, popular application to include malicious code. Malware authors can also create a *fake app* with the appearance of a clean program (using the same name, icon etc.) but none of the same functionality.

Whether repackaged or faked, the counterfeit app can be made to contain any kind of malicious routine. For example an often-seen inclusion is simple, limited functionality to silently send SMS messages that fraudulently force the user to pay for an app that should actually be free. Less commonly, the fake app would be a fully-fledged trojan, with additional capabilities that endanger the user's data or device, as well as their charge bills. A grayer area involves apps that are repackaged, but not to contain malicious code. In such cases, the app may be repackaged to contain an advertisement-related module for the benefit of the party that did the

DEVELOPERS/PUBLISHERS TARGETED IN H2 2013



TOP 8 PLAY STORE APPS TARGETED FOR REPACKAGING



repackaging (rather than the developer of the original program). Another scenario involves cracked programs in which the additional code enables use of the app without having to pay for it, again to the detriment of the original developer(s).

TROJANIZED POPULAR APPS

Some software developers/publishers (above) seem to particularly suffer from rampant repackaging or faking of their products, as a significant percentage of their app inventory have trojanized or fake versions available in third-party markets.

In mid-December 2013, we looked at the top 20 most popular apps listed in the Google Play Store and investigated the rate of trojanization for these apps. In this case, we considered a trojanized version of an application to be one which uses the original package and application name, but also requests more permissions than the original. Out of the 20 most popular Play Store apps, we found that 8 have multiple trojanized versions available in third-party markets (left).

It was interesting to note that the apps for which we found the highest percentage of trojanized and re-permissioned versions were both casino programs. Of all the 'Doubledown Casino - Free Slots' samples we found in H2 2013, 33% were repackaged and redistributed versions from third-party markets, as were 23% of the 'Slotmania - Free Slots' samples seen in that time. Given that gambling-related apps are, apart from banking apps, one of the few types of programs to involve monetary transactions, the high prevalence of trojanized versions of these particular apps may not be too surprising. The remaining 6 apps with plentiful trojanized versions available are popular games.

TOP 10 PERMISSIONS REQUESTED BY REPACKAGED APPS, BY PERCENTAGE



Moving on to look at the additional permissions requested by the trojanized versions, the most common ones are related to the inclusion of an ad module, but some included permissions that facilitated malware code as well. These extra permissions are something that careful users can leverage to spot applications they might not want to install. As an example, above is an image of the extra permissions requested by a trojanized version of the popular game Pet Rescue Saga. When you install an application and see a permission like “Phone calls”, you should ask yourself, “Why would a game want this permission?”

Looking more generally at the overall statistics for permission requests by malware, of the 182,015 malicious apps we found in H2 2013, 99% requested multiple permissions. The 10 most commonly requested permissions are listed above. It is quite obvious why the top 4 looks like that. The (INTERNET) permission is needed since it's one of the fundamental elements of malware. Also, malware needs to be able to access the external storage (WRITE_EXTERNAL_STORAGE) to write downloaded data, a common routine for malware. For mobile devices, it also makes perfect sense why the (SEND_SMS) permission is requested, to exploit SMS sending for malicious/abusive reasons.

Of all the malware we saw in this period, just 1% asked for only a single permission. Of this subset, the number one most requested permission is SEND_SMS, and it's quite obvious what that does.

23% of the malware we examined make themselves appear to be legitimate applications by using authentic-looking package names, as shown in the text cloud (right). Other malware (particularly the Fakeinst family) don't bother and simply use random looking package names (right), which are usually strong indicators that the file is suspicious.

%	PERMISSION REQUESTED	%
	<i>android.permission.</i>	
1	INTERNET	98
	READ_PHONE_STATE	96
	WRITE_EXTERNAL_STORAGE	90
98	SEND_SMS	84
	RECEIVE_SMS	77
	ACCESS_NETWORK_STATE	72
	READ_SMS	67
	WAKE_LOCK	57
	RECEIVE_BOOT_COMPLETED	52
1	OTHERS	<50
	<i>com.android.launcher.permission.</i>	
	INSTALL_SHORTCUT	67

[illegible]

It is surprising that when a user installs an Android application, these tell-tale package names aren't displayed - it would be a good idea if this was addressed in future versions of the OS.

MALWARE IN MARKET PLACES

Nowadays third-party Android markets seem to grow quite rapidly. This is clear just from a rough glance at the total number of app samples we received (both malicious and non-malicious) with a known app store origin in H2 2013 (depicted by size of circle at right). What is not surprising is that, apart from the massive global Google Play Store, the top four biggest marketplaces - Anzhi, Mumayi, Baidu and eoeMarket - cater to the mainland Chinese user population, who have restricted access to the Play Store.

Popular wisdom has it that third-party app stores are the most likely sources of malware. To roughly gauge how exposed a user would be to malware when browsing these markets, we counted the number of malware found in the samples we received originating from the store and compared that to the total number of samples from the same source. We counted only unique, discrete samples, so multiple samples of a unique malware were only counted once.

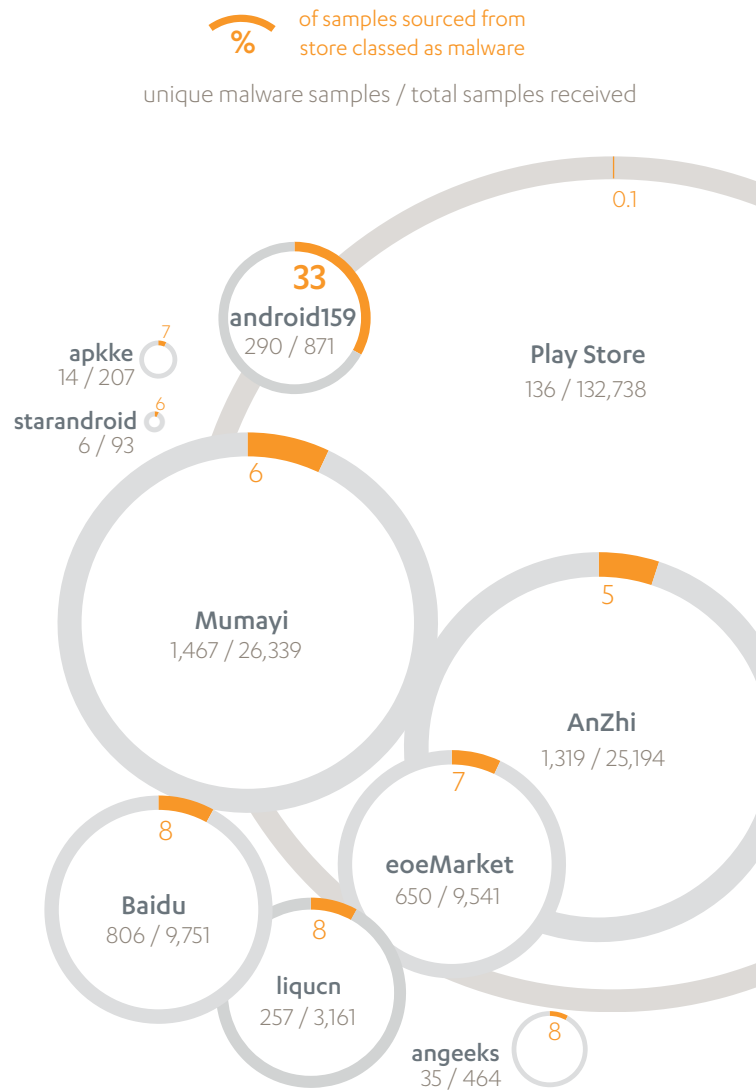
As it turns out, for the top four stores, less than 10% of the samples we traced to them were identified as malicious. Of all the markets, the one with the highest percentage of malware turns out to be Android159, with 33.3% of samples from it being classed as malware.

Luckily at the bottom we have Google Play with the lowest percentage of malware in the gathered samples, at 0.1% - in this case, it's good to be last! In addition, the Play Store is most likely to promptly remove nefarious applications, so malware encountered there tends to have a short shelf life.

ADWARE & RISKWARE IN GOOGLE PLAY MARKET

And finally, as a comparison we look at the statistics for adware and riskware found in the Google Play Store (bottom).

MALWARE SAMPLES RECEIVED, BY APP STORE



COUNT* OF ADWARE & RISKWARE SAMPLES FOUND IN GOOGLE PLAY STORE

Adware	Family	Total Count	Family	Total Count	Riskware
Apps are classed as Adware if they contain advertisement display functionality that potentially exposes the user to privacy or security risks, such as leakage/collection of personal details or exposure/redirection to unsolicited or question-able applications, websites or content.	AirPush	9,382	Minimob	51	Apps are classed as Riskware if they include functionality that may pose a risk to the user's privacy or security if the app were misused. Note: variants in the PremiumSMS family may be classed as Riskware or Malware depending on their behavior.
	AdWo	369	SmsReg	4	
	Ropin	59	PremiumSMS	1	
	Dowgin	22			
	Waps	23			
	Gappusin	2			
* Count is based on discrete unique samples; multiple copies of a unique sample are counted only once.					

ANDROID VULNERABILITIES

AS OF THE END OF H2 2013, THE NUMBER OF KNOWN VULNERABILITIES ON THE ANDROID PLATFORM REMAINS REMARKABLY LOW, CONSIDERING THE AMOUNT OF SOFTWARE CARRIED IN THE WHOLE ECOSYSTEM.

As a general rule of thumb, vulnerability-based attacks against Android devices do not directly target a loophole in the device's own operating system. Instead, the attacker targets a vulnerability in an installed app, which in turns allows them to manipulate the device.

VENDORS AS A VULNERABILITY SOURCE

The most popularly cited way in which exploitable vulnerabilities are introduced onto a device is via user-installed, third-party applications. There are however are other, 'silent' sources of introduced vulnerabilities, over which users usually have no control. Research^[1] published in 2013 shows that a significant vector for introduced vulnerabilities is *vendor customizations*, in which a device manufacturer customizes the stock Android firmware to install vendor-specific features or apps on a device. The study goes so far as to suggest that as much as 85% of applications pre-loaded onto shipped devices increase risk by declaring wider permissions than are absolutely necessary. The same research also indicates that anywhere between 65% to 85% of all vulnerabilities arise from vendor customizations.

The premise of the Android ecosystem allows numerous manufacturers to produce multiple devices, each running a different version of the platform (and often each with its own version update schedule). This has led to another phenomenon that contributes to the presence of vulnerabilities on Android devices: *platform fragmentation*. With a huge variety of platform configurations to maintain, manufacturers have faced difficulties in pushing out periodic security updates for all their users. Though community-based efforts to product 'unofficial' patches have gone some way toward rectifying the problem, this does require at least a modicum of user awareness and technical ability.

ATTACK SURFACES

Leaving aside the issue of whether the user or a vendor installed an app, let's now consider the apps themselves. The most obvious remotely exploitable application on any Internet-capable device is the web browser. This is readily evident on desktop computers, but mobile devices are no exception, and there are already some exploits taking advantage of both the standard Android web browser as well as the Firefox browser for Android (next page).

SOURCES

1. North Carolina State University; Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, Xuxian Jiang; *The Impact of Vendor Customizations on Android Security*; published 4 November 2013; <http://www.cs.ncsu.edu/faculty/jjiang/pubs/CCS13.pdf>
2. CVE Details; *Vulnerability Details : CVE-2013-3363*; <http://cvedetails.com/cve/2013-3363>
3. CVE Details; *Vulnerability Details : CVE-2013-6632*; <http://www.cvedetails.com/cve/CVE-2013-6632>
4. IBM:Security Intelligence Blog; Roee Hay; *A New Vulnerability in the Android Framework: Fragment Injection*; published 10 December 2013; <http://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/>
5. Pwn2Own 2013, PacSec 2013 Conference; Heather Goudey; *Local Japanese team exploits mobile applications to install malware on Samsung Galaxy S4*; published 13 November 2013; <http://www.pwn2own.com/local-japanese-team-exploits-mobile-applications-install-malware-samsung-galaxy-s4/>
6. CVE Details; *Vulnerability Details : CVE-2013-4787*; <http://www.cvedetails.com/cve/CVE-2013-4787>
7. Bluebox Blog; Jeff Forristal; *Uncovering Android Master Key That Makes 99% of Devices Vulnerable*; published 3 July 2013; <http://bluebox.com/corporate-blog/bluebox-uncovers-android-master-key/>
8. Bluebox Blog; Jeff Forristal; *Commentary on the Android "Master Key" Vulnerability "Family"*; published 29 July 2013; <http://bluebox.com/corporate-blog/commentary-on-the-android-master-key-vulnerability-family/>
9. Saurik; Jay Freeman; *Android Bug Superior to Master Key*; <http://www.saurik.com/id/18>
10. Saurik; Jay Freeman; *Exploit (& Fix) Android "Master Key"*; <http://www.saurik.com/id/17>



Adobe Flash player for Android is another lucrative target for remote exploitation. The Flash player's long history of security issues (on PC) certainly suggests that its mobile counterpart may have vulnerabilities yet to be discovered. The latest high-impact vulnerability, discovered in 2013 (next page) concerns multiple Adobe products and is also cross-platform.

As users have a very limited view into an app's potentially harmful behavior, rogue or malicious apps can increase the impact factor of locally exploitable vulnerabilities (next page). Escalation of privilege exploits can allow apps to do their unwanted things out of sight, while theft of sensitive information can be enabled by vulnerable apps and services on the device.

EXPLOITATION

Even if a vulnerability is present on an Android device, custom exploit code must be created to attack it. As of the time of writing, the website for **Metasploit**, a common framework used for penetration testing, lists very few exploits for the Android platform. This may be a result of many things, such as the target still being too esoteric or too new. Having said that however, it is quite easy to find resources to guide those interested in creating such code, which those unwilling to do the work can just buy other people's labor from sites such as **in3ct0r**.

ANDROID IN 2013

The following Android-related vulnerabilities were publicly reported in 2013.

1 CONFIGURATION, 2 VULNERABILITIES (CVE-2013-4777 & CVE-2013-5933)

Two separate vulnerabilities in a specific configuration of the 2.3.7 version of Android on a Motorola Defy XT phone for Republic Wireless allow local users to either execute shell commands as the root user or create a stack-based buffer overflow. In either case, the exploit leads to the attacker potentially gaining unauthorized access to information or the ability to modify the device configuration.

DEVICE LOCK BYPASS (CVE-2013-6271)

A vulnerability in the 'com.android.settings.ChooseLockGeneric' in Android versions 4.0 to 4.3, which allows a user to modify the device's lock mechanism, could be exploited by a specially crafted app to bypass access restrictions (PINs, passwords, gestures, etc), essentially unlocking the device.

LOCAL UI FRAGMENT INJECTION (CVE-2013-3666)

Application security researchers at IBM reported finding a vulnerability in the user interface framework. In their proof-of-concept demonstration, a specially crafted Intent could be used to override a display Fragment in a known Activity class in the system settings application. The injected Fragment can then be instructed with extra parameters in the same Intent to skip PIN query. This would allow the attacker to change privileged settings on the device without proper authorization. The attack works at least on devices preceding the latest Android 4.4 (KitKat) release.

BROWSER EXPLOIT EXPOSED (CVE-2013-6632)

This vulnerability affects all Chrome web browser for Android versions before 31.0.1650.57. It was first disclosed when a Japanese team exploited it to install malware on a phone during the Mobile Pwn2Own competition at the PacSec 2013 security conference. The vulnerability allows remote attackers to execute arbitrary code or cause memory corruption in the Chrome web browser process. There have been no known attacks against this vulnerability in the wild.

FLASH EXPLOIT (CVE-2013-3363)

This vulnerability can be remotely exploited using a specially crafted Adobe Flash file and is found in multiple Adobe products, notably all Adobe Flash player versions before 11.1.111.73 on Android 2.x and 3.x, and version 11.1.115.81 on Android 4.x. There have been no known attacks against this vulnerability in the wild.

THE "MASTER KEY" (CVE-2013-4787)

Previously highlighted in our Q4 2013 Mobile Threat Report, this vulnerability was also found in the Android operating system itself, and has its roots in the way the platform handles software installation packages (APKs). These are regular ZIP archives, which include certain files needed to check archive integrity and origin. The software installation process uses two separate implementations to read these manifest files and validate the archive integrity, but unfortunately, slight differences in the implementation allow an attacker to smuggle arbitrary files overriding the original files in any installation package. Later work on this issue led to the discovery of further vulnerabilities in Android's ZIP archive handling, allowing much more sophisticated attacks. As of late 2013, multiple malicious apps containing exploits targeting this vulnerability have been found in third-party app sites.

THE STATE OF WEB PRIVACY

Though online privacy has long been a concern among the security-minded, the revelations of NSA spying activities throughout 2013 has lead to a surge in privacy worries among the general population of netizens. Internet users are growing more alert to the possibility of prying eyes while they surf the Internet, now adding governments (their own or others) alongside other parties who may be engaging in user surveillance. In this article, we cover some of the ways a netizen may unwittingly have their browsing activities or personal information captured and collected online, for someone else's benefit.

WEB ANALYTICS

As Internet usage keeps growing, *web analytics* - or the analysis of net traffic to improve a website's effectiveness - has become an indispensable tool for studying a website visitor's behavior, providing insight into how information flows from the web to the users and vice-versa. To perform such analysis, website operators may simply install open-source software such as AWStats to collect data on their visitors. There are also cloud-based services provided by various companies specializing in web analytics, which is the preferred option for commercially-oriented operators.

In general, web analytics involves collecting and analyzing data to provide a useful "profile" of the visitors to a site. The information collected can include things like the user's browser type, the device used to access the site, device screen resolution, keywords entered in the search bar, clicks made by the user in online web stores, time spent between pages, etc. Large-scale web-based services attempt to automate the measurement and collection of such data.

Due to the nature of the data collected, web analytics may raise many questions and concerns, not just among security professionals, but among privacy-minded Internet users. Speaking very generally, the aggregation of the data is not in itself considered a privacy violation; many people however object to the profiling done based on the collected data.

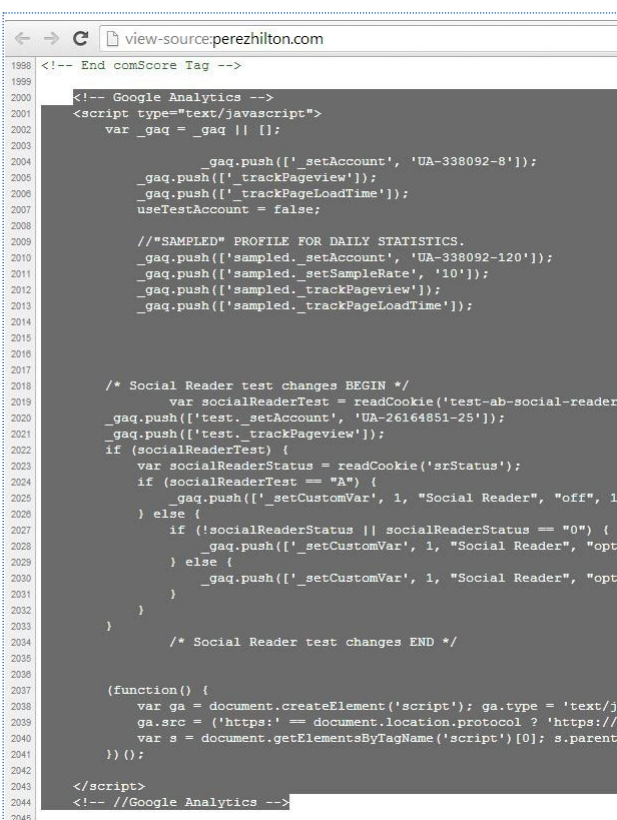
The most common and most obvious commercial use of web analytics is by online advertisers, who typically try to collect information about a website's visitors in order to better target advertising materials. The collected data is used in conjunction with *tracking cookies* (more on these later) to help advertisers boost their clients' (the publishers) sales, by directing appropriate advertisement materials to users who, the thinking goes, would appreciate seeing such ads. The advertiser's clients would then benefit in having their products or services pushed with less effort (since this method is mostly automated) and with greater accuracy to the most appropriate users. Some online marketing research firms use above-the-board web analytics services to legitimately gather a vast amount of data to perform profiling.

E-mail marketing firms are also enthusiastic web analytics users, as they use similar techniques to advertisers to track the user's behavior pattern when an e-mail is read.

COOKIES

The most common type of web data storage vehicle the "average Joe" user knows about is the cookie - a text file that allows certain information from a website's server to be stored locally on the user's computer. The "basic" cookies are an integral part of how the modern web works, as they facilitate such basic activities as automated web access or "stateless" HTTP requests.

There are however other, more sophisticated cookies that cause more concern in privacy-minded users - foremost, the tracking cookie or third-party tracking cookie. This is commonly used to store the user's browsing history and can be planted onto the user's computer using JavaScript on a website, or via the HTTP response header when a user accesses the site. Tracking cookies are able to maintain a history of the user's activities (pages already visited, items held in shopping carts, etc). While they are often used more or less legitimately by advertisers to assist in ad targeting, the collection of such data and its potential for personally identifying the user has lead to rumblings of disquiet among those concerned about their privacy.



```

1998 <!-- End comScore Tag -->
1999
2000 <!-- Google Analytics -->
2001 <script type="text/javascript">
2002   var _gaq = _gaq || [];
2003
2004   _gaq.push(['_setAccount', 'UA-338092-8']);
2005   _gaq.push(['_trackPageview']);
2006   _gaq.push(['_trackPageLoadTime']);
2007   useTestAccount = false;
2008
2009   /*SAMPLED PROFILE FOR DAILY STATISTICS.
2010   _gaq.push(['_sampled._setAccount', 'UA-338092-120']);
2011   _gaq.push(['_sampled._setSampleRate', '10']);
2012   _gaq.push(['_sampled._trackPageview']);
2013   _gaq.push(['_sampled._trackPageLoadTime']);
2014
2015
2016
2017
2018   /* Social Reader test changes BEGIN */
2019   var socialReaderTest = readCookie('test-ab-social-reader');
2020   _gaq.push(['_test._setAccount', 'UA-26164851-25']);
2021   _gaq.push(['_test._trackPageview']);
2022   if (socialReaderTest) {
2023     var socialReaderStatus = readCookie('srStatus');
2024     if (socialReaderTest == "A") {
2025       _gaq.push(['_setCustomVar', 1, "Social Reader", "off", 1
2026     } else {
2027       if (!socialReaderStatus || socialReaderStatus == "0") {
2028         _gaq.push(['_setCustomVar', 1, "Social Reader", "opt
2029       } else {
2030         _gaq.push(['_setCustomVar', 1, "Social Reader", "opt
2031       }
2032     }
2033   }
2034   /* Social Reader test changes END */
2035
2036
2037   (function() {
2038     var ga = document.createElement('script'); ga.type = 'text/j
2039     ga.src = ('https:' == document.location.protocol ? 'https://
2040     var s = document.getElementsByTagName('script')[0]; s.parent
2041   })();
2042
2043 </script>
2044 <!-- //Google Analytics -->
2045

```

Image 1: Google analytics script on a popular gossip site

An alternative to tracking cookies are Flash cookies, also known as Local Shared Objects. These were developed to counter the fact that many users block or remove cookies in their browser - a tactic that does not affect Flash cookies, making them popular among online advertisers. One research paper in 2009 ^[4] and a few studies showed that Flash cookies were commonly found on the top 100 most visited sites. Another social media study conducted in 2011 found that 31 out of 100 web sites had at least one overlap between HTTP cookies and Flash cookies ^[5].

Another cookie type known as Evercookie ^[6] was developed by Samy Kamkar with the aim of being extremely persistent in the browser. Its behavior is so aggressive that techniques that successfully removed other cookie types are still insufficient to remove traces of identifiable information. It has a built-in defensive mechanism that will detect any attempt to remove it and will react by recreating itself if such action is attempted. Due to Evercookies' aggressive behavior, they are also known as super or zombie cookies^[7]. Sources from a top-secret NSA document^[8] also claimed that Evercookie was used to track down Tor users hiding behind the anonymous network.

SCRIPTS IN DATA COLLECTION

Since most modern Internet browsers support the popular JavaScript language, scripts are also widely used for data collection. Much information can be derived from client-side JavaScript objects, such as user agents, browser language settings, platforms and so on. An aggregation of information from this as well as other sources may be used to generate a "signature" that can distinguish one user from another. In the Labs, our network and web reputation service has noted the 'trails' of this tracking method in high-traffic websites, especially in blogs and news sites with huge volumes of daily visitors.

The web analytics script offered by Google is one of the most commonly used of such devices. Their Web Analytics service provides a snippet of its analytics script, which can be easily copied-and-pasted by a website owner into their web page. The structure of these codes is clean and easily spotted. **Image 1** shows an example that can be seen on a popular celebrity gossip blog, *perezhilton.com*.

In addition to scripts, most modern web browsers now support HTML5, which allows more and more client-side information to be captured via scripting. For example, HTML5's Geolocation capability can be used to obtain the user's latitude and longitude for use in displaying their position on a web page. Whether the user is comfortable with such information being gathered however is another matter.

To take rich content to the next level, HTML5 also brought in Web Storage ^[2], which allows data (and much more of it) to be stored locally on the user's system, with the intent of making web usage faster and more secure. Before this, data storage was normally done with cookies, which has had the drawback that the data in these files may be sent out in requests - something privacy-minded individuals tend to resent, and has led to the

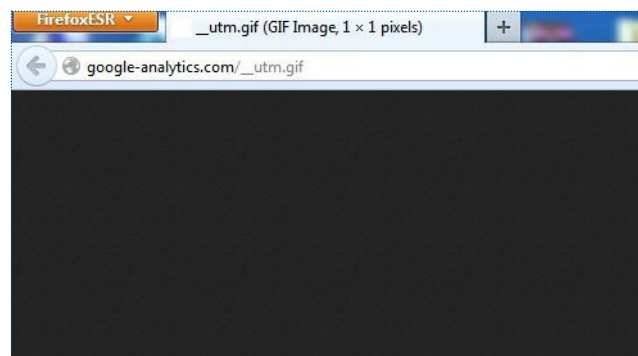


Image 2: A 1x1 pixel image file used in a web page

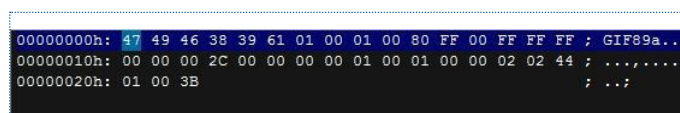


Image 3: Content of the file

practice of removing cookies to prevent potential tracking. On a related note, Web technology providers deal with this 'weak spot' in the current web model by creating products or services that addresses the user's privacy concerns. The well-known browser plug-in NoScript^[3] allows users to block JavaScript, Flash, Java and other similar plugins from being run on web pages. One notable consequence of this however is that though disabling JavaScript helps users protect their privacy, such an action may result in restraining the functionality of many web sites, and making some sites totally unusable - forcing users to choose between accessing a website and putting their privacy at risk.

WEB BUGS

Apart from the (mis)use of cookies or scripts, the user's information can be captured in other ways during a visit to a web site. The act of doing so is called 'placing a "web bug"', or a burying special object on the web site which is invisible to the users. Web bugs may be called by different names - web beacon, tracking bug, tag or page tag^[1] - but all of them serve the same purpose.

One implementation of a web bug found on many web sites is to hide an image file in a web page, along with the actual content intended for the users to view. The image file is tiny (**Image 2**), usually measuring 1-pixel in both width and height and the file content is typically in a GIF format (**Image 3**) or similar. Understandably, this method is often referred to as the tracking pixel, 1x1 pixel or pixel tag. When a user visits a page containing a tracking pixel, the server is able to identify the user as having visited before.

TRACKING WITH FONTS

In addition to the common tracking methods, more advanced techniques may be used while researching user tracking on the Internet. One user-tracking method researched hinged on the fonts installed on the user's computer. The idea was based on the fact that different operating systems, such as Microsoft's

Windows and Apple's Macintosh, come pre-installed with their own unique sets of fonts, which can be easily distinguished. The researchers investigating this type of tracking were then able to build on this foundation and classify the font sets for each system to identify different system versions, architecture (32-bit or 64-bit) and even office suites. The results of the research suggest that this font-based method was able to distinguish one user from another without using a more active fingerprinting method^[9].

THE FUTURE OF TRACKING

Tracking plays a big role in advertising and will continue to do so in the near future. Google, the Internet giant that also happens to be the leading company in online advertising industry worldwide, is researching new ways to enable user tracking. One way would involve replacing cookies with an anonymous identifier, tied to users of the Chrome browser, which would serve a similar function as cookies^[10]. In other news, Microsoft has also announced that it is looking into developing its own cross-platform tracking technology to replace the ubiquitous cookie. This new technology will be able to facilitate tracking of individuals across desktop computers, tablets, smartphones, gaming consoles and other services^[11]. Such developments are only likely to raise more questions about how to ensure a user's privacy in an increasingly exposed environment.

For Internet users with privacy concerns, how much protection, if any, could they expect from the law if their privacy is breached? While the issue is startlingly complex, especially when dealing with web-based services catering to an international audience, it may be instructive to revisit a relevant case in the not-too-distant past. In December 2007, Facebook launched a program known

as Beacon, in which Facebook users' private information was automatically publicly posted without the users' consent. This was seen as a breach of privacy and eventually led to lawsuits being filed against the company. The Beacon program was subsequently terminated and a USD9.5 million fund was created to enhance privacy and security. No compensation however was made to Facebook users negatively affected by the Beacon program^[12].

SOURCES

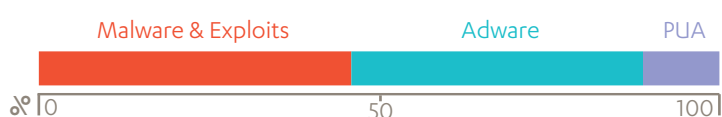
1. Wikipedia; *Web bug*; updated 26 December 2013;
http://en.wikipedia.org/wiki/Web_bug
2. W3C; Ian Hickson; *Web Storage*; updated 30 July 2013;
<http://www.w3.org/TR/webstorage/>
3. NoScript;
<http://noscript.net/>
4. Wikipedia; *Internet Privacy*; updated 22 January 2014;
http://en.wikipedia.org/wiki/Internet_privacy#cite_note-21
5. Wikipedia; *Internet Privacy*; updated 22 January 2014;
http://en.wikipedia.org/wiki/Internet_privacy#cite_note-Heyman.2C_R._2011-22
6. Evercookie; Samy Kamkar; *Evercookie – Never Forget*; published 11 October 2010;
<http://samy.pl/evercookie/>
7. Enshighten; *Super Cookies, Ever Cookies, Zombie Cookies, Oh My!*;
<http://www.ensighten.com/blog/super-cookies-ever-cookies-zombie-cookies-oh-my>
8. Wikipedia; *Evercookie*; updated 18 December 2013;
<http://en.wikipedia.org/wiki/Evercookie>
9. Károly Boda, Ádám Máté Földes, Gábor György Gulyás, Sándor Imre; *User Tracking on the Web via Cross-Browser Fingerprinting*; published 2011;
http://pet-portal.eu/files/articles/2011/fingerprinting/cross-browser_fingerprinting.pdf
10. The New York Times; Claire Cain Miller; *Google Is Exploring an Alternative to Cookies for Ad Tracking*; published 19 September 2013;
http://bits.blogs.nytimes.com/2013/09/19/google-is-exploring-an-alternative-to-cookies-for-ad-tracking/?_php=true&_type=blogs&_r=1
11. Ad Age; Tim Peterson; *Bye, Bye Cookie: Microsoft Plots Its Own Tracking Technology to Span Desktop, Mobile, Xbox*; published 9 October 2013;
<http://adage.com/article/digital/microsoft-cookie-replacement-span-desktop-mobile-xbox/244638>
12. Wikipedia; *Lane v. Facebook, Inc.*; updated 4 October 2013;
http://en.wikipedia.org/wiki/Lane_v._Facebook,_Inc.

PROFILING INFECTION VECTORS

We take a brief look at the most common distribution channels for attackers during the second half of 2013 and find out why avoiding porn and Java may be the key to saving your online existence.

Most computer users today accept as common knowledge (through having it repeated at them ad nauseum) the idea that most infections nowadays come via the Internet - and of course, they are right. But just how much is “most”, and what kinds of sites are involved?

**SAMPLE TOP 100 DETECTIONS,
BY PERCENTAGE OF TYPE**



To find out, we compiled a list of the top 100 detections reported to our cloud-based reporting system over a few weeks in H2 2013, then categorized each detection in our final list by the type of software identified (above). We then examined the known *infection vectors*, or the pathway they used to reach the target, for each detection and ended up with the following breakdown (bottom).

IT'S MAINLY ABOUT THE WEB

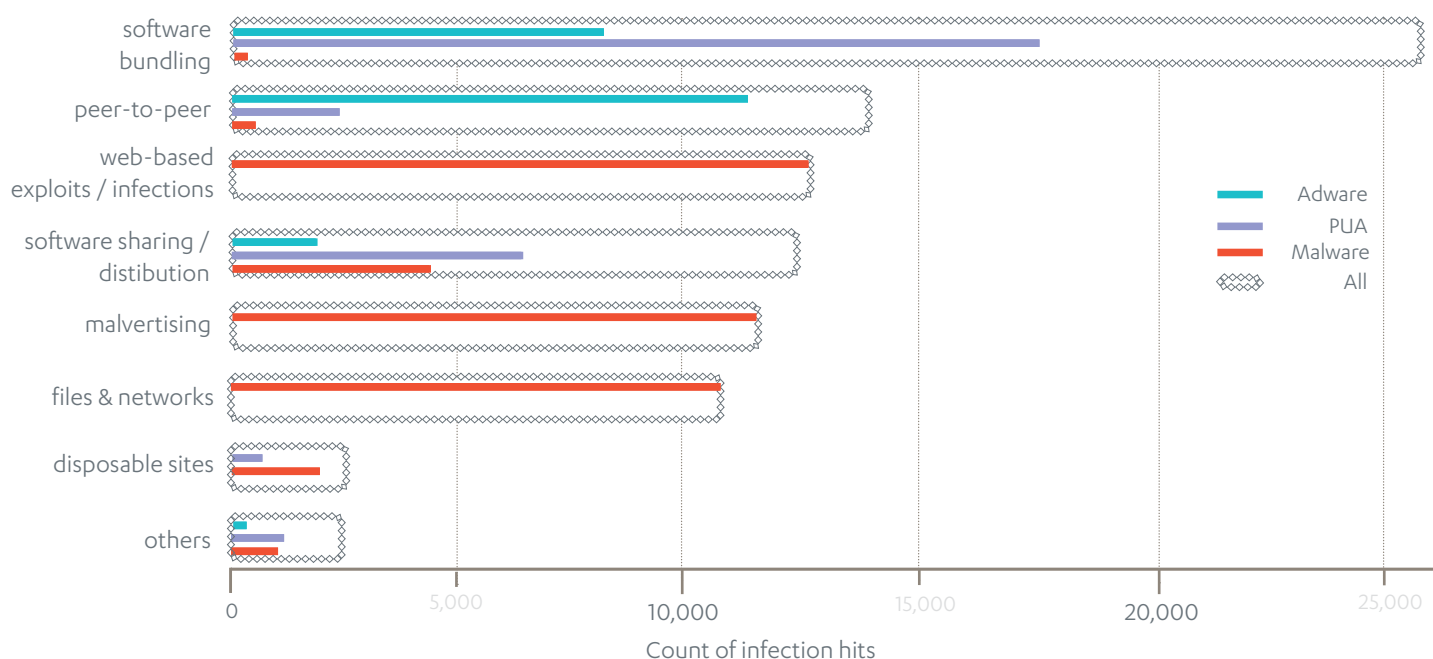
Looking at the results, we see that malware unsurprisingly has the lead with 47% of all software in our sample top 100 detections. Adware is not far behind at 42%, while Potentially Unwanted Applications (PUA) trails at 11%. Looking at the total counts for the various infection vectors, it appears that software bundling

COMMON INFECTION VECTORS

The following is an abbreviated list of the various pathways or channels used to deliver a malicious file to a target:

- **Files and networks**
Software distributed through file infection, or in the payloads of worms spreading through networks, removable media, etc.
- **Software bundling**
Software packaged into the installer of another (often free) software. Also includes software downloaded from the Internet during another program's installation.
- **Peer-to-Peer**
Files distributed over a peer-to-peer (P2P) networks.
- **Software sharing / distribution**
Software distributed via file sharing sites or platforms.
- **Malvertising**
Malicious advertising used to silently download software onto a user's system, or to redirect them to a disposable site.
- **Web-based exploits/ infections**
Malicious or compromised sites exploit a vulnerability on the user's machine to silently download the software.
- **Disposable sites**
A site created and dedicated solely to distributing the software.
- **Others**
Files distributed by any other means not defined here.

BREAKDOWN OF SAMPLE TOP 100 DETECTIONS BY INFECTION VECTOR



is the clear leader. Is this really the most common pathway for malware though (the software type of most concern)? We further categorized the software distributed by this method by type and ended up with a clearer picture.

It turns out, software bundling is mainly used to distributed adware and PUAs. Actually malicious files were instead mostly distributed by what we class here as 'web-based methods' - that is, by exploits hosted on websites, malvertising, downloading software bundles from software sharing and distribution sites and finally from disposable sites (which, unlike compromised legitimate sites, are purely bred for malicious purposes). Even if we don't include files distributed by Peer-to-Peer (P2P) sharing, software distributed via the web accounted for 72% or the lion's share of the detections in our sample top 100. So the web is clearly the biggest source of malicious infections.

PUAs appear to be bucking the trend by having P2P as the leading vector for delivery. Looking closer at our data however, we find that this is due to the numbers produced by one highly prevalent software - Application:W32/BProtector (covered in more detail in the Mevade article in this Threat Report). Without the numbers from this infection, the web would be the source of 94% of the detections on our list.

Predictably, adware also leans heavily on web-based pathways, with 88% coming from software bundles tied to file sharing or distribution sites and also from disposable sites. If these numbers are any indication, most adware comes from sites which add it as an 'extra' when users download other, desired software.

SCRUTINIZE THAT DOWNLOAD

So, we've established that users are mainly coming into contact with the bad stuff from being exposed while surfing the Web - but we're not likely to be letting the Internet go anytime soon. So are there precautions a user can take to prevent unwanted software from arriving on their systems?

Compared to dealing with malware, avoiding Adware and PUA's is easier. The most common vectors for these are software bundles from software download sites and P2P networks where the user is usually hunting for a specific utility or software, and are more likely to catch the unwary, rather than the unwilling. Unlike more aggressive distribution methods that force a software onto a user, these sites allow a user to decline a download if they spot something fishy about a file. As more users become aware that a particular file being offered is undesirable, this method of distributing it becomes less and less effective.

IS THAT AN AD FOR MALWARE?

Avoiding malware online however needs more than the average amount of care, since it is deliberately designed to be difficult to spot. Malvertising is the second-most common malware distribution method, accounting for 37% of all malicious web-based infections even though it is only used by 8 of the 47 malware in our list.

Though only a handful of malware families are spread this way (in our top 100 list, these were Redirector, Salama and Browlock),

the potential audience of victims for this vector is vast. We therefore profiled the URLs gathered from the above families, to find popular malvertising topics.



As it turns out, the majority are related to adult content and dating. This is fortuitous because while it's impossible to filter websites that discuss general topics like cabinetry and roofing, most antivirus programs include a 'parental control' functionality that filters out specific content types, including adult and dating. Using this feature mean that at least 93% of the most popular malvertising campaigns can be avoided.

WEB EXPLOITS, SITE INFECTIONS AND DISPOSABLE SITES

Malware is most commonly pushed by web exploits, site infections and disposable sites, and unlike malvertising, isn't neatly confined to topics or website types that can be filtered. There is still hope though - while topics can't be isolated, targeted browser plug-ins can be. While examining the malware in our sample set, we saw that 94% used exploits targeting vulnerabilities in the browser plug-in for the Java development platform.



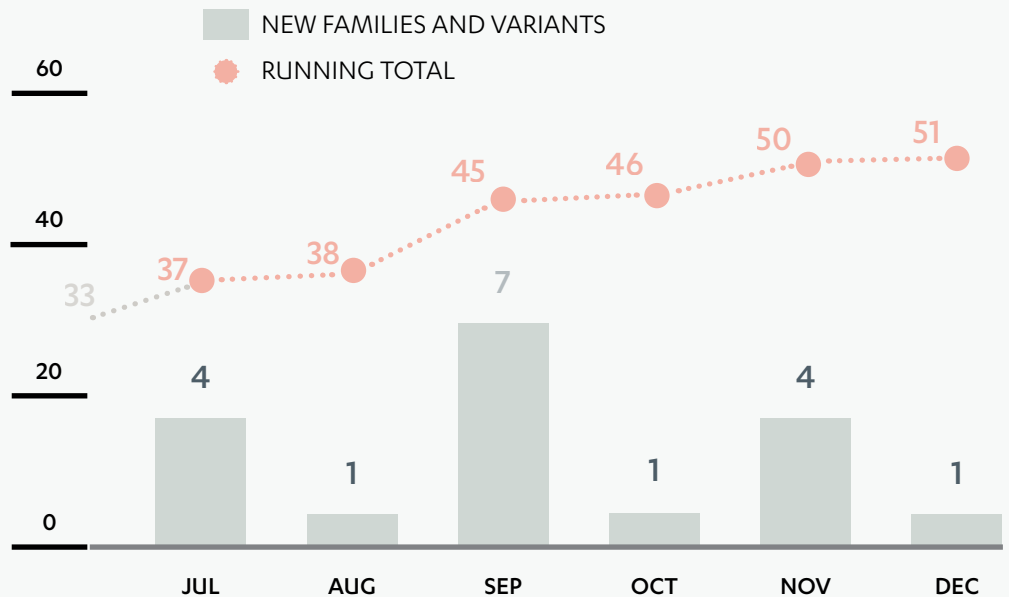
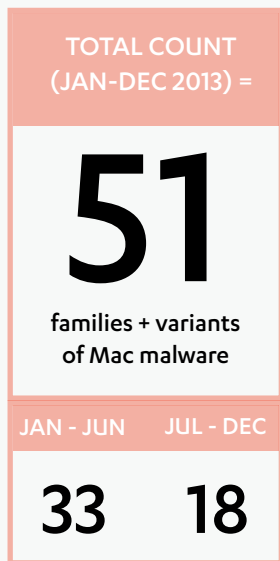
While this is disconcerting for developers and other users who actually need to make daily use of that plug-in, the preference for targeting it does have a barely silver lining for users who don't often use Java - removing the plug-in when not needed also closes off one very popular pathway for malware to arrive on the system.

CONCLUSION

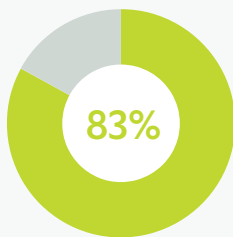
In the end, avoiding unwanted software while online comes down to three simple guidelines, which are very easy to remember:

- If a software seems even just a tiny bit funny, don't install it, no matter where you got it
- Avoid porn and dating sites - or turn on Parental Control in your antivirus program to filter that type of content
- If you rarely use the Java browser plug-in, uninstall it

Or course, these tips won't keep you 100% safe - but they will get you closer to that.

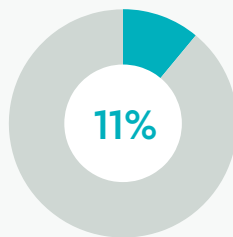


BACKDOOR



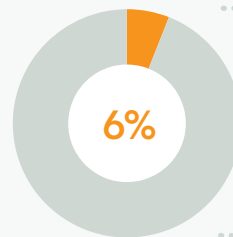
15/18

TROJAN



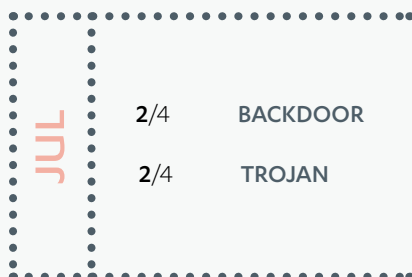
2/18

OTHERS



1/18

1/18 ROOTKIT



Note: numbers shown are the count of unique variants detected.
This means repackaged installers are not counted and multiple-component malware are counted as one.

SOURCES

HACKS & ESPIONAGE

NSA

1. Washington Post; Ellen Nakashima; *FISA court releases opinion upholding NSA phone program*; published 17 Sep, 2013
http://www.washingtonpost.com/world/national-security/fisa-court-releases-opinion-upholding-nsa-phone-program/2013/09/17/66660718-1fd3-11e3-b7d1-7153ad47b549_story.html
2. The Verge; Bryan Bishop; *NSA reportedly collecting millions of email address books and IM contact lists worldwide*; published 14 Oct 2013;
<http://www.theverge.com/2013/10/14/4838966/nsa-reportedly-collecting-millions-of-email-address-books-and-im>
3. AP for Yahoo! News; Deb Riechmann & Kimberly Dozier; *France joins list of allies angry over NSA spying*; published 21 Oct 2013;
<http://news.yahoo.com/france-joins-list-allies-angry-over-nsa-spying-224519206.html>
4. Arstechnica; Sean Gallagher; *How the NSA's MUSCULAR tapped Google's and Yahoo's private networks*; published 1 Nov 2013
<http://arstechnica.com/information-technology/2013/10/how-the-nas-muscular-tapped-googles-and-yahoos-private-networks/>
5. PCWorld; Lucian Constantin; *NSA infected 50,000 networks with specialized malware*; published 25 Nov 2013
<http://www.pcworld.com/article/2066840/nsa-reportedly-compromised-more-than-50000-networks-worldwide.html>
6. Washington Post; Barton Gellman and Ashkan Soltani; *NSA tracking cellphone locations worldwide, Snowden documents show*; published 5 Dec 2013;
http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
7. ZDNet; Larry Seltzer; *NSA using Google cookies, app location data to track targets*; published 11 Dec 2013;
<http://www.zdnet.com/nsa-using-google-cookies-app-location-data-to-track-targets-7000024178>
8. International Business Times; Eric Brown; *NSA Phone Spying Program Ruled Unconstitutional By Federal Judge*; published 16 Dec 2013;
<http://www.ibtimes.com/nsa-phone-spying-program-ruled-unconstitutional-federal-judge-1510756>
9. The Register; John Leyden; *Latest Snowden reveal: It was GCHQ that hacked Belgian telco giant*; published 20 Sep 2013;
http://www.theregister.co.uk/2013/09/20/gchq_belgacom_hack_link/
10. Arstechnica; Dan Goodin; *Password hack of vBulletin.com fuels fears of in-the-wild 0-day attacks*; published 18 Nov 2013;
<http://arstechnica.com/security/2013/11/password-hack-of-vbulletin-com-fuels-fears-of-in-the-wild-0-day-attacks/>
11. F-Secure Weblog; Sean Sullivan; *Adobe Hacked*; published 4 Oct 2013
<http://www.f-secure.com/weblog/archives/00002617.html>
12. Renesys Blog; Jim Cowie; *The New Threat: Targeted Internet Traffic Misdirection*; published 19 Nov 2013;
<http://www.renesys.com/2013/11/mitm-internet-hijacking/>
13. Krebs on Security; Brian Krebs; *Cupid Media Hack Exposed 42M Passwords*; published 20 Nov 13
<http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/>
14. Arstechnica; Dan Goodin; *Bitcoin's skyrocketing value ushers in era of \$1 million hacker heists*; published 27 Nov 2013;
<http://arstechnica.com/security/2013/11/bitcoins-skyrocketing-value-ushers-in-era-of-1-million-hacker-heists/>
15. Trustwave SpiderLabs Blog; Daniel Chechik; *Look What I Found: Moar Pony!*; published 3 Dec 2013;
<http://blog.spiderlabs.com/2013/12/look-what-i-found-moar-pony.html>

SECURITY & ENFORCEMENT

1. The Wired; Kim Zetter; *Feds Identify the Young Russians Behind the Top U.S. Cyber Thefts in Last 7 Years*; published 25 Jul 2013
<http://www.wired.com/threatlevel/2013/07/albert-gonzalez-conspirators/>
2. Krebs on Security; Brian Krebs; *Pavel Vrublevsky Sentenced to 2.5 Years*; published 02 Aug 2013
<http://krebsonsecurity.com/2013/08/pavel-vrublevsky-sentenced-to-2-5-years/>
3. Forbes; Andy Greenberg; *End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market*; published 2 Oct 2013;
<http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/>

4. F-Secure Weblog; Karmina Aquino; *Blackhole, Supreme No More*; published 11 Oct 2013
<http://www.f-secure.com/weblog/archives/00002622.html>
5. InfoSecurity-Magazine; *Fidelity Investments Cyber-heist Suspects Arrested in California*; 16 NOV 13
<http://www.infosecurity-magazine.com/view/35641/fidelity-investments-cyberheist-suspects-arrested-in-california/>
6. The Register; Iain Thomson; *Stratfor email, credit-card hacker Hammond thrown in cooler for 10 YEARS*; published 15 Nov 2013;
http://www.theregister.co.uk/2013/11/15/judge_throws_book_at_stratfor_hacker_with_decadelong_sentence/
7. Krebs on Security; Brian Krebs; *Spam-Friendly Registrar 'Dynamic Dolphin' Shuttered*; published 25 Nov 13
<http://krebsonsecurity.com/2013/11/spam-friendly-registrar-dynamic-dolphin-shuttered/>
8. The Register; John Leyden; *PayPal 13 plead guilty to launching DDoS attacks*; published 9 Dec 2013;
http://www.theregister.co.uk/2013/12/09/paypal_13_guilty_pleas/
9. Krebs on Security; Brian Krebs; *Microsoft Patches Plug 23 Security Holes*; published 13 Aug 2013
<http://krebsonsecurity.com/2013/08/microsoft-patches-plug-23-security-holes/>
10. F-Secure Weblog; Sean Sullivan; *iOS 7 Security Prompts*; published 19 Sep 2013
<http://www.f-secure.com/weblog/archives/00002610.html>
11. Microsoft Security Research & Defense Blog; *CVE-2013-3906: a graphics vulnerability exploited through Word documents*; published 5 Nov 13
<http://blogs.technet.com/b/srd/archive/2013/11/05/cve-2013-3906-a-graphics-vulnerability-exploited-through-word-documents.aspx>
12. ZDNet; Larry Seltzer; *Adobe patches security issues in Flash and Shockwave players*; published 10 Dec 2013;
<http://www.zdnet.com/adobe-patches-security-issues-in-flash-and-shockwave-players-7000024150/>
13. ZDNet; Larry Seltzer; *Microsoft patches 4 zero-day vulnerabilities in major Patch Tuesday event*; published 10 Dec 2013;
<http://www.zdnet.com/microsoft-patches-4-zero-day-vulnerabilities-in-major-patch-tuesday-event-7000024145/>
14. F-Secure Weblog; Sean Sullivan; *EU Parliament Civil Liberties Committee on US Surveillance*; published 5 Sep 2013
<http://www.f-secure.com/weblog/archives/00002603.html>
15. The Wired; Kim Zetter; *RSA Tells Its Developer Customers: Stop Using NSA-Linked Algorithm*; published 19 Sep 2013;
<http://www.wired.com/threatlevel/2013/09/rsa-advisory-nsa-algorithm/>
16. Los Angeles Times; Carol J. Williams; *Amid NSA spying, European lawmakers vote to tighten data protection*; published 21 Oct 2013;
http://www.latimes.com/world/worldnow/la-fg-wn-europe-data-protection-nsa-spying-20131021,0,1164544_story
17. The Register; Iain Thomson; *Microsoft breaks bug-bounty virginity in \$100,000 contest*; published 19 Jun 2013;
<http://technet.microsoft.com/en-US/security/dn425036>
18. Washington Post; Craig Timberg, Barton Gellman and Ashkan Soltani; *Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic*; published 27 Nov 2013;
http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html
19. Krebs on Security; Brian Krebs; *Facebook Warns Users After Adobe Breach*; published 11 Nov 2013;
<http://krebsonsecurity.com/2013/11/facebook-warns-users-after-adobe-breach/>
20. The Guardian; Ian Traynor; *NSA surveillance: Europe threatens to freeze US data-sharing arrangements*; published 26 Nov 2013;
<http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing>
21. Naked Security Blog; Lee Munson; *Microsoft and partners fight back against the ZeroAccess botnet*; published 6 Dec 2013;
<http://nakedsecurity.sophos.com/2013/12/06/microsoft-and-partners-take-down-zeroaccess-botnet/>

MALWARE & VULNERABILITIES

1. F-Secure Weblog; Brod Aquilino; *Windows Version of the Janicab Malware*; published 23 July 2013
<http://www.f-secure.com/weblog/archives/00002581.html>
2. F-Secure Weblog; SecResponse; *Browlock Ransomware Targets New Countries*; published 14 Aug 2013
<http://www.f-secure.com/weblog/archives/00002590.html>
3. F-Secure Weblog; Sean Sullivan; *IE Vulnerability Update #Japan #Metasploit*; published 2 Oct 2013;
<http://www.f-secure.com/weblog/archives/00002615.html>
4. The Register; Neil McAllister; *Malware culprit fingered in mysterious Tor traffic spike*; published 9 Sep 2013;
http://www.theregister.co.uk/2013/09/09/malware_culprit_fingered_in_mysterious_tor_traffic_spike/

5. US-CERT; *CryptoLocker Ransomware Infections*; published 5 Nov 2013
<http://www.us-cert.gov/ncas/alerts/TA13-309A>
 6. F-Secure Weblog; Sean Sullivan; *Microsoft Security Advisory (2896666) #APT*; published 6 Nov 2013
<http://www.f-secure.com/weblog/archives/00002634.html>
 7. ZDNet; Michael Lee; *Google catches French govt spoofing its domain certificates*; published 9 Dec 2013;
<http://www.zdnet.com/google-catches-french-govt-spoofing-its-domain-certificates-7000024062/>
 8. F-Secure Weblog; SecResponse; *Sharking: High-Rollers in the Crosshairs*; published 10 Dec 2013
<http://www.f-secure.com/weblog/archives/00002647.html>
-
9. Naked Security Blog; Lee Munson; *Anatomy of another Android hole - Chinese researchers claim new code verification bypass*; published 17 July 2013;
<http://nakedsecurity.sophos.com/2013/12/06/microsoft-and-partners-take-down-zeroaccess-botnet/>
 10. F-Secure Mobile Threat Report Q3 2013; *Threat Highlights (p. 10)*; published 6 Nov 2013;
http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf
 11. F-Secure Mobile Threat Report Q3 2013; *Threat Highlights (p. 8)*; published 6 Nov 2013;
http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf
 12. F-Secure Weblog; Mikko Hypponen; *FinFisher Range of Attack Tools*; published 30 Aug 2013;
<http://www.f-secure.com/weblog/archives/00002601.html>
 13. Bluebox Blog; *Black Hat Presentation on Android "Master Key"*; published 16 Aug 2013;
<http://bluebox.com/corporate-blog/android-master-key-presentation/>
 14. F-Secure Mobile Threat Report Q3 2013; *Threat Highlights (p. 9)*; published 6 Nov 2013;
http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf
 15. Forbes; *iPhone Fingerprint Scanner Hacked; Should You Care?*; Mark Rogowsky; published 22 Sep 2013;
<http://www.forbes.com/sites/markrogowsky/2013/09/22/iphone-fingerprint-scanner-hacked-should-you-care/>
 16. FireEye Blog; *Ad Vulna: A Vulnaggressive (Vulnerable & Aggressive) Adware Threatening Millions*; published 4 Oct 2013;
<http://www.fireeye.com/blog/technical/2013/10/ad-vulna-a-vulnaggressive-vulnerable-aggressive-adware-threatening-millions.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 2013, the company's revenues were EUR 155 million and it has over 900 employees in more than 20 offices worldwide. F-Secure Corporation is listed on the NASDAQ OMX Helsinki Ltd. since 1999.

Protecting the Irreplaceable

F-Secure proprietary materials. © F-Secure Corporation 2014.
All rights reserved.

F-Secure and F-Secure symbols are registered trademarks of
F-Secure Corporation and F-Secure names and symbols/logos
are either trademark or registered trademark of F-Secure
Corporation.