THREAT REPORT

H2 2014

F-Secure

CONTENTS

CONTENTS 2

AT A GLANCE 3

FOREWORD 4

OF NOTE 5

ARTICLE 6

INCIDENTS CALENDAR 8

THREAT LANDSCAPE SUMMARY 10

MOBILE THREATS 14

MAC MALWARE 15

SOURCES 16

H2 2014 THREAT REPORT AT A GLANCE...

INCIDENTS CALENDAR

Page 8

JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER
	SynoLocker trojan targets NAS devices	POODLE bug hits SSL web encryption EU launches pilot cybercrime taskforce	Global spike in malware-assisted ATM threats Google accounts add USB Security Keys option		NSA's Auragold reportedly able to hack any wireless network Massive Sony data hack prompts FBI warning

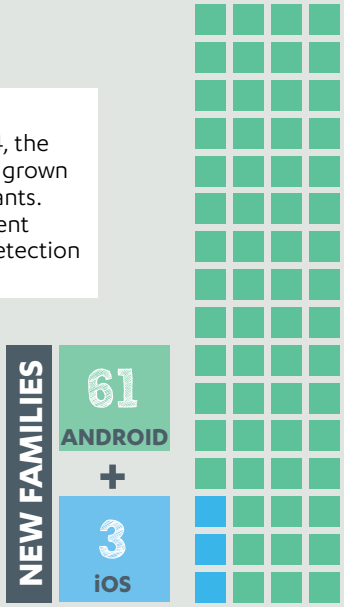
MOBILE THREATS

Page 14

Android continues to be the favored target for the majority of mobile malware. Threats directed towards iOS exist but there are far fewer of them.

KOLER & SLOCKER
Since their debut in the first half of 2014, the Koler and Slocker ransom families have grown rapidly as their authors create new variants. These families are now the most prevalent Android ransomware reported in the detection statistics from our product users.

TROJAN-SPY:IPHONEOS/WIRELURKER
Pirated apps containing Wirelurker are offered on third-party app sites for OS X machines. iOS devices connected via USB to the infected machine have apps downloaded onto them. Apple subsequently blocked Wirelurker-tainted apps in its store.



MAC MALWARE

Page 15

The Mac threat landscape sees newcomers trying to fill up the previously quiet scene. The malware are getting more sophisticated in terms of their capabilities and their distribution methods.

WIRELURKER
Infects iOS devices that are connected to infected OS X machines via USB.

VENTIR
Steals username and password credentials and forwards them to a remote server.

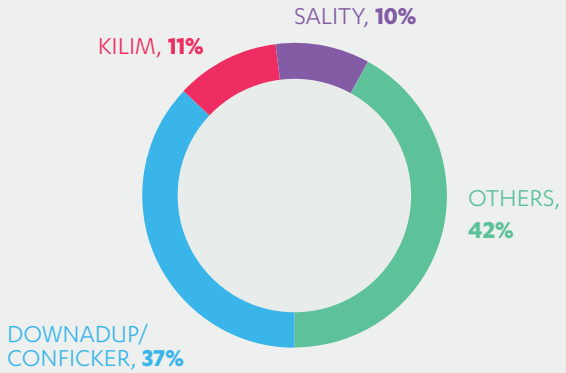
XLSXMD
Used in Advance Persistent Threat (APT) attacks.

PC MALWARE TOP-10 THREATS

Page 11

The list of top threats in the Windows landscape continues to be dominated by existing malware families. Some of these families have been around for years, and sustain themselves by infecting unpatched machines.

BY PERCENTAGE



RANKED

1 DOWNADUP (aka CONFICKER)
This 7-year old worm exploits the MS08-067 vulnerability in Windows. It spreads over the Internet and through removable media and network shares.

2 KILIM
A family of malicious browser extensions that post unwanted content (messages and/or links, Likes, etc) to the user's Facebook accounts. They can also alter web browser settings.

3 SALITY
A large family of viruses that infect EXE files and hide their presence on infected system. Variants may kill processes, steal data and perform other harmful actions.

4 RAMNIT
5 AUTORUN
6 RIMECUD
7 MAJAVA
8 ANGLEREK
9 WORMLINK
10 BROWLOCK

FOREWORD

by
Mikko Hypponen
Chief Research Officer
F-Secure
@Mikko

I spend a lot of time thinking about our enemies.

I strongly believe that attacker attribution is one of the most important things an organization can do to protect itself. That is, figuring out who is out to get you.

This is not as straightforward as it might seem — different kinds of organizations are targeted by different kinds of attackers. And we have no hope of defending ourselves if we don't understand who the attackers are. The various attackers have different motives; they use different techniques and they pick different targets.

Different attacks require organizations to implement different safeguards. Protecting data and credit card numbers from online criminals is completely different from protecting a network against a distributed denial-of-service attack launched by a hacktivist gang.

> "... attacker attribution is one of the most important things an organization can do to protect themselves."

It's also different to protect your organization against an espionage attack launched by a hostile nation-state. Some organizations might even be targeted by extremists or terrorist groups.

The good news is that not every organization is targeted by all the attackers.

The bad news is that no one can identify your potential attackers as well as yourself. Attacker attribution work is hard to outsource.

We all have limited resources and limited budgets to defend our networks. Understanding the enemy enables us to focus our resources to where it matters the most.

PRIVACY ADVOCATES ASKING THE WRONG QUESTIONS DO MORE HARM THAN GOOD

by
Sean Sullivan
Security Advisor
F-Secure
@5ean5ullivan

F-Secure recently conducted a short security and privacy perception survey [1] with 1,004 people (501 in the United Kingdom / 503 in the United States) and asked the following question:

Do you have anything to hide?

I predicted the majority of respondents would answer "no". And in fact, 83% did just that. UK respondents had a slightly higher rate of "no" than did the US.

Is this result evidence that people don't care about their privacy? No! Of course not. Did the survey participants give the "wrong" answer? (As some of my colleagues have suggested in the past.) No. The answer is right – it's the question that's wrong. What do I mean by that?

Asking people if they have anything to "hide" summons up complicated and often conflicting emotions. You might as well be asking people – **are you a dishonest person**? The question is emotionally charged and so of course people react to it in a defensive manner – I think it is perfectly natural that 83% of people said no. Expecting any other result is just daft.

The next question survey question was as follows:

Would you want to share everything about your life with everyone everywhere, all the time, forever?

I predicted the majority would again say "no". And my prediction was proven correct – 89% of respondents did not want to be exhibitionists. Once again the UK respondents had a slightly higher rate of "no" than did the US.

In my opinion, both questions are attempting to get at the same basic thing – is privacy important?

I think privacy is important.

Unfortunately, I fear too many privacy advocates are currently asking people if they have anything to hide. And I believe this approach is counterproductive to the cause.

In future surveys, I plan to test questions such as this:

Are there things in your past that are best left forgotten?

I predict the majority of people asked will say "yes".

And "yes" is the gateway to opening minds to your message.

NOTE

1. For more details of the survey, including a copy of the data, feel free to contact Sean Sullivan via Twitter.

ARTICLE

WHY?

by
David Perry
Guest contributor
http://davidperryvirus.com/

What is the nature of the threat we face?

What does it mean to you personally?

How will this threat manifest in your own life?

How does this threat measure up against threats that we have faced in the past?

What can we do about it?

The loss of Privacy will be a much bigger deal than malware ever was.

We are all aware that there are programs intended to destroy our computers, only there aren't. Despite working every day of the last 24 years in the computer security business and an expert's view of malware [1] under a microscope's lens, I have yet to see any virus, any Trojan or worm or any of the assorted programs known as malware ever damage a computer system in any way. Data, yes, a tiny fraction of malware will destroy computer data and software, and an even tinier fraction will erase or overwrite the flash ROM BIOS that is in your computer, but, damaged monitors or hard drives or systems so severely hacked that they need to be tossed in the trash? Not one. Not ever.

If you have thrown away a computer system because it was damaged by viruses then you were mistaken. That just doesn't happen. You might believe that it does. Your cousin who works on computers at his work might tell you it does. You might know a person who knows somebody at the CIA that swears that it does but it doesn't. Now it's possible that some time in the future, some sort of as yet unknown type of computing hardware might be damaged by some also as yet unknown piece of malware, but despite a mountain of folklore and plenty of popular movies to the contrary, this does not happen.

Second, you might be using a program to protect your computer called antivirus (AV). You also might be using a program called antimalware (AM). Overall there are no functional differences between these two packages. No AV or AM program has ever specialized in just detecting viruses. Even the earliest AV programs to my knowledge began life with Trojan and Worm detection built right in. The majority of malicious software that is detected, blocked and removed by your modern Antivirus program are not viruses. Viruses, although they still exist and are still created are only a tiny minority of the malware seen in the world today.

This does not matter; all of these programs are about detecting all of the malware, all of the time. Don't be fooled by the name on the box. The marketing department names the box and might just be banking on familiarity to sell their product. Other marketing departments might be counting on your misunderstanding of what's going on to sell you a second program to defend what you are already defending. It's not the job of the marketing department to educate you about what you need. That's my job.

WHAT IS MALWARE AND WHAT DOES IT DO?

As we have recently pointed out, malware is malicious and unwanted software. It is used by a number of different sorts of people, for a number of different sorts of purposes. It could draw a picture on your screen or write text to you. It might destroy your data. (It seldom does these days.) It might steal your password or your credit card number or even your access to your own computer system. It might encrypt your data and ransom it back to you. It might even be used to gain access to your employer, or your relative's employer, or your friend's employer.

Frequently in modern times, it might just be using your system as a staging area to attack people you don't even know. For all these reasons and a thousand more it is

FOOTNOTE

1. The term malware was invented by Yisrael Radai, a recently deceased virus expert, in 1990. Malware is the umbrella term that covers viruses, Trojans, rootkits, worms, ransomware, adware, spyware, etc. Malicious and Unwanted software is all Malware. It's all malware, so my saying that computer hardware is never destroyed by malware is not just a matter of semantics (no pun intended) it is merely a matter of fact. This doesn't happen. Get used to that idea.

worth blocking. But there is something else that is a far worse threat to you. I am talking about the loss of your privacy.

PRIVACY

It's just possible that privacy as we understand it today is a recent historical development. In the past people knew what you did behind closed doors, because there really weren't any closed doors. The whole extended family lived in one room. Yet for centuries we have seen privacy as a right. We hold dear the idea of civil rights and civil liberties. We believe that we are entitled to freedom. These things are often referred to as our birthright. I quote from the American Declaration of Independence.

> *"We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. — That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, — That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness."*

Notice that privacy is not specifically listed as among these rights. Recent argument has been made, against both; equality under the law and about the nature of unalienable rights. However, from its beginnings in the Magna Carta, in the founding of the USA and in centuries of other advances in human history these assertions proved to be universal. They have been expanded to include a number of other rights, including the right to be secure in the privacy of your home, your person and your conscience. I could summarize the struggles of history as a search for and a battle for fairness. If this is important to you, then it is time for you to pay attention.

If there is no privacy, no place of refuge for an opposing view or a different trend than the majority or ruling trend, then there is no fairness. I will elaborate.

SCIENCE FICTION

In his book *Count Zero*, William Gibson proposes a world where, in order to avoid prying eyes, extreme measures are needed. The characters enlist the help of a man called "the Finn", who seals them into a cage of circuitry designed to block out any and all surveillance from the outside world. In the movie the *Enemy of the State*, the lead character lives in a metal cage that protects him from electronic snooping. What might surprise you is that there are such cages in the world. They are called Faraday cages and they are used for all kinds of purposes. There's one at F-Secure that was used to test wireless malware that transmitted from one phone to another, without fear of infecting phones in the office.

But you can't live your life in a cage. You are out in public, on the street and more importantly you are connected. You might not know it but your every step is being recorded and analyzed. This creates a world of nearly universal surveillance.

Think of the information your phone can gather. It contains all your email, texting, gps positioning, web browsing, photos, and telephone exchanges. This is not some evil scheme, but the ordinary means of advertising and marketing.

But what happens when all walls are transparent? Are you denied an apartment or auto loan? Are you cut from the work force? Do you lose status at school or at work? Are you paying too much for your health insurance because you have a family history of diabetes or other diseases? Did you vote for a candidate that somebody doesn't like? These things might not be directly reported by the record but they can easily be logically deduced. You could be denied all kinds of things without ever knowing why.

FEAR

Viruses never scared me, I have no fear of losing my data or my credit card number or even money. I can get more money, or more digital photos, these things are just an annoyance or at worst just a loss. But if I lose my privacy, it will be extremely difficult and very costly to get back. Do yourself a favor, and consider some privacy protection. All the experts agree that you should get on a virtual private network (VPN), and we happen to make a VPN that is easy to run and very secure. It is not a universal cure. But it is the best foot forward to a better tomorrow.

Switch on Freedom.

H2 2014
INCIDENTS CALENDAR

DIGITAL FREEDOM

Court rules US police needs warrants to search mobile devices

June: US Supreme Court rules that police officers must obtain search warrants to investigate the devices of individuals held under arrest

Malware reportedly tracks Umbrella movement activists

Oct: Apps distributed to protestors involved in demonstrations in Hong Kong were caught harvesting data stored on devices

ATTACKS

Eskimo trojan steams twitch.tv users

Sep: Twitch-bot account exposes users on gaming platform twitch.tv to malware that hijacks their Steam gaming account

Home Depot confirms breach in in-store POS systems

Sep: Cash register systems used in specific stores in the US & Canada were affected by malware that steals customer card numbers and email addresses

Global spike in malware-assisted ATM threats

Oct: Malaysia, Russia & other countries report cases of malware being installed on ATMs and later used to dispense cash from infected machines

MALWARE

CosmicDuke combines Cosmu & MiniDuke threats

July: First threat seen to combine MiniDuke-derived loader and Cosmu-derived payload to steal data from infected systems

SynoLocker ransom trojan targets NAS devices

Aug: Synolocker trojan targets network attached storage (NAS) devices; operator later offers to sell all keys still being held for ransom

Pitou updates Srizbi malware for more spamming

Aug: New Pitou spambot updates old Srizbi code with more features and uses infected systems for sending spam emails

New BlackEnergy variant moves from crimeware to APT

Sep: New BlackEnergy variant of crimeware trojan used by Quedagh gang to steal data from targets in Ukraine & Poland

VULNERABILITIES

Shellshock bug hits Linux, Unix machines

Sep: Developers scramble to update programs affected by a flaw in popular GNU Bourne Again Shell (BASH) that allows remote attackers to run code on affected machines

ENFORCEMENT

EU launches pilot cybercrime taskforce

Sep: EU launches cybercrime taskforce, 6-month pilot program draws personnel from European Cybercrime Center, FBI, NCA, German Federal Police

UK arrests 3 for malware-assisted ATM thefts

Oct: London Regional Fraud Team arrests 3 individuals for ATM thefts, charges them with conspiracy to defraud and money laundering

RAT users arrested in EU joint police operation

Nov: 15 individuals in several EU countries arrested for BlackShades RAT use in coordinated crackdown

PRODUCT SECURITY

Xiaomi plugs Mi-Cloud data leak on phone

Aug: Xiaomi RedMi 1S model updated to make cloud messaging opt-in and to encrypt data transmitted from device to cloud

Google accounts add USB Security Keys option

Oct: Additional two-factor authentication method using a physical USB stick now available for Google accounts security

Microsoft releases emergency Windows bug fix

Nov: All supported Windows versions receive patch for user authentication bug in Kerberos component

The Incidents Calendar lists interesting developments in digital security that took place in the second half of 2014. Items in the Calendar were reported in various technology portals, security research publications, law enforcement sites, major newspapers, and the F-Secure Weblog. Sources are listed on page 16.

DIGITAL FREEDOM

UK tribunal rules TEMPORA surveilllance doesn't breach human rights

Dec: Investigatory Powers Tribunal (IPT) rules that UK spy agency GCHQ's TEMPORA surveillance program is within legal framework

NSA's Auroragold reportedly able to hack any wireless network

Dec: American spy agency NSA reportedly monitors emails between telco providers for technical documents that can assist wireless networks hacking

ATTACKS

OnionDuke found infecting TOR exit node traffic

Nov: Russia-based TOR exit node found inserting malware into Windows programs transiting through it to steal data

Regin toolkit identified in EU APT attacks

Nov: Snowden-leaked documents claim Regin toolkit used by NSA & GCHQ to spy on EU government agencies and Belgian telco

Massive Sony data hack prompts FBI warning

Dec: Following news of Sony data hack, FBI warns US businesses about malware's capability in overriding all data on affected systems

MALWARE

Cryptowall 2.0 ransomware reported in the wild

Oct: New variant of ransom-trojan seen, throws in more anti-analysis features, updates communication methods

Turla Linux backdoor operable on Solaris

Dec: Analysis of Linux backdoor connected to Turla APT threat reveals environment set that allows it to work on Solaris

Archie & Astrum exploit kits hit the market

Dec: New exploit kits Archie & Astrum start gaining foothold in underground market for crimeware toolkits

VULNERABILITIES

Poodle bug hits web encryption

Sep: Bug found in Secure Socket Layer (SSL) 3.0 standard, which is still used by older browsers and servers, could allow a nearby attacker to hijack a user's Internet connection

ENFORCEMENT

China reportedly arrests 3 for Wirelurker malware

Nov: Suspects allegedly created programs used to attack non-jailbroken iOS devices connected to infected machines

CME campaigns against Moudoor APT trojan

Dec: Security vendors launch Coordinated Malware Eradication (CME) initiative to detect Moudoor trojan used by espionage groups

UK teen pleads guilty to Spamhaus DDoS attacks

Dec: London teen pleads guilty to DDoS attacks last year on anti-spam service and CloudFlare content distribution network

PRODUCT SECURITY

Out-of-band CVE-2014-8439 Adobe Flash Player fix

Nov: Adobe releases fix for CVE-2014-8439 vulnerability in Flash Player that is being actively targeted by the Angler exploit kit

Adobe hardens CVE-2014-8439 patch

Nov: Adobe releases additional patch to harden Flash Player against CVE-2014-8439 flaw found earlier

Apple updates OS X to close NTP flaws

Dec:Apple releases first automated patch for OS X machines to close critical vulnerability in Network Time Protocol (NTP)

H2 2014 THREAT LANDSCAPE SUMMARY

EMERGING TOP THREATS

The detections reported to our telemetry systems by F-Secure product users in the second half of 2014 included some notable changes from the reports collected during the first half of the year.

As in our previous half-year reports, Downadup (also known as Conficker) continues to perch atop the Top 10 Threats list. But of more interest in this period however is the ascendance of **Kilim**, **AnglerEK**, **Rimecud** and **Browlock** families, which mirror underlying changes and trends in the threat landscape in 2014.

EXPLOITING VULNERABILITIES

The most notable trend in our detection reports has been the increasing dominance of vulnerability-leveraging malware. This means that unpatched operating systems and applications continue to contribute to these detection statistics, though in far lower numbers than in previous years.

One particular form of such malware is *exploit kits* — toolkits planted on compromised websites that exploit vulnerabilities on a site visitor's device in order to silently drop malware onto his or her machine. The Angler and Astrum exploit kits (listed as **AnglerEK** and **AstrumEK** in our statistics) surged in our detection statistics in 2014. Reports of detections of the AnglerEK kit have skyrocketed since we started detecting it in September 2014 — making it a clearly visible presence in the Threat Prevalence Trends chart (page 13).

Malware targeting vulnerabilities in the Java platform (collectively identified as **Majava**) are still effective enough to appear in our Top 10 Threats list. We can infer from this that people continue to use unpatched versions of the popular development platform. Variants in the **Wormlink** family, which exploit a vulnerability in the Windows operating system, point to another common target — unpatched Windows machines.

A quick glance at a breakdown of threats by region (page 12) shows that these vulnerability-targeting malware appear most active in North America and Europe. While generalizations are tricky at best, the other regions appear to be more affected by 'older' threats that are no longer effective against newer or more up-to-date operating systems or programs.

As such, it is at least plausible that the prevalence of vulnerability-targeting malware in North America and Europe is loosely correlated to a difference in the behavior and machine setup of users in the various regions.

SOCIAL MEDIA & WORMS

The introduction of **Kilim**, a family of malicious browser extensions that target Facebook users, in the Top 10 Threats chart also highlights the continuing misuse of social networking sites as a medium for spreading malware.

While threats targeting and/or spreading on social media networks are hardly new, this is perhaps the first year in which we saw a threat family targeting a single social media network gains such widespread prevalence. Kilim's presence in South America, the Middle East and Oceania is more of a testament to Facebook's global reach than anything else, but it nonetheless speaks to the severity of the threat.

While nowhere near the same level of prevalence, the **Rimecud** worm family also uses social media networks to spread its infections across continents.

Continued on page 13

TOP 10 THREATS, H2 2014

37% CONFICKER/DOWNADUP

A worm that exploits the MS08-067 vulnerability in Windows to spread over the Internet, removable media and network shares. It has been a constant global presence over the last 7 years.

TOP 5 COUNTRIES (PER 10,000 USERS)	
United Arab Emirates	8,385
Malaysia	6,274
Serbia	3,606
Romania	3,502
Brazil	1,556

11% KILIM

A family of browser extensions that post unwanted content (messages and/or links, Likes, etc) to Facebook accounts. They can also alter web browser settings.

TOP 5 COUNTRIES (per 10,000 users)	
Vietnam	7,469
Philippines	2,046
Thailand	1,776
Mexico	1,265
Brazil	1,388

10% SALITY

A large family of viruses that infect EXE files and hide their presence on infected systems. Variants may kill processes, steal data and perform other harmful actions.

TOP 5 COUNTRIES (per 10,000 users)	
Pakistan	3,523
Egypt	1,856
Tunisia	1,095
Malaysia	1,041
Turkey	1,020

8% RAMNIT

A family of viruses that infect EXE, DLL and HTML files. Variants may also drop a file that tries to download more malware from a remote server.

TOP 5 COUNTRIES (per 10,000 users)	
Indonesia	6,527
Pakistan	3,976
Vietnam	2,645
Tunisia	1,486
Malaysia	1,248

7% AUTORUN

A family of worms that spread mostly via infected removables and hard drives, and can perform harmful actions such as stealing data, installing backdoors and so on.

TOP 5 COUNTRIES (per 10,000 users)	
Malaysia	669
Turkey	315
India	306
Brazil	160
Taiwan	143

7% MAJAVA

A collection of exploits against vulnerabilities in the popular Java development platform. A successful attack can, among other things, give the attacker total system control.

TOP 5 COUNTRIES (per 10,000 users)	
Brazil	132
United States	131
Canada	113
Netherlands	89
Italy	54

7% RIMECUD

A family of worms that spread mostly over removable drives and instant messaging networks. They can also install a backdoor that allows a remote attacker to access and control the system.

TOP 5 COUNTRIES (per 10,000 users)	
Spain	196
France	188
Italy	89
United States	86
United Kingdom	81

6% ANGLEREK

A collection of exploits for multiple vulnerabilities. A successful attack can, at worst, give the attacker total system control.

TOP 5 COUNTRIES (per 10,000 users)	
United States	185
Switzerland	133
Canada	122
United Kingdom	84
Netherlands	62

5% WORMLINK

Specifically-crafted shortcut icons used to exploit the critical CVE-2010-2568 vulnerability in Windows to gain total system control.

TOP 5 COUNTRIES (per 10,000 users)	
Vietnam	2,945
Pakistan	1,438
Malaysia	1,364
Tunisia	903
Philippines	413

4% BROWLOCK

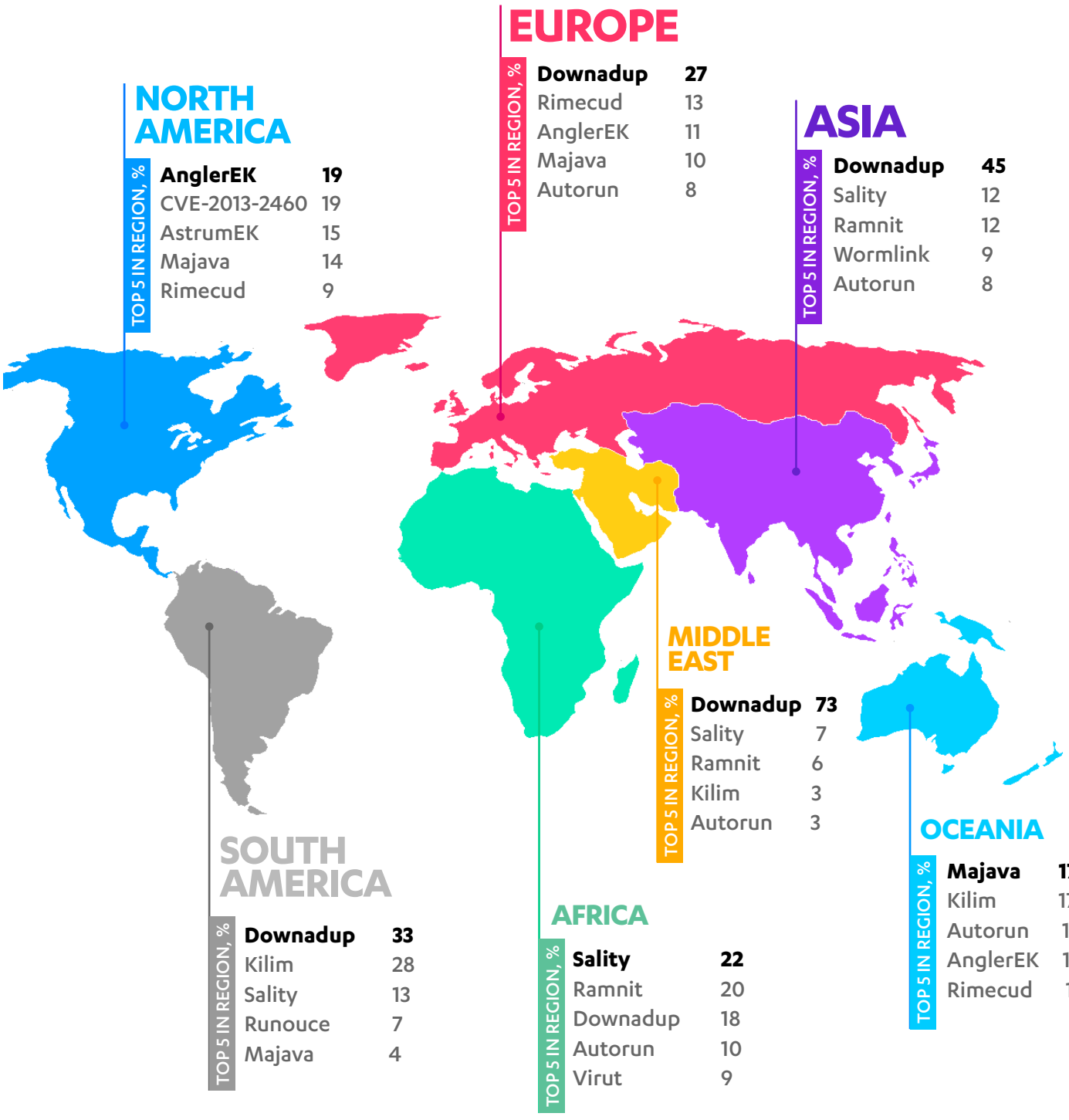
A "police-themed" ransomware family that steals control of the users' system, allegedly for possession of illegal materials. It then demands payment of a "fine" to restore normal access.

TOP 5 COUNTRIES (per 10,000 users)	
Switzerland	138
Belgium	57
United States	55
Netherlands	54
Germany	49

THREATS BY REGION, H2 2014

Most reports of threats seen by F-Secure users in H2 2014 originated from Europe and Asia, but there has been a significant increase in activity reports from South America.

The 7-year old Downadup worm continues to bother four regions, but North America's top threat is now the Angler exploit kit. In Africa, the ancient Sality virus family dominates. The biggest threat in Oceania comes from malware targeting the Java platform.



Continued from page 10

RANSOMWARE

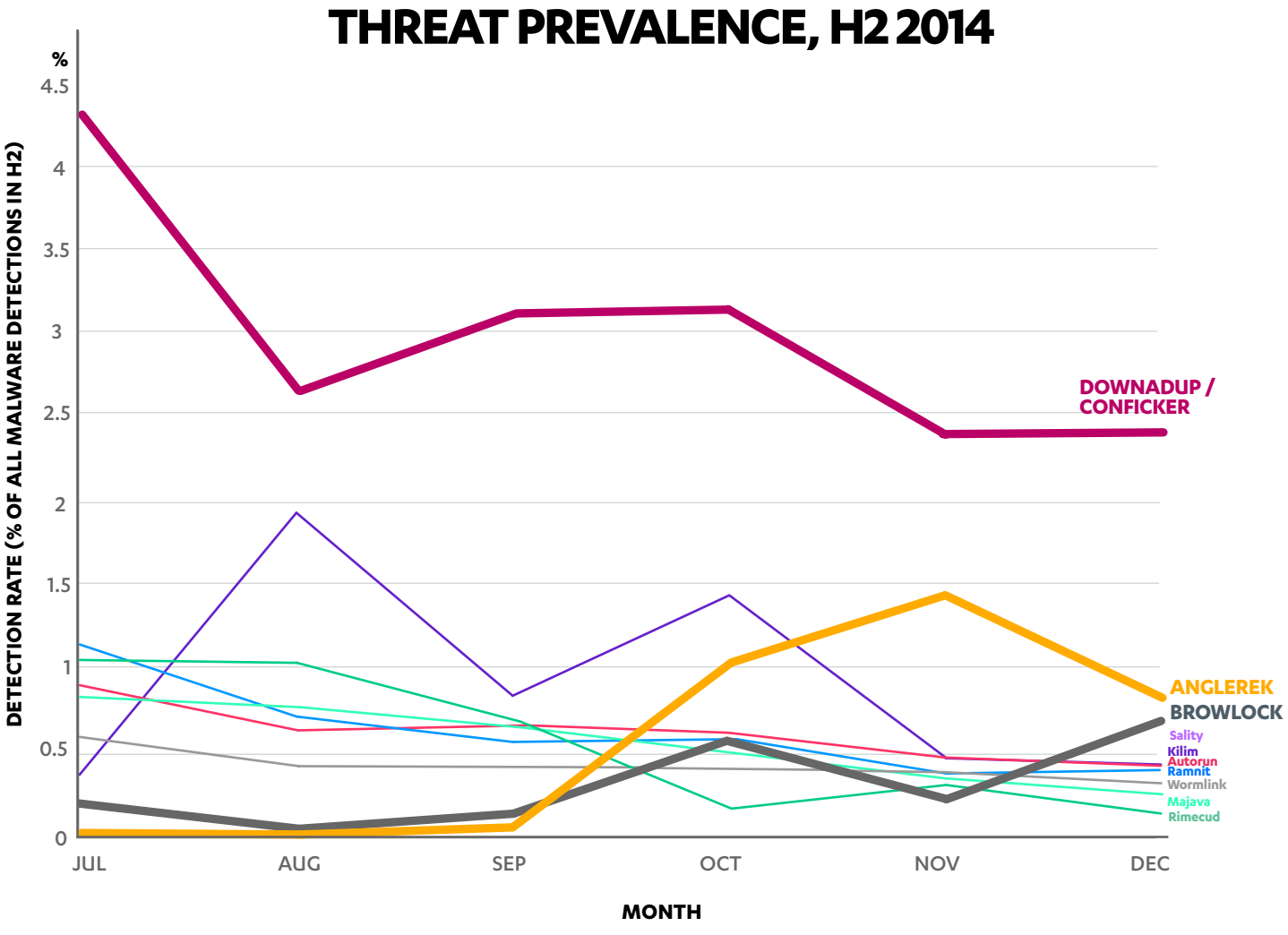
And finally, when we look at the pattern of prevalent threats being reported by users of our products (below), the rising presence of the **Browlock** family in the statistics reflects the growth of ransomware as a whole.

This particular form of malware has been a noticeable problem for users in the past couple of years, and of all the threats seen, may be the most problematic. Though the details may differ between families, this current crop of ransomware typically encrypts files held for ransom, making them effectively impossible to recover without the decryption key held by the attacker(s).

In addition to older threats such as **Cryptolocker** and **CryptoWall**, new families such as **CTB-Locker** and **SynoLocker** are emerging as noteworthy PC-targeted menaces. The emergence of the SynoLocker family, which infects network attached storage (NAS) devices, is also a clear indication that malware developers are expanding their products' targeting capabilities.

On Android, the Koler and Slocker ransom-trojan families have also been busy increasing their count of variants, making them the largest ransomware families on that platform.

The extreme difficulty in decrypting affected files without a decryption key, and the various thorny issues involved in paying a ransom (especially if a business is affected), makes ransomware a particularly difficult threat to resolve. The recommended remediation for recovering from a ransomware infection is to report the incident to the appropriate legal authorities and to restore the affected files from a clean, recent backup onto a cleaned system.



MOBILE THREATS, H2 2014

NEW FAMILIES

Android **61** iOS **3**

Ransomware on Android

Threats locking the user's data and/or device for payment continue to grow

KOLER & SLOCKER

Since their debut in the first half of 2014, the Koler and Slocker ransom families have grown rapidly as their authors create new variants. These families are now the most prevalent Android ransomware reported in our users' detection statistics.

TROJAN:ANDROID/SVPENG

Spreading via SMS messages, this banking trojan displays a phishing page when the user launches a banking app to phish for account login details. Variants also act as ransomware, blocking the device and demanding payment of a "fine" for alleged criminal activity.

LOCKSCREEN & SCAREPACKAGE

Also reported by security researchers in the second half of 2014, these two ransom-trojans use 'police-themed' notifications to scare the user into paying a "fine" for supposed illegal activity. Both threats are detected by F-Secure as variants of the Koler or Slocker families.

Trying to infiltrate iOS

Attackers keep probing the edges of the iOS security envelope, looking for a way in

EXPLOIT:IPHONEOS/CVE-2014-4377

A specially-crafted PDF document when opened on devices using unpatched versions of iOS 7.1.x can exploit the CVE-2014-4377 flaw in the system; an attacker would also need to exploit a second flaw to remotely execute code.

TROJAN-SPY:IPHONEOS/WIRELURKER

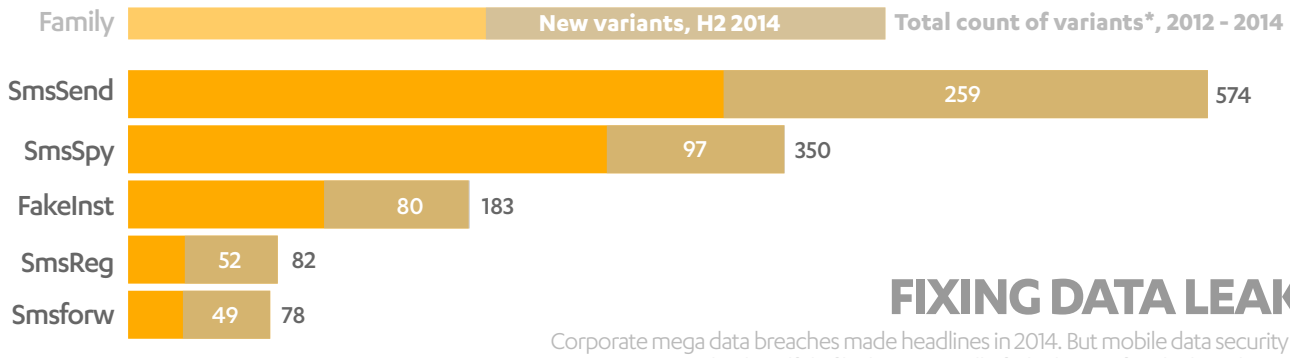
Pirated apps containing Wirelurker are offered on third-party app sites for OS X machines. iOS devices connected via USB to the infected machine have apps downloaded onto them. Apple subsequently blocked Wirelurker-tainted apps in its store.

BACKDOOR:IPHONEOS/XSSER

A remote admin tool ported from Android to iOS that's capable of harvesting data (such as SMS messages, stored photos and contacts) from the device. Installation requires a specific third-party app store repository on a jailbroken device.

FASTEST GROWING FAMILIES

Families engaged in premium-SMS message sending saw the greatest rate of development, as their operators ramp up operations and churn out more variants in the last six months.



FIXING DATA LEAKS

Corporate mega data breaches made headlines in 2014. But mobile data security saw only a handful of leaks in 2014, all of which were fixed relatively quickly.

XIAOMI UPDATES PHONE

Smartphone producer Xiaomi updated their Redmi Note model in August to change a cloud-based service from enabled by default to opt-in. They also hardened data transmission related to the service.

SNAPCHAT PLUGS LEAK

Social media company Snapchat updates its Android and iOS app to address the 'abuse' of its API that lead to the leak of 4.6 million usernames and passwords from its servers in December.

***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.

RESOURCES

1. Forbes; Anthony Kosner; ; 1 January 2014; https://www.forbes.com/sites/anthonykosner/2014/01/01/4-6-million-snapchat-usernames-and-phone-numbers-captured-by-api-exploit/
2. FSLabs; F-Secure Weblog; *Testing the Xiaomi RedMi 1S - now with OTA update*; 14 August, 2014; https://www.f-secure.com/weblog/archives/00002734.html
3. New York Times; Nicole Perlroth; *Android Phones Hit by 'Ransomware'*; 22 August 2014; https://bits.blogs.nytimes.com/2014/08/22/android-phones-hit-by-ransomware/?_r=0

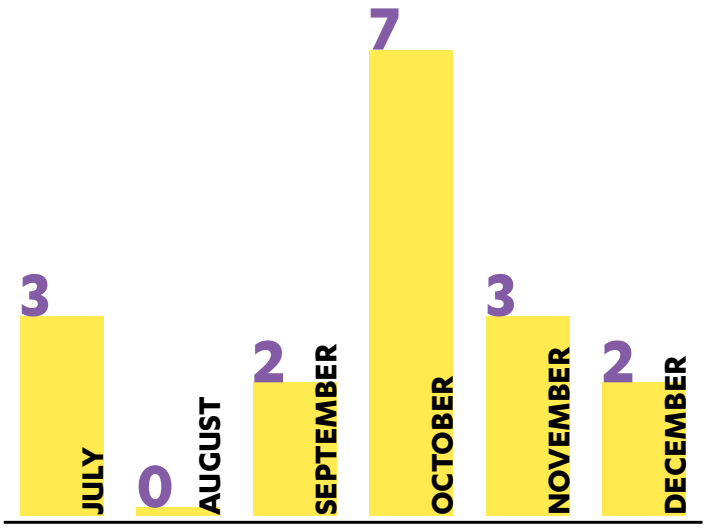
MAC MALWARE H2 2014

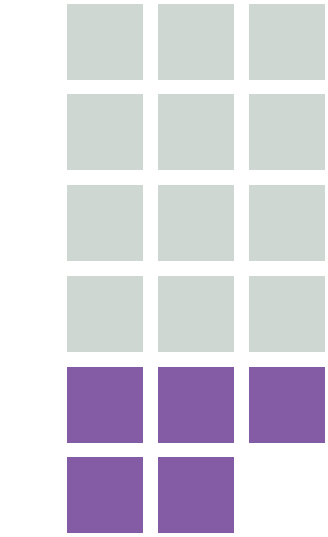
17 NEW VARIANTS of Mac malware in total were discovered between JULY to DECEMBER 2014

= **16** BACKDOOR

\+ **1** ROGUE

NEW VARIANTS DISCOVERED PER MONTH





3 NEW FAMILIES

WIRELURKER

3 VARIANTS

The **WireLurker** family consists of backdoors that were found distributed via a third-party app store in China. Malware in this family are capable of infecting an iOS device if the device is connected to an OS X machine via USB. Even a non-jailbroken device is susceptible to infection [1].

VENTIR

1 VARIANT

The **Ventir** family comprises of a backdoor that logs its victims' username and password credentials,[2] and forwards the data to a remote server.

XLSCMD

1 VARIANT

The **XLSCmd** family is made up of a backdoor that is used in Advance Persistent Threat (APT) attacks. Its code is pretty similar to its Windows-based counterpart, but the Mac version carries two extra features: keylogging and screen capturing [3].

***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.

RESOURCES

1. Palo Alto Networks; Claud Xiao; *WireLurker: A New Era In OS X And iOS Malware;* 5 November 2014; https://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/
2. Securelist; Mikhail Kuzin; *The VentirTrojan: assemble your Mac OS spy*; 16 October 2014; https://securelist.com/blog/research/67267/the-ventir-trojan-assemble-your-macos-spy/
3. SC Magazine; Danielle Walker; *Modular malware for OS X includes backdoor, keylogger components*; 20 October 2014; https://www.scmagazine.com/modular-malware-for-os-x-includes-backdoor-keylogger-components/article/378245/

SOURCES

INCIDENTS CALENDAR

DIGITAL FREEDOM

1. Adam Liptak; New York Times: *Major Ruling Shields Privacy of Cellphones; Supreme Court Says Phones Can't Be Searched Without a Warrant;* 25 June, 2014; https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0
2. Sean Gallagher, Arstechnica; *Year of the RAT: China's malware war on activists goes mobile; 3 October, 2014;* https://arstechnica.com/security/2014/10/year-of-the-rat-chinas-malware-war-on-activists-goes-mobile/
3. Owen Bowcott; The Guardian; *UK mass surveillance laws do not breach human rights, tribunal rules*; 5 December, 2014; https://www.theguardian.com/uk-news/2014/dec/05/uk-mass-surveillance-laws-human-rights-tribunal-gchq
4. Ryan Gallagher; The Intercept; *Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide*; 4 December, 2014; https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/

ATTACKS

5. FSLabs; F-Secure Weblog; *Twitch of Fate: Gamers Shamelessly Wiped Clean*; 12 September 2014; https://www.f-secure.com/weblog/archives/00002742.html
6. Maggie McGrath; Forbes; *Home Depot Confirms Data Breach, Investigating Transactions From April Onward*; 8 September 2014; https://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/
7. Brian Krebs; Krebs on Security; *Spike in Malware Attacks on Aging ATMs*; 20 October, 2014; https://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms/
8. FSLabs; F-Secure Weblog; *OnionDuke: APT Attacks Via the Tor Network*; 14 November, 2014; https://www.f-secure.com/weblog/archives/00002764.html
9. Morgan Marquis-Boire, Claudio Guarnieri, and Ryan Gallagher; *Secret Malware in European Union Attack Linked to U.S. and British Intelligence*; 24 November 2014; https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/
10. Sean Sullivan; F-Secure Weblog; *Who hacked Sony Pictures Entertainment and why?*; 4 December 2014; https://www.f-secure.com/weblog/archives/00002771.html

MALWARE

11. Timo Hirvonen; F-Secure Weblog; *CosmicDuke: Cosmu With a Twist of MiniDuke*; 2 July, 2014; https://www.f-secure.com/weblog/archives/00002723.html
12. FSLabs; F-Secure Weblog; *Pitou Q&A*; 28 August, 2014; https://www.f-secure.com/weblog/archives/00002738.html
13. Arturri Lehtio; F-Secure Weblog; *Ransomware Race (part 2): Personal media the next frontier?*; 6 August, 2014; https://www.f-secure.com/weblog/archives/00002730.html
14. Sean Sullivan; *BlackEnergy 3: An Intermediate Persistent Threat*; 25 September 2014; https://www.f-secure.com/weblog/archives/00002747.html
15. Arturri Lehtio; F-Secure Weblog; *CryptoWall Updated to 2.0*; 2 October, 2014; https://www.f-secure.com/weblog/archives/00002750.html
16. FSLabs; F-Secure Weblog; *Mysterious Turla Linux Backdoor Also For Solaris?*; 11 December, 2014; https://www.f-secure.com/weblog/archives/00002775.html
17. Patricia Dacuno; *Archie and Astrum: New Players in the Exploit Kit Market*; 11 December, 2014; https://www.f-secure.com/weblog/archives/00002776.html

VULNERABILITIES

18. Tom Fox-Brewster; The Guardian; *What is the Shellshock bug? Is it worse than Heartbleed?* 25 September, 2014; https://www.theguardian.com/technology/2014/sep/25/shellshock-bug-heartbleed
19. Peter Bright; Arstechnica; *SSL broken, again, in POODLE attack*; 15 October, 2014; https://arstechnica.com/security/2014/10/ssl-broken-again-in-poodle-attack/

ENFORCEMENT

20. Tom Brewster; The Guardian; *Europol launches taskforce to fight world's top cybercriminals*; 1 September, 2014; https://www.theguardian.com/technology/2014/sep/01/europol-taskforce-cybercrime-hacking-malware
21. Tim Ring; SC Magazine; *UK police arrest trio over £1.6 million cyber theft from cash machines*; 24 October, 2014; https://www.scmagazineuk.com/uk-police-arrest-trio-over-16-million-cyber-theft-from-cash-machines/article/379115/
22. Europol; *Users of Remote Access Trojans arrested in EU cybercrime operation*; 20 November, 2014; https://www.europol.europa.eu/content/users-remote-access-trojans-arrested-eu-cybercrime-operation

23. John Leyden; The Register; *Three WireLurker suspects arrested in China – reports*; 17 November, 2014; https://www.theregister.co.uk/2014/11/17/wirelurker_suspects_china_arrests/
24. Timo Hirvonen; F-Secure Weblog; *One Doesn't Simply Analyze Moudoor*; 14 October, 2014; https://www.f-secure.com/weblog/archives/00002753.html
25. John Leyden; The Register; *London teen pleads guilty to Spamhaus DDoS*; 17 December 2014; https://www.theregister.co.uk/2014/12/17/london_teen_pleads_guilty_to_spamhaus_ddos/

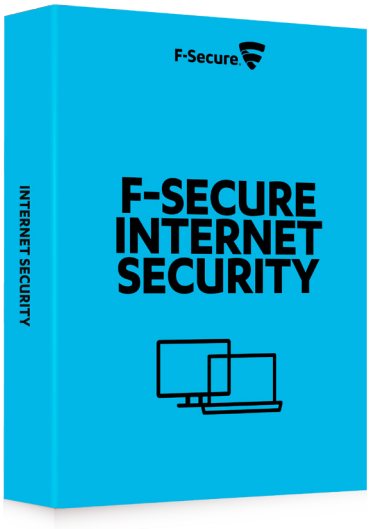
PRODUCT SECURITY

26. FSLabs; F-Secure Weblog; *Testing the Xiaomi RedMi 1S - now with OTA update*; 14 August, 2014; https://www.f-secure.com/weblog/archives/00002734.html
27. Google; *Using Security Key for 2-Step Verification*; 21 October, 2014; https://support.google.com/accounts/answer/6103523?hl=en
28. Brian Krebs; Krebs on Security; *Microsoft Releases Emergency Security Update;* 18 November, 2014; https://krebsonsecurity.com/2014/11/microsoft-releases-emergency-security-update/
29. Timo Hirvonen; F-Secure Weblog; *Out-of-Band Flash Player Update for CVE-2014-8439;* 25 November, 2014; https://www.f-secure.com/weblog/archives/00002768.html
30. Adobe; *Security updates available for Adobe Flash Player*; 25 November, 2014; https://helpx.adobe.com/security/products/flash-player/apsb14-26.html
31. Gregg Keizer; Computerworld; *Apple deploys first-ever automatic patch to fix NTP flaw*; 23 December, 2014; https://www.computerworld.com/article/2862976/apple-deploys-first-ever-automatic-patch-to-fix-ntp-flaw.html

F-SECURE INTERNET SECURITY

The best protection in the world for surfing, banking and shopping online.

Complete protection for surfing, shopping, banking and using social media. F-Secure Internet Security protects your digital content and you with real-time protection against malware, hackers and identity theft. Your online transactions are secured with banking protection, and you and your children are protected against harmful and unsavory web sites.



AV-TEST BEST PROTECTION AWARD
www.av-test.org

PREISTIPP LOGO FOR GOOD VALUE
www.com-magazin.de

PC ADVISOR ONLINE
www.pcadvisor.co.uk

F-SECURE FREEDOME

We've gathered the most sophisticated security features — VPN, anti-virus, anti-tracking, and anti-phishing — into one intuitive service. With the push of a button, Freedome watches your back.

Available in Europe, North America, Latin America, Thailand, Turkey and Russia.

BECOME UNTRACKABLY INVISIBLE

"If you want a secure connection between your IOS or Android device and the online world, Freedome provides it."

- PCWorld on Apr 25, 2014

GET IT ON Google play

Download on the App Store

SWITCH ON FREEDOM