THREAT REPORT

2015

F-Secure

AT A GLANCE

2015 HIGHLIGHTS

08

A few of the major events in 2015 concerning security issues.

ENFORCEMENT

02/15: Europol joint op takes down Ramnit botnet

07/15: FBI Darkode bazaar shutdown

ATTACKS

07/15: Hacking Team breached, data released online

09/15: XcodeGhost tainted apps prompts AppStore cleanup

VULNERABILITY

07/15: Bugs prompt Ford, Range Rover, Prius, Chrysler recalls

07/15: Android Stagefright flaw reported

PRODUCT SECURITY

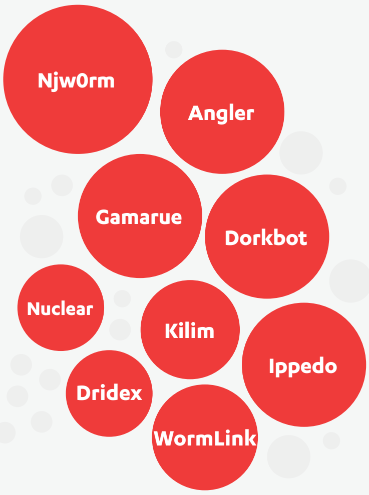
08/15: Google patches Android Stagefright flaw

08/15: Amazon, Chrome drop Flash ads

TOP MALWARE FAMILIES

12

Njw0rm was the most prominent new malware family in 2015.



BREACHING THE WALLED GARDEN

18

In late 2015, the Apple App Store saw a string of incidents where developers had used compromised tools to unwittingly create apps with malicious behavior. The apps were able to bypass Apple's review procedures to gain entry into the store, and from there into an ordinary user's iOS device.

MEET THE DUKES

20

The Dukes are a well-resourced, highly dedicated and organized cyberespionage group believed to be working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

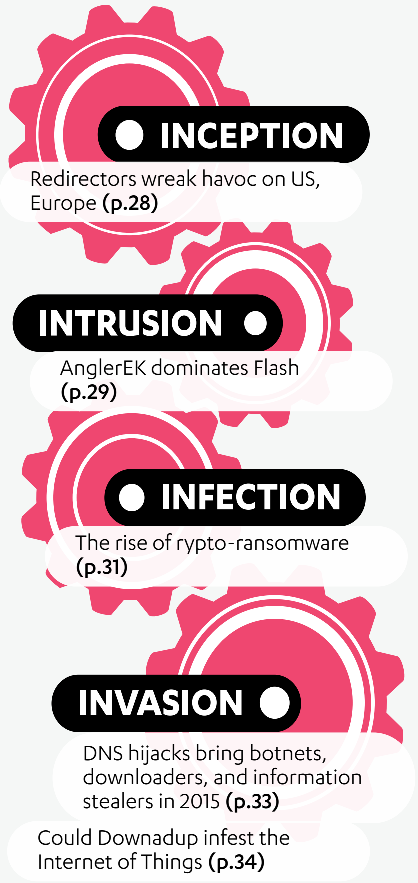
THE CHAIN OF COMPROMISE

23

The **Chain of Compromise** is a user-centric model that illustrates how cyber attacks combine different techniques and resources to compromise devices and networks. It is defined by 4 main phases: **Inception, Intrusion, Infection, and Invasion.**

THE CHAIN OF COMPROMISE: The Stages

28



● INCEPTION

Redirectors wreak havoc on US, Europe **(p.28)**

INTRUSION ●

AnglerEK dominates Flash **(p.29)**

● INFECTION

The rise of rypto-ransomware **(p.31)**

INVASION ●

DNS hijacks bring botnets, downloaders, and information stealers in 2015 **(p.33)**

Could Downadup infest the Internet of Things **(p.34)**

THREATS BY REGION

Europe was particularly affected by the Angler exploit kit. Users across the region also frequently reported Trojan:JS/Redirector detections, and document files with embedded macros that download ransomware.

15

EXECUTIVE SUMMARY

The 2015 Threat Report provides a comprehensive overview of the cyber threat landscape facing both companies and individuals. Using data from 2015, this report combines our observations on reported malware encounters with threat intelligence, and identifies several key trends and developments.

The report introduces the Chain of Compromise as an analytical concept to help readers, particularly those working in cyber security and information technology roles, understand how attackers compromise security using different combinations of tactics and resources. Some of 2015's most prominent threats, such as exploit kits, ransomware, and DNS hijacks, are discussed in relation to this model, demonstrating how users become compromised by modern cyber attacks.

Key findings discussed in the report include the establishment of worms, exploits, and macro malware as trending threats; the increasing use of crypto-ransomware for online extortion; and an increase in the use and efficiency of Flash vulnerabilities in exploit kits. The report also highlights the significance of different cyber security events that occurred in 2015, including the discovery of the XcodeGhost bug in Apple's App Store, the exposure of the Dukes advanced persistent threat group, and signs that the intersection between geopolitics and cyber security is paving the way toward a cyber arms race.

Information on the global threat landscape is supplemented with details on the prominent threats facing different countries and regions, highlighting the fact that while the Internet connects everyone, attackers can develop and distribute resources to selectively target people and companies with greater efficiency.

Authors

Edilberto Cajucom Labs • **Patricia Dacuno** Threat Intelligence, Labs • **Karmina Aquino** • Threat Intelligence, Labs • **Broderick Aquilino** Malware Protection, Labs • **Alia Hilyati** Antimalware Unit • **Sarah Jamaludin** Antimalware Unit • **Adam Pilkey** Global Communications & Brand • **Melissa Michael** Global Communications & Brand

Contributors

Mikko Hypponen Labs • **Sean Sullivan** Security Advisor • **Andy Patel** Technology Outreach • **Zimry Ong** Malware Protection, Labs • **Artturi Lehtiö** Threat Intelligence, Labs • **Janne Kauhanen** Cyber Security Services • **Dariusz Jastrzebski** Cyber Security Services

FOREWORD

Conflict used to be about borders. A long time ago, we would defend ourselves by living in cities surrounded by walls. Those walls kept the enemies away. Over time, the walls around cities became higher, longer and wider. The longer and wider these walls, the more invisible they became, marking areas of wealth, prosperity, power and belief systems. Eventually, those walls became borders. And for hundreds of years, conflict was about borders. Conflicts were about conquering land or converting people from one belief system to another.
Conflict and war have always been fueled by technology. Technology like gunpowder, steel blades, and fighter jets. The staggering possibilities of technology always seem to shine the strongest during periods of war. War has been a real driver of technology. And technology has driven war.

One of the side effects of the cold war was that the Internet was created. The US military created a way to uphold a chain of command during nuclear war. So the Internet was created as a piece of military infrastructure. By developing the Internet, mankind opened up a whole new way of waging war on one another. And the Internet has no geography. It has no borders. By creating the Internet, mankind opened up a Pandora's Box where tangible borders and recognizable enemies ceased to exist.

In addition, conflict used to be symmetric. Armies would fight other armies. But now, the technology of war has moved on. We no longer know, or can clearly describe who the enemy is, what they want to achieve, or what their motives are. We go into battle using technologies we don't fully understand, against enemies that remain in the shadows, and into wars that we will never know if they are over or not. Who is the enemy? Hackers? Anonymous? The Russian Mafia? North Korea?

It's a complex world of online conflict. And the only thing we can really be sure of is that we've seen the beginning of the next arms race: the cyber arms race.

MIKKO HYPPÖNEN
Chief Research Officer
@mikko

> "WE GO INTO BATTLE USING TECHNOLOGIES WE DON'T FULLY UNDERSTAND, AGAINST ENEMIES THAT REMAIN IN THE SHADOWS"

CONTENTS

01 GENERAL

02 RETROSPECTIVE

03 NOTABLE CASES

04 CHAIN OF COMPROMISE

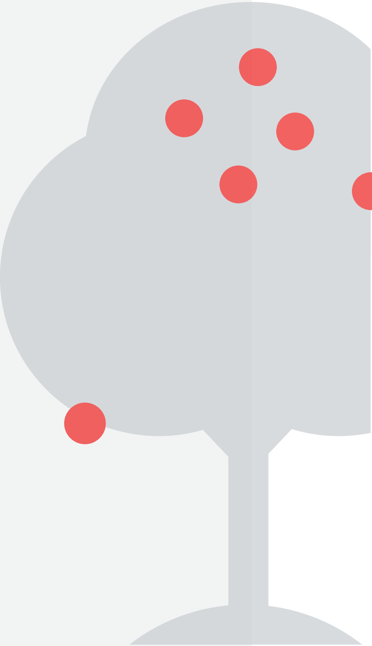
OF NOTE

Flash: The Last of the Low-Hanging Fruit

Malware exploits have been a commodity for more than a decade. So much so that during 2006, the day following Microsoft's monthly "Patch Tuesday" began to be jokingly referred to by InfoSec analysts as "Exploit Wednesday". Quick turnaround was the key to success. On Tuesday, Microsoft released its updates which were then quickly reverse engineered in order to discover the underlying vulnerability. And then, once the vulnerability was known, an exploit was crafted for use in malware attacks, which aimed to hit those who had not yet updated.

In late 2006, malware became further commoditized with the advent of malware kits. Early kits such as MPack were victims of their own success, unable to scale rapidly to meet the ever-growing demand. But such growing pains were soon enough overcome by malware services and today there are numerous exploit kits available via underground markets.

Exploit Wednesday is no longer a thing. Microsoft's software[1] is far more secure than it was 10 years ago and its patches roll out much more quickly. Exploit kits moved on from Microsoft to Adobe. Reader was the biggest target for a time (also Flash). But browsers began to offer native PDF support and Reader became unnecessary for most. Adobe adopted strong update cycles and its software moved, for a time, out of harm's way. Then Java's browser plugin became the favorite target — the weakest of the herd. Browser developers more or less forced it into a very restricted place.



And so at the moment… Adobe's Flash is the last "best" plugin still standing for exploit kits to target. But for how long?

On April 29, 2010, Steve Jobs published an open letter called "Thoughts on Flash" explaining why Apple would not allow Flash on iOS devices. Many technology analysts point to this as the beginning of the end for Flash Player, at least on mobile devices. This proved to be true. On June 28, 2012, Adobe announced there would be no certified implementations of Flash Player for Android 4.1 and it would limit installations via Google Play on August 15th 2012 [2].

Flash has since hung on to its desktop market, but everywhere you look, it's being deprecated. In August 2015, Amazon announced that "Beginning September 1, 2015, Amazon no longer accepts Flash ads." Google followed Amazon's lead in February 2016. Its ad networks, AdWords and DoubleClick, will no longer accept Flash-based display ads starting from June 30th, 2016. They'll disable Flash-based ads on January 2nd, 2017.

It's at this point that I'll make the following prediction for early 2017 — once it no longer needs to support Flash-based ads — the Google Chrome browser will start aggressively forcing users to whitelist sites that require any sort of Flash. Mozilla's Firefox and Microsoft Edge will do the same, and by spring of 2017… Flash will be effectively decapitated as far as exploit kits are concerned.

Exploit kits face a disruptive future without much new fruit in sight. Commoditized malware services will turn even further toward the use of malware attachments such as the macro-based malware that is currently trending.

If only we could keep people from clicking "okay" to make the box go away.

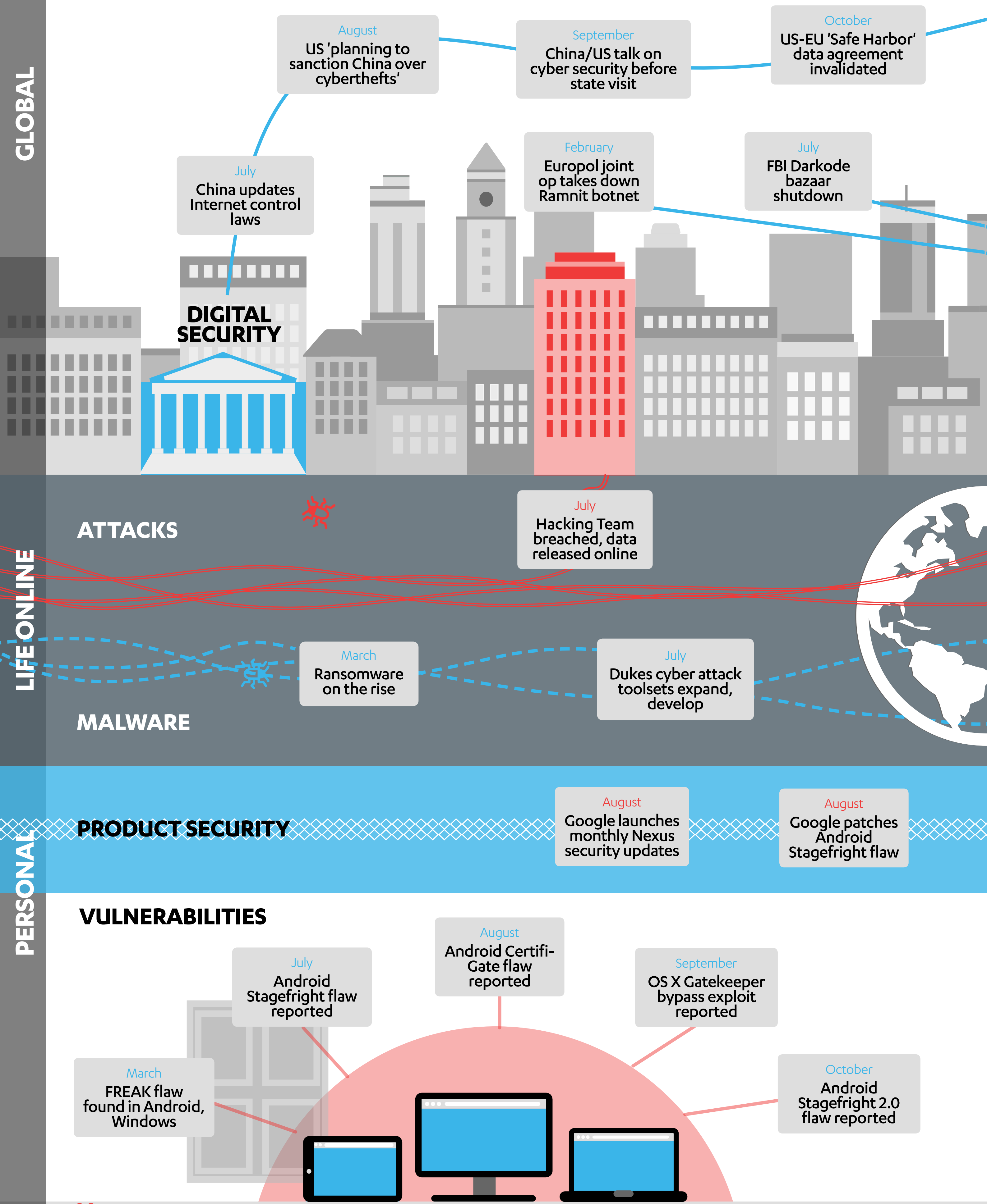
SEAN SULLIVAN
Security Advisor
@5ean5ullivan

[1] Silverlight is a general exception, it is currently exploited by kits. But hopefully Silverlight will soon go extinct as Netflix is dumping the technology.

[2] Ironically, a great deal of Android malware is pushed at people via deceptive ads claiming that a Flash update is required. Even when there is no Flash, its legacy provides a social engineering vulnerability. Google's search engineers are beginning to configure Chrome to warn about sites that display such ads.

02 RETROSPECTIVE

2015 HIGHLIGHTS



GLOBAL

DIGITAL SECURITY

July
China updates Internet control laws

August
US 'planning to sanction China over cyberthefts'

September
China/US talk on cyber security before state visit

October
US-EU 'Safe Harbor' data agreement invalidated

February
Europol joint op takes down Ramnit botnet

July
FBI Darkode bazaar shutdown

LIFE ONLINE

ATTACKS

July
Hacking Team breached, data released online

MALWARE

March
Ransomware on the rise

July
Dukes cyber attack toolsets expand, develop

PERSONAL

PRODUCT SECURITY

August
Google launches monthly Nexus security updates

August
Google patches Android Stagefright flaw

VULNERABILITIES

March
FREAK flaw found in Android, Windows

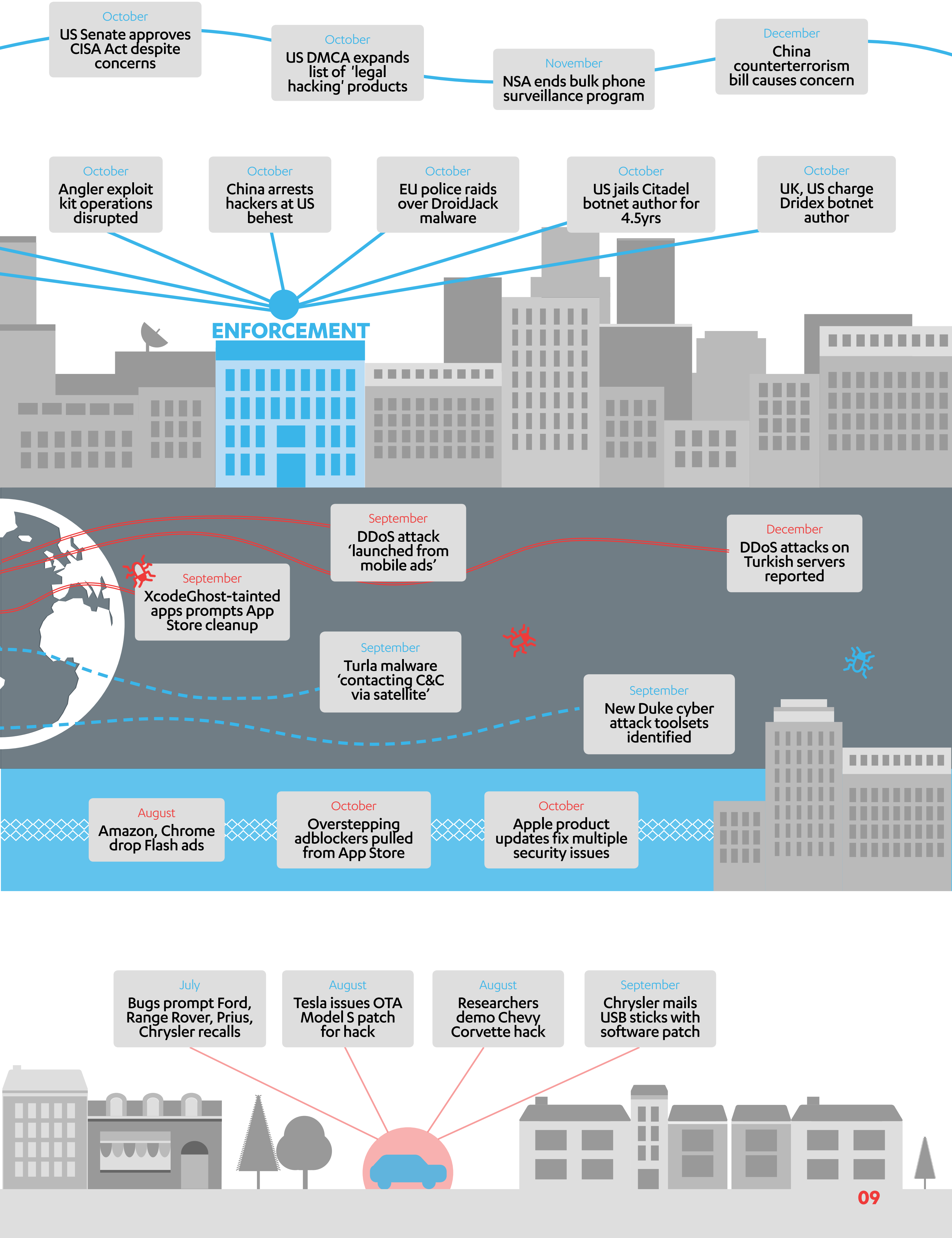
July
Android Stagefright flaw reported

August
Android Certifi-Gate flaw reported

September
OS X Gatekeeper bypass exploit reported

October
Android Stagefright 2.0 flaw reported

2015 was an eventful year for digital privacy and security. Listed below are just a few of the major events that occurred during the year that will have an impact on how users interact with technology, and each other. Sources for the listed items are on page 36.



October
US Senate approves CISA Act despite concerns

October
US DMCA expands list of 'legal hacking' products

November
NSA ends bulk phone surveillance program

December
China counterterrorism bill causes concern

October
Angler exploit kit operations disrupted

October
China arrests hackers at US behest

October
EU police raids over DroidJack malware

October
US jails Citadel botnet author for 4.5yrs

October
UK, US charge Dridex botnet author

ENFORCEMENT

September
DDoS attack 'launched from mobile ads'

December
DDoS attacks on Turkish servers reported

September
XcodeGhost-tainted apps prompts App Store cleanup

September
Turla malware 'contacting C&C via satellite'

September
New Duke cyber attack toolsets identified

August
Amazon, Chrome drop Flash ads

October
Overstepping adblockers pulled from App Store

October
Apple product updates fix multiple security issues

July
Bugs prompt Ford, Range Rover, Prius, Chrysler recalls

August
Tesla issues OTA Model S patch for hack

August
Researchers demo Chevy Corvette hack

September
Chrysler mails USB sticks with software patch

THREAT SUMMARY

The threat landscape in 2015 had similarities with trends that were observed in 2014, but there were also some significant differences. One surprise was the resurgence of macro malware — something that hasn't been seen since the early 2000s. Worms also accounted for a greater percentage of overall malware detections, which is attributable largely to the appearance of several new families in certain parts of the globe.

However, exploits and exploit kits continue to be trending threats facing people and companies in Europe and North America. Not only are they frequently detected, but 2015 saw indicators that they continue to expand their capabilities and work across a variety of attack vectors. 2015 saw a decrease in police-themed ransomware, but also more activity from a diverse number of crypto-ransomware families (more on page 31) distributed through both exploit kits and macro malware.

While they don't impact the majority of consumers, Advanced Persistent Threats (APTs) are of particular interest to governments and major corporations. In 2015, F-Secure Labs published a whitepaper detailing the various toolsets used by the Dukes, a well-resourced, highly dedicated and well-organized cyber espionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

Worms

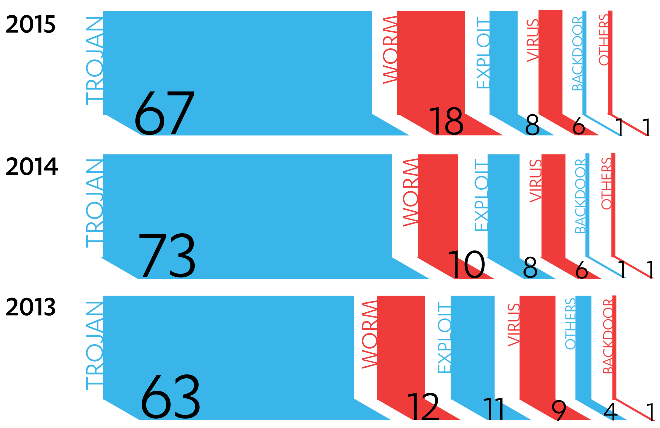
While the aging **Downadup** (also known as Conficker) worm's position as the perennial top detection has helped keep worms in general more prominent in the threat landscape than they would be otherwise, the appearance of several new families that have successfully spread through networks in certain parts of the world has made worms as a whole a more noticeable presence overall.

The most prominent of these new families is **Njw0rm** — a VBS worm that spreads through removable drives, malicious email attachments and drive-by downloads. The worm has backdoor capabilities and is essentially designed to steal information from victims. Njw0rm was detected far more often in the latter half of the year than the former, but it was more than enough to make it the most notable new malware family in last year's threat landscape.

Dorkbot is another new worm that made a noticeable impact. It shared many characteristics with Njw0rm. Both spread using removable drives. Both use backdoors, are capable of stealing information from their victims, and communicate with remote servers in order to receive additional instructions from attackers. However, Dorkbot is also able to spread itself by posting malicious links in instant messages and social media sites.

Ippedo, a third new worm that was reported frequently enough to be considered one of 2015's top threats, is another infostealer that is distributed on removable drives. However, it was not observed to be capable of spreading via other means, making it considerably less prevalent than other families.

MALWARE BY TYPE



% OF MALWARE DETECTIONS REPORTED

Worms gained notable traction during 2015 compared to the previous two years

As a broad threat classification, worms gained notable traction last year. Detections of worm families rose to 18 percent of 2015's total malware detections, compared to 10% and 12% during 2014 and 2013, respectively. However, with the exception of the now infamous Downadup worm (which was prominent all over the globe), detections of many of these worm families came from countries in Asia, the Middle East, and to a lesser extent, South America. Despite this increase, trojans (such as **Gamarue** and **Kilim**) remained the predominant type of malware users encountered in 2015.

Exploits and exploit kits

Exploits were a notable threat in 2015, and were observed to be active in many different countries. The **Angler** exploit kit was particularly noticeable in the detection reports from different areas around the globe, and was the most prevalent threat in the United States, the United Kingdom, Sweden and Australia.

The Angler exploit kit demonstrated the most comprehensive arsenal of exploits last year, but part of its success (and the success of the exploit kit business in general) appeared to be an increasingly efficient use of different attack vectors. This is signified by the prominence of the generic **Trojan:JS/Redirector** detection reports. These trojans are insinuated onto legitimate websites by attackers to redirect website visitors to sites hosting exploit kits, including Angler and **Nuclear**. They were prominent enough last year to earn the dubious distinction of being the top threat in Switzerland and Denmark.

Flash vulnerabilities greatly contributed to the success of exploits, even when not used as part of an exploit kit. Exploits identified by the generic **Exploit:SWF/Salama** detection were a noticeable part of the threat landscape, particularly in Europe and the US. While not quite as significant as Angler, both capitalized on the seemingly endless supply of users running versions of Flash containing security vulnerabilities.

Overall, the threat posed by exploits did not evolve much from previous years. They still capitalize on people and companies running outdated or unpatched software (for example, the

WormLink exploits require users to open a document file that contains code to exploit an unpatched vulnerability). They still accounted for eight percent of overall malware detections, just as they did in 2014. However, the malicious payloads that exploits deliver, such as ransomware, have diversified and become more severe, making it more important than ever to ensure people update their software when new security patches become available.

Macro malware

One interesting development in 2015's threat landscape was the resurgence of macro malware. Macro malware — documents containing hidden malicious code — was a major threat in the late 1990s to early 2000s. But when Microsoft released Office 2003, the default security settings were amended to stop macros from automatically running when a document opened, greatly stymieing attackers looking to spread malware with this method.

However, beginning in June 2015, macro malware became a notable presence in the telemetry reports again. While it was by no means as prevalent as other threats, macro malware made an impact in several European countries. They are typically spread via malicious documents attached to emails, and utilize social engineering techniques to manipulate users into opening the documents and enabling the macros, allowing the malicious code to run.

This type of macro malware is similar to exploits in that the intent is to compromise users in a way that allows attackers to drop malicious payloads. In 2015, these payloads included severe threats such as the **Dridex** banking trojan, and crypto-ransomware such as **Cryptowall**.

Android malware

The Android ecosystem saw **Slocker** rise to become a more prominent threat in 2015. While premium SMS-sending trojans remained significant — particularly in France — the growing popularity of Slocker signals a shift in mobile malware toward targeting content users store on their devices. Backdoors such as **CoudW** also indicate an increasing shift of compromise types on the operating system compared to previous years.

Mac and iOS

Backdoors were the dominant type of malware detected on Apple's operating systems in 2014 — an interesting contrast to the consistent dominance of trojans for Windows and Android.

2015 saw the biggest attack yet on Apple's ecosystem. In the **XcodeGhost** incident, tainted copies of the company's Xcode app development tool being shared on public download forums in China allowed attackers to infiltrate the highly secure AppStore. By compromising the copies of the legitimate tool that developers used to create their apps, the attackers were able to insert malicious code into the apps which were eventually uploaded to the App Store.

In this instance, the attackers took advantage of a situation unique to China, wherein developers having difficulties accessing Apple's download servers outside the country resorted to obtaining copies of the tool from local sources. This laid the foundation for the tainted apps to successfully make their way into the App Store.

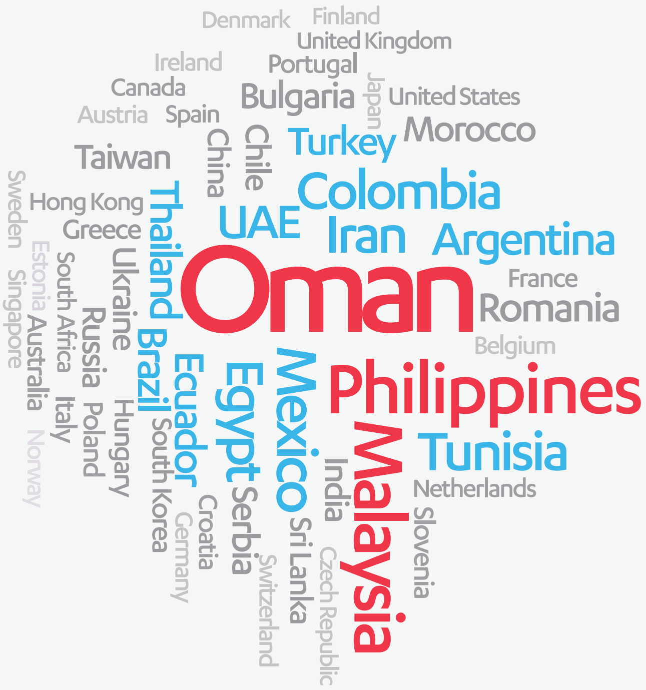
The Dukes unveiled

APTs are sophisticated programs that are usually custom-designed to stealthily infiltrate and lurk in the computer systems and networks of targeted organizations, making them a silent menace to companies that deal in sensitive trade or production information. In 2015, a whitepaper from F-Secure Labs exposed a group behind such a threat - the Dukes cyber espionage group. The Dukes are responsible for a family of toolsets that have been in use since 2008, and developed continuously over the past seven years.

The toolsets — **CozyDuke, MiniDuke, HammerDuke** and **SeaDuke** to name just a few — were all built with varying functionalities, such as password stealing, opening backdoor access on an affected system, and carrying out Distributed Denial of Service (DDoS) attacks.

While these toolsets are highly targeted and are unlikely to ever be seen by most consumers, they are of much more interest and direct relevance to individuals who are associated with state bodies or corporations that are thought to be of interest to the Dukes.

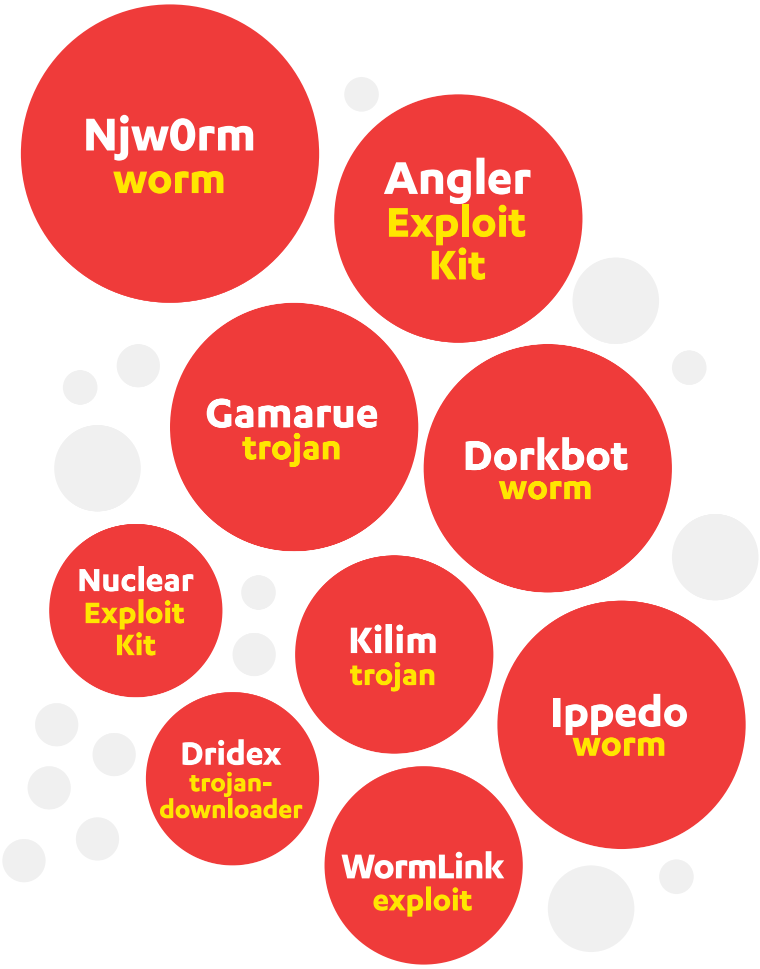
TOP REPORTING COUNTRIES



Above is a representation of the volume of detection reports we receive from a particular country versus the user population in that country (the number of people using our security products).

For example, despite a large user population in Finland, we receive relatively few detection reports from there in comparison to Oman, which has both a large user population and high rates of detections.

TOP THREATS



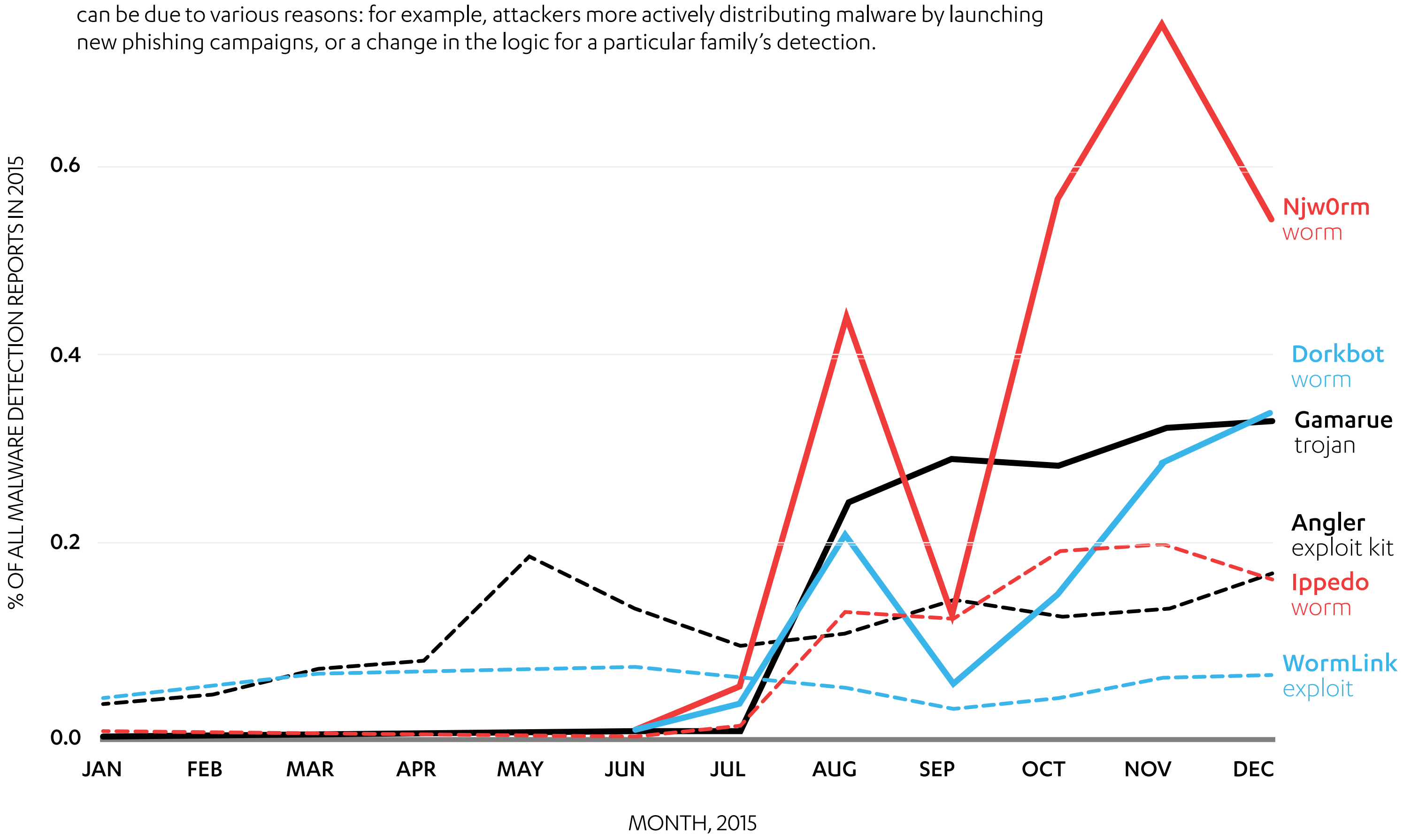
TOP MALWARE FAMILIES

When one malicious program shares distinctive code or behavioral features with another, they are usually considered to belong to the same **family**. Individual threats in a malware family are often caught by security software using a detection that identifies the family's unique characteristics.

On the right are the top threats of 2015 that belonged to unique malware families. The bubbles are sized based on percentage of all malware detections reported from our security products over the entire year.

PREVALENCE TREND FOR TOP FAMILIES

There were notable upticks in the prevalence of these top malware families throughout 2015. Detections of new worm families increased dramatically in the latter half of 2015. The changing prevalence levels can be due to various reasons: for example, attackers more actively distributing malware by launching new phishing campaigns, or a change in the logic for a particular family's detection.

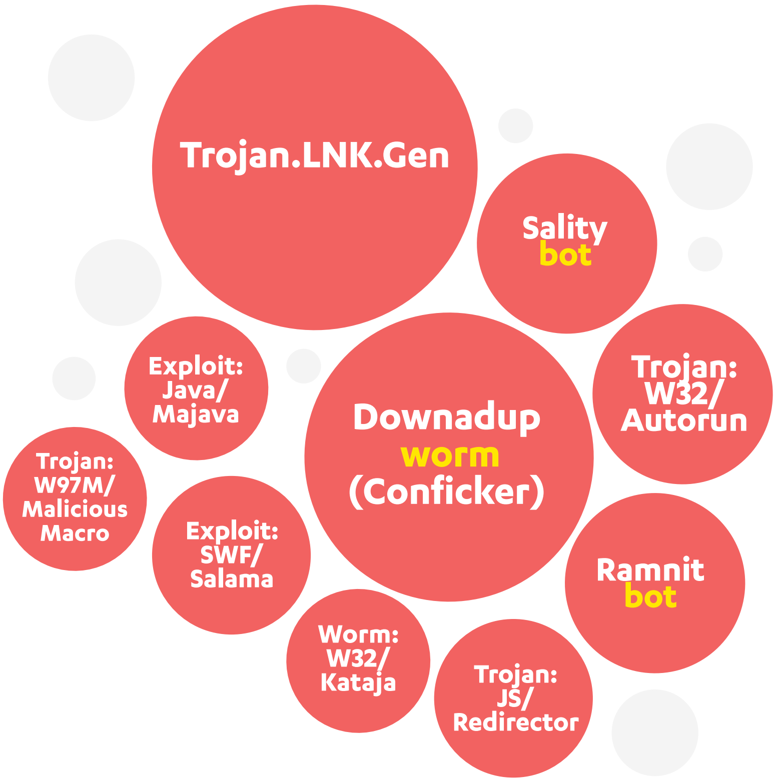


TOP LEGACY FAMILIES & GENERICS

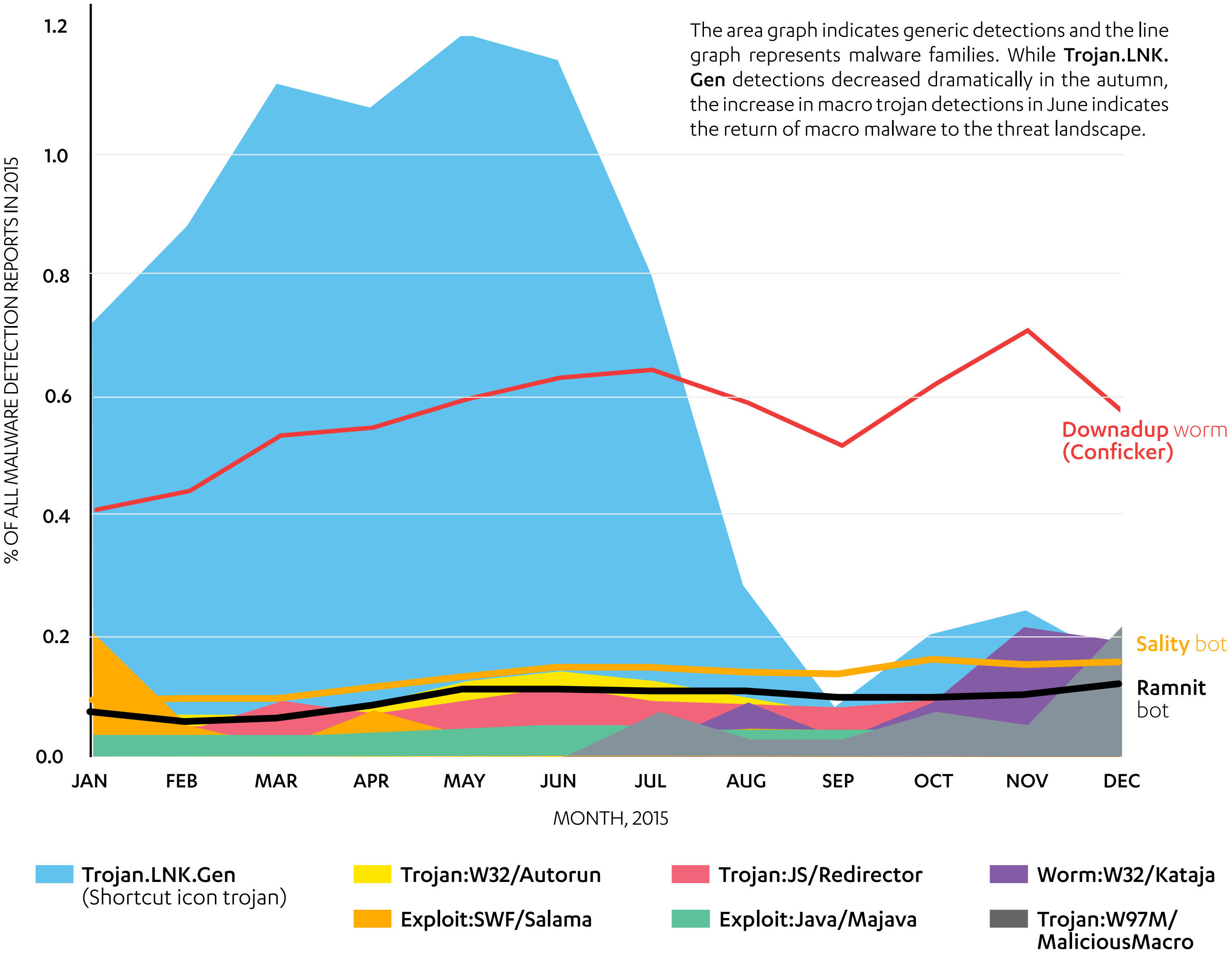
Some malware remains persistent in the wild for years on end. These legacy families can persist for a number of reasons: for example, new users may become infected for the first time, or the attackers alter the existing malware to re-attack the same targets.

Some malware isn't identified by family detections, but is instead found by a generic detection that looks for broadly similar characteristics.

On the right are the top threats of 2015 that belonged to legacy families or were detected by generics (identified by their full detection names). The bubbles are sized based on percentage of all malware detections reported from our security products over the entire year.



PREVALENCE TREND FOR LEGACY FAMILIES & GENERICS



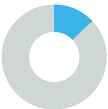
The area graph indicates generic detections and the line graph represents malware families. While **Trojan.LNK. Gen** detections decreased dramatically in the autumn, the increase in macro trojan detections in June indicates the return of macro malware to the threat landscape.

MAC MALWARE

58% (67 SAMPLE COUNTS)

BACKDOOR

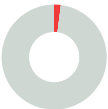
Availability of the source code for various backdoors could be a factor that contributes to backdoors making up a huge portion of OS X threats.



13% (15 SAMPLE COUNTS)

TROJAN

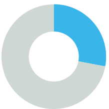
73% of the total trojan samples belong to the **Flashback** family, a group of malware that connects to a remote site to download additional malicious files.



1% (1 SAMPLE COUNT)

EXPLOIT

Exploit:OSX/CVE-2009-1237 takes advantage of an old vulnerability that could cause denial of service.



28% (32 SAMPLE COUNTS)

OTHERS

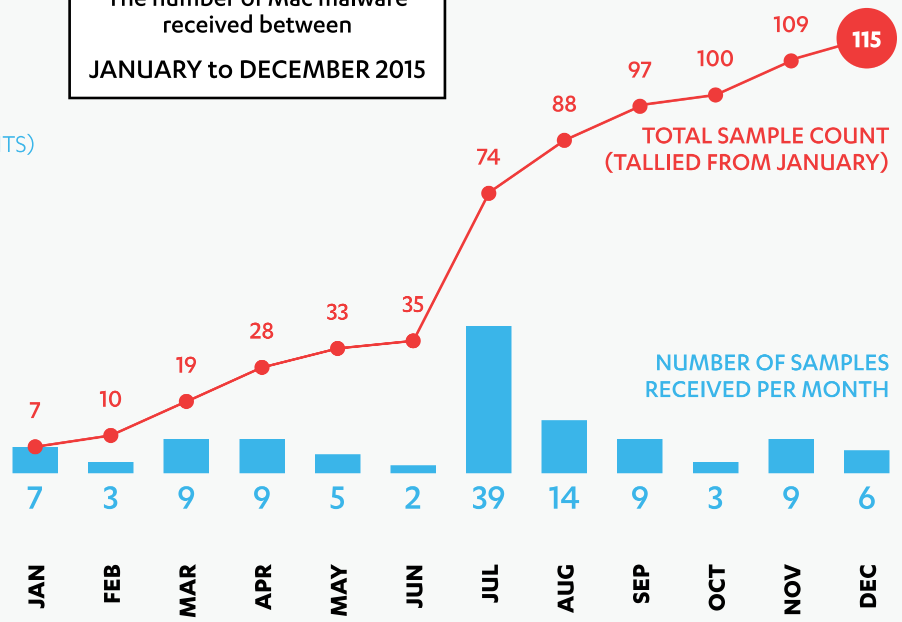
Other discovered threats, **excluding** potentially unwanted applications (PUAs).

115

UNIQUE SAMPLES

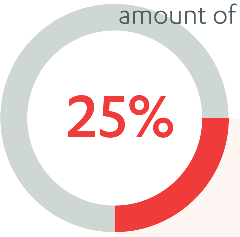
The number of Mac malware received between

JANUARY to DECEMBER 2015



ANDROID MALWARE

The **TOP 10 ANDROID MALWARE** makes up **25%** of the total amount of Android malware detected in 2015.



TOP 10 ANDROID MALWARE

1 **SMSSEND** 15.0%
TROJAN
Sends SMS messages to premium-rate numbers, charging the user's phone bill.

2 **SLOCKER** 2.5%
TROJAN
Encrypts image, document and video files, then demands ransom payment to unlock the device and decrypt the affected files.

3 **FAKEINST** 2.3%
TROJAN
Appears to be an installer for a popular app but instead sends SMS messages to premium-rate numbers or services.

4 **GINMASTER** 1.7%
TROJAN
Steals confidential information from the device and sends it to a remote website.

5 **GINGERBREAK** 1.2%
EXPLOIT
Exploits a vulnerability in Android operating systems prior to version 2.34 to gain root privileges on the device.

6 **SMSPAY** 0.5%
TROJAN
Sends SMS messages to premium-rate numbers, charging the user's phone bill.

7 **DROIDROOTER** 0.5%
EXPLOIT
Gains device root privileges. Also used as a hack-tool when users deliberately run it to 'jailbreak' the device.

8 **DIALER** 0.4%
TROJAN
Porn-related app persistently displays a full-screen page urging the user to call a number.

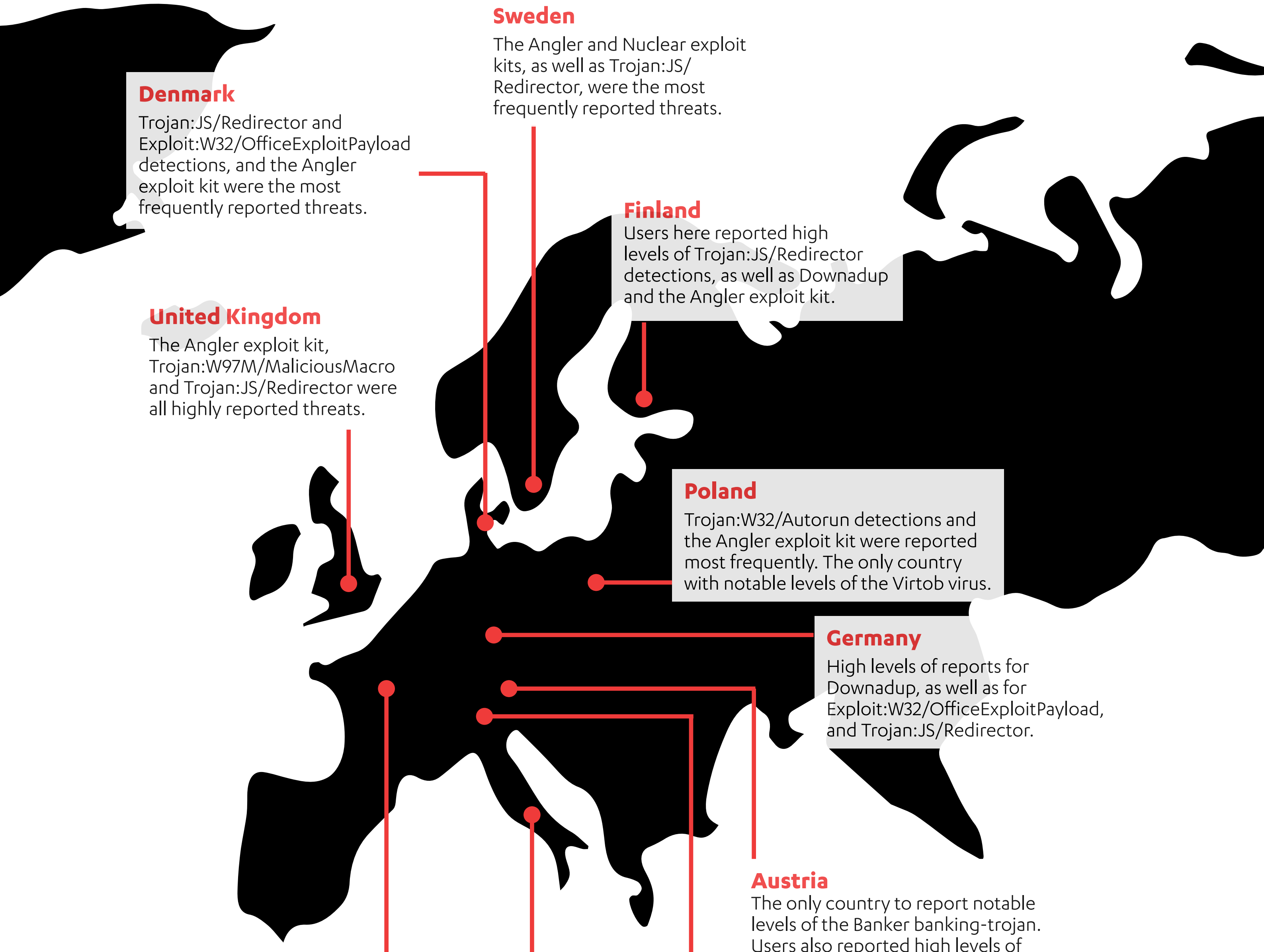
9 **SMSKEY** 0.3%
TROJAN
Sends SMS messages to premium-rate numbers, charging the user's phone bill.

10 **COUDW** 0.2%
TROJAN
Backdoor to the device, gives attackers access to the device to do as they please.

THREATS BY REGION

EUROPE

Though the Top 10 Threats were present to varying degrees in almost every country in 2015, telemetry reports from our users in each region displayed unique threat profiles. Europe was particularly affected by the Angler exploit kit. Users across the region also frequently reported Trojan:JS/Redirector detections, and document files with embedded macros that download ransomware. Some European countries reported notable levels of particular threats.



Sweden

The Angler and Nuclear exploit kits, as well as Trojan:JS/Redirector, were the most frequently reported threats.

Denmark

Trojan:JS/Redirector and Exploit:W32/OfficeExploitPayload detections, and the Angler exploit kit were the most frequently reported threats.

Finland

Users here reported high levels of Trojan:JS/Redirector detections, as well as Downadup and the Angler exploit kit.

United Kingdom

The Angler exploit kit, Trojan:W97M/MaliciousMacro and Trojan:JS/Redirector were all highly reported threats.

Poland

Trojan:W32/Autorun detections and the Angler exploit kit were reported most frequently. The only country with notable levels of the Virtob virus.

Germany

High levels of reports for Downadup, as well as for Exploit:W32/OfficeExploitPayload, and Trojan:JS/Redirector.

Austria

The only country to report notable levels of the Banker banking-trojan. Users also reported high levels of FakePDF trojans and Trojan:JS/Redirector.

France

The only country that reported notable levels of Smssend Android trojans. Downadup and Trojan:JS/Redirector reports were also frequent.

Switzerland

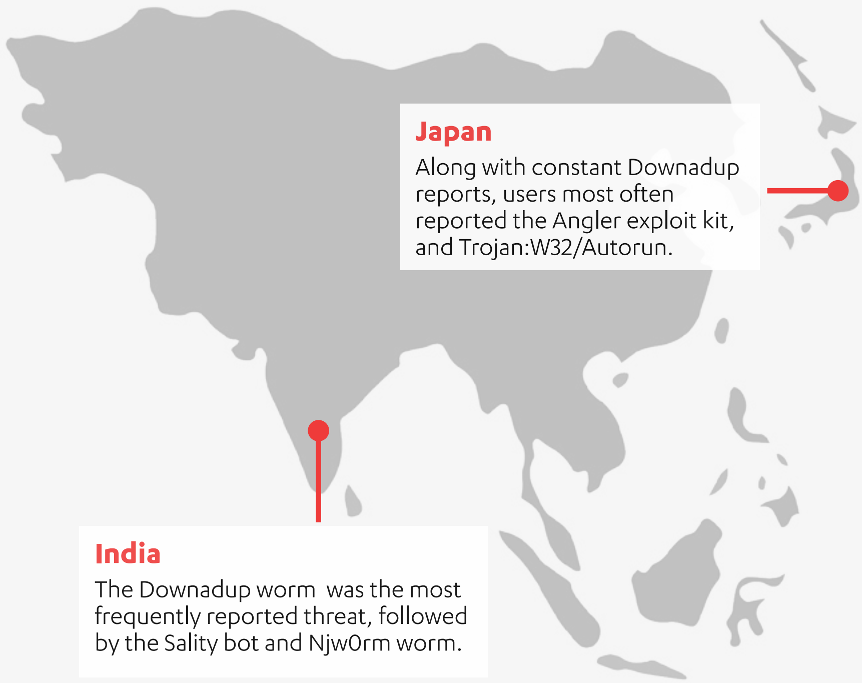
Users mainly reported Trojan:JS/Redirector and the Angler exploit kit. Exploit:SWF/Salama was the third most frequently detected threat.

Italy

The only country to report notable levels of the Expiro banking theft malware. Also reported high levels of Downadup worm and Trojan:W32/Autorun.

REST OF THE WORLD

Telemetry reports from regions other than Europe showed a more diverse range of malware being encountered by our users, with some countries reporting higher levels of a particular malware than was seen in the rest of the same region.



Japan

Along with constant Downadup reports, users most often reported the Angler exploit kit, and Trojan:W32/Autorun.

India

The Downadup worm was the most frequently reported threat, followed by the Sality bot and Njw0rm worm.

Asia

Users in Asia were most often troubled by malicious shortcut files, as well as the Downadup and Njw0rm worms. Botnet-related threats (Sality and Ramnit) were also reported frequently.

Middle East

Downadup continues to be the most reported threat, followed by malicious shortcut files and Njw0rm.

Oman

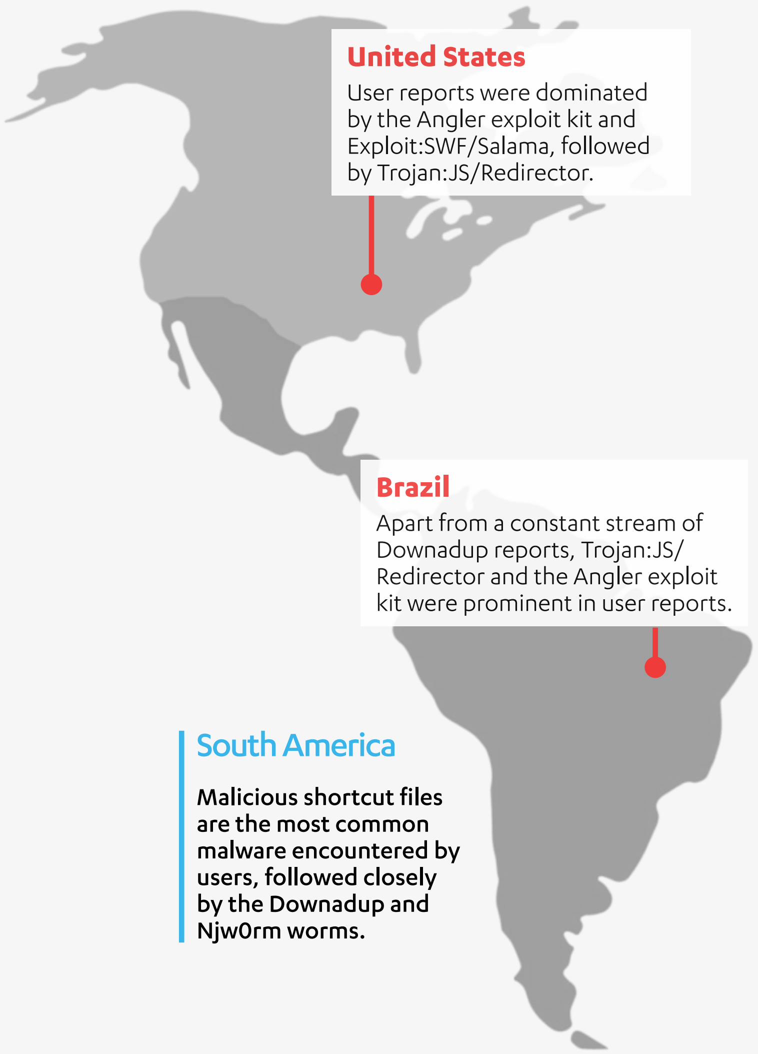
Notably high levels of the Njw0rm and Dorkbot worms, as well as Worm:W32/Kataja, were reported.

Africa

Malicious shortcut files were commonly reported by users in the region, followed by the Ippedo worm and the Sality bot.

North America

The dominant threat in this region is the Angler exploit kit, followed by Salama exploits that target Flash Player vulnerabilities.



United States

User reports were dominated by the Angler exploit kit and Exploit:SWF/Salama, followed by Trojan:JS/Redirector.

Brazil

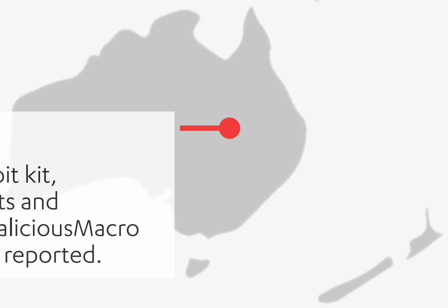
Apart from a constant stream of Downadup reports, Trojan:JS/Redirector and the Angler exploit kit were prominent in user reports.

South America

Malicious shortcut files are the most common malware encountered by users, followed closely by the Downadup and Njw0rm worms.

Oceania

Users most frequently reported malicious shortcut files and the Angler exploit kit. WormLink exploits were also notable in the user reports.



Australia

The Angler exploit kit, Wormlink exploits and Trojan:W97M/MaliciousMacro were most often reported.

03 NOTABLE CASES

BREACHING THE WALLED GARDEN

Most attacks today are directly targeted at the user. One popular method attackers use to get their malicious programs onto a user's device is by tricking the user into unwittingly downloading and installing the malware themselves (a tactic known as *social engineering*). Another popular, but technically difficult, method used by attackers is to exploit flaws or loopholes to quietly slip the malware into the device. Usually these weak points are in the app or the device itself. More rarely, they are in programs, processes or systems that aren't directly related to the user.

Sometimes however, attacks don't take the direct path. In late 2015, the Apple App Store became the target of a notable string of incidents that underlines the possible ramifications when attackers change tactics and target the *app developers*. In these incidents, the developers used compromised tools to unwittingly create apps with secretly malicious behavior. The apps were then able to bypass Apple's app code review procedures to gain entry into the store, and from there, onto an ordinary user's iOS device.

XCODEGHOST APPS PULLED FROM STORE

Apple's software repository requires all submitted programs to pass a rigorous vetting process before they can be offered in the store, and has historically been admirably free of malicious programs. In 2012, the first reported instance of malware was found in the App Store[1] when the Find & Call app turned out to be misusing contact information on the device to send spam. In the following three years, there were only a couple of relatively minor incidents, when apps that did not play by Apple's strict rules were booted from the store.

This happy state of affairs was shattered in September 2015 when news broke that Apple had removed multiple apps from the store because they were found to be embedded with a malicious program, dubbed **XCodeGhost**. Initial news reports said over 30 apps were affected, though subsequent reports put the number at over 300 [2,3].

What was particularly noteworthy about the affected apps was that at least some of them were from well-known and reputable software development companies. Perhaps the best known was WeChat, a popular messaging program. But other apps such as Railway 12306, Camcard, NetEase Cloud Music and so on had millions, or even tens of millions of users. While the majority of these users were located in mainland China, many of the apps also had users in other regions around the world, such as the United States and Europe.

Investigations by researchers from, among other organizations, Weibo, Alibaba and Palo Alto Networks, traced the 'contamination' of these apps to the use of a compromised version of Apple's Xcode software creation tool. Xcode is used to compile apps for the iOS and OS X platforms and is provided for free from the company's own servers. As with many other enterprise or commercial programs however, copies of the Xcode program are also unofficially available on file-sharing services, where they can be downloaded by developers who, for one reason or another, are unable to use the official source.

According to news reports, due to the idiosyncracies of Internet connectivity in mainland China, developers there face significantly slower connections to servers located outside the country, particularly for large files (the latest Xcode version is about 3.5GB in size). This difficulty led many of the developers to use copies of the Xcode tool that had been hosted on servers within the country. Unfortunately, some of these copies included extra lines of code. When the developers used the compromised Xcode program to create apps, it also quietly inserted additional code, without the developer's knowledge.

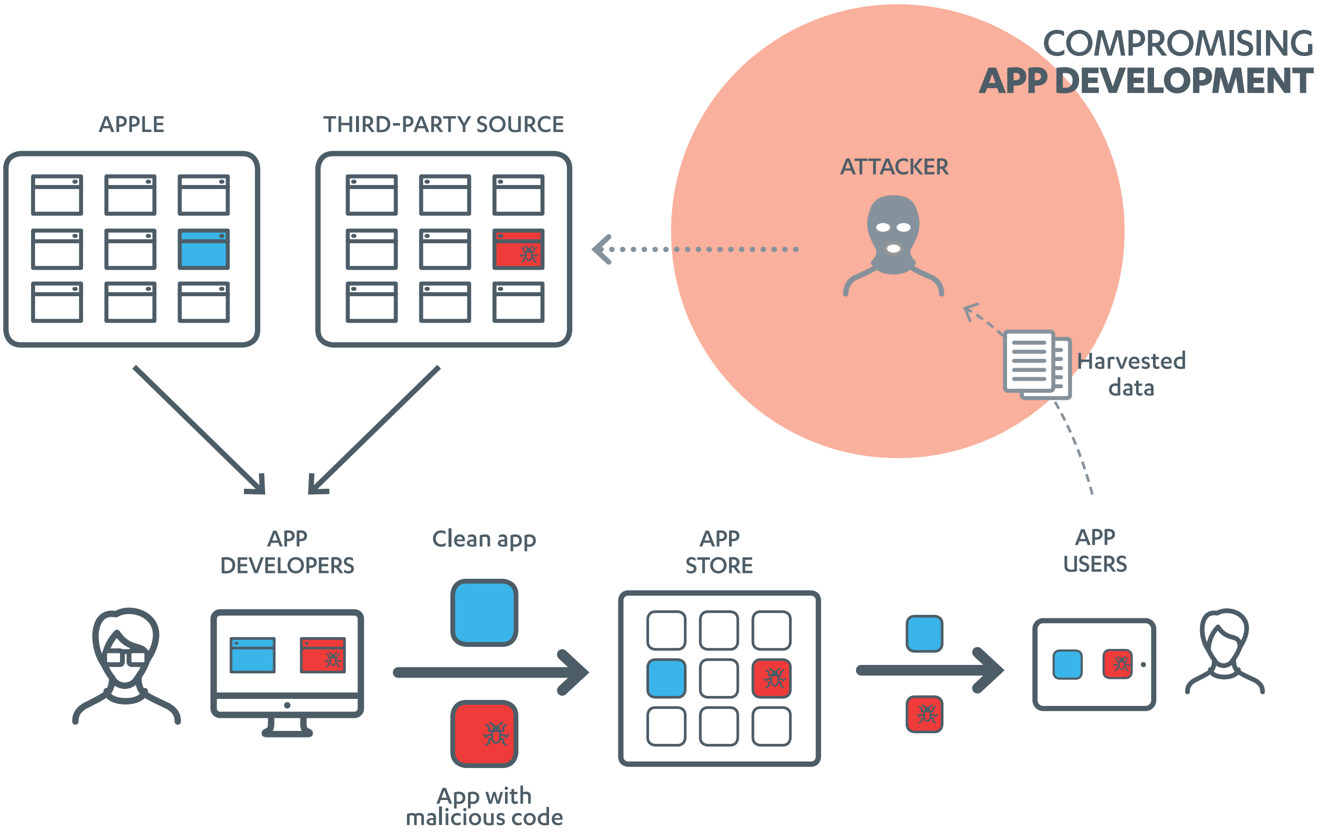
The inserted code was designed to report details of the affected device to a remote server. Researchers have however been quick to note that they have found no evidence of actual data theft or harm. Nevertheless, for users of affected apps, the recommended action is to remove them from all devices until an updated clean version is published by the developer, and in the meantime change the login credentials for any email and social media accounts associated with the apps.

UNITY FRAMEWORK ALSO AFFECTED

Shortly after news of the XcodeGhost apps broke, security researchers at PwC announced that they found cloned copies of the Unity framework being distributed that had been modified in a similar manner to the cloned Xcode programs, leading them to name the altered clones **UnityGhost** [4]. Unity is a commercial third-party development framework that can be used to create iOS apps (as well as programs for other platforms such as Android and Windows). Fortunately, in this instance there were no reports of apps created with the compromised framework copies being found in the App Store.

YOUMI-COMPILED APPS ALSO PULLED

A month later, a broadly similar situation cropped up again, when apps were booted out of the App Store for quietly collecting user and device information [5]. In this case, the affected apps had been created using the third-party



COMPROMISING APP DEVELOPMENT

Youmi software development kit (SDK), which allowed the developers to include ads in their app. Again, the developers were unaware that the apps they had created were poisoned with routines that would break Apple's strict security and privacy guidelines. Though Apple didn't specify how many apps were removed, news reports mentioned "over 250 apps" were affected. The China-based company that developed the Youmi SDK also subsequently issued an apology [6] and said it was "working with Apple to resolve the issue".

TARGETING THE DEVELOPERS

Taken together, these incidents clearly demonstrate that it is possible to circumvent the protective walls guarding the App Store and reach iOS users by using a more indirect path and first targeting the app developers. In each case, the development tool was tinkered with so that when it was used in good faith by the developer, it also silently introduced unwanted code into the final product.

This was not the first instance of this kind of attack - for example, in 2010 the Delphi program was targeted by a virus that inserted code whenever an executable was created using the affected program [7, 8]. It is, however, the first instance where such an attack had this kind of public impact.

Most of today's mobile device users have become wearily familiar with the standard security advice: 'be wary of third-party app stores'. Clearly, app developers are no more immune from the same pressures that drive 'the average user' into patronizing such sources - most commonly, limitations on bandwidth, restrictions on accessing extra-national websites, and the tempting accessibility offered by third-party repositories. To at least partly address some of these factors, Apple has announced that it planned to also offer the official Xcode program on servers located in China, making it more accessible to developers in the country [9].

Despite the recent misfortune, the Apple App Store remains a tougher nut to crack than the Android ecosystem (where directly attacking the users via social engineering remains the easiest and most effective attack vector). However, it is not impregnable. The incidents highlight the importance of maintaining rigorous security along the entire length of the app development chain. The domino effects that result from such a successful compromise impact not only the users' security, but also the reputation and trustworthiness of the affected developers and the App Store itself.

>> Sources on page 38.

MEET THE DUKES

The Dukes are a well-resourced, highly dedicated and well-organized cyber espionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

THE STORY

2008

Chechnya
Two PinchDuke campaigns traced in November 2008, with references to two Turkish websites containing Chechnya-related content.

PinchDuke & GeminiDuke
Two toolsets believed to be developed in 2008: (1) PinchDuke, launched in the same year, and (2) GeminiDuke, launched in January 2009.

2009

Campaigns against the West
PinchDuke launched two notable clusters of campaigns. The first targeted a US-based foreign policy think tank and government institutions in Poland and the Czech Republic. The second one was aimed at gathering information on Georgia-NATO relations.

2010

CosmicDuke in Caucasus
PinchDuke continued its campaigns against some countries in the Caucasus — Turkey, Georgia, Kazakhstan, Kyrgyzstan, Azerbaijan and Uzbekistan — while slowly passing the baton to a new toolset, CosmicDuke.

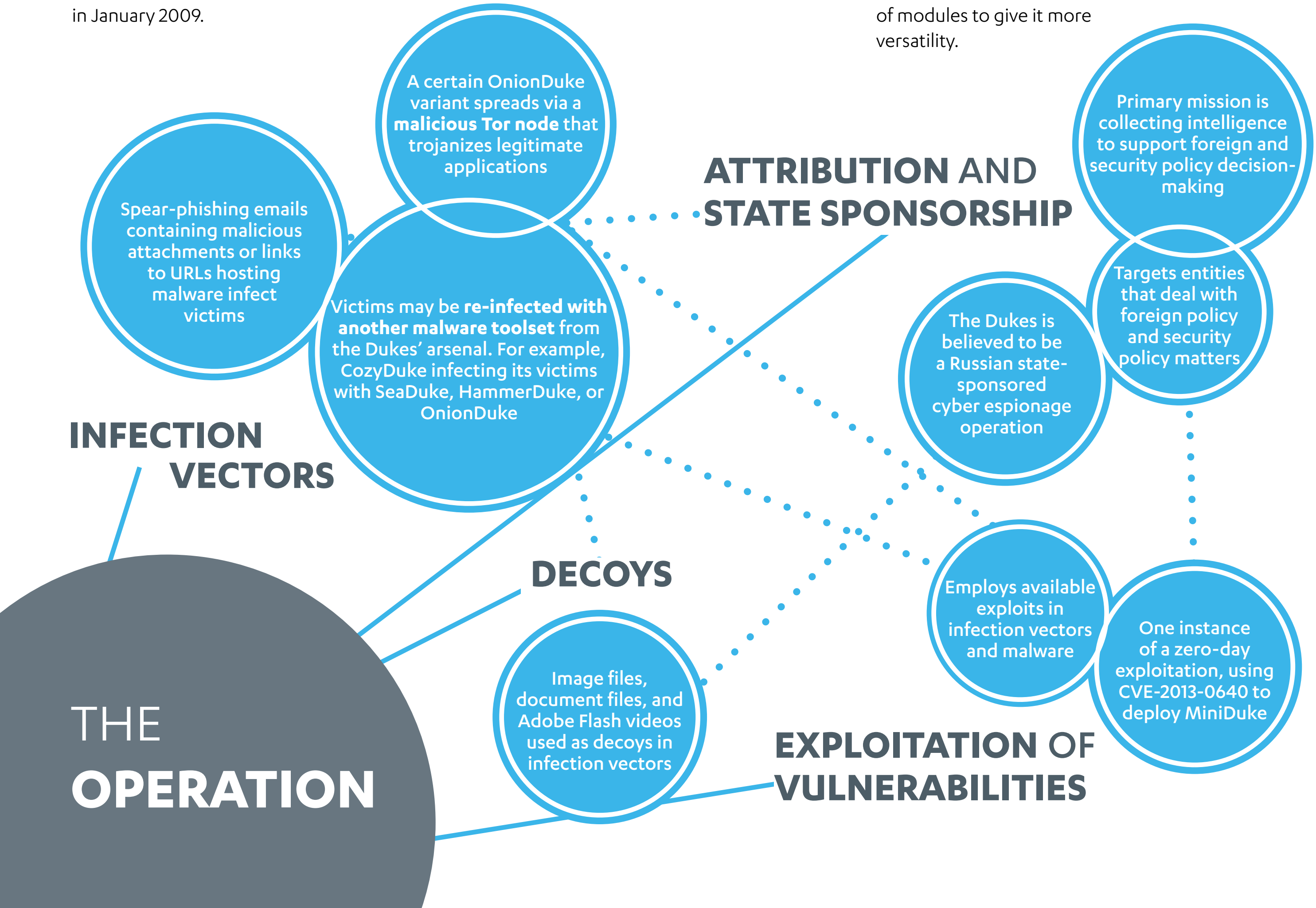
2011

John Kasai of Klagenfurt
A large group of domain names registered under the alias John Kasai of Klagenfurt, Austria. These domains were used in subsequent Dukes' campaigns up to 2014.

Expansion of Dukes' arsenal
MiniDuke and CozyDuke entered the scene. The former revolves around a simplistic backdoor component, while the latter comprises an array of modules to give it more versatility.

2012

Hiding in shadows
The Dukes lay low in 2012. CosmicDuke and MiniDuke saw active usage but received minor updates. GeminiDuke and CozyDuke, on the other hand, saw less use but received significant updates.



THE OPERATION

INFECTION VECTORS

Spear-phishing emails containing malicious attachments or links to URLs hosting malware infect victims

A certain OnionDuke variant spreads via a **malicious Tor node** that trojanizes legitimate applications

Victims may be **re-infected with another malware toolset** from the Dukes' arsenal. For example, CozyDuke infecting its victims with SeaDuke, HammerDuke, or OnionDuke

DECOYS

Image files, document files, and Adobe Flash videos used as decoys in infection vectors

ATTRIBUTION AND STATE SPONSORSHIP

Primary mission is collecting intelligence to support foreign and security policy decision-making

Targets entities that deal with foreign policy and security policy matters

The Dukes is believed to be a Russian state-sponsored cyber espionage operation

EXPLOITATION OF VULNERABILITIES

Employs available exploits in infection vectors and malware

One instance of a zero-day exploitation, using CVE-2013-0640 to deploy MiniDuke

The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as PinchDuke, GeminiDuke, CosmicDuke, MiniDuke, CozyDuke, OnionDuke, SeaDuke, HammerDuke, and CloudDuke.

In recent years, the Dukes have engaged in large, biannual spear-phishing campaigns against hundreds or even thousands of recipients associated with government institutions and affiliated organizations.

2013

MiniDuke flew too close to the sun
MiniDuke attracted the attention of security researchers, who proceeded to dissect the samples and publish their findings in papers.

The curious case of OnionDuke
OnionDuke made its debut, equipped with capabilities to steal passwords, gather data, perform DoS attacks, and post spam.

The Dukes and Ukraine
In 2013, many decoy documents used in Dukes' campaigns were related to Ukraine. But once the country's political crisis erupted and Russia made a stand, Ukraine became irrelevant to the Dukes.

CosmicDuke's war on drugs
In September 2013, a CosmicDuke campaign targeted Russian speakers involved in the trade of illegal and controlled substances.

2014

MiniDuke rises from ashes
After slowing down its activities in 2013 to avoid attention, MiniDuke was back in full force in 2014. Its components were revamped to become more stealthy.

CosmicDuke's moment of fame
F-Secure and Kaspersky published research papers on CosmicDuke. Despite the exposure, the Dukes prioritized continuing their operations rather than go into hiding.

CozyDuke and monkey videos
CozyDuke launched spear-phishing emails containing a decoy Flash video file of a Superbowl commercial from 2007, purporting to show monkeys at an office.

OnionDuke caught using Tor node
In October 2014, the Leviathan Security Group discovered a malicious Tor exit node. An investigation by F-Secure found that the node was used to wrap executables with OnionDuke. This variant was not intended for pursuing targeted attacks, but rather to form a small botnet.

2015

The Dukes up the ante
January 2015 kickstarted the most high-volume Duke campaign yet by sending spear-phishing emails to a vast number of recipients. CozyDuke continued running its campaigns, which were later carried on by SeaDuke and HammerDuke. SeaDuke, writted in Python, works on Windows and Linux. HammerDuke, written in .NET, only works on Windows.

CloudDuke
Another large-scale phishing campaign launched in July 2015 using a new toolset, CloudDuke. The campaign was carried out in two waves.

CosmicDuke continues surgical strikes
While CozyDuke and CloudDuke carried out large-scale campaigns, CosmicDuke focused on covert, surgical campaigns.

The full research on The Dukes is published on the F-Secure Labs website.

THE DUKES: 7 YEARS OF RUSSIAN CYBERESPIONAGE
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

THE TOOLSETS

Debut:	November 2008
Alias:	-
Communication:	HTTP(S)
Components:	Multiple loaders, information stealer

PINCHDUKE

Debut:	January 2009
Alias:	-
Communication:	HTTP(S)
Components:	Loaders, information stealer, multiple persistence components

GEMINIDUKE

Debut:	January 2010
Alias:	Tinybaron, BotgenStudios, NemesisGemina
Communication:	HTTP(S), FTP, WebDav
Components:	Information stealer, multiple loaders, privilege escalation component, multiple persistence components

COSMICDUKE

Debut:	July 2010 (loader), May 2011 (backdoor)
Alias:	-
Communication:	HTTP(S), Twitter
Components:	Downloader, backdoor, loader

MINIDUKE

Debuts:	January 2010
Alias:	CozyBear, CozyCar, Cozer, EuroAPT
Communication:	HTTP(S), Twitter (backup)
Components:	Dropper, modular backdoor, multiple persistence components, information gathering module, screenshot module, password stealing module, password hash stealing module

COZYDUKE

Debut:	February 2013
Alias:	-
Communication:	HTTP(S), Twitter (backup)
Components:	Dropper, loader, multiple modular core components, information stealer, DDoS module, password stealing module, information gathering module, social network spamming module

ONIONDUKE

Debut:	October 2014
Alias:	SeaDaddy, SeaDask
Communication:	HTTP(S)
Components:	Backdoor

SEADUKE

Debut:	January 2015
Alias:	HAMMERTOSS, Netduke
Communication:	HTTP(S), Twitter
Components:	Backdoor

HAMMERDUKE

Debut:	June 2015
Alias:	MiniDionis, CloudLook
Communication:	HTTP(S), Microsoft OneDrive
Components:	Downloader, loader, two backdoor variants

CLOUDDUKE

04 CHAIN OF COMPROMISE

THE CHAIN OF COMPROMISE
A user-centric model

The **Chain of Compromise** is a user-centric model that illustrates how cyber attacks combine different techniques and resources to compromise devices and networks. Such models are a necessity given the evolution of the threat landscape over the past decade. Gone are the days of hobbyist hackers who write computer viruses out of mere curiosity. Today's threats are dynamic and sophisticated, and created by criminals, saboteurs, hacktivists, and even nation states, who all have different goals and objectives they use cyber attacks to achieve. As the threats have evolved, so must the understanding of security researchers, IT administrators, and the general public. The Chain of Compromise highlights the sophistication of today's threats by showing attacks as multi-phased events, where the completion of each phase has unique effects that are often combined by attackers to increase the potential damage done during an attack.

The Chain of Compromise is not the only model designed to break down cyber attacks as dynamic, multi-phased processes. Lockheed Martin's Cyber Kill Chain [1] and Mandiant's Exploitation Life Cycle [2], for example, are both familiar to security researchers around the world. But whereas those models are designed to explicate the attack process utilized by APTs, the Chain of Compromise provides a user-centric model to help companies and individuals understand threats in relation to their own systems. By understanding how systems are compromised differently by different phases of an attack, the hope is that IT administrators and other readers can gain new insights into how to predict, prevent, and intercept attacks before they escalate into costly data breaches or other security incidents.

There are 4 main phases to the Chain of Compromise. While attacks and toolsets can limit themselves to a single phase, this is rarely the case in today's threats. Modern attacks typically connect different phases together, as this allows attackers to accomplish much more with their efforts. And while it is possible for attackers to abandon a particular attack or campaign, it is often better for companies and individuals to be prepared to defend against attacks with multiple phases and components, which will prevent them from being an easy target for attackers.

The different phases of the chain can be intuitively understood as "the four in's":

- **Inception** — the phase where a system or device becomes exposed to a potential threat
- **Intrusion** — the phase where an attacker successfully gains access to a system
- **Infection** — the phase where an attacker successfully installs a malicious payload in an exposed system
- **Invasion** — the phase where a malicious payload persists beyond the initial infection, often escalating the consequences of the attack

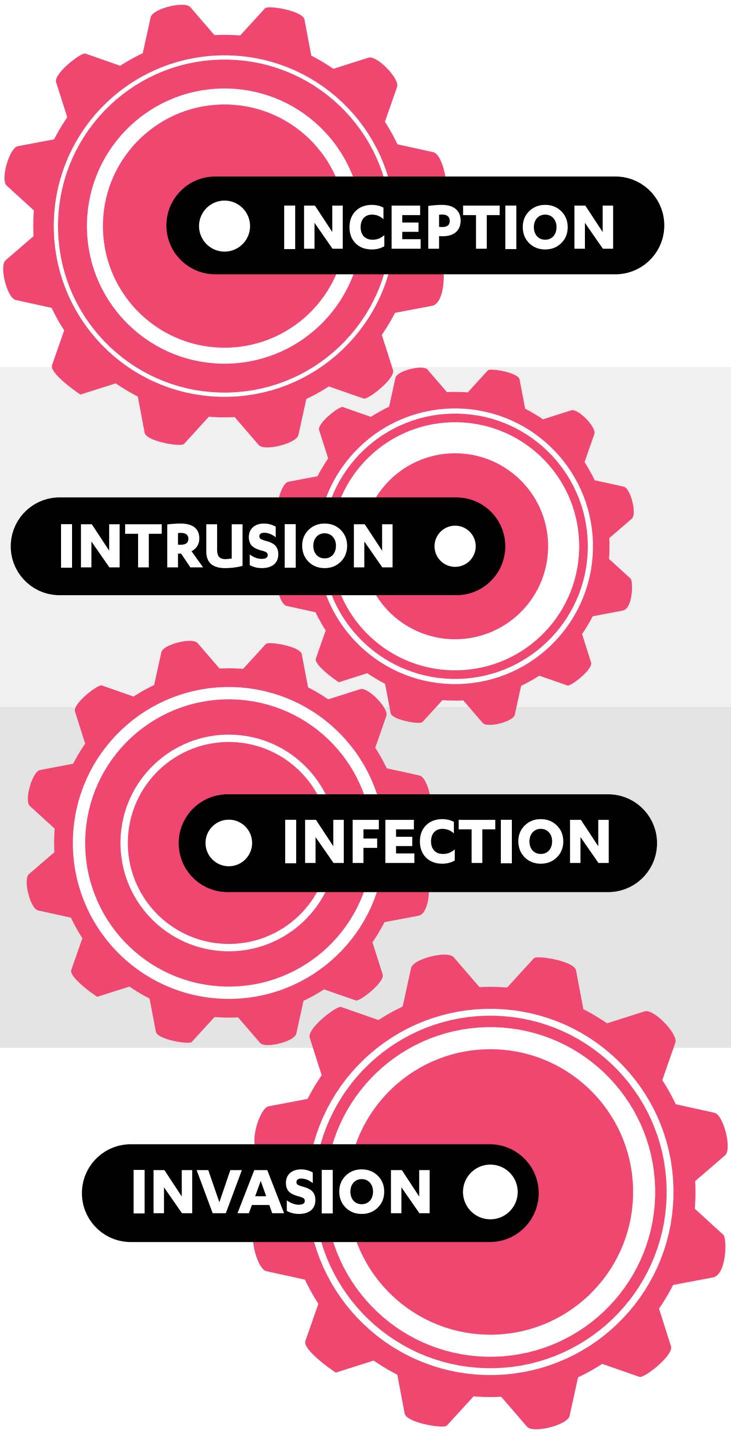
Examples of each of these phases will be discussed in the following pages. However, it is important to highlight that the Chain of Compromise has been formulated to be user-centric. Because of this, the resources used in each phase are relative to the way the user experiences the attack. The use of social engineering exemplifies this dynamic: attackers can employ such tactics during both the inception and intrusion phases.

Additionally, defenders should realize that becoming compromised at one level does not mean that they are suddenly "pwned". This is particularly important for IT administrators responsible for the security of networks. Companies, even small ones, should have solutions in place that can disrupt an attack at any point in the chain, as well as a plan for limiting how attackers can move along this chain to accomplish their goals.

>> **Sources on page 39.**

THE CHAIN OF COMPROMISE

Stage by stage



USERS, AND THEIR DEVICES, ARE EXPOSED TO ATTACKERS

Users may unknowingly come into contact with threats during normal activities, such as web browsing, emailing or using removable drives. Attackers may also try to lure or force potential targets into a position where they can be compromised, either with technical means (such as a redirectors or malware) and/or social engineering (such as phishing campaigns).

ATTACKERS GAIN ACCESS TO EXPOSED SYSTEMS

Attackers might use special code (exploits) to take advantage of vulnerabilities in the exposed systems. They might also trick the user into unknowingly granting the attackers access to the system (social engineering).

MALICIOUS CODE IS EXECUTED WITHIN THE USER'S SYSTEM

Attackers can install ("drop") a payload, which typically runs malicious code or software to produce unwanted effects. These payloads include malware such as ransomware, bots, viruses, or trojans.

ATTACKERS USE COMPROMISE TO MAINTAIN OR ESCALATE EFFECTS

The attack persists on the user's system, or escalates to further compromise the user's system or exposed networks.

THE CHAIN OF COMPROMISE

Top threats by stage

USERS, AND THEIR DEVICES, ARE EXPOSED TO ATTACKERS

The main purpose of these threats is to put the user into a position where they can be compromised. Redirector trojans send users to malicious sites, where they are often exposed to exploit kits. Macro, Autrorun, shortcut icon file trojans (and the Njw0rm worm) generally use the facade of an innocuous file to get themselves saved on the user's system, where there's a greater chance they will be launched.

ATTACKERS GAIN ACCESS TO EXPOSED SYSTEMS

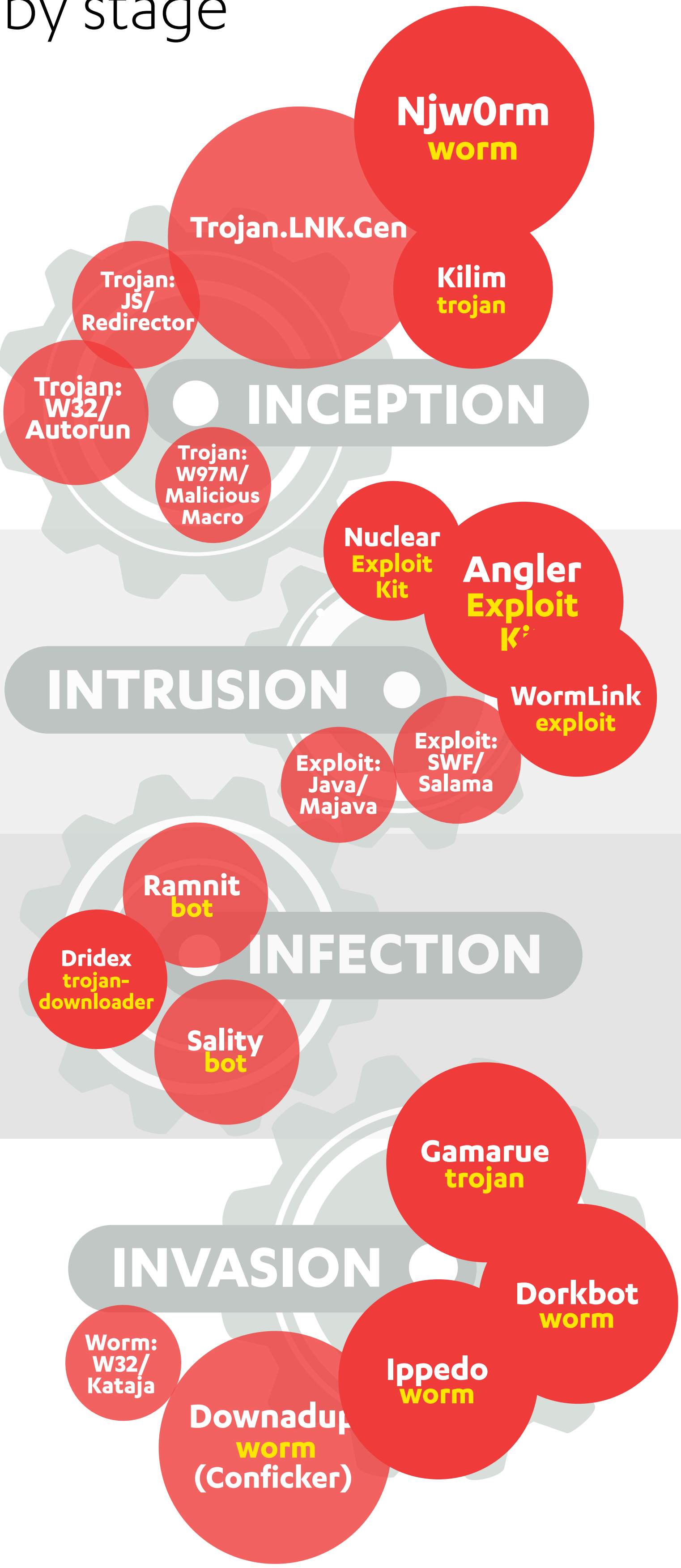
These threats (all exploits) are used by attackers to gain direct access and/or control of a user's system by taking advantage of vulnerabilities in the system, or in programs installed on it.

MALICIOUS CODE IS EXECUTED WITHIN THE USER'S SYSTEM

These threats are often dropped onto a system by other malware, or are delivered once a system has been compromised by an exploit kit.

ATTACKERS USE COMPROMISE TO MAINTAIN OR ESCALATE EFFECTS

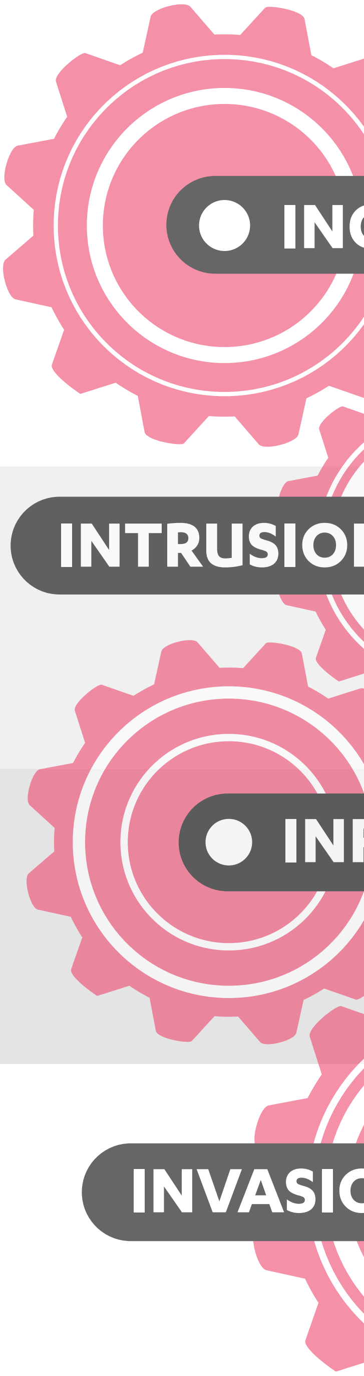
Once present on an affected system, these threats can spread copies of themselves to other machines on the same network, compounding the effects of the original infection. Some, such as Gamarue or Dorkbot, also include the ability to contact a remote server and retrieve additional instructions from an attacker, potentially increasing the impact of an infection.

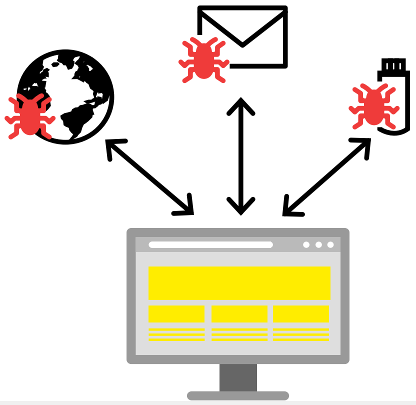


NJW0RM

Chain of Compromise

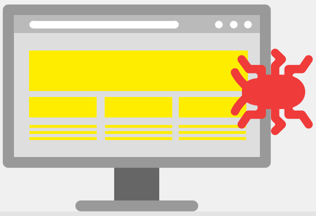
A VBS worm that spreads via removable drives, in files that are attached to email messages crafted to target particular people or companies, and drive-by downloads when a user visits malicious web sites. Once the malware is in the user's system, it executes other files; steals usernames, passwords and the details of the online portal that they are used for; updates or uninstalls itself, and contacts a remote command and control (C&C) server for additional instructions. It also sends information about the affected system such as IP addresses visited, operating system details, etc. to the attacker.





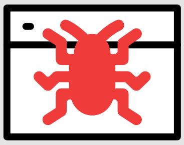
USERS, AND THEIR DEVICES, ARE EXPOSED TO ATTACKERS

Njw0rm is distributed through infected removable drives, email messages that have been crafted to target particular people or companies (spear-phishing) and malicious websites.



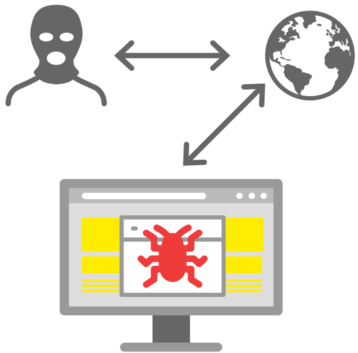
ATTACKERS GAIN ACCESS TO EXPOSED SYSTEMS

Njw0rm intrudes into the system in two ways; via drive-by downloads when visiting malicious websites or by exploiting the user's curiosity to lure them into executing an email attachment or file on an infected removable drive.



MALICIOUS CODE IS EXECUTED WITHIN THE USER'S SYSTEM

Once launched, Njw0rm is installed in several key system folders. It also manipulates the system registry to make sure it is executed every time the system is rebooted.



ATTACKERS USE COMPROMISE TO MAINTAIN OR ESCALATE EFFECTS

Njw0rm opens backdoor access to the affected system so that an attacker can potentially compromise it in the future. It also functions as a bot, so that the affected system can be remotely controlled by the attacker. It is capable of stealing online credentials, updating or uninstalling itself, as well as sending information about the affected system to the attacker.

COSMICDUKE

Chain of Compromise

CosmicDuke is one of the toolsets used by the Dukes — a cyber espionage group believed to be operating with Russian state sponsorship (see Meet the Dukes on **page 20**). The Dukes have been actively using at least nine different toolsets to steal information in intelligence gathering operations since at least 2008. Their typical targets include governments, political organizations, and other entities that possess information about the security and foreign policies of different countries.

The CosmicDuke toolset is designed around a main information stealer component. This information stealer is augmented by a variety of components that the toolset operators may selectively include with the main component. The components provide additional functionalities, such as multiple methods of establishing persistence, and modules that attempt to exploit privilege escalation vulnerabilities in order to execute CosmicDuke with higher privileges.

USERS, AND THEIR DEVICES, ARE EXPOSED TO ATTACKERS

Users' initial exposure to CosmicDuke is via spear-phishing campaigns containing malicious attachments.

ATTACKERS GAIN ACCESS TO EXPOSED SYSTEMS

CosmicDuke intrudes on systems by either exploiting software vulnerabilities when a user opens or views a malicious attachment, or exploiting the user's curiosity to execute the attachment's code.

MALICIOUS CODE IS EXECUTED WITHIN THE USER'S SYSTEM

CosmicDuke infects systems with an information stealer capable of keylogging, taking screenshots, exporting decryption keys, and stealing credentials from browsers and email or chat clients.

ATTACKERS USE COMPROMISE TO MAINTAIN OR ESCALATE EFFECTS

CosmicDuke uses command-and-control servers to exfiltrate stolen data via HTTP, HTTPS, FTP, or WebDav. This data includes login credentials that attackers use to access the system remotely without the use of additional malware or special tools, allowing the compromise to persist well beyond the initial infection.

INCEPTION

Inception is the first phase in the Chain of Compromise. It involves users, whether individuals or companies, exposing themselves to a particular threat or threats. Businesses and individuals will often expose themselves to threats unknowingly, which is something anticipated by today's attackers. However, many attackers will take a more active role, and employ technical means (such as malware), social engineering (such as phishing campaigns) or both to manipulate potential targets into a position where they can be compromised.

Redirectors wreak havoc on US, Europe

Trojan:JS/Redirector is a set of web-based attacks that allow attackers to redirect users from the website they intend to visit toward a different, unsolicited website. While legitimate websites may redirect visitors for a number of reasons, attackers have repurposed this tactic to manipulate traffic toward malicious websites. Attackers typically conduct these attacks by compromising a legitimate website with the intent to reach that website's visitors.

Unsolicited websites used by Trojan:JS/Redirector may have any or all of the following characteristics:

- Hosting pornographic content
- Pushing malware onto the visitor's computer
- Exfiltrating data from the visitor's computer
- Committing fraud by manipulating the incoming Internet traffic

Redirects are a popular and effective way for attackers to initiate attacks on potential victims, and using them to steer traffic toward exploit kits was a particularly common attack strategy in 2015.

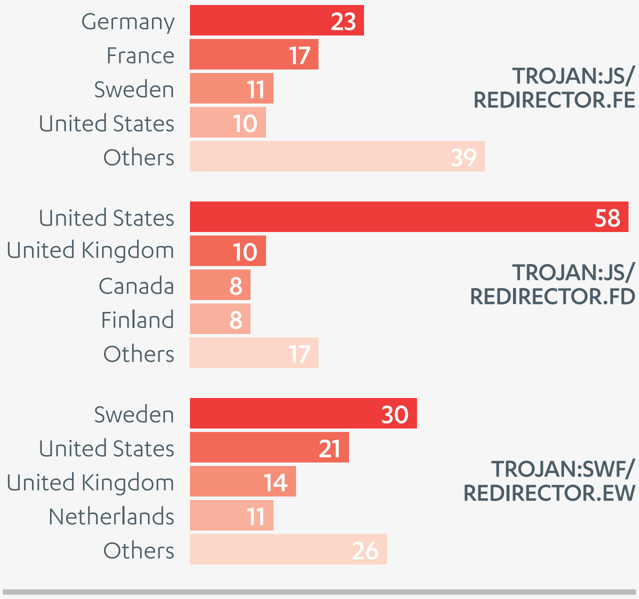
Trojan:JS/Redirector.FE was the most active redirector observed in 2015. It redirected users to servers hosting exploit kits, including prominent threats such as Angler and **Neutrino**. The majority of Trojan:JS/Redirector.FE hits were detected in Germany, followed by France, Sweden, and the United States.

Trojan:JS/Redirector.FD (also known as BizCN [1]) was another active redirector in 2015. Initially it directed users toward servers hosting **FiestaEK**, but later switched to NuclearEK and NeutrinoEK. The redirector was detected far more prominently in the United States than in other countries, but was also a significant threat to users in the United Kingdom, Finland, and Canada.

Trojan:SWF/Redirector.EW (also known as EITest Flash Redirector[2]) was another redirector that was quite pronounced in 2015, particularly in the spring and autumn. Attackers seemed to use it as an initiation technique for AnglerEK campaigns in the spring and autumn. And once again, it was detected prominently in North American and European countries, including Sweden, the United States, the United Kingdom, and the Netherlands.

As mentioned above, many of the websites hosting these redirectors are not malicious themselves. They are simply legitimate websites that have been built in a way that leaves them susceptible to attacks, making them victims rather than perpetrators. For example, many of the websites discovered to be hosting **Trojan:SWF/Redirector.EW** were built using WordPress. It's entirely possible that the compromised websites were targeted based on this, or possibly because they were using a vulnerable plug-in.

COUNTRIES MOST AFFECTED



% OF DETECTIONS REPORTED, BY COUNTRY

However, there is also strong evidence suggesting the use of other techniques, including the use of brute-force password attacks to gain administrative rights to the targeted websites. Once an attacker has administrative access to a website, it is a trivial matter for them to upload malicious scripts such as redirectors.

The prominence of Trojan:JS/Redirector detections in North America and Europe is consistent with observations regarding the prevalence of exploit kits in these regions. As such, redirectors should be recognized as significant threats used by attackers looking to initiate attacks against people and companies in these regions.

>> Sources on page 39.

INTRUSION

Intrusion is the phase of the Chain of Compromise where the actual attack begins. Companies and individuals who expose themselves to threats give attackers the opportunity to break into exposed systems. Social engineering techniques can be used to manipulate users into giving attackers access to systems. But perhaps the most common Intrusion resource used by attackers is the exploit. Exploits allow the attackers to utilize software vulnerabilities in exposed systems to acquire a degree of access, or even control, over their targets.

AnglerEK dominates Flash

Exploits are bits of code written to take advantage of vulnerabilities found in computer software, and are a prominent attack resource used in the modern threat landscape. The success of an exploit is contingent upon it finding a corresponding software vulnerability in users' systems. These exploits are often bundled together into groups by attackers as part of an exploit kit, which scans the software on a user's device to find unpatched vulnerabilities and match it with an appropriate exploit. After accomplishing this, the exploit kit uses this vulnerability as a security hole to deliver malicious payloads, such as ransomware.

Exploit kits making use of Flash vulnerabilities were a prominent threat in 2015, which is consistent with observations from the previous year. Whereas in 2013 exploit kits targeting multiple Java vulnerabilities were found, exploit kit authors have moved on to targeting Flash.

AnglerEK was the most active and most efficient at integrating exploits for Flash vulnerabilities, and was observed to be active in a number of campaigns throughout last year. The authors behind AnglerEK integrated support for Flash vulnerabilities more often than other prominent exploit kits. AnglerEK detections in 2015 were prevalent in many different countries, and prominent enough in Sweden, the United States, the United Kingdom and Australia to make it the top threat in those countries. Angler has demonstrated the capability to add support for Flash vulnerabilities faster, and more often than other prominent exploit kits. The 2015 hack of the Italian surveillance software firm Hacking Team exemplifies how efficiently exploit kits, particularly Angler, make use of new vulnerabilities.

The Hacking Team incident

In the first week of July 2015, a considerable amount of Hacking Team's data was made publicly available. Two zero-day Flash vulnerabilities were included in this data dump.

The first vulnerability, CVE-2015-5119, was taken into use the very same day by three different exploit kits (Angler, Neutrino, and Nuclear). Two additional exploit kits added support for the vulnerability within two days, despite Adobe releasing a patch the day after the vulnerability was disclosed to the public [1].

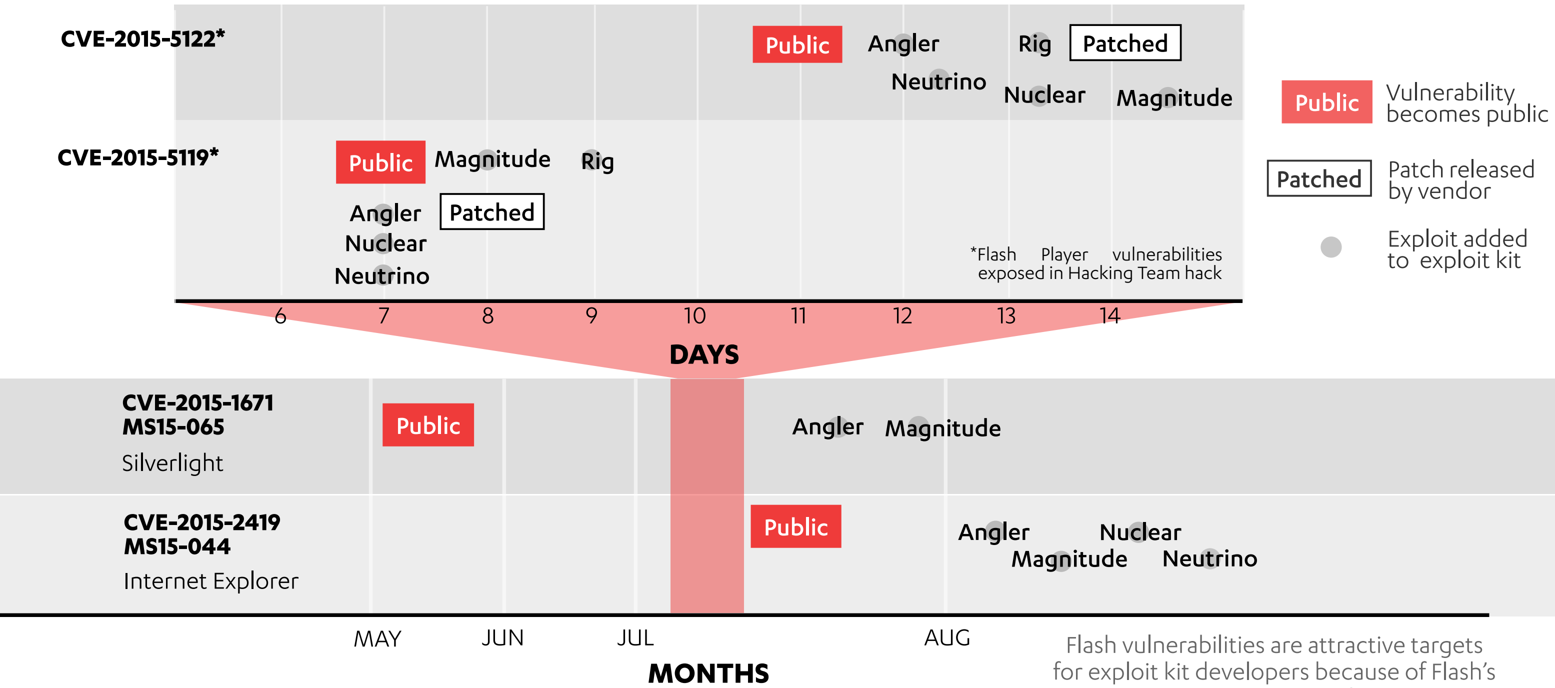
AnglerEK adopted the second zero-day vulnerability, CVE-2015-5122, the day after it was discovered in Hacking Team's data [2]. NeutrinoEK added support for the vulnerability the next day. Two days later, the authors behind NuclearEK and **RigEK** added exploits for the vulnerability to their kits. All of this occurred before Adobe was able to develop and release a patch.

TOP VULNERABILIITIES USED BY TOP 5 EXPLOIT KITS IN 2015

VULNERABILITIES		TOP 5 EXPLOIT KITS				
Program	CVE No.	Angler	Neutrino	Nuclear	Magnitude	Rig
Flash Player	CVE-2015-0310	●				
Flash Player	CVE-2015-0311	●	●	●	●	●
Flash Player	CVE-2015-0313	●	●			
Flash Player	CVE-2015-0336	●	●	●	●	
Flash Player	CVE-2015-0359	●	●	●	●	●
Flash Player	CVE-2015-3090	●	●	●	●	●
Flash Player	CVE-2015-3105	●		●	●	
Flash Player	CVE-2015-3113	●	●	●	●	●
Flash Player	CVE-2015-5119	●	●	●	●	●
Flash Player	CVE-2015-5122	●	●	●	●	●
Silverlight	CVE-2015-1671	●			●	
Internet Explorer	CVE-2015-2419	●	●	●	●	●
Flash Player	CVE-2015-5560	●		●		
Flash Player	CVE-2015-7645	●	●	●	●	
Flash Player	CVE-2015-8446	●				

Angler was the exploit kit that was most active and efficient at integrating exploits into its arsenal

TIMELINE OF NOTABLE EXPLOITS BEING ADDED TO EXPLOIT KITS



Flash vulnerabilities are attractive targets for exploit kit developers because of Flash's use on multiple platforms

Flash vulnerabilities are attractive targets for exploit kit developers because of Flash's use on multiple platforms. The speed and popularity of developing exploits targeting Flash vulnerabilities contrasts with how exploit kit developers adapt to vulnerabilities targeting other pieces of software. For example, a Silverlight vulnerability (CVE-2015-1671) was disclosed in May, but wasn't integrated into Angler and **Magnitude** exploit kits for two months. The top five exploit kits had a similar reaction to an Internet Explorer vulnerability disclosed in mid-July, waiting until August before adding support for the vulnerability.

AnglerEK was detected prominently enough in 2015 to make it one of the most commonly encountered forms of Intrusion by both individuals and businesses.

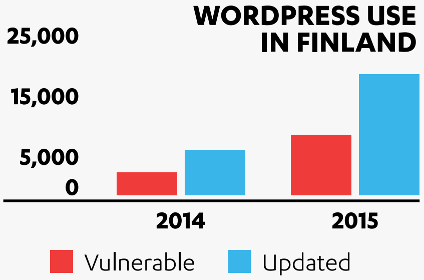
>> **Sources on page 39.**

WordPress woes in Finland

Last April, the United States Computer Emergency Readiness Team issued an alert regarding the use of unpatched software by companies. According to the alert, as many as 85 percent of targeted attacks are preventable, and companies should be more diligent in patching and updating their software to minimize their attack surface [3].

However, it appears that this warning has yet to have its intended effect. According to research, over one in four versions of WordPress currently in use within Finland contains exploitable vulnerabilities. And historical data implies this is getting worse. A similar investigation conducted in 2014 found that 24 percent of WordPress versions were vulnerable, which rose to 26 percent in 2015.

Software vulnerabilities are the lifeblood of the exploit market, and the ongoing use of outdated/unpatched software explains why this market is able to thrive. The use of software with exploitable vulnerabilities helps create demand for the very exploits that target them, thereby encouraging exploit writers to create more supply for this demand. The fact that the observed use of WordPress in Finland doubled between 2014 and 2015 should be seen as an indicator of the growing potential market for WordPress exploits.



INFECTION

Infection is the phase of the Chain of Compromise that involves a malicious payload executing code within the user's system. Once a user's system has been broken into, attackers are free to install ("drop") a malicious payload, which typically runs some kind of malicious code to produce unwanted effects. These payloads can include malware such as ransomware, bots, viruses, or trojans.

The rise of crypto-ransomware

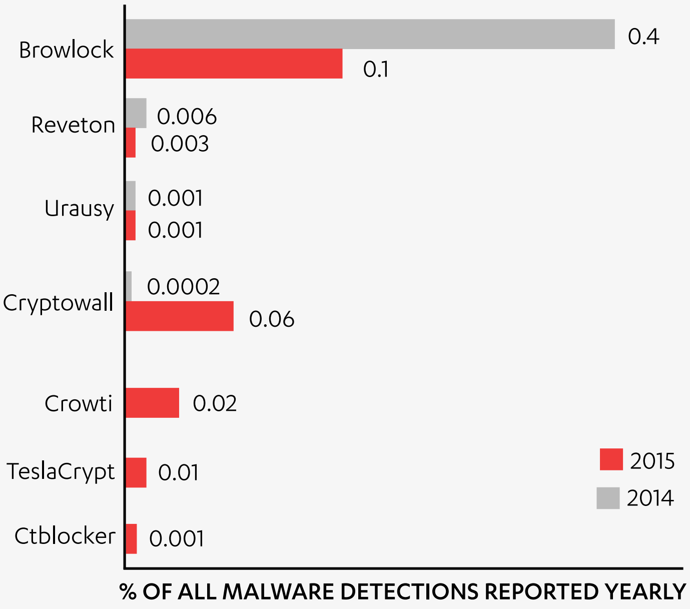
Malware infections generally cause the most concern for companies and individuals, as it is what typically determines how the attack impacts targets. After an attacker is able to access an exposed system, they are able to drop a malicious file or files to produce unwanted effects. Depending on the specifics of the attack, these malware infections lead to things like data breaches, loss of control over information or critical infrastructure, degraded system performance, and other security incidents or violations. Malicious payloads used to infect systems in 2015 include things like banking trojans (such as Dridex), bots (such as **Ramnit** or **Sality**), infostealers (such as **Fareit**), and different families of ransomware.

RANSOMWARE PAYLOADS
DELIVERED BY NOTABLE EXPLOIT KITS

	EXPLOIT KITS			
	Angler	Nuclear	Magnitude	Fiesta
PAYLOAD	Alpha Crypt	Cryptowall	Cryptowall	Cryptowall
	Cryptowall	CTB-Locker		
	Reveton	TeslaCrypt		
	TeslaCrypt	Troldesh		

Ransomware was a popular payload for many of the most prevalent exploit kits detected in 2015, and has become an effective tool to extort money from both organizations and individuals. Ransomware families are designed to extort victims by locking them out of their devices and data until they pay a fee to the attackers (hence the phrase "ransomware"). Different families employ different approaches to locking users out of their devices. However, they can all typically be classified as either "police-themed ransomware" or "crypto-ransomware." Police-themed ransomware will prevent users from accessing their devices and data by masquerading as law enforcement officials, claiming that the user has broken some type of law and needs to pay a fine to use the infected device. Crypto-ransomware relies on encrypting the contents found on a device, essentially preventing users from accessing the device or contents until a ransom is paid for the decryption keys.

RANSOMWARE DETECTIONS FROM 2014 TO 2015

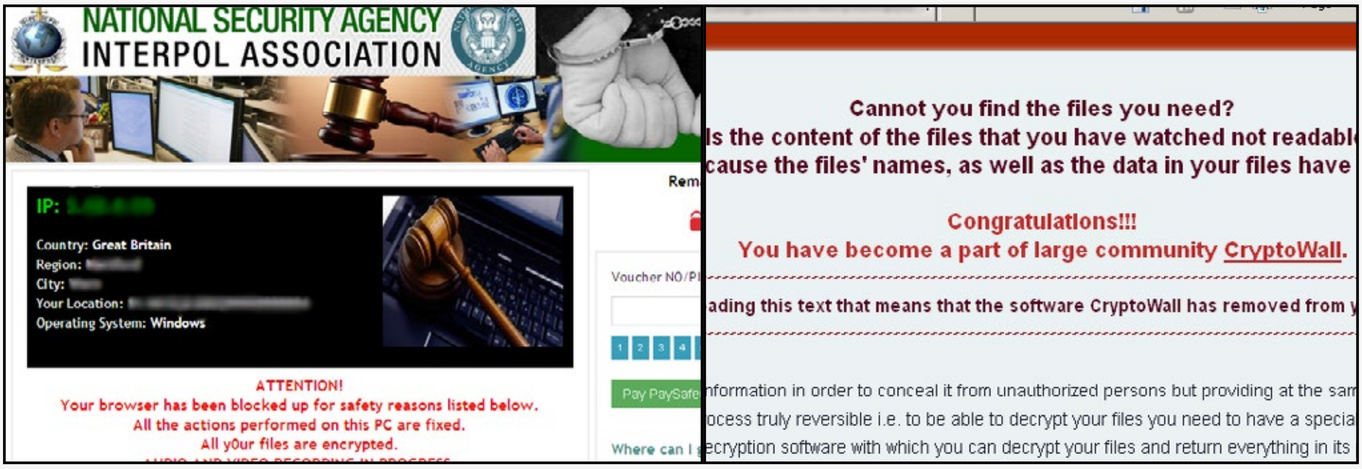


While 2015 saw a decrease in detections of police-themed ransomware, several families of crypto-ransomware rose in popularity, essentially maintaining the overall threat posed by ransomware

While 2015 saw a decrease in detections of police-themed ransomware, several families of crypto-ransomware rose in popularity, essentially maintaining the overall threat posed by ransomware.

The **Browlock** family of police-themed ransomware was not as dominant in the detections as it was in 2014, although it was still prominent enough in early 2015 to account for more detections than any other family for the entire year. Several crypto-ransomware variants, on the other hand, became more active as the year progressed. **Cryptowall** saw enough growth in 2015 to eclipse several police-themed ransomware families that were prominent in 2014, making it the most active crypto-ransomware family for the majority of the year. Both the **Crowti** and **Teslacrypt** crypto-ransomware families saw increasing amounts of activity in the final quarter of the year, giving them a more noticeable presence in the threat landscape. All in all, more crypto-ransomware families were more active in 2015 than in the year before.

RANSOM DEMANDS DISPLAYED



IP: [redacted]

Country: Great Britain
Region: [redacted]
City: [redacted]
Your Location: [redacted]
Operating System: Windows

ATTENTION!
Your browser has been blocked up for safety reasons listed below.
All the actions performed on this PC are fixed.
All y0ur files are encrypted.

Cannot you find the files you need?
Is the content of the files that you have watched not readabl
cause the files' names, as well as the data in your files have

Congratulatlons!!!
You have become a part of large community CryptoWall.

ading this text that means that the software CryptoWall has removed from y

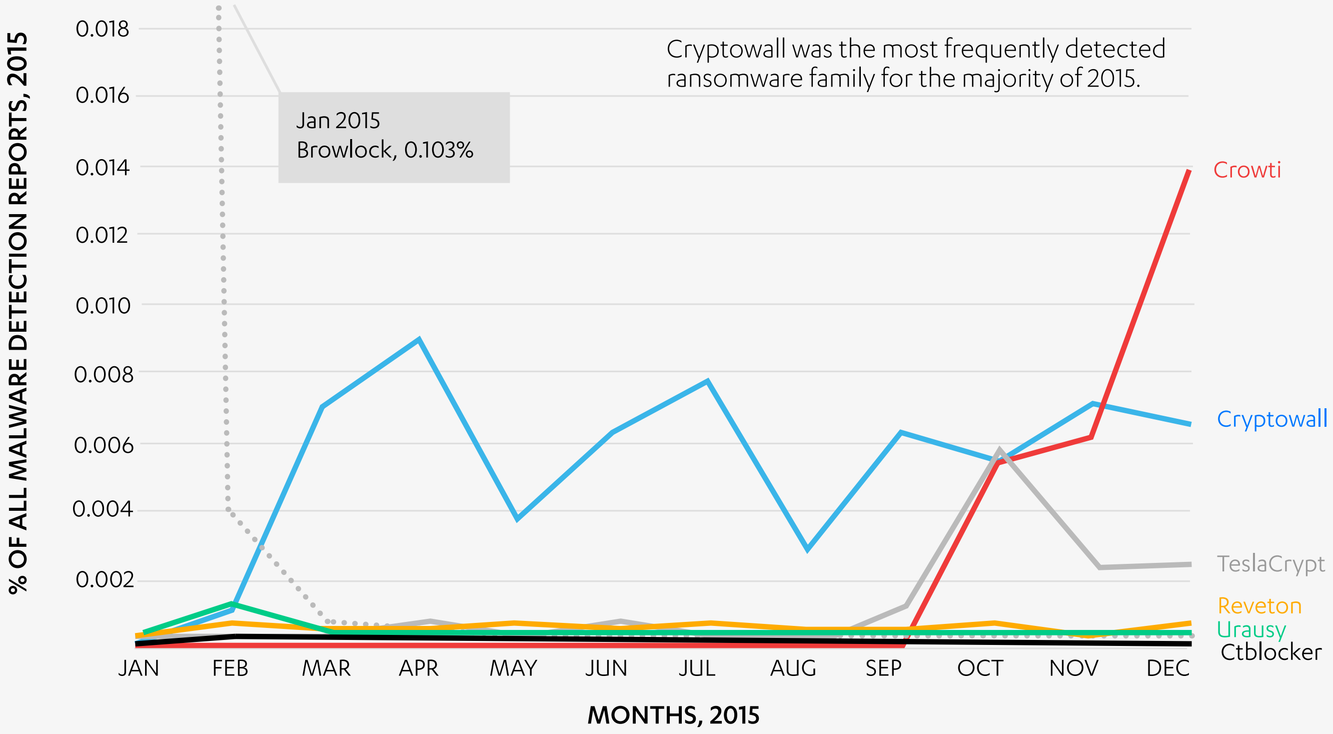
nformation in order to conceal it from unauthorized persons but providing at the sam
ocess truly reversible i.e. to be able to decrypt your files you need to have a specia
ecryption software with which you can decrypt your files and return everything in its

Ransom demands displayed by police-themed ransomware Browlock (left) and crypto-ransomware CryptoWall (right)

Researchers have previously noted that crypto-ransomware campaigns have support infrastructure in place to encourage their targets to pay the ransom, and consistently give victims decryption keys after receiving the payment [1]. Attackers behind police-themed ransomware campaigns, on the other hand, tend to simply take the ransom without helping the victims remove the infections [2]. The fact that the attackers behind crypto-ransomware families will often help their victims to ensure payment, combined with the relatively affordable payments requested, has lead the FBI to recommend companies simply pay the ransom if infected [3]. In 2015, several police departments followed this advice and paid online extortionists hundreds of dollars each to release systems locked by ransomware [4]. Stories like these highlight both the effectiveness of using ransomware as an extortion tool, and the importance of disrupting attacks before they infect systems.

>> Sources on page 39.

TOP RANSOMWARE DETECTIONS IN 2015



Cryptowall was the most frequently detected ransomware family for the majority of 2015.

INVASION: INFILTRATION

Invasion is the final phase in the Chain of Compromise. During this phase, the initial infection will persist until the victim takes measures to disrupt the attack, or escalate in order to further compromise the user's system or network. While the specifics of such escalation varies according to the particulars of the attack, there are two main evolutionary paths today's attacks typically follow: infiltration and infestation.

Infiltration allows attackers to penetrate further into the user's system, which can be used in planning future attacks or creating a persistent compromise that prolongs the effects of the attack for an extended period of time.

DNS Hijacks bring bots, downloaders, and information stealers in 2015

While DNS hijacks differ based on their target (for example, a DNS hijack against a large corporation would look quite different from the DNS hijack targeting an individual or micro business), their basic aim is to alter the domain name system (DNS) configurations of their targets in order to monitor or manipulate Internet traffic. Various security flaws can lead to these DNS hijacks, including weak passwords, software vulnerabilities, or malware. DNS hijacks are an effective way for attackers to make contact with a large number of potential targets at once, as it provides them with the opportunity to compromise all of the devices connected to a particular network.

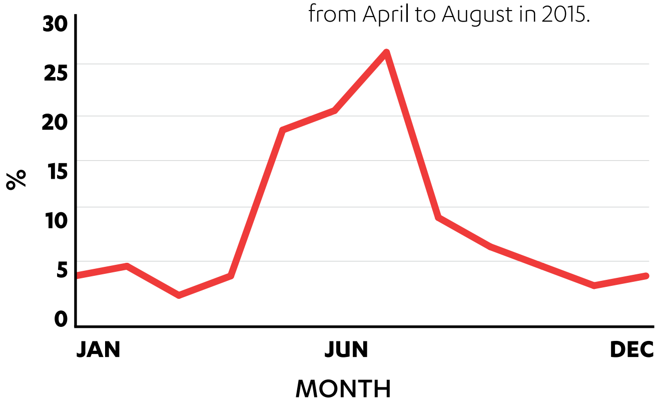
Although DNS hijacks are a frequent type of attack in today's threat landscape, a significant spike in these hijacks was observed during the spring and summer months of 2015, specifically April through August. These attacks changed the default DNS configuration in order to manipulate Internet traffic. The majority of the observed hijacks in 2015 occurred in Italy and Poland, followed by Egypt, Sweden, and India.

Out of the observed DNS hijacks in 2015, the most common strategy used by attackers was to direct Internet traffic to malicious IP addresses that would then infect devices with **Kelihos** malware. Kelihos is a prominent botnet that can be used for sending spam and DDoS attacks. It can also steal information from infected devices, including credentials. Other prominent payloads delivered through these hijacks in 2015 included the Fareit, **Pkybot**, and **Zbot** trojans, as well as the **Aprox** malware used in the botnet of the same name.

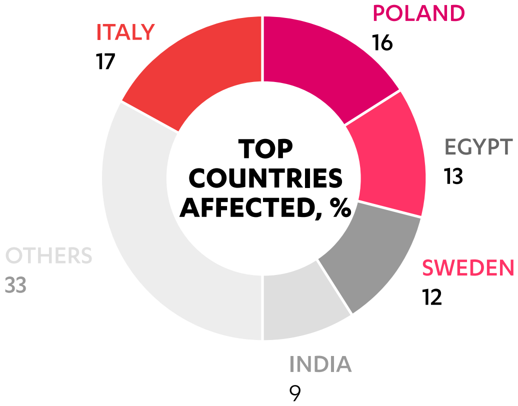
Like many modern cyber attacks, these DNS hijacks did not limit themselves to a single phase in the Chain of Compromise – altering DNS configurations was rather a means to an end. Nearly half of all of these detections – 48 percent – were used to establish botnets. Additionally, both Pkybot and Fareit function as both information stealers and downloaders, allowing the attackers to download additional payloads after the initial infection.

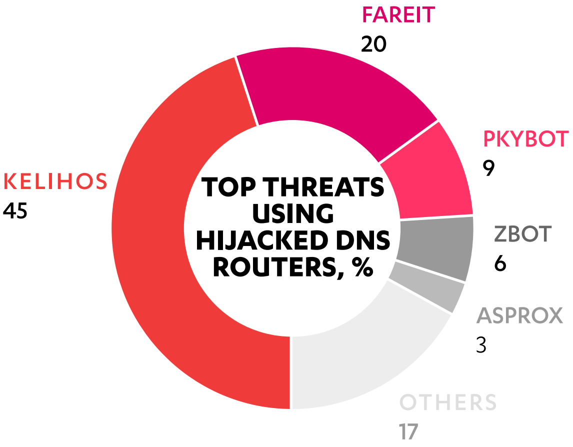
Thus, an overwhelming 77 percent of these cases attempted to give attackers persistent access to the users' systems, allowing them to further infiltrate systems to create new infections or otherwise compromise devices on an ongoing basis. Based on this, users should consider DNS hijacks as a potential ongoing compromise of their devices and networks that can help attackers achieve a variety of goals over an extended period of time.

INFECTIONS VIA DNS HIJACKING, 2015



A spike in DNS hijacks was observed from April to August in 2015.





INVASION: INFESTATION

Invasion is the final phase in the Chain of Compromise. During this phase, the initial infection will persist until the victim takes measures to disrupt the attack, or escalate in order to further compromise the user's system or network. While the specifics of such escalation varies according to the particulars of the attack, there are two main evolutionary paths today's attacks typically follow: infiltration and infestation.

Infestation occurs when an attack successfully propagates beyond a single device or system to compromise a larger network.

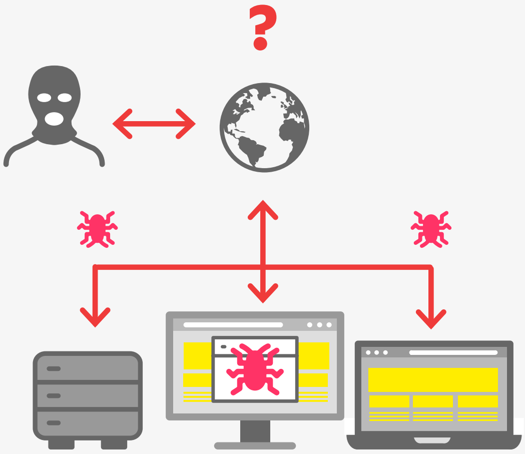
Could Downadup find new life through the Internet of Things?

In 2015, Downadup retained its previous position as the most frequently detected type of malware. The computer worm was first discovered in 2008, and is now recognized as one of today's most widepread malware infections. Downadup is a computer worm that infects unpatched Windows machines (including various versions of Windows Server), and then invades exposed networks attached to infected devices.

Downadup has infected millions of computers since its release in 2008, and caused disruptions on an industrial scale as organizations attempted to combat the worm [1]. At one point, Microsoft was offering a USD 250,000 reward for information regarding the worm's authors [2]. Downadup's combination of different tactics gave it a sophistication beyond other computer worms known to researchers at the time, making it one of history's most invasive families of malware.

Downadup remains a prominent malware family to this day, and is the most frequently detected threat in Finland, France, Germany, India, Italy, and Norway. While many anti-virus products can detect and remove the infection for individual consumers, it is still quite challenging to purge the worm once it infects large networks, such as those run by telecommunication companies or global enterprises.

And in spite of its age, Downadup is finding new ways to propagate itself. Downadup infections were discovered on wearable cameras manufactured for police officers in November 2015 [3]. Because devices like wearable cameras and many other Internet of Things (IoT) devices are unable to run traditional anti-virus software, it is entirely possible that threats such as Downadup could see a resurgence if non-secure IoT devices proliferate.



CONCLUSION

The malware commoditization market continues to strengthen, with malware-as-a-service ventures becoming increasingly sophisticated and organized. Customized end-to-end malware campaigns can be easily purchased online. Once launched, botnets distribute spam which leads to infected machines. Delivered payloads report back to a managed backend infrastructure that is provided as part of the service. We've even observed beta tests happening before a real campaign begins. Although predominantly being used for financial gain, these malware-as-a-service campaigns are sometimes used for other nefarious purposes, such as data theft or public embarassment. Compared to the cost of damages that an organization or individual can incur, the price of a malware campaign is incredibly cheap.

We're continuing to see an upsurge in ransomware, and that trend is likely to continue through 2016. Not only are ransomware campaigns becoming increasingly organized and sophisticated, the malware itself is becoming more insidious. Crypto-ransomware represents some of the most destructive software we've seen in recent times. Files are encrypted wholesale on the end-user's machine, and the only recourse a victim has is to pay the criminals for the decryption key. More recently, this malware has been able to encrypt files on non-mapped network shares, making it a nightmare for company networks. Ransoms per infected system can be upwards of $400.

We also expect APTs to continue gaining prevalence during 2016. Organized groups such as nation states, hacktivists, industrial espionage and sabotage providers, and cyber criminals are turning their eyes towards corporations and government agencies with financial gain, data theft, operations disruption, and destruction of reputation as their motives. Unlike criminalware, which will indiscriminately target every system it can, advanced persistent threats are highly focused and difficult to detect by conventional means. Tackling such threats requires a much wider cyber security strategy.

Both ransomware and APTs are making headline news on an almost weekly basis, and these stories are no longer confined solely to tech news sites. As awareness of the reality of cyber crime and cyber war increases, governments are scrambling to draft new regulations which will inevitably guide businesses going forward. This coming year will also see a great deal of debate on encryption and access to personal data — something that is likely to affect every single computer and smartphone owner. On top of all of this, the Internet of Things will continue to expand, and could very well play a role in the ongoing dialogue about cyber security.

ANDY PATEL
Technology Outreach
@r0zetta

"AS AWARENESS OF THE REALITY OF CYBER CRIME AND CYBER WAR INCREASES, GOVERNMENTS ARE SCRAMBLING..."

SOURCES

2015 HIGHLIGHTS (PAGE 08-09)

Digital security

1. **China updates Internet control laws**
   New York Times: Austin Ramzy; *What You Need to Know About China's Draft Cybersecurity Law*; published 9 Jul 2015;
   http://sinosphere.blogs.nytimes.com/2015/07/09/what-you-need-to-know-about-chinas-draft-cybersecurity-law/?_r=1
2. **US 'planning to sanction China over cyberthefts'**
   Washington Post; Ellen Nakashima; *U.S. developing sanctions against China over cyberthefts*; published 30 Aug 2015;
   https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html
3. **China/US talk on cybersecurity before state visit**
   The Guardian: *US and China officials talk cybersecurity after Obama's warning about attacks*; published 13 Sep 2015;
   http://www.theguardian.com/us-news/2015/sep/13/us-and-china-officials-talk-cybersecurity-after-obamas-warning-about-attacks
4. **US-EU 'Safe Harbor' data agreement invalidated**
   Washington Post; Ellen Nakashima; *Top E.U. court strikes down major data-sharing pact between U.S. and Europe*; published 6 Oct 2015; https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html
5. **US Senate approves CISA Act despite concerns**
   PCWorld; Martyn Williams; *CISA sails through Senate despite tech opposition*; published 28 Oct 2015;
   http://www.pcworld.com/article/2998171/privacy/cisa-sails-through-senate-despite-tech-opposition.html
6. **US DMCA expands list of 'legal hacking' products**
   Arstechnica; David Kravets; *US regulators grant DMCA exemption legalizing vehicle software tinkering*; published 27 Oct 2015;
   http://arstechnica.com/tech-policy/2015/10/us-regulators-grant-dmca-exemption-legalizing-vehicle-software-tinkering/
7. **NSA ends bulk phone surveillance program**
   Engadget; Jon Fingas; *The NSA's mass US phone surveillance ends tonight*; published 28 Nov 2015;
   http://www.engadget.com/2015/11/28/nsa-bulk-nsa-phone-surveillance-ends/
8. **China counterterrorism bill causes concern**
   PCWorld; Jeremy Kirk; *New Chinese law takes aim at encryption*; published 27 Dec 2015;
   http://www.pcworld.com/article/3018426/new-chinese-law-takes-aim-at-encryption.html

Enforcement

1. **Europol joint op takes down Ramnit botnet**
   The Wired UK; Emiko Jozuka; *Europol cracks down on botnet infecting 3.2m computers*; published 25 Feb 2015;
   http://www.wired.co.uk/news/archive/2015-02/25/europol-ramnit-crackdown
2. **FBI Darkode bazaar shutdown**
   Arstechnica; Dan Goodin; *Criminal hacking bazaar Darkode is dismantled and 70 members are busted*; published 15 Jul 2015;
   http://arstechnica.com/tech-policy/2015/07/criminal-hacking-bazaar-darkode-is-dismantled-and-70-members-are-busted/
3. **Angler exploit kit operations disrupted**
   PC Mag; Stephanie Mlot; *Cisco Disrupts $30M Ransomware Operation*; published 7 Oct 2015;
   http://www.pcmag.com/article2/0,2817,2492718,00.asp?kc=PCRSS03069TX1K0001121
4. **China arrests hackers at US behest**
   Washington Post; Ellen Nakashima and Adam Goldman; *In a first, Chinese hackers are arrested at the behest of the U.S. government*; published 9 Oct 2015; https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html?postshare=9811444395972124
5. **EU police raids over DroidJack malware**
   BBC; Chris Baraniuk; *Police raid homes across Europe over DroidJack malware*; published 30 Oct 2015;
   http://www.bbc.com/news/technology-34668337
6. **US jails Citadel botnet author for 4.5yrs**
   Naked Security; John Zorabedian; *Jail for Russian man who distributed Citadel banking malware to thousands*; published 1 Oct 2015;
   https://nakedsecurity.sophos.com/2015/10/01/jail-for-russian-man-who-distributed-citadel-banking-malware-to-thousands/
7. **UK, US charge Dridex botnet author**
   Labs Weblog; Gerald Carsula; *Dridex Takedown*; published 15 Oct 2015;
   https://labsblog.f-secure.com/2015/10/15/dridex-takedown/

Attacks

1. **Hacking Team breached, data released online**
   Forbes; Thomas Fox-Brewster; *Hacking Team Breach Exposes Insecurities Of A Controversial Surveillance Dealer*; published 6 Jul 2015;
   http://www.forbes.com/sites/thomasbrewster/2015/07/06/hacking-team-hacked/#64c1d0cc350f
2. **XcodeGhost-tainted apps prompts App Store cleanup**
   Reuters: Jum Finkle; *Apple cleaning up iOS App Store after first major attack*; published 21 Sep 2015;
   http://www.reuters.com/article/us-apple-china-malware-idUSKCN0RK0ZB20150921

3. **DDoS attack 'launched from mobile ads'**
PCWorld; Lucian Constantin; *After pushing malware, ad networks also used for DDoS*; published 28 Sep 2015; http://www.pcworld.com/article/2986966/security/after-pushing-malware-ad-networks-also-used-for-ddos.html
4. **DDoS attacks on Turkish servers reported**
International Business Times; Vasudevan Sridharan; *Anonymous: Turkey reeling under cyberattack as government and banks websites paralysed*; 26 Dec 2015; http://www.ibtimes.co.uk/anonymous-turkey-reeling-under-cyber-attack-government-banks-sites-paralysed-1534984

Malware

1. **Ransomware on the rise**
United States Federal Bureau of Investigations; *Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat*; published 20 Jan 2015; https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise
2. **Dukes cyberattack toolsets expand, develop**
F-Secure Labs Weblog; Artturi Lehtio; *Duke APT group's latest tools: cloud services and Linux support*; published 22 Jul 2015; https://www.f-secure.com/weblog/archives/00002822.html
3. **Turla malware 'contacting C&C via satellite'**
The Wired; Kim Zetter; *Russian spy gang hijacks satellite links to steal data*; published 9 Sep 2015; http://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/
4. **New Duke cyberattack toolsets identified**
F-Secure Labs Weblog; Artturi Lehtio; *The Dukes: 7 Years Of Russian Cyber-Espionage*; published 17 Sep 2015; https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/

Product Security

1. **Google launches monthly Nexus security updates**
CNet: Scott Webster; *Google's Nexus line will get monthly security updates*; published 5 Aug 2015; http://www.cnet.com/news/google-to-deploy-monthly-security-updates-to-nexus-line
2. **Google patches Android Stagefright flaw**
PCWorld; Jeremy Kirk; *Google has another try at patching Stagefright flaw*; published 13 Aug 2015; http://www.pcworld.com/article/2971332/google-has-another-try-at-patching-stagefright-flaw.html
3. **Amazon, Chrome drop Flash ads**
F-Secure Labs Weblog; Sean Sullivan; *Amazon Says No to Flash Ads*; published 21 Aug 2015; https://labsblog.f-secure.com/2015/08/21/amazon-says-no-to-flash-ads/
4. **Overstepping adblockers pulled from App Store**
Business Insider; Lara O'Reilly; *Apple has dumped ad blockers that block in-app ads from the App Store*; published 9 Oct 2015; http://www.businessinsider.my/apple-removes-been-choice-and-other-ad-blockers-from-its-app-store-2015-10/
5. **Apple product updates fix multiple security issues**
The Register; Shaun Nichols; *Got an Apple Mac, iThing? Update it right now - there's a shedload of security holes fixed*; published 21 Oct 2015; http://www.theregister.co.uk/2015/10/21/apple_updates_ios_os_x_and_watchos/

Vulnerabilities

1. **FREAK flaw found in Android, Windows**
Arstechnica; Dan Goodin; *"FREAK" flaw in Android and Apple devices cripples HTTPS crypto protection*; 3 Mar 2015; http://arstechnica.com/security/2015/03/freak-flaw-in-android-and-apple-devices-cripples-https-crypto-protection/
2. **Android Stagefright flaw reported**
Time; Robert Hackett; *Stagefright: Everything You Need To Know About Google's Android Megabug*; published 28 Jul 2015; http://www.time.com/3976049/stagefright-google-android-bug/
3. **Android Certifi-Gate flaw reported**
Endgadget; Roberto Baldwin; *Stagefright: Researchers can take complete control of Android phones*; 6 Aug 2015; http://www.engadget.com/2015/08/06/android-certifigate/
4. **OS X Gatekeeper bypass exploit reported**
Macworld; Glenn Fleishman; *Gatekeeper bypass in OS X relies on renaming an app*; published 30 Sep 2015; http://www.macworld.com/article/2988059/security/gatekeeper-bypass-in-os-x-relies-on-renaming-an-app.html
5. **Android Stagefright 2.0 flaw reported**
The Guardian; Samuel Gibbs; *Stagefright 2.0: over 1bn Android smartphones vulnerable to latest bug*; published 2 Oct 2015; http://www.theguardian.com/technology/2015/oct/02/stagefright-20-android-smartphones-vulnerable-security-bug-hackers
6. **Bugs prompt Ford, Range Rover, Prius, Chrysler recalls**
Ford; *Ford issues safety compliance recall in North America*; published 2 Jul 2015; https://media.ford.com/content/fordmedia/fna/us/en/news/2015/07/02/ford-issues-safety-compliance-recall-in-north-america.html
BBC; *Software bug prompts Range Rover recall*; published 13 Jul 2015; http://www.bbc.com/news/technology-33506486
Reuters; *Toyota recalls 625,000 hybrid cars globally for software glitch*; published 15 Jul 2015; http://www.reuters.com/article/us-toyota-recall-idUSKCN0PP0EF20150715

7. **Tesla issues OTA Model S patch for hack**
TechCrunch; Fitz Tepper; *Researchers Hack A Model S, Tesla Sends Out Over-The-Air Fix*; published 6 Aug 2015; http://techcrunch.com/2015/08/06/researchers-hack-a-model-s-tesla-sends-out-over-the-air-fix/

8. **Researchers demo Chevy Corvette hack**
The Wired; Andy Greenberg; *Hackers cut a Corvette's brakes via common car gadget*; published 11 Aug 2015; http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

9. **Chrysler mails USB sticks with software patch**
The Wired; Andy Greenberg; *Chrysler Catches Flak for Patching Hack Via Mailed USB*; published 3 Sep 2015; http://www.wired.com/2015/09/chrysler-gets-flak-patching-hack-via-mailed-usb/

BREACHING THE WALLED GARDEN (PAGE 18-19)

1. Arstechnica; Jacqui Cheng; *"Find and Call" app becomes first trojan to appear on iOS App Store*; published 6 Jul 2012; http://arstechnica.com/apple/2012/07/find-and-call-app-becomes-first-trojan-to-appear-on-ios-app-store/

2. Palo Alto Networks; Claud Xiao; *Malware XcodeGhost Infects 39 iOS Apps, Including WeChat, Affecting Hundreds of Millions of Users*; published 18 Sept 2015; http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/#

3. The Guardian; Alex Hern; *Apple removes malicious programs after first major attack on app store*; published 21 Sep 2015; http://www.theguardian.com/technology/2015/sep/21/apple-removes-malicious-programs-after-first-major-attack-on-app-store

4. PwC; Michael Yip; *UnityGhost: the ghost adventure continues*; published 6 Oct 2015; http://pwc.blogs.com/cyber_security_updates/2015/10/unityghost-the-adventure-continues.html

5. Business Insider; Lisa Eadicicco; *Hundreds of apps have been banned from Apple's App Store for spying on your personal information*; published 20 Oct 2015; http://www.businessinsider.my/apple-removes-apps-youmi-sdk-personal-information-2015-10/?op=1?r=US&IR=T

6. ZDNet; Charlie Osborne; *Chinese firm behind snooping iOS apps admits guilt*; published 20 Oct 2015; http://www.zdnet.com/article/chinese-firm-behind-snooping-ios-apps-pulled-by-apple-apologizes/

7. The Wired; Kevin Poulsen; *Malware Turns Software Compilers into Virus Breeders*; published 21 Aug 2009; http://www.wired.com/2009/08/induc/

8. Naked Security; Graham Cluley; *W32/Induc-A virus being spread by Delphi software houses*; published 19 Aug 2009; https://nakedsecurity.sophos.com/2009/08/19/w32induca-spread-delphi-software-houses/

9. Apple Insider; *Apple to officially host Xcode on Chinese servers in wake of malware issue*; published 23 Sept 2015; http://appleinsider.com/articles/15/09/23/apple-to-officially-host-xcode-on-chinese-servers-in-wake-of-malware-issue

CHAIN OF COMPROMISE (PAGE 23-34)

Chain of Compromise

1. Lockheed Martin Corporation; Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin; *Intelligence-Driven Computer*
Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains; http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

2. Mandiant; *[the advanced persistent threat]*; published 2010; https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf

Inception: Redirectors

1. SANS ISC InfoSec Forums; Brad Duncan; *BizCN gate actor changes from Fiesta to Nuclear exploit kit;* https://isc.sans.edu/forums/diary/BizCN+gate+actor+changes+from+Fiesta+to+Nuclear+exploit+kit/19875

2. Malwarebytes Labs; Jerome Segura; *Exposing the Flash 'EITest' malware campaign*; published 29 Oct 2014; https://blog.malwarebytes.org/exploits-2/2014/10/exposing-the-flash-eitest-malware-campaign/

Intrusion: Exploits

1. Malware don't need coffee; Kafeine; *CVE-2015-5119 (HackingTeam 0d - Flash up to 18.0.0.194) and Exploit Kits*; published 8 Jul 2015; http://malware.dontneedcoffee.com/2015/07/hackingteam-flash-0d-cve-2015-xxxx-and.html

2. Malware don't need coffee; Kafeine; *CVE-2015-5122 (HackingTeam 0d two - Flash up to 18.0.0.203) and Exploit Kits*;
published 11 Jul 2015; http://malware.dontneedcoffee.com/2015/07/cve-2015-5122-hackingteam-0d-two-flash.html

3. US-CERT; *Alert (TA15-119A): Top 30 Targeted High Risk Vulnerabilities*; published 29 Apr 2015; https://www.us-cert.gov/ncas/alerts/TA15-119A?hootPostID=b6821137ae5173095390bd502ae04892

Infection: Ransomware

1. Labs Weblog; Sean Sullivan*; CryptoWall's "Customer Journey" Sounds Like A Real Nightmare*; published 28 Sep 2015; https://labsblog.f-secure.com/2015/09/28/cryptowalls-customer-journey/
2. F-Secure Labs; *Removal Instructions: Removing 'Police-Themed' Ransomware*; published 14 Aug 2014; https://www.f-secure.com/en/web/labs_global/removing-police-themed-ransomware
3. The Security Ledger; *FBI's Advice on Ransomware? Just Pay The Ransom.*; published 22 Oct 2015; https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/
4. Dark Reading; Sara Peters; *Police Pay Off Ransomware Operators, Again*; published 14 Apr 2015; http://www.darkreading.com/attacks-breaches/police-pay-off-ransomware-operators-again/d/d-id/1319918

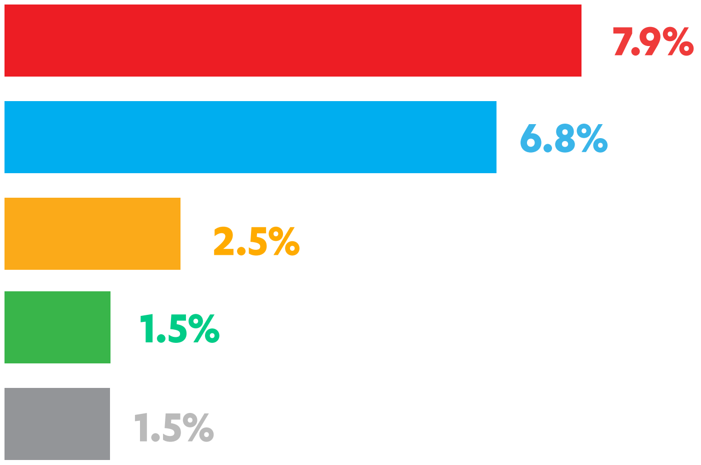
Invasion: Infestation

1. The Telegraph; Kim Willsher; *French fighter planes grounded by computer virus*; published 7 Feb 2009; http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html
2. Microsoft; *Microsoft Collaborates With Industry to Disrupt Conficker Worm*; published 12 Feb 2009; https://news.microsoft.com/2009/02/12/microsoft-collaborates-with-industry-to-disrupt-conficker-worm/
3. Arstechnica; Dan Goodin; *Police body cams found pre-installed with notorious Conficker worm*; published 16 Nov 2016; http://arstechnica.com/security/2015/11/police-body-cams-found-pre-installed-with-notorious-conficker-worm/

APPENDIX | COUNTRY REPORTS

GLOBAL

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

TROJAN.LNK.GEN

A generic detection for malicious .LNK files that are created by AutoIT, VBS and Powershell malware.

WORM:W32/DOWNADUP

Spreads by exploiting an unpatched vulnerability in Windows machines in order to distribute copies of itself.

WORM:W32/NJW0RM

Spreads via infected removable drives and files attached to e-mails. If the user unwittingly uses the drive or file, it opens a backdoor on the device, steals saved passwords, and contacts a web site for more instructions.

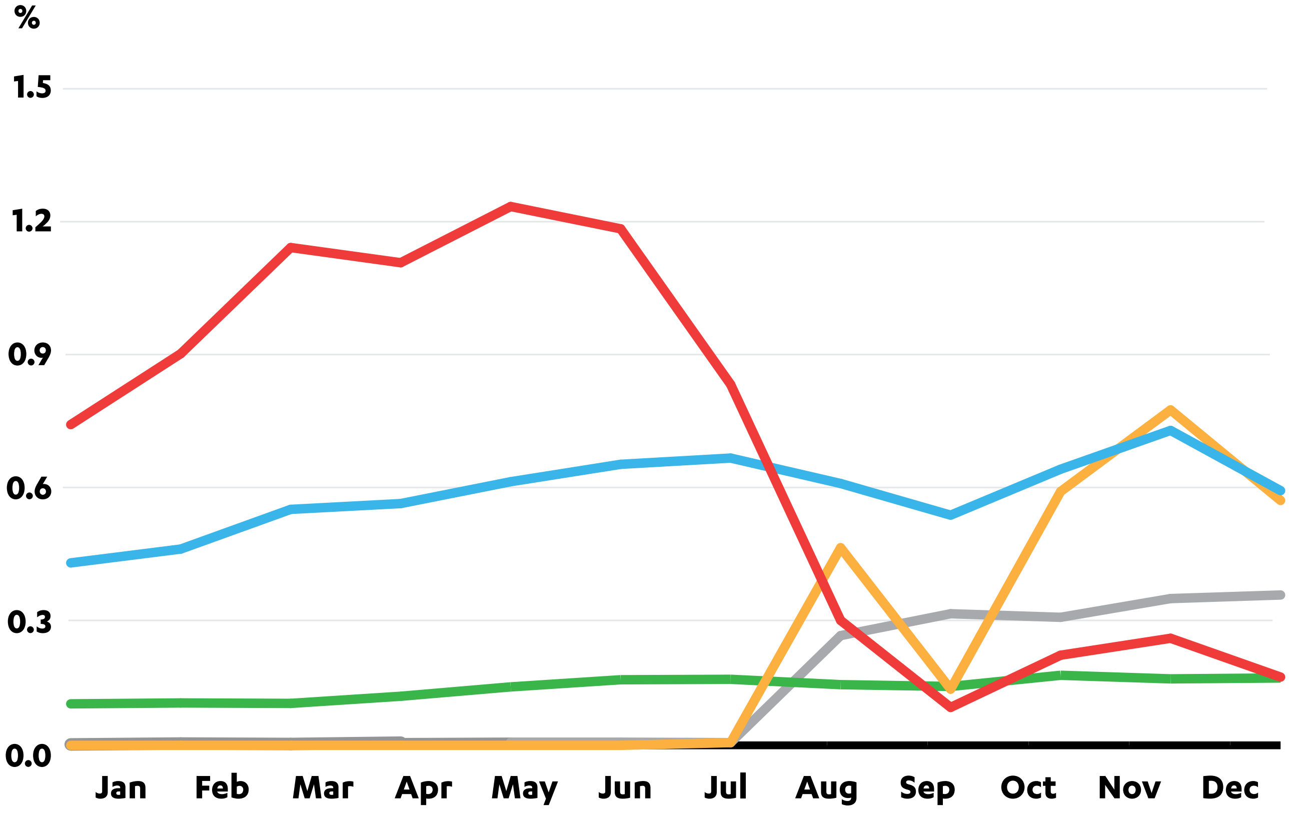
WIN32.SALITY

Adds an infected device into pool of similarly affected machines (a botnet) that an attacker can control and use to perform various malicious activities.

TROJAN:W32/GAMARUE

Uses the infected machine to send out spam emails. May also download and install other malware.

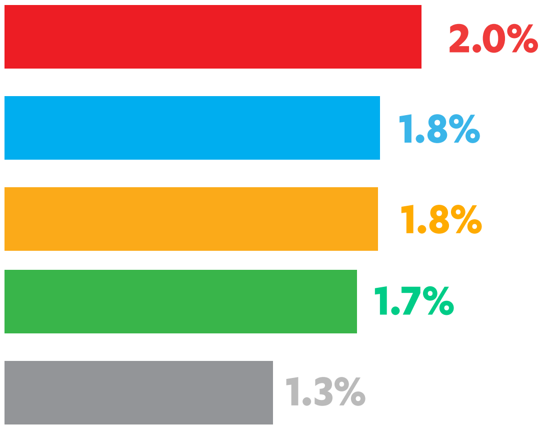
PREVALENCE TRENDS*



*Percentage of all malware detection reports in 2015.

FINLAND

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

WORM:W32/DOWNADUP

Spreads by exploiting an unpatched vulnerability in Windows machines in order to distribute copies of itself.

TROJAN:JS/REDIRECTOR

This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

EXPLOIT:JS/ANGLEREK

This detection identifies the code used by the Angler Exploit Kit to find and target vulnerabilities on the user's machine.

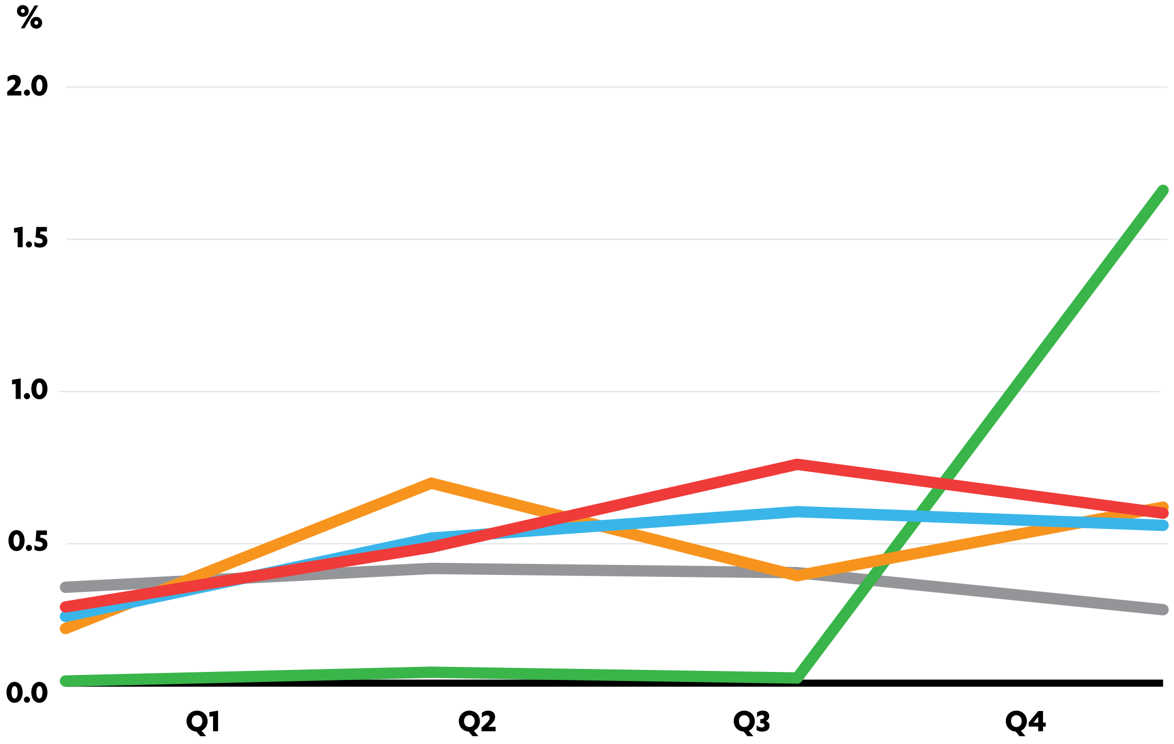
TROJAN-DOWNLOADER:W97M/DRIDEX

A banking Trojan that steals credentials of online banking websites. One of its components is a document file containing macro code that downloads the banking Trojan.

EXPLOIT:JAVA/MAJAVA

Exploits that target vulnerabilities in the widely used Java development platform.

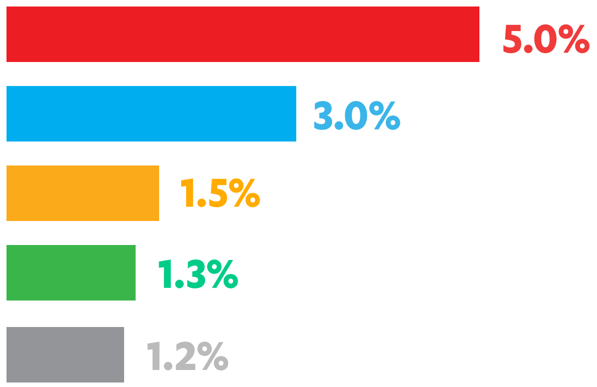
PREVALENCE PER QUARTER*



*Percentage of all malware detection reports from Finland in 2015.

SWEDEN

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

EXPLOIT:JS/ANGLEREK

This detection identifies the code used by the Angler Exploit Kit to find and target vulnerabilities on the user's machine.

TROJAN:JS/REDIRECTOR

This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

EXPLOIT:JS/NUCLEAREK

This detection identifies the code used by the Nuclear Exploit Kit to find and target vulnerabilities on the user's machine.

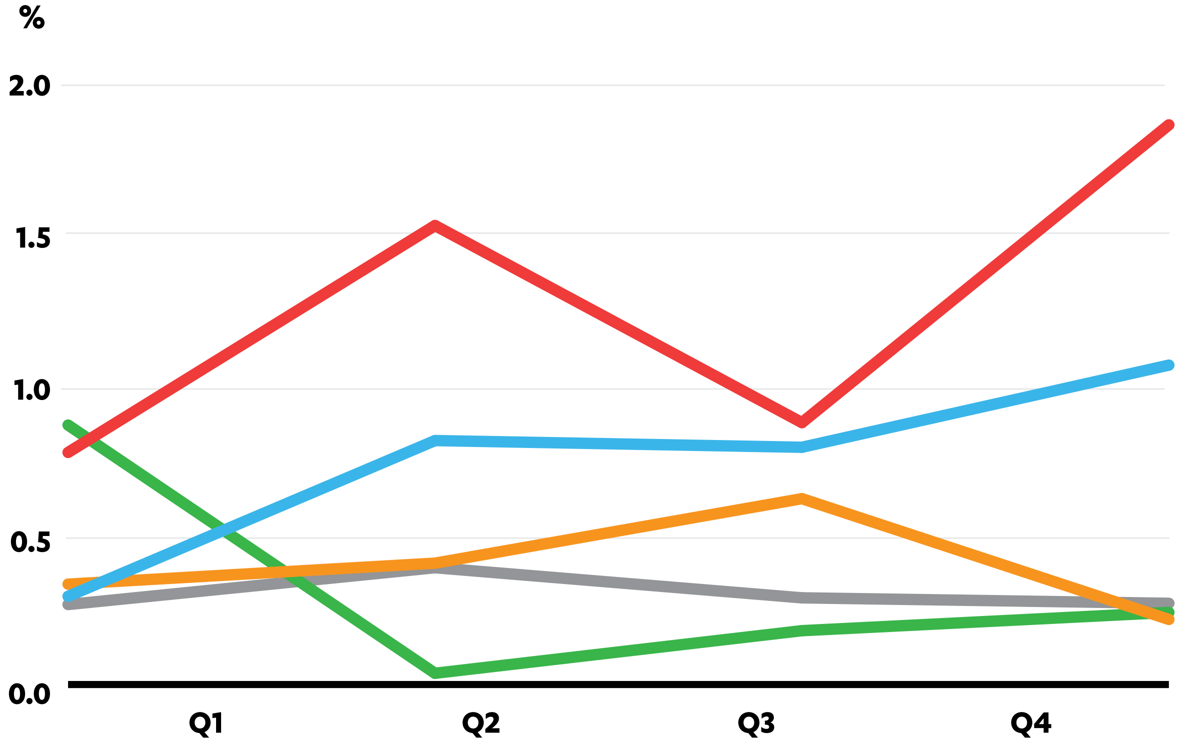
EXPLOIT:SWF/SALAMA

Exploits that target vulnerabilities in Adobe's popular Flash Player program.

EXPLOIT:JAVA/MAJAVA

Exploits that target vulnerabilities in the widely used Java development platform.

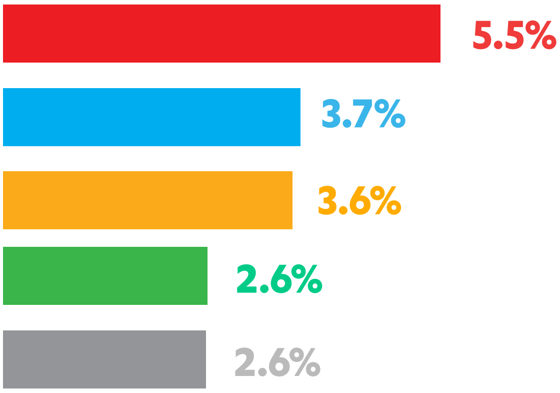
PREVALENCE PER QUARTER*



*Percentage of all malware detection reports from Sweden in 2015.

GERMANY

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

WORM:W32/DOWNADUP

Spreads by exploiting an unpatched vulnerability in Windows machines in order to distribute copies of itself.

EXPLOIT:W32/OFFICEEXPLOITPAYLOAD

Code embedded in a document file that exploits a Windows vulnerability. If the user opens the file, the code is automatically run and its payload is executed.

TROJAN:JS/REDIRECTOR

This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

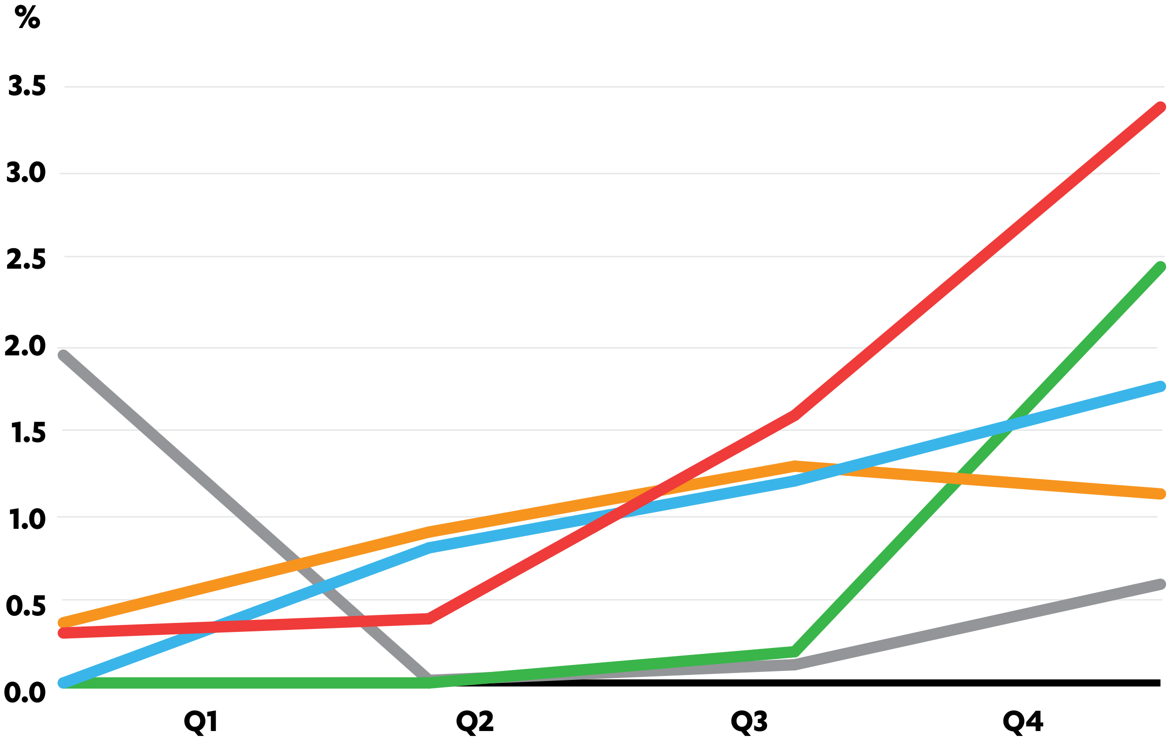
TROJAN:W97M/MALICIOUSMACRO

This generic detection finds malicious macros embedded in email file attachments.

EXPLOIT:SWF/SALAMA

Exploits that target vulnerabilities in Adobe's popular Flash Player program.

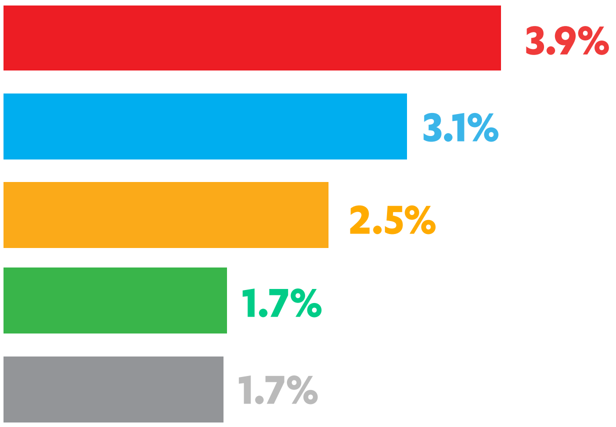
PREVALENCE PER QUARTER*



*Percentage of all malware detection reports from Germany in 2015.

FRANCE

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

WORM:W32/DOWNADUP

Spreads by exploiting an unpatched vulnerability in Windows machines in order to distribute copies of itself.

TROJAN:ANDROID/SMSSEND

Sends SMS messages to premium-rate numbers, charging the user's phone bill.

TROJAN:JS/REDIRECTOR

This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

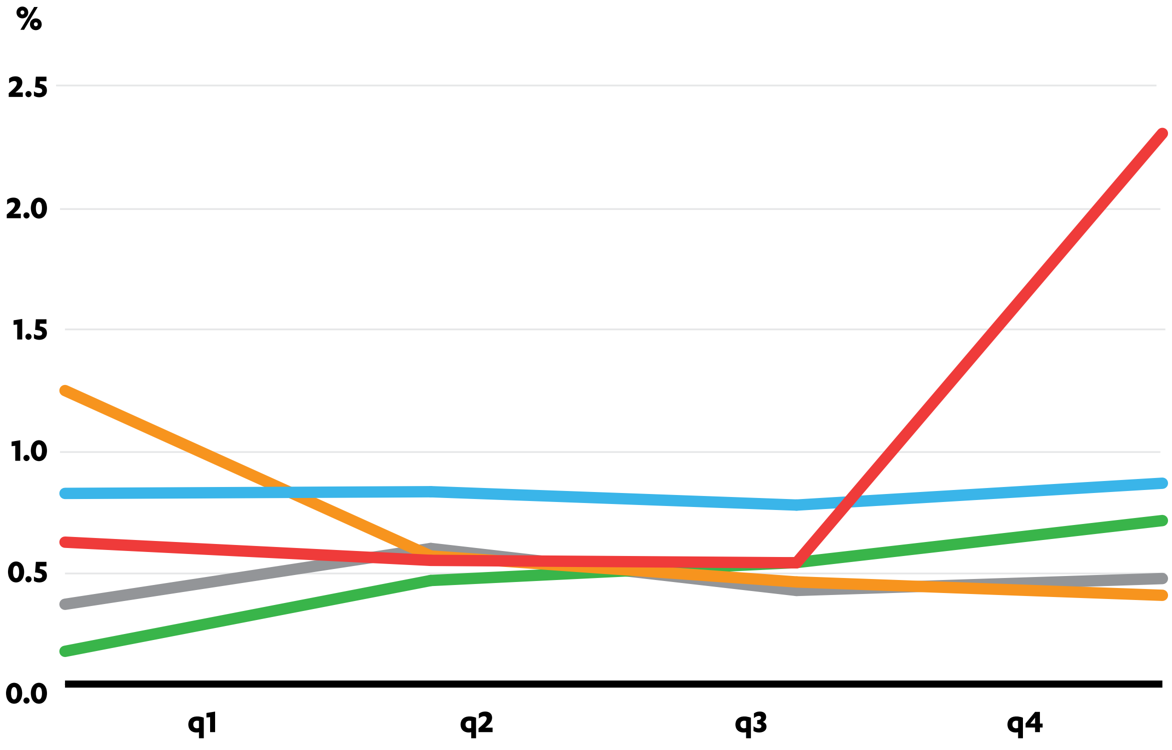
EXPLOIT:JS/ANGLEREK

This detection identifies the code used by the Angler Exploit Kit to find and target vulnerabilities on the user's machine.

TROJAN:W32/AUTORUN

This detection identifies Autorun files that automatically executes malware when a removable media is accessed (and if Windows' Autoplay feature is enabled).

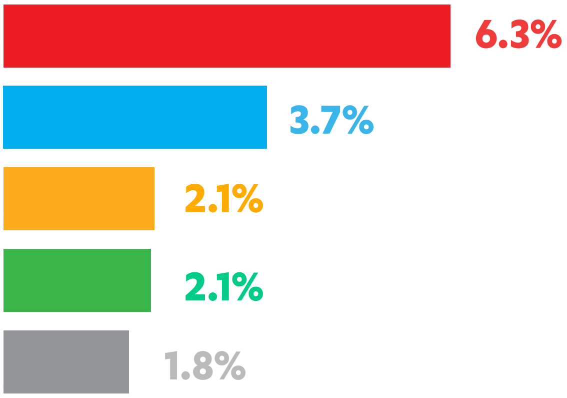
PREVALENCE PER QUARTER*



*Percentage of all malware detection reports from France in 2015.

UNITED STATES

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

EXPLOIT:JS/ANGLEREK

This detection identifies the code used by the Angler Exploit Kit to find and target vulnerabilities on the user's machine.

EXPLOIT:SWF/SALAMA

Exploits that target vulnerabilities in Adobe's popular Flash Player program.

TROJAN:JS/REDIRECTOR

This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

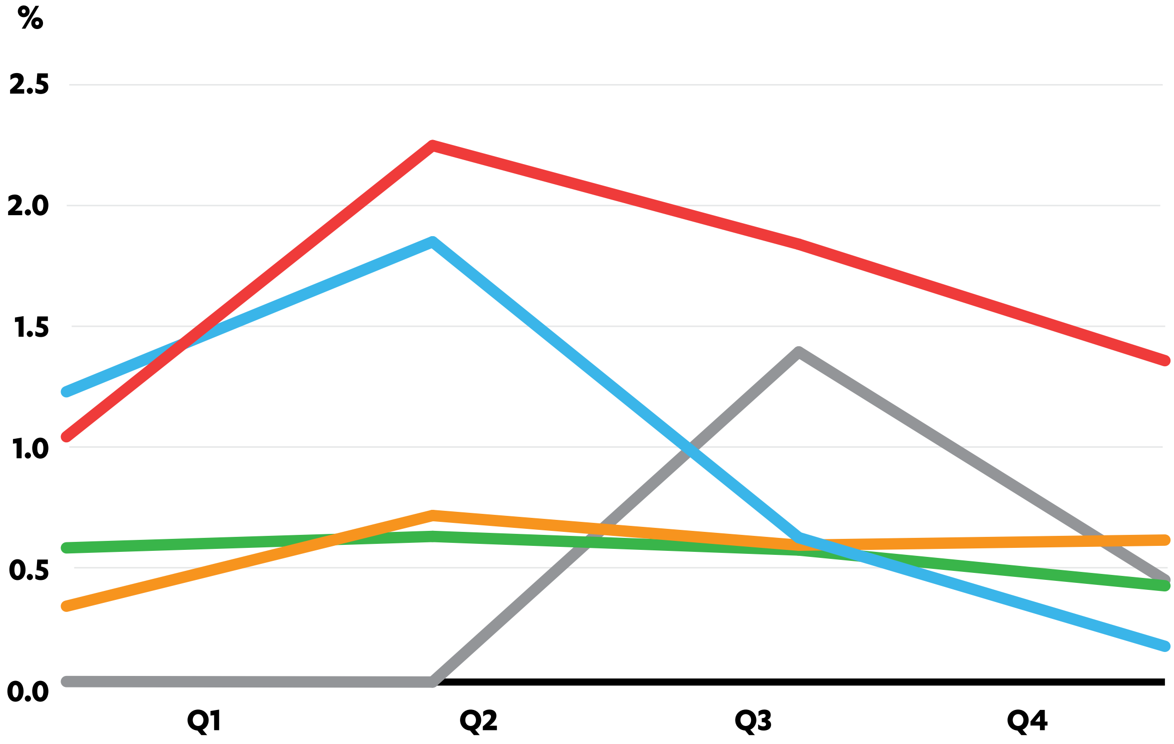
EXPLOIT:JAVA/MAJAVA

Exploits that target vulnerabilities in the widely used Java development platform.

EXPLOIT:JS/HANJUANEK

This detection identifies the code used by the Han Juan Exploit Kit to find and target vulnerabilities on the user's machine.

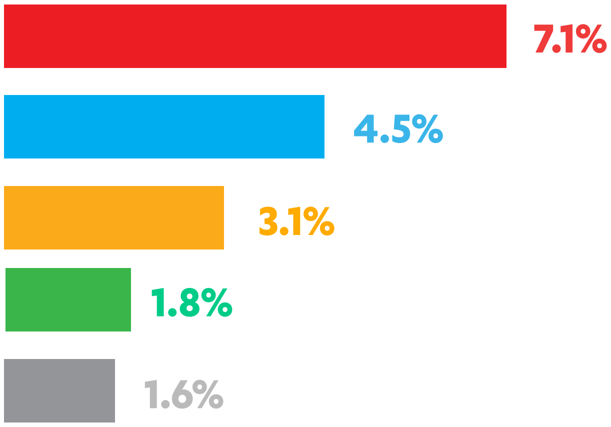
PREVALENCE PER QUARTER*



*Percentage of all malware detection reports from the United States in 2015.

UNITED KINGDOM

TOP 5 THREATS*



TOP 5 THREATS IN 2015*

EXPLOIT:JS/ANGLEREK

This detection identifies the code used by the Angler Exploit Kit to find and target vulnerabilities on the user's machine.

TROJAN:JS/REDIRECTOR

This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

TROJAN:W97M/MALICIOUSMACRO

This generic detection finds malicious macros embedded in email file attachments.

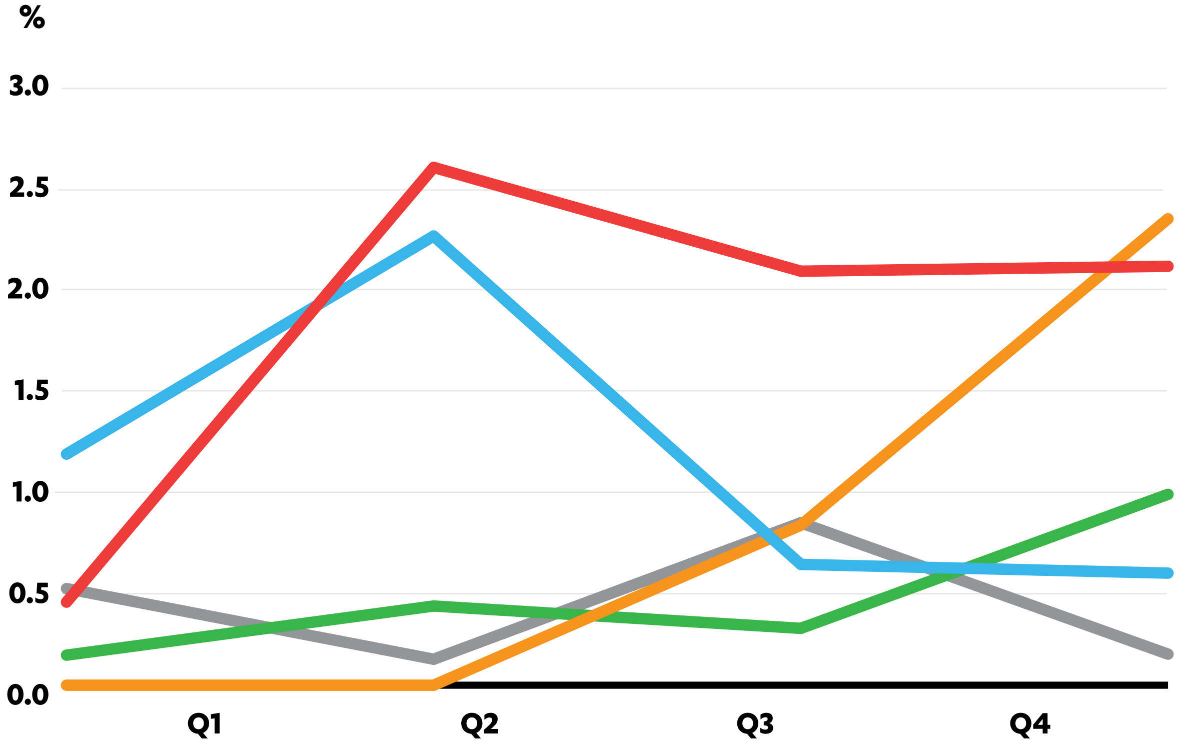
TROJAN-DOWNLOADER:W97M/DRIDEX

A banking Trojan that steals credentials of online banking websites. One of its components is a document file containing macro code that downloads the banking Trojan.

EXPLOIT:SWF/SALAMA

Exploits that target vulnerabilities in Adobe's popular Flash Player program.

PREVALENCE PER QUARTER*



*Percentage of all malware detection reports from the United Kingdom in 2015.

APPENDIX | THREAT DESCRIPTIONS

Alpha Crypt
This is ransomware that silently encrypts files on the user's machine and demands a ransom to provide the decryption key needed to decrypt the files.

AnglerEK (Angler exploit kit)
This detection identifies the code used by the Angler Exploit Kit to find and target vulnerabilities on the user's machine.

Asprox
Also known as Kuluoz, this malware is able to download and execute additional components. It is able to send spam emails and has been associated with ad-fraud activities.

Banker
Banker variants attempt to steal access information for various online banking and payment system websites. Details stolen include login credentials, passwords, PINs and so on. The stolen information is usually uploaded to a hacker's website using a webform.

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.

CloudDuke
CloudDuke is a malware toolset known to consist of, at least, a downloader, a loader and two backdoor variants.

CosmicDuke
The CosmicDuke toolset is designed around a main information stealer component. This information stealer is augmented by a variety of components that the toolset operators may selectively include with the main component to provide additional functionalities.

CoudW
Backdoor to the device, gives attackers access to the device to do as they please.

CozyDuke
CozyDuke is a modular malware platform formed around a core backdoor component. This component can be instructed by the C&C server to download and execute arbitrary modules.

Crowti
This is ransomware that silently encrypts files on the user's machine and demands a ransom to provide the decryption key needed to decrypt the files.

Cryptowall
Trojan:W32/Cryptowall is a ransomware that silently encrypts files on the user's machine and demands a ransom to provide the decryption key needed to decrypt the files.

CTB-Locker
CTB-Locker is ransomware that encrypts files on the affected machine and demands payment in return for the decryption key needed to restore access to the files.

Dialer
Porn-related app persistently displays a fullscreen page urging the user to call a number.

Dorkbot
This worm spreads via removable drives and Instant messaging networks. It steals passwords, downloads malware and contacts a web site for more instructions.

Downadup/Conficker
This ancient worm family exploits a vulnerability in unpatched Windows systems to spread copies of itself to any other accessible machines on the same network. It also attempts to download a file from a web site.

Dridex
A banking Trojan that steals credentials of online banking websites. One of its components is a document file containing macro code that downloads the banking Trojan.

DroidRooter
Gains device root privileges. Also used as a hack-tool when users deliberately run it to 'jailbreak' the device.

Expiro
Infects executable files and uses a keylogger component to steal credit card details.

Exploit:Java/Majava
This generic detection finds exploits that target flaws in the Java platform.

Exploit:W32/OfficeExploitPayload
Code embedded in a document file that exploits a Windows vulnerability. If the user opens the file, the code is automatically run and its payload is executed.

Exploit:OSX/CVE-2009-1237
This detection identifies the exploit code used by attackers to target the CVE-2009-1237 vulnerability in Apple Mac OS X 10.5.6 and earlier.

Exploit:SWF/Salama
This generic detection finds exploits that target flaws in Adobe Flash Player.

Fakeinst
Appears to be an installer for a popular app but instead sends SMS messages to premium rate numbers or services.

FakePDF
This malware is distributed via fraudulent spam e-mail attachments; once it has infected a system, the trojan downloads additional files onto the affected machine.

Fareit
This malware steals credentials from FTP clients and cryptocurrency wallets, and passwords stored in web browsers. It also downloads other malware, including Zbot.

FiestaEK (Fiesta exploit kit)
This detection identifies the code used by the Fiesta Exploit Kit to find and target vulnerabilities on the user's machine.

Flashback
A family of malicious applications which when installed on a computer will download a payload from a remote site, then modify targeted webpages displayed in the web browser. Variants in the Flashback family may include additional malicious functionalities or characteristics.

Gamarue
Also known as Andromeda, this malware ropes an infected device into a botnet. It will often also download and install other malware onto the infected machine.

GeminiDuke
The GeminiDuke toolset consists of a core information stealer, a loader and multiple persistence-related components. It primarily collects information on the victim computer's configuration.

Gingerbreak
Exploits a vulnerability in Android operating systems prior to version 2.34 to gain root privileges on the device.

Ginmaster
Steals confidential information from the device and sends it to a remote website.

HammerDuke
HammerDuke is a simple backdoor. The only known infection vector for HammerDuke is to be downloaded and executed by CozyDuke onto a victim that has already been compromised by that toolset.

HanJuanEK (Han Juan exploit kit)
This detection identifies the code used by the Han Juan Exploit Kit to find and target vulnerabilities on the user's machine.

Ippedo
This worm spreads via removable drives. It steals information from the infected machine and downloads other malware.

Kelihos
This malware steals credentials from FTP and mail clients, browsers, etc. It also harvests email addresses from the infected machine, and functions as a bot that is able to send spam emails using a peer-to-peer (P2P) infrastructure.

Kilim
This family of malicious web browser extensions post unauthorized content to a user's Facebook Wall.

MagnitudeEK (Magnitude exploit kit)
This detection identifies the code used by the Magnitude Exploit Kit to find and target vulnerabilities on the user's machine.

MiniDuke
The MiniDuke toolset consists of multiple downloader and backdoor components. Additionally, a specific loader is often associated with the MiniDuke toolset and is referred to as the "MiniDuke loader".

NeutrinoEK (Neutrino exploit kit)
This detection identifies the code used by the Neutrino Exploit Kit to find and target vulnerabilities on the user's machine.

Njw0rm
This worm spreads via infected removable drives and files attached to e-mails. If the user unwittingly uses the drive or file, it opens a backdoor on the device, steals saved passwords, and contacts a web site for more instructions.

NuclearEK (Nuclear exploit kit)
This detection identifies the code used by the Nuclear Exploit Kit to find and target vulnerabilities on the user's machine.

OnionDuke
The OnionDuke toolset includes at least dropper, a loader, an information stealer trojan and multiple modular variants with associated modules.

PinchDuke
The PinchDuke toolset consists of multiple loaders and a core information stealer trojan. The PinchDuke information stealer gathers system configuration information, steals user credentials, and collects user files from the compromised host transferring these via HTTP(S) to a C&C server.

Pkybot
Also known as Bublik, this malware gathers system information from the infected machine and communicates it back the malware's command and control (C&C) server. It is able to download further malware and has a man-in-the-browser functionality.

Ramnit
This ancient malware will add the infected device to a botnet that is known for engaging in stealing account logins and online banking theft.

Reveton
Reveton fraudulently claims to be from a legitimate law enforcement authority and prevents users from accessing their infected machine, demanding that a 'fine' must be paid to restore normal access.

RigEK (Rig exploit kit)
This detection identifies the code used by the Rig Exploit Kit to find and target vulnerabilities on the user's machine.

Sality
This malware adds an infected device into pool of similarly affected machines (a botnet) that an attacker can control and use to perform various malicious activities.

SeaDuke
A simple backdoor that focuses on executing commands retrieved from its C&C server, such as uploading and downloading files, executing system commands and evaluating additional Python code.

Slocker
Encrypts image, document and video files, then demands ransom payment to unlock the device and encrypt the affected files.

SmsKey
Sends SMS messages to premium-rate numbers, charging the user's phone bill.

SmsPay
Sends SMS messages to premium-rate numbers, charging the user's phone bill.

SmsSend
Sends SMS messages to premium-rate numbers, charging the user's phone bill.

TeslaCrypt
TeslaCrypt is ransomware that silently encrypts files on the user's machine and demands a ransom to provide the decryption key needed to decrypt the files.

Trojan.LNK.Gen
A generic detection for malicious .LNK files that are created by AutoIT, VBS and Powershell malware.

Trojan:JS/Redirector
This group of programs or scripts redirects a user from the website they are on or want to visit to another, unsolicited website.

Trojan:W32/Autorun
This detection identifies Autorun files that automatically executes malware when a removable media is accessed (and if Windows' Autoplay feature is enabled).

Trojan:W97M/MaliciousMacro.GEN
This generic detection finds malicious macros embedded in email file attachments.

Troldesh
This is ransomware that silently encrypts files on the user's machine and demands a ransom to provide the decryption key needed to decrypt the files.

UnityGhost
Identifies iOS apps that include code introduced when the software was created using a maliciously-modified version of the Unity app development tool.

Urausy
This is ransomware that fraudulently claims to be from a legitimate law enforcement authority and prevents users from accessing their infected machine, demanding that a 'fine' must be paid to restore normal access.

Virtob
Viruses belonging to this family (also known as Virut) infect files with .EXE and .SCR extensions. All viruses belonging to the Virut family also contain an IRC-based backdoor that provides unauthorized access to infected computers.

WornLink
A generic detection for malicious shortcut (.LNK) files embedded in a document file that can exploit the CVE-2010-2568 vulnerability in various versions of Windows.

Worm:W32/Kataja
This generic detection identifies shortcut icon files used by some USB worms to trick users into running malicious code.

WormLink
This detection identifies shortcut icon files embedded in documents that exploit a vulnerability in Windows.

XcodeGhost
Identifies iOS apps that include code introduced when the software was created using a maliciously-modified version of the Xcode app creation framework.

Zbot
Trojan:W32/Zbot (also known as Zeus or Wsnpoem) is a large family of malware that steals information from an infected system.

F-Secure.