Setting the Stage:
Landscape Shifts Dictate Future Threat Response Strategies

Contents

A broader and deeper threat landscape greeted 2016—a playing field shaped by the introduction of new technologies and attack models from the year before. 2015 laid the groundwork for what we can now consider the new status quo in cybersecurity.

Familiar challenges got more complicated given recent changes in attackers' modus operandi. Data breaches, for example, did not just end with compromised confidential data being leaked to the public. Instead, we saw how exposed data was further utilized in more damaging schemes. Attacks using zero-days still prevailed, with advancements in exploit kits allowing attackers to use them in ongoing cyberespionage campaigns like Pawn Storm.

In global cybercrime, different underground markets continued to grow not only in breadth but in depth. Crimeware offerings, portals, and cybercriminal training evolved to match the demands of their respective countries. Fledgling marketplaces emerged alongside their more mature counterparts—established underground regions that found ways to take advantage of darknets and the Deep Web.

Developments in 2015 had also created a much broader attack surface. This is partly due to the proliferation of the Internet of Things (IoT). Smart devices have been security concerns for organizations since their conception, and with the number of successful hacks reported over the past months, it is only a matter of time before cybercriminals and attackers find ways to use these weak points for large-scale operations.

The stage is set. With these paradigms now in place, traditional methods of protecting data and assets may need to be reconsidered, especially when creating critical security strategies that will govern organizations in the years to come.

Dissecting Breaches

Several high-profile organizations came under fire in 2015 when breaches led to the exposure of critical data and put their clients and employees at risk. Although incidents of this magnitude have become common, as of last year, we noted the more active use of compromised data for online extortion and cyber attacks.

For instance, people whose names were linked to the Ashley Madison data dump received blackmail letters[1] coercing them to pay bribes in exchange for their anonymity. These cases happened only a few days after 30 million of the site's member records were released.[2,3]

The Italian surveillance company, Hacking Team was also a victim of a massive breach. Around 400 gigabytes of company emails and documents were taken and dumped online.[4] Included in these dumps were a number of zero-day vulnerabilities and exploits we discovered. This allowed attackers to use the data in attacks against entities in Korea and Japan, while also compromising a number of websites in Taiwan and Hong Kong.[5]

2015 offered no respite from data breaches in the healthcare industry. Protected health information (PHI) of 80 million Anthem consumers, including names, addresses, birth dates, income data, and Social Security numbers were compromised. A month after, health insurer Premera Blue Cross[6] also suffered from a major data breach—exposing up to 11 million customers' banking account numbers and other sensitive data such as patient treatment information.

Breaches have also found their way to the federal level. An estimate of around 21.5 million records[7] got stolen from the U.S. Office of Personnel Management's (OPM) in two separate but related incidents. The data included the employment history, residence, medical and financial history, and even the fingerprints of some 5.6 million federal employees.[8]

These high-profile incidents are consistent with our data breach analysis. In our research paper "Follow the Data: Dissecting Data Breaches and Debunking the Myths,"[9] healthcare and government sectors are some of the most affected industries in terms of breaches. Other sectors include education, retail, and finance.

Anthem

February 10
80M records (personal information)

Premera Blue Cross

March 20
11M records (personal information and financial data)

UCLA Health System

May 5
4.5M records (personal information and medical records)

CareFirst BlueCross BlueShield

May 20
1.1M records (personal information)

IRS Washington DC

May 26
100K records (financial data)

Japan Pension Service

June 1
1M records (personal information)

OPM

June 4
21.5M records (personal information)

Hacking Team

July 7
Undetermined number (trade secrets)

Ashley Madison

July 21
37M records (personal information)

Excellsus BlueCross BlueShield

September 10
10M records (personal information and financial data)

Systema Software

September 21
1.5M records (medical records)

Scottrade

October 1
4.6M records (personal information)

Experian

October 1
15M records (personal information)

Vtech

November 30
6.4M records (email addresses)

Secretary of State **Brian Kemps**

November 18
6M records (personal information)

JAN · FEB · MAR · APR · MAY · JUN · JUL · AUG · SEP · OCT · NOV · DEC

■ Healthcare ■ Government ■ IT ■ Commercial ■ Business Service

2015's biggest data breaches

●	Healthcare	26.9%
●	Education	16.8%
●	Government	15.9%
●	Retail	12.5%
●	Financial	9.2%
●	Service	3.5%
●	Banking	2.8%
●	Technology	2.6%
●	Insurance	1.6%
●	Media	1.4%
●	Others	6.8%
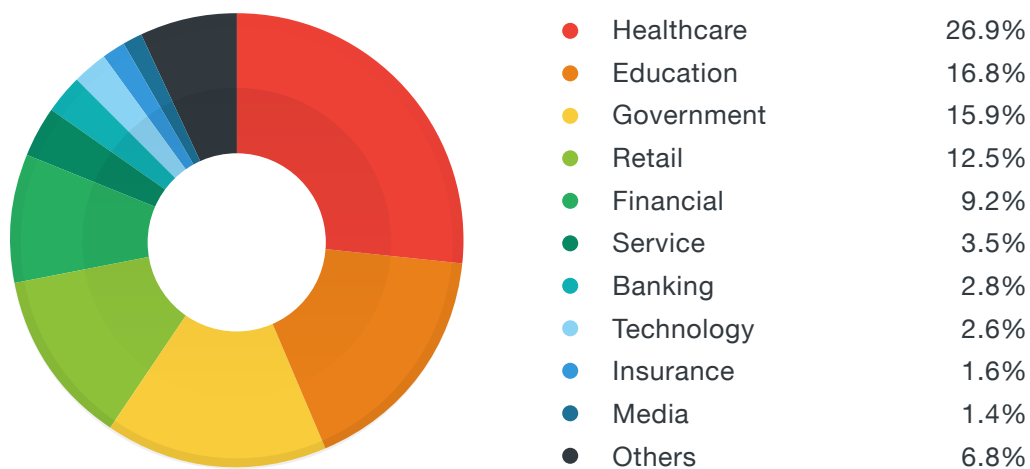
The healthcare industry is the most affected sector in data breaches.

Around 41% of data breaches in the US have been caused by device loss. Remote device wipe, disk encryption, the use of virtual infrastructure, and enforcement of stricter policies can help mitigate such cases. But for those that involve malware and hacking, breach detection and network security solutions are required.

System administrators and managers need solutions that allow them to monitor network traffic across all ports to spot any anomalies and prevent attackers before they can advance. Custom sandboxing, on the other hand, would give them the capabilities needed to single out malware, identify C&C activity, and pinpoint other tell-tale signs of impending or ongoing attacks.

Pawn Storm Zero-Days and Other Vulnerabilities

In our continuous monitoring of Pawn Storm,[10] a long-running cyberespionage campaign, we discovered it using zero-day exploits to target high-profile entities. In July, email messages were sent to a US defense organization and the armed forces of a North Atlantic Treaty Organization (NATO) country that contained a URL hosting a Java exploit—the first one seen in nearly two years.[11] This was followed up in October when the people behind Pawn Storm used an Adobe Flash zero-day exploit in spear phishing emails sent to several foreign affairs ministries across the globe.[12]

Other noteworthy zero-days were discovered during the days succeeding the Hacking Team breach. We found a new zero-day vulnerability in Internet Explorer (CVE-2015-2425),[13] two Flash Player zero-day vulnerabilities (CVE-2015-5122[14] and CVE-2015-5123[15]), and one particular Flash zero-day that was used in limited attacks in Japan and Korea. This said zero-day (CVE-2015-5119)[16] was also integrated into both the Angler Exploit Kit and Nuclear Exploit Pack.

Zero-days can be used on any target. We have seen this in the way they have been incorporated in spear phishing campaigns launched against individuals and organizations. We know they can be added into known exploit kits that abuse a wide array of users. If a system is unpatched and exposed to such threats, compromise is almost certain. Organizations looking to protect their networks and data should consider virtual patching as an interim solution. Virtual patches can protect vulnerable systems from unknown exploits in the absence of an official patch, especially with operating systems (OS) and applications which are no longer being supported by the vendor.

Adobe Flash Player	**Adobe Flash Player***	**Adobe Flash Player***	**FREAK**	**Android Manifest File***
January 22 CVE-2015-0310	January 22 CVE-2015-0311	February 2 CVE-2015-0313	March 15 CVE-2015-0204	April 6 CVE-2015-0313
Apache Cordova*	**Samsung Swift Key**	**Adobe Flash Player**	**Android Debugger***	**Adobe Flash Player***
May 27 CVE-2015-1835	June 19	June 23 CVE-2015-3113	June 26	July 7 CVE-2015-5119
Adobe Flash Player*	**Adobe Flash Player***	**Oracle Java SE***	**Internet Explorer***	**Windows***
July 11 CVE-2015-8122	July 11 CVE-2015-5123	July 11 CVE-2015-2590	July 14 CVE-2015-2425	July 20 CVE-2015-2426
Android Media Server*	**Stagefright**	**Android Media Server**	**Android Messaging***	**Android Messaging***
July 29 CVE-2015-3861	July 31 CVE-2015-3824	August 4 CVE-2015-3823	August 11 CVE-2015-3839	August 11 CVE-2015-3840
Android Media Server*	**iOS Quicksand**	**Adobe Flash Player***	**Stagefright***	**Baidu**
August 17 CVE-2015-3842	September 6 CVE-2015-5749	October 13 CVE-2015-7645	October 15 CVE-2015-6600	November 1
iOS Siri	**Netflix, Tencent***			
November 18	December 3			

● PC   ● Mobile

▢ Zero-day   ▢ Used in Operation PawnStorm

* Discovered by Trend Micro

2015 in vulnerabilities

Mobile devices continued being hotbeds for cybercriminals looking to exploit security flaws. Android's MediaServer component took a lot of hits in 2015. Vulnerabilities found in the component can be exploited to perform attacks using arbitrary code execution. Such attacks could force a device's system to go on endless reboot, draining its battery.[17,18] It can also be used to render Android devices silent and unable to make calls due to unresponsive screens.[19] A vulnerability in Android's manifest file may also cause devices to experience constant rebooting, making the device totally useless.[20]

Some other Android vulnerabilities include the Android debugger Debuggered vulnerability[21] we discovered in June. It can be utilized to expose a device's memory content. The Android Installer Hijacking vulnerability,[22] meanwhile, gives hackers the ability to replace legitimate apps with malicious versions in order to steal information from the user.

The Samsung SwiftKey Keyboard vulnerability[23] (CVE-2015-4640 and CVE-2015-4641[24]) had a pre-loaded malicious code masquerading as additional language packs that put over 600 million Samsung Galaxy series phones at risk. We also uncovered the Apache Cordova[25] mobile API framework flaw, which remotely exploits applications with a mere click of a URL.

Although the state of Apple security is relatively better than of Android's, Apple's trusted walled garden also took some hits in 2015. The emergence of vulnerabilities like iOS Quicksand and AirDrop proved that iOS users could potentially be hit with exploits. The malicious code XcodeGhost[26], while technically not a vulnerability, was also able to affect several users in China and the US.

Since personal mobile devices are heavily used in the enterprise setting, it is important for corporate data to never reside in them. But this would be impractical given the need for employee mobility. Enterprises hoping to keep confidential data within their own servers can invest in virtual mobile infrastructure. A solution like this allows employees to access company files and records without ever having to save the data on their physical gadget. In case an employee device ever gets rendered useless by mobile exploits or compromised by malware, the data remains separate and intact.

Deep Web and Underground Explorations

The arrest and sentencing of Silk Road founder Ross Ulbricht—the man responsible for heading the billion-dollar narcotics black market[27]—drew a lot of interest to the Deep Web, more specifically, to darknets. Although many of the sites found on the Deep Web were originally designed to protect user anonymity and foster the free exchange of information that is normally restricted in certain regions, some of them have been repurposed for cybercriminal use. In 2015, we saw cybercriminal markets branch out into the deeper recesses of the Deep Web.

As for cybercriminal underground economies, China remained a global leader in terms of innovation. Chinese cybercriminals developed PoS (point of sale), ATM (automated teller machine), and pocket skimmers to steal credit card information. These crimeware offerings reflect the country's retail sector migrating to noncash payment systems. The Chinese also created leaked-data search engines that allow the querying of information found in data dumps resulting from breaches.[28] Another advanced marketplace, the Russian underground, showed enhancements through sales automation. This improvement made it easier for threat actors to find whichever stolen information they want.[29]

Younger underground markets slowly gained ground in 2015. This was mostly due to lax laws against cybercrime and increasing interest in coding and software development. The Brazilian cybercriminal underground, for example, began offering training services to cybercriminal aspirants.[30] Some of these tutorials included how to set up botnets and how to execute payment card theft. Most of the transactions in this region were publicly advertised via social media sites, showing a blatant disregard for law enforcement. The underground in Japan was quite the opposite. While Brazil thrived on being blatant, Japanese cybercriminals made their business exclusive by closing off outsiders through localized screening methods.[31] Illegal contraband and paraphernalia like drugs, child pornography, and high-caliber weaponry were present in the flourishing Japanese underground despite the country's strict laws against the said goods.

Global underground trends in 2015
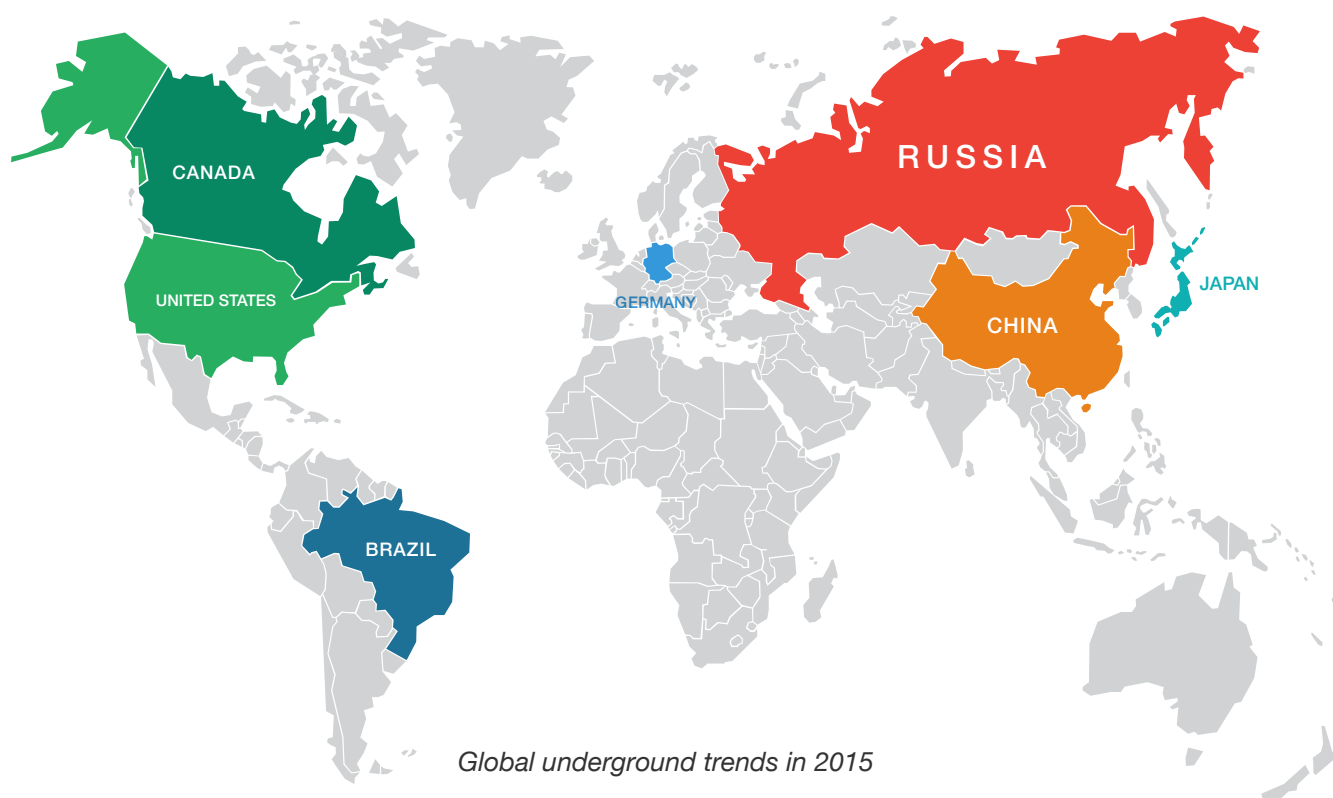
RUSSIA

One of the most established cybercriminal marktplaces, the Russian underground continues to open its doors to anyone interested in launching their own enterprise by offering them optimized crimeware tools and even partnerships.

CHINA

The Chinese underground continues to pioneer new innovations—hardware and channels like portable PoS skimmers and data leaked-data search engines—that drive cybercriminal trends in the region.

UNITED STATES

North American underground sites can be easily found in the Surface Web, open and visible to both cybercriminals and law enforcement. Its fiercely competitive nature drives down prices, making them favorable for newbie cybercriminals.

CANADA

While it is not as large or well-developed as other underground communities, there is a viable Canadian underground community primarily focused on the sale of fake or stolen documents and credentials.

JAPAN

The Japanese underground is a new marketplace characterized by the taboo and the vindictive. Its offerings are often found behind gated bulletin boards that screen users, creating a highly exclusive localized environment.

GERMANY

Deemed the fastest developing underground within the European Union, the German underground is getting known for offering locally produced crimeware designed to target citizens in the region.

BRAZIL

The Brazilian underground is populated by young, bold individuals with no regard for the law. They use popular social media sites like Facebook™ and other public forums and apps to openly flaunt and promote their illegal activities.

Although relatively small compared to other cybercriminal markets, the German underground appeared to be already well-developed. Aside from using of escrows as middlemen for transactions, many German cybercriminals relied on Packstations[32] or delivery services that allowed them to conveniently do dead drops in locations across the country. In North America, its underground continued to grow. Ransomware, narcotics, and even murder-for-hire services were all made available on the Surface Web, visible to cybercriminals and their customers as well as to law enforcement.[33]

Each region's cybercriminal underground trends have bearing in the real world. The offerings found in these marketplaces reflect the emerging and ongoing threats prevalent in each region. The production of credit card skimmers in China, for example, spells trouble for small businesses in the country. Most of these devices work against business owners who may unknowingly purchase tainted PoS machines and lose income in the process. Knowing these trends could help local law enforcement protect their citizens better. By partnering with security researchers, they can gain valuable sources of threat intelligence concerning both the cybercriminal underground and illegal transactions in the Deep Web.

Smart Technology Nightmares

The successful hacks on IoT devices in 2015 put an end to speculations regarding their susceptibility to attacks. Although there have been a number of previous reports on compromised baby monitors[34] and smart refrigerators,[35] it was only last year when researchers proved smart cars could be tampered with in real time.

Our own research on Škoda Auto's SmartGate System in Fabia III cars[36] revealed that an attacker could alter the car's system if the vehicle were within its Wi-Fi network range. The system flaw could also allow any attacker to track the driver's whereabouts and even lock out the driver from accessing the SmartGate system.

Similar researches echoed these findings. A report analyzing the flaws of several 2010 Ford Escape and Toyota Prius[37] units proved that these vehicles could be commandeered wirelessly, letting attackers control the steering wheel and disable the breaks. In another experiment, a researcher was able to take control of a Jeep Cherokee[38] while it was being driven on a highway at 70 mph. If that were a real attack, it could have potentially ended with injuries.

IoT devices used in businesses are also prone to hacks, as our researchers demonstrated in their GasPot experiment.[39] They created a custom honeypot tool called GasPot, which lets other researchers and gas tank owners set up their own virtual monitoring systems to track and record hacking attempts on gas station supervisory systems or automatic tank-gauging (ATG). Based on the honeypot results, US gas stations were the most popular targets by attackers from across the globe. If these were actual gas pumps, attackers could have launched distributed denial of service (DDoS) attacks which could cripple station operations. If the said attackers set their sights on the gas tank levels or overflow limits, they could even cause major accidents and explosions.

● US		44%
● Jordan		17%
● Brazil		11%
● UAE		11%
● UK		11%
● Russia		6%
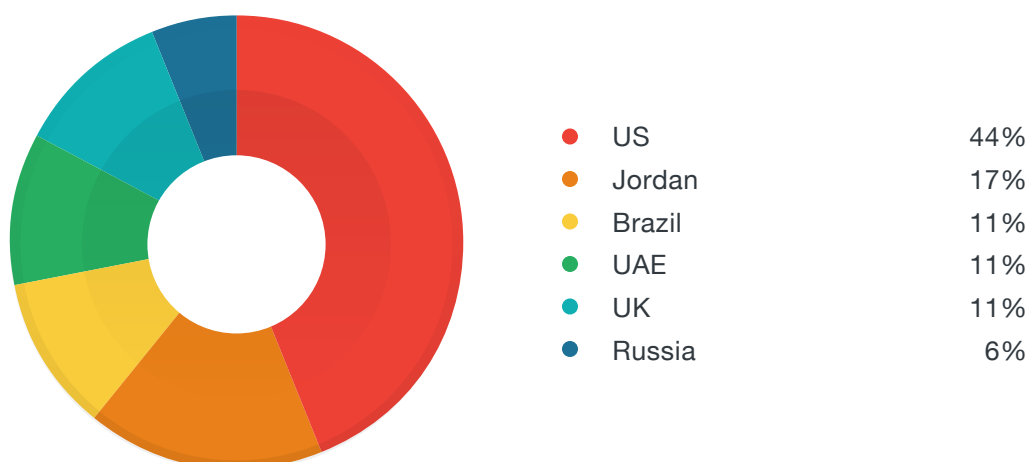
Breakdown of attacks of GasPot deployments observed by country

One of the challenges we noted in our 2016 security predictions[40] is the likelihood of more hacks on smart technologies that could result to serious and even fatal damages. These incidents serve as proofs of concept, solidifying what we previously thought was only possible in fiction. The need for security and testing of IoT devices is much stronger now, and manufacturers are expected to step up to the plate to protect their customers' privacy and physical safety.

These Internet-connected devices can still be avenues to data loss and compromise. Most of these devices were designed with functionality in mind; security, only secondary. In order to keep these devices protected from attacks, developers need to be able to push regular updates and patches to close off any holes attackers can exploit. This problem is synonymous to when Android devices were first introduced to the workplace. The same fragmentation issue Android continues to experience plagues IoT as well. Since these devices do not run using a single OS—such as the case of Android—it complicates the updating process and leaves large windows open for compromise. While there are no current solutions designed to protect IoT, enterprises need to start building their security posture around these potential liabilities.
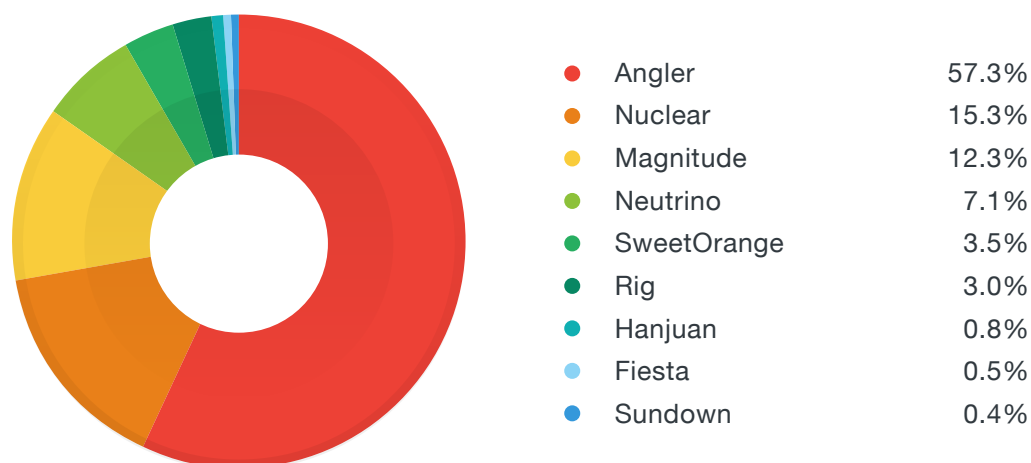
Angler, the King of Exploit Kits

The Angler exploit kit has gained a lot of buzz in the past year. Due to its easy integration, it became the most used exploit in 2015.

In February, we linked it to a series of malvertisement attacks. Cybercriminals enticed their targets to click on ads,[41] which lead to ransomware infection. By December, the blog of prominent news website The Independent got hacked. The cybercriminals behind the ploy also used Angler in conjunction to an advertisement displayed on the page to infect users with TeslaCrypt Ransomware.[42]

Japan felt the brunt of Angler in September. Three waves of malvertising campaigns designed to target Japanese users were launched. Around 3,000 high-profile Japanese sites were affected, and around 500,000 users were exposed to the said malvertisements.[43]

In July, Angler got updated to include a Flash zero-day that was part of the Hacking Team leak.[44] By November, it included a Flash exploit used in the Pawn Storm[45] campaign.

●	Angler	57.3%
●	Nuclear	15.3%
●	Magnitude	12.3%
●	Neutrino	7.1%
●	SweetOrange	3.5%
●	Rig	3.0%
●	Hanjuan	0.8%
●	Fiesta	0.5%
●	Sundown	0.4%

Angler climbed up to over 1,600,000 URL access count by the end of 2015,
significantly getting ahead of other exploit kits such as Nuclear and Magnitude.

| | | | | | | | | |
|15M — 15.44M | | | | | | | | |
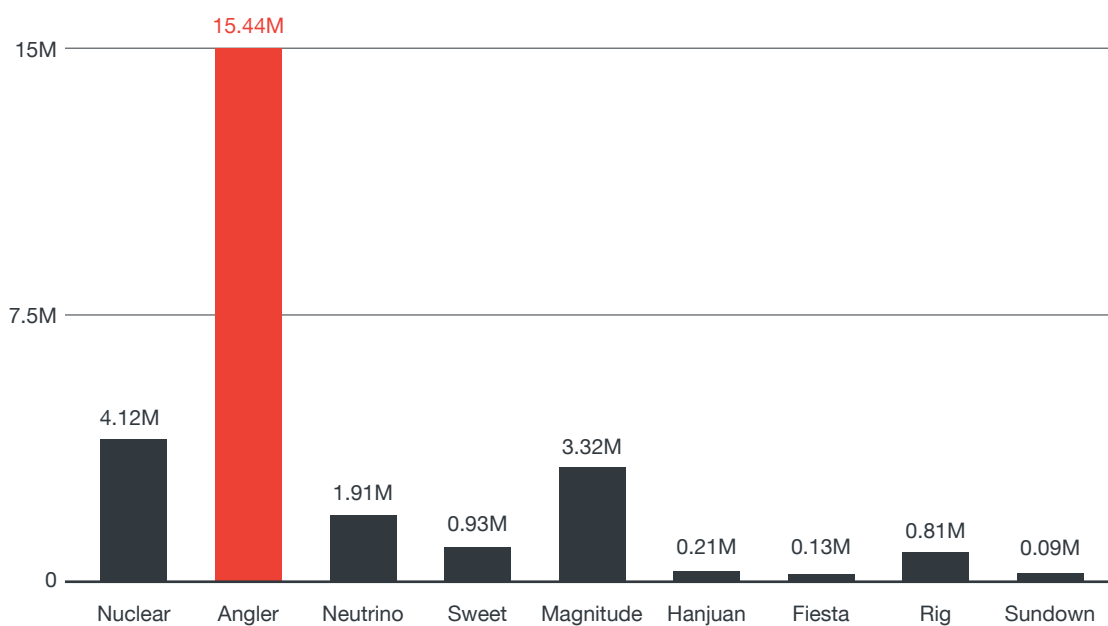
Angler-exploit-kit-hosting URLs were the most accessed in 2015.
SweetOrange, Hanjuan, Fiesta, and Sundown exploit kits were rarely updated in 2015.

●	Japan	50%
●	US	23%
●	Australia	7%
●	Canada	2%
●	Germany	2%
●	France	2%
●	UK	1%
●	Taiwan	1%
●	Thailand	1%
●	Italy	1%
●	Others	10%
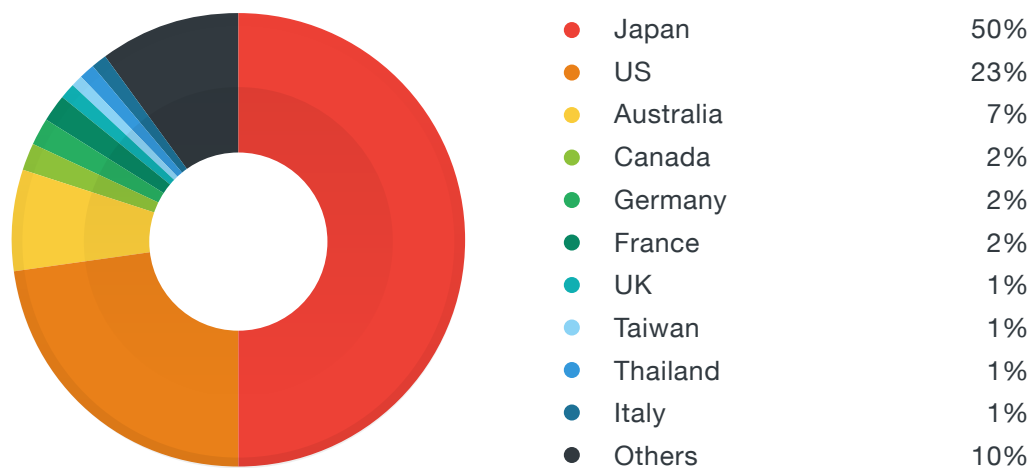
Users in Japan, United States, and Australia were the most affected countries in 2015. Japan users were
exposed to Angler exploit kits because of two major malvertisement campaigns observed in 3Q and 4Q.

Angler

CVE-2015-2419	CVE-2015-3104
CVE-2015-1671	CVE-2015-3090
CVE-2015-8446	CVE-2015-0359
CVE-2015-7645	CVE-2015-0336
CVE-2015-5560	CVE-2015-0313
CVE-2015-5122	CVE-2015-0311
CVE-2015-5119	CVE-2015-0310
CVE-2015-3113	

Rig

CVE-2015-2419
CVE-2015-5122
CVE-2015-5119
CVE-2015-3113
CVE-2015-3090
CVE-2015-0359
CVE-2015-0311

Magnitude

CVE-2015-2419	CVE-2015-3105
CVE-2015-1671	CVE-2015-3090
CVE-2015-7645	CVE-2015-0359
CVE-2015-5122	CVE-2015-0336
CVE-2015-5119	CVE-2015-0311
CVE-2015-3113	

Neutrino

CVE-2015-2419	CVE-2015-3090
CVE-2015-7645	CVE-2015-0359
CVE-2015-5122	CVE-2015-0336
CVE-2015-5119	CVE-2015-0313
CVE-2015-3113	CVE-2015-0311

Sundown

CVE-2015-2444
CVE-2015-0313
CVE-2015-0311

Nuclear

|	
CVE-2015-2419	CVE-2015-3104
CVE-2015-7645	CVE-2015-3090
CVE-2015-5560	CVE-2015-0359
CVE-2015-5122	CVE-2015-0336
CVE-2015-5119	CVE-2015-0313
CVE-2015-3113	CVE-2015-0311

Angler has been the most prolific in incorporating exploits into 2015 vulnerabilities.
Some of the exploits it added to its arsenal are zero-days.

Sandboxing isolates programs in a protected environment. It allows administrators to safely manipulate, run programs, and discover threats and their various evasion techniques. It helps detect and analyze threats and obfuscated exploits that target organizations. Solutions like this can aid organizations to spot and provide fixes against zero-days and other exploits.
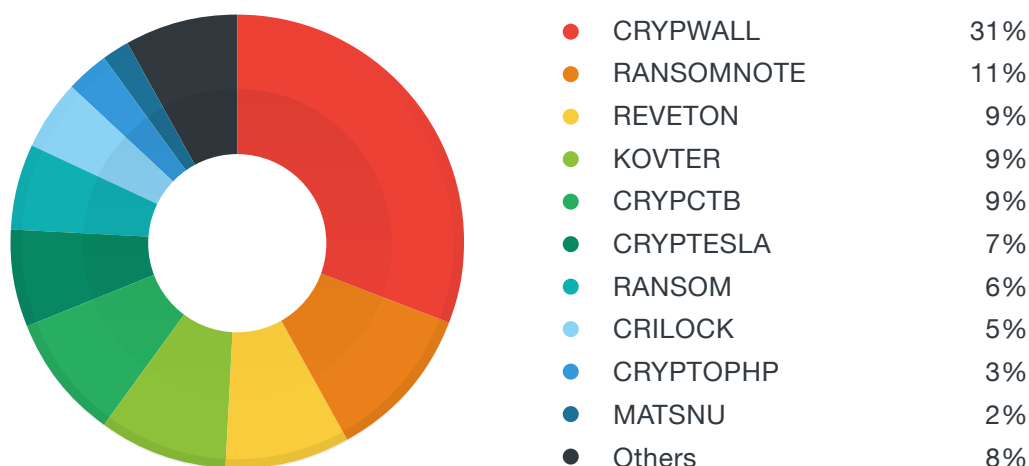
Data Held Hostage

In a span of 12 months, we saw ransomware evolve not only in code and structure but also in terms of the way it was used and the targets it was used against. A review of the trend shows a decline in cybercriminals' use of traditional ransomware in their modus operandi. Instead, they have opted to use crypto-ransomware,[46] a type of malware that employs strong cryptography to hold a large collection of data hostage. An upward trend in crypto-ransomware detections supports this shift.
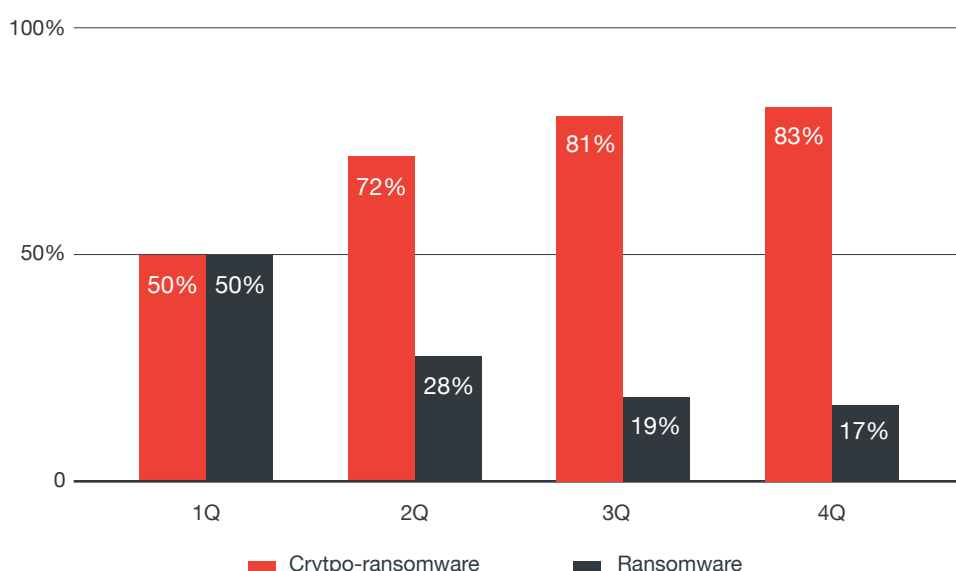
*Compared to last year's data, this year's crypto-ransomware numbers
steadily rose up to the end of 2015 and even overtook ransomware.*

In 2015, we saw more incidents involving the crypto-ransomware variant called Cryptowall.[47] It arrives on users' computers through email or malicious downloads and then subsequently encrypts files afterward. Once all of the files have been encrypted, cybercriminals will then ask for a ransom in exchange for decryption. Its third iteration, Cryptowall 3.0, emerged in 2015. It utilizes C&C servers, spammed messages, spyware, and compromised websites as modes of infection.[48]
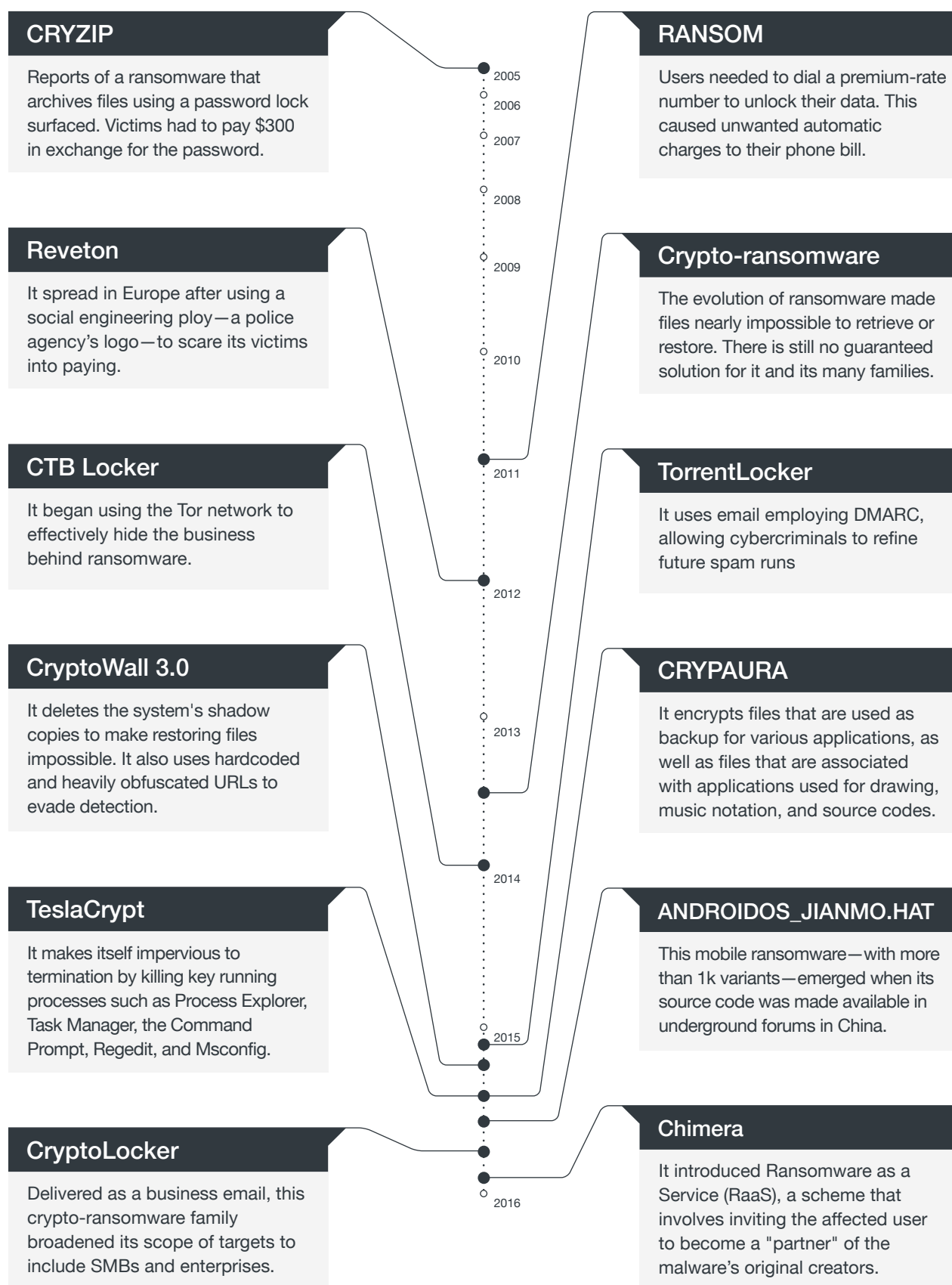
Cryptowall topped the list of 2015's most notorious ransomware families. It is followed by Ransomnote, a crypto-ransomware family known for leaving ransom note traces on infected machines. It is different from most ransomware variants that perform file-less installations.

● CRYPWALL	31%
● RANSOMNOTE	11%
● REVETON	9%
● KOVTER	9%
● CRYPCTB	9%
● CRYPTESLA	7%
● RANSOM	6%
● CRILOCK	5%
● CRYPTOPHP	3%
● MATSNU	2%
● Others	8%

The ransomware family Chimera[49] not only encrypts files, it extorts money from targets by threatening to post the data online. On top of that, the malware creators offer their targets an opportunity to join their ranks. Through their ransom note, they call for interested affiliates to help them peddle ransomware as a service (RaaS).

Ransomware typically sells for US$10 in the US underground.[50] In regions like Brazil, cybercriminals can use an unlimited number of multiplatform ransomware to target their victims for a week for only US$3,000 or 9 BTC.[51] This is a small price they pay to get big returns. The typical ransom fee demanded from victims ranges from US$200 to US$10,000. A report from the FBI's Internet Crime Complaint Center (IC3)[52] revealed that between April 2014 and June 2015, a total of $18 million in losses was reported by Cryptowall victims. Once crypto-ransomware encrypts user data, they have no guarantee of getting it back. The risk and damages resulting to this loss is much higher depending on the kind of data locked out.

The best way of dealing with ransomware of any type is still prevention using a multi-layered strategy of advanced threat defenses specifically created for crypto-ransomware. It is crucial to protect any means by which ransomware can infect a system. Since the most common infection vectors are spam and malicious URLs, individuals and organizations can benefit from email and web reputation and filtering. It also always advised for organizations, especially very large enterprises, to back up critical data in case of ransomware outbreaks within their network.

CRYZIP

Reports of a ransomware that archives files using a password lock surfaced. Victims had to pay $300 in exchange for the password.

RANSOM

Users needed to dial a premium-rate number to unlock their data. This caused unwanted automatic charges to their phone bill.

Reveton

It spread in Europe after using a social engineering ploy—a police agency's logo—to scare its victims into paying.

Crypto-ransomware

The evolution of ransomware made files nearly impossible to retrieve or restore. There is still no guaranteed solution for it and its many families.

CTB Locker

It began using the Tor network to effectively hide the business behind ransomware.

TorrentLocker

It uses email employing DMARC, allowing cybercriminals to refine future spam runs

CryptoWall 3.0

It deletes the system's shadow copies to make restoring files impossible. It also uses hardcoded and heavily obfuscated URLs to evade detection.

CRYPAURA

It encrypts files that are used as backup for various applications, as well as files that are associated with applications used for drawing, music notation, and source codes.

TeslaCrypt

It makes itself impervious to termination by killing key running processes such as Process Explorer, Task Manager, the Command Prompt, Regedit, and Msconfig.

ANDROIDOS_JIANMO.HAT

This mobile ransomware—with more than 1k variants—emerged when its source code was made available in underground forums in China.

CryptoLocker

Delivered as a business email, this crypto-ransomware family broadened its scope of targets to include SMBs and enterprises.

Chimera

It introduced Ransomware as a Service (RaaS), a scheme that involves inviting the affected user to become a "partner" of the malware's original creators.

Timeline years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016

Ransomware timeline

Takedowns versus DRIDEX

In October, the FBI and the National Crime Agency of the UK (NCA) seized multiple command-and-control (C&C) servers used by the notorious DRIDEX botnet.[53] DRIDEX is an advanced information-stealing malware that targets users' online banking data.[54] The malware is spread via spam that contain malicious file attachments that use macros.[55]
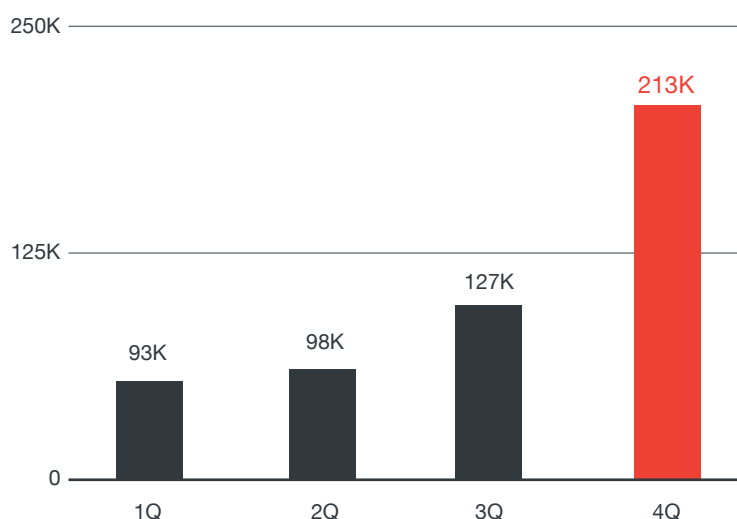
The big increase in macro malware was caused by DRIDEX and its spam runs in 4Q.

The said takedown contributed to a significant drop in in the number of DRIDEX detections within the US, but the threat still persisted in other countries.[56] The reason for which was that a number of DRIDEX-related C&Cs were still hosted in regions beyond the reach of the abovementioned law enforcement bodies.
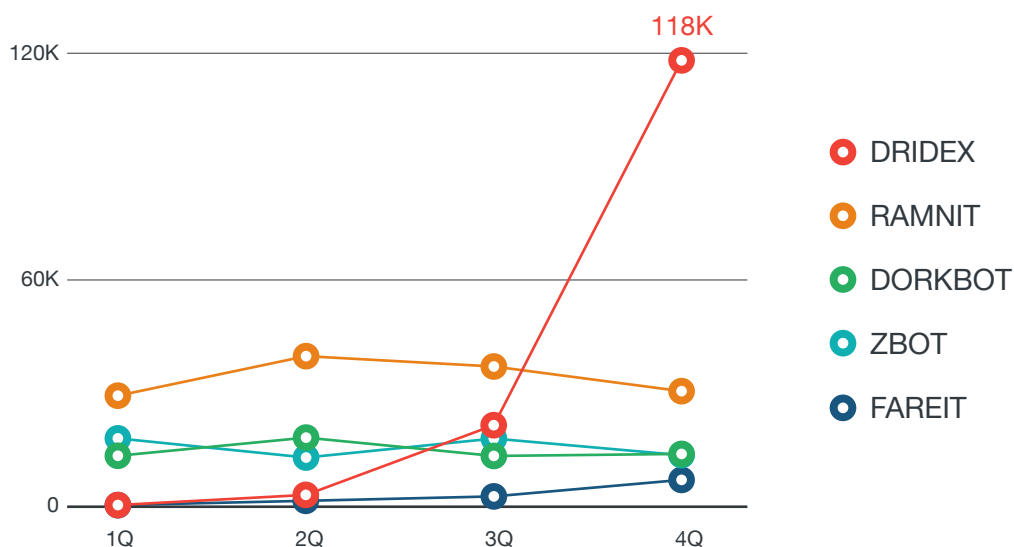
*For the last quarter of 2015, DRIDEX appeared to have significantly picked up steam,
with other banking malware treading far behind.*

US felt a resurgence of DRIDEX in November, just a month after the major takedown. We saw multiple DRIDEX-related spam campaigns[57] using macro malware-laden Microsoft Excel® and Word® attachments disguised as invoices and financial statements. This scenario demonstrates the challenges posed by C&C infrastructure hosted on bulletproof hosting services (BPHS).[58] The nature of these hosting services makes it difficult to permanently eradicate these kinds of botnets.

Organizations looking to protect themselves from threats like DRIDEX can invest in reputation-based solutions. Since DRIDEX is delivered via spam and relies on C&C communications, it is important to monitor email and URL reputation. Given DRIDEX's macro malware component, traditional antivirus may not be enough to stop infections. Solutions that allow sandbox analysis of files can better protect against malicious programs that reside in the system's memory.
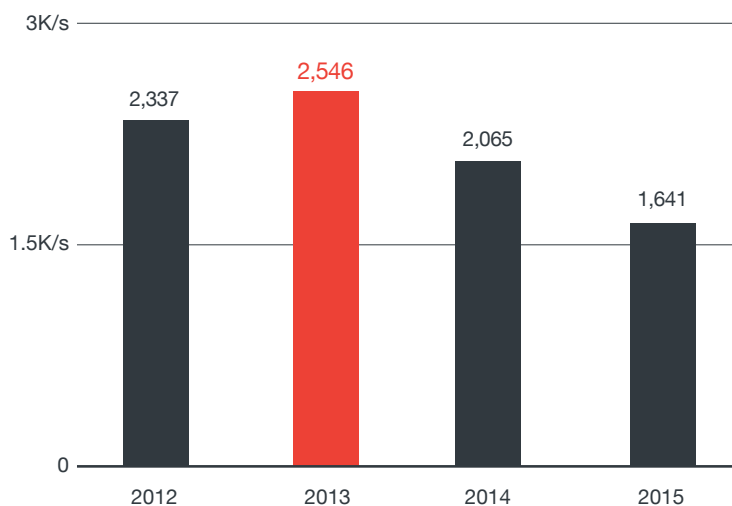
Threat Landscape in Review

The Trend Micro™ Smart Protection Network™ blocked over 52 billion threats in 2015, a 25% decrease from 2014. This decrease is consistent with the downward trend of system infections since 2012, caused by attackers who have become more selective of their targets as well as the shift in technologies they use.
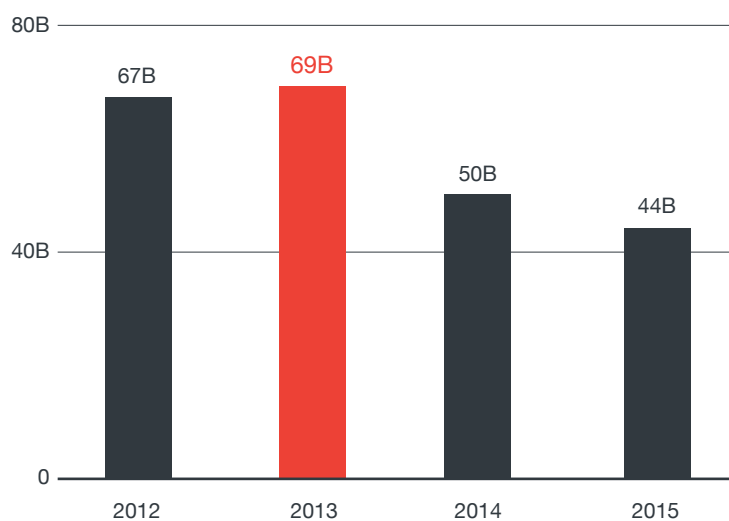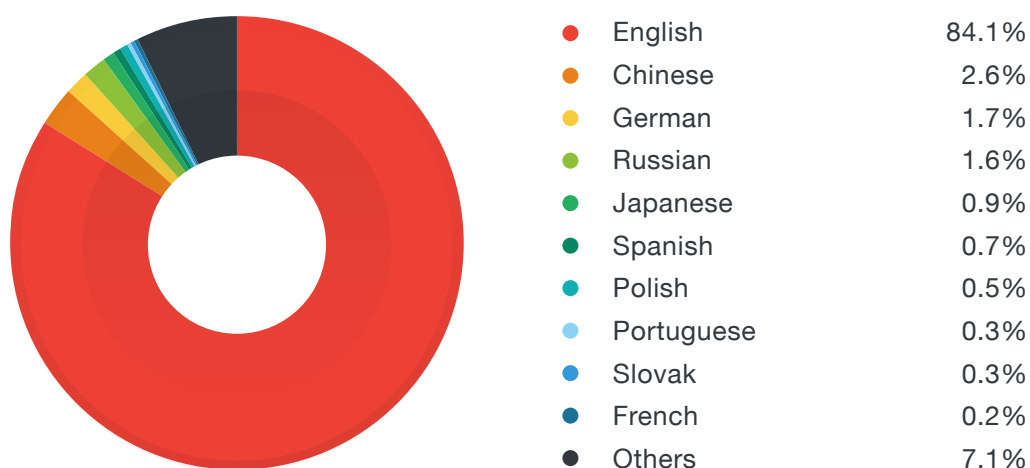
Total number of threats blocked
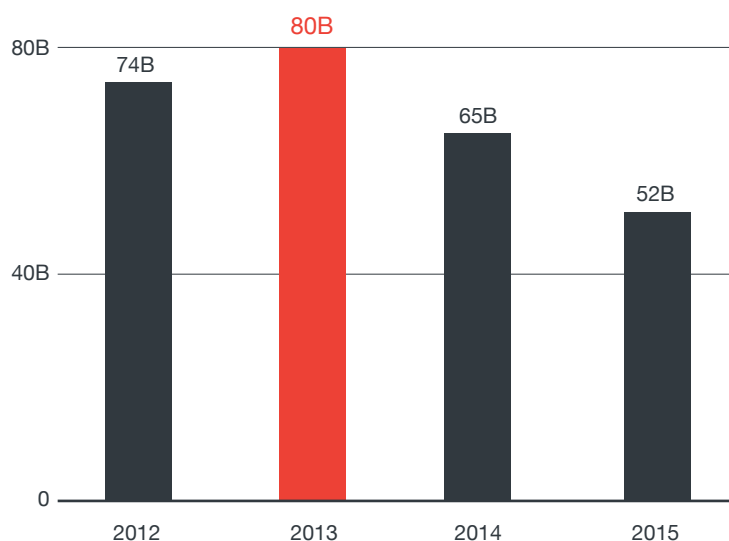
Trend Micro overall detection rates
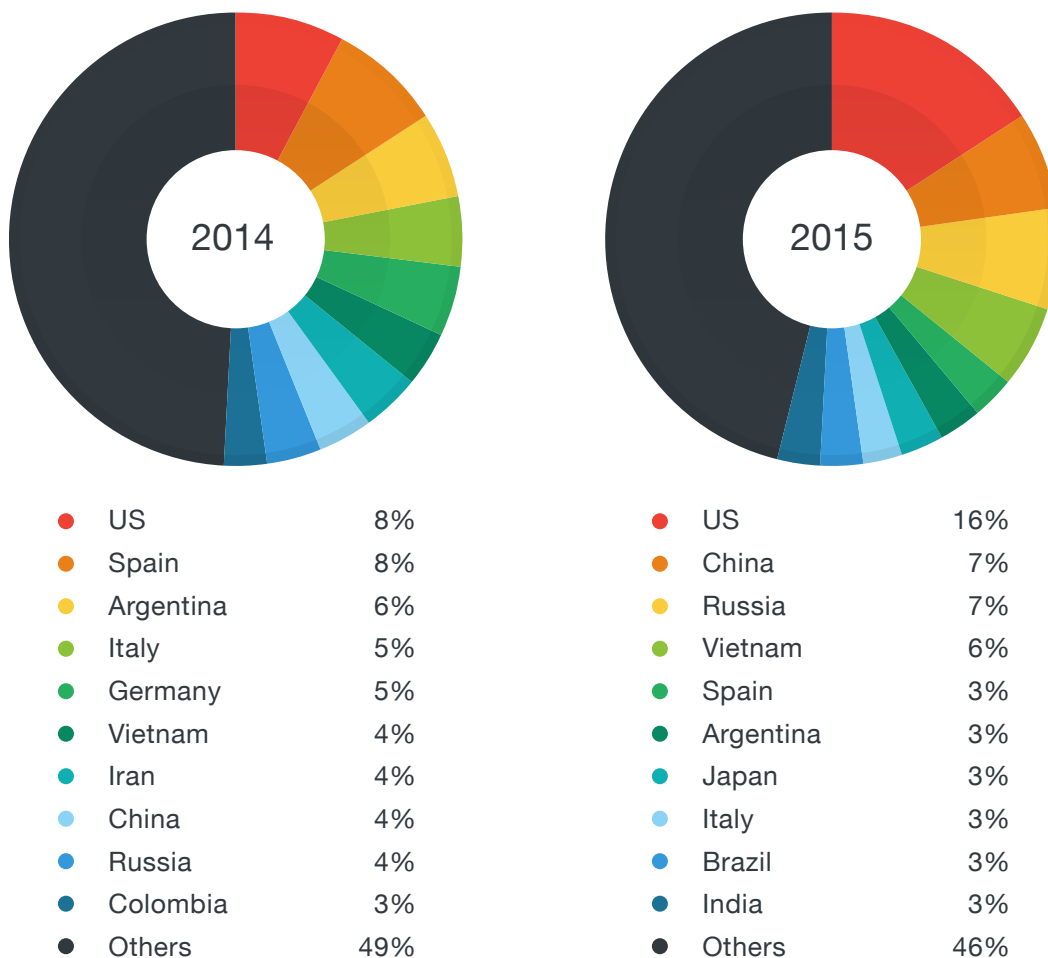
Number of email reputation queries categorized as spam

Top spam languages

●	English	84.1%
●	Chinese	2.6%
●	German	1.7%
●	Russian	1.6%
●	Japanese	0.9%
●	Spanish	0.7%
●	Polish	0.5%
●	Portuguese	0.3%
●	Slovak	0.3%
●	French	0.2%
●	Others	7.1%

English remained the most-used spam language in 2015.

Top spam-sending countries

2014

●	US	8%
●	Spain	8%
●	Argentina	6%
●	Italy	5%
●	Germany	5%
●	Vietnam	4%
●	Iran	4%
●	China	4%
●	Russia	4%
●	Colombia	3%
●	Others	49%

2015

●	US	16%
●	China	7%
●	Russia	7%
●	Vietnam	6%
●	Spain	3%
●	Argentina	3%
●	Japan	3%
●	Italy	3%
●	Brazil	3%
●	India	3%
●	Others	46%

The number of spam doubled in the US in 2015. China and Russia moved up the ranks,
while Japan joined the top 10.
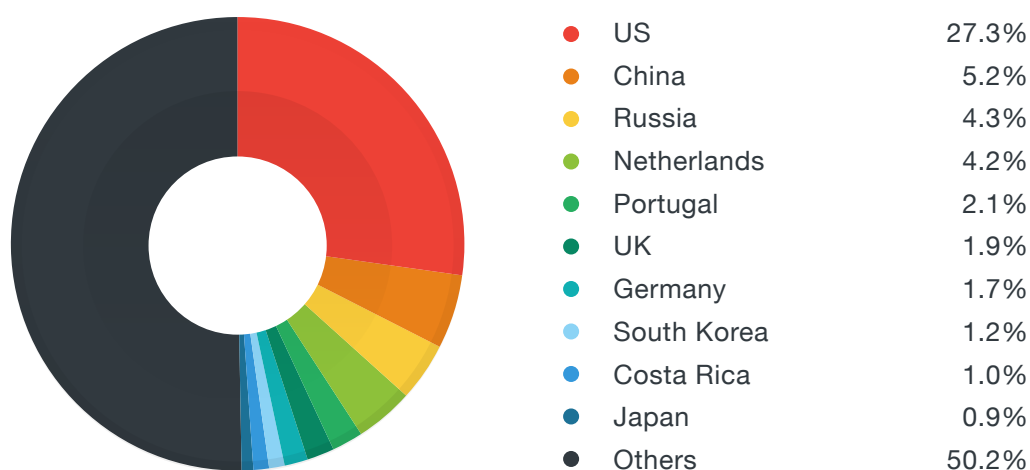
Number of user visits to malicious sites blocked
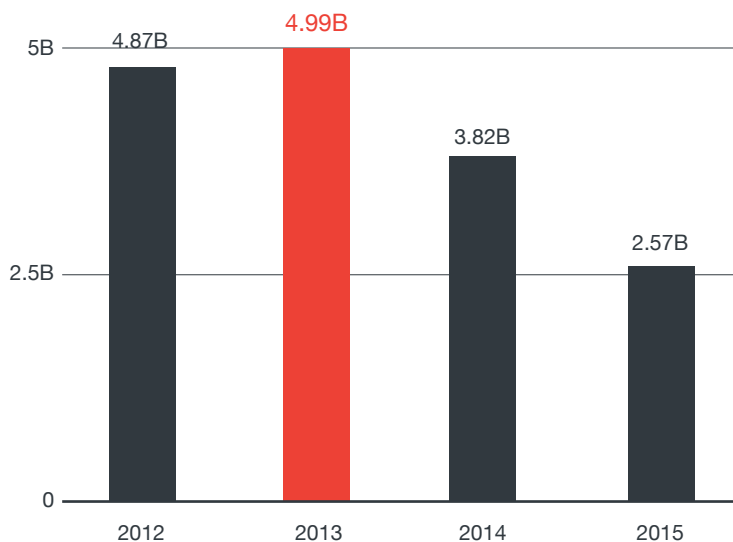
Top malicious domains users were prevented from visiting in 2015

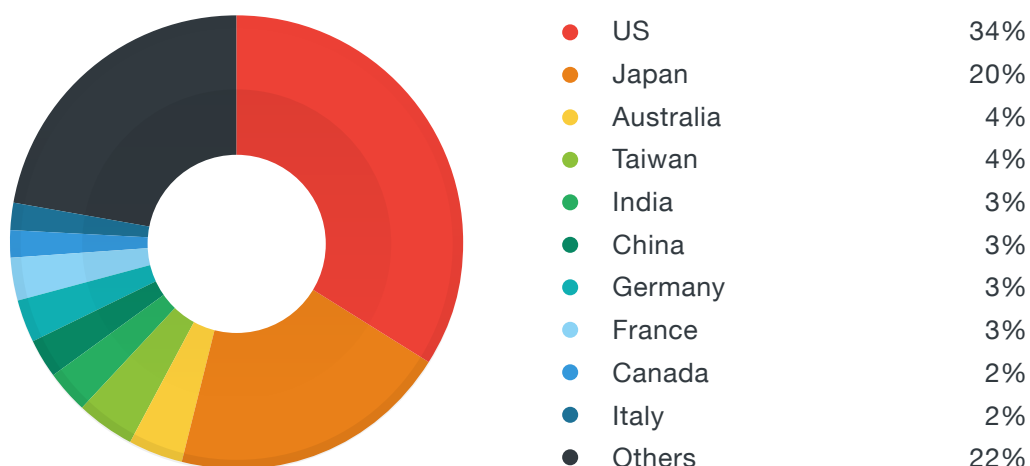| Malicious URL Blocked	Reason for blocking access to
www.adnetworkperformance.com	Known browser hijacker
jsgnr.eshopcomp.com	Hosts potentially malicious hijacking browsers
facebook.tbccint.com	Known to host malware
sso.anbtr.comc	Known to host malware
bugreport.yac.mx	Known to host unwanted applications
sp-storage.spccint.com	Known to host unwanted applications
checkver.dsiteproducts.com	Known to host unwanted applications
a020f0.com	Related to TROJ_POWELIKS
ffb6c1.com	Known to produce multiple website pop-ups
dda0dd.com	Known to produce continuous website pop-ups

The most accessed malicious URLs were composed of unwanted applications and sites hosting malware.

## Countries that hosted the highest number of malicious URLs in 2015

US	27.3%
China	5.2%
Russia	4.3%
Netherlands	4.2%
Portugal	2.1%
UK	1.9%
Germany	1.7%
South Korea	1.2%
Costa Rica	1.0%
Japan	0.9%
Others	50.2%

The US consistently dominated the list of malicious-URL-hosting countries in 2015.
China and Russia came in 2nd and 3rd.

Countries with the highest number of users who clicked malicious URLs in 2015

● US	34%
● Japan	20%
● Australia	4%
● Taiwan	4%
● India	3%
● China	3%
● Germany	3%
● France	3%
● Canada	2%
● Italy	2%
● Others	22%

There were no notable changes observed in the list of countries with the most number of users who clicked malicious URLs.

Number of malicious files blocked
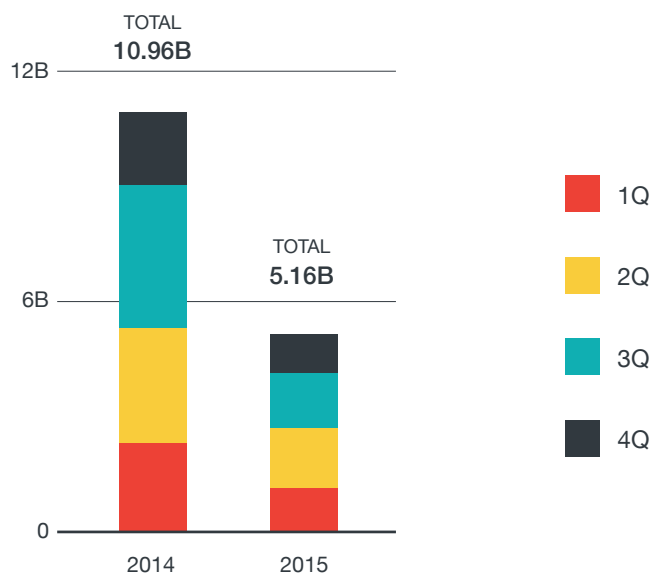
We prevented about 5.16 billion malicious files from infecting devices in 2015. While this number seems huge, it is half of what we blocked in 2014 (10.96B). As mentioned in previous quarters, this downward trend is reflective of the changes in the global threat landscape. These include file-less malware installations and threats that are not entirely malware-based such as exploit kits.

Top malware families of 2015

Family	Count
SALITY	325K
DOWNAD	298K
GAMARUE	207K

Top malware families of 2015 by segment

Segment	Family	Count
Enterprise	DOWNAD	231K
	SALITY	132K
	DUNIHI	111K
SMB	DOWNAD	37.2K
	DLOADR	36.1K
	DRIDEX	35.6K
Consumer	SALITY	123K
	GAMARUE	112K
	Virux	74K

DOWNAD, SALITY, and GAMARUE continue to be the top infectors in 2015.

Top 10 online banking malware families of 2015

1Q	
● RAMNIT	24%
● ZBOT	14%
● QAKBOT	13%
● DORKBOT	12%
● DYRE	7%
● QBOTCONF	5%
● EMOTET	4%
● BANKER	3%
● VAWTRAK	2%
● URSNIF	2%
● Others	14%

2Q	
● RAMNIT	35%
● DORKBOT	13%
● ZBOT	13%
● EMOTET	10%
● DYRE	7%
● QAKBOT	3%
● DRIDEX	2%
● BANKER	2%
● FAREIT	2%
● BANLOAD	2%
● Others	11%

3Q	
● RAMNIT	31%
● DRIDEX	18%
● ZBOT	16%
● DORKBOT	11%
● DYRE	4%
● QAKBOT	3%
● FAREIT	2%
● BANKER	2%
● BANLOAD	2%
● EMOTET	1%
● Others	10%

4Q	
● DRIDEX	56%
● RAMNIT	14%
● DORKBOT	6%
● ZBOT	6%
● FAREIT	4%
● QAKBOT	3%
● SHIZ	2%
● DYRE	2%
● BANLOAD	1%
● BANKER	1%
● Others	5%

While RAMNIT consistently held the top spot for three quarters, DRIDEX overtook RAMNIT in the last quarter. This is likely due to its increased botnet activity even after a DRIDEX-related botnet takedown in October 2015.

Macro malware detection distribution per application in 2015

● Microsoft Word	76%
● Microsoft Excel	22%
● Microsoft Power Point, Etc.	2%
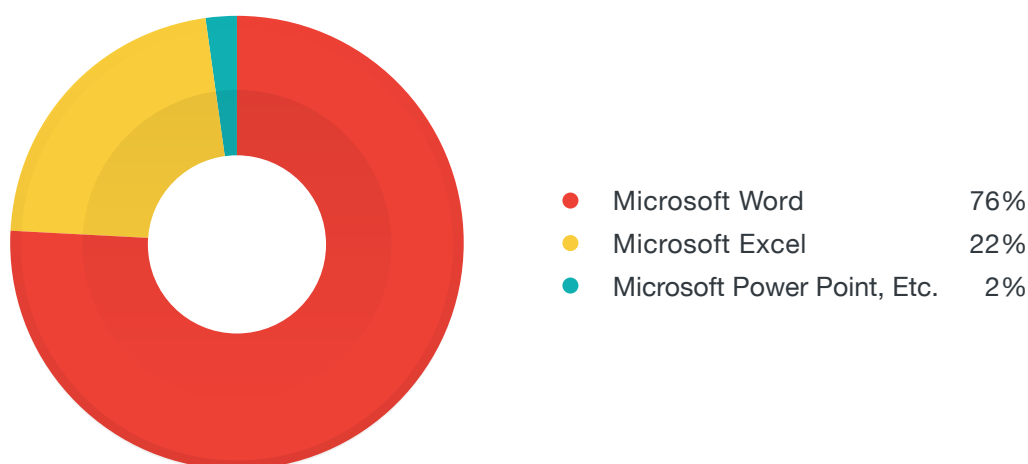
Microsoft Word® documents were the most used for macro malware in 2015.

Top adware families for 2015

Family	Count
OPENCANDY	1.9M
MYPCBACKUP	504K
DEALPLY	407K

Top adware families in 2015 by segment

Segment	Family	Count
Enterprise	OPENCANDY	223K
	DEALPLY	76K
	TOMOS	45K
SMB	OPENCANDY	81K
	DEALPLY	34K
	VPAYD	25K
Consumer	OPENCANDY	1.5M
	FakeGooG	386K
	MYPCBACKUP	264K

OPENCANDY was the top adware family affecting all sectors in 2015.

Cumulative Number of Android Malware in 2015
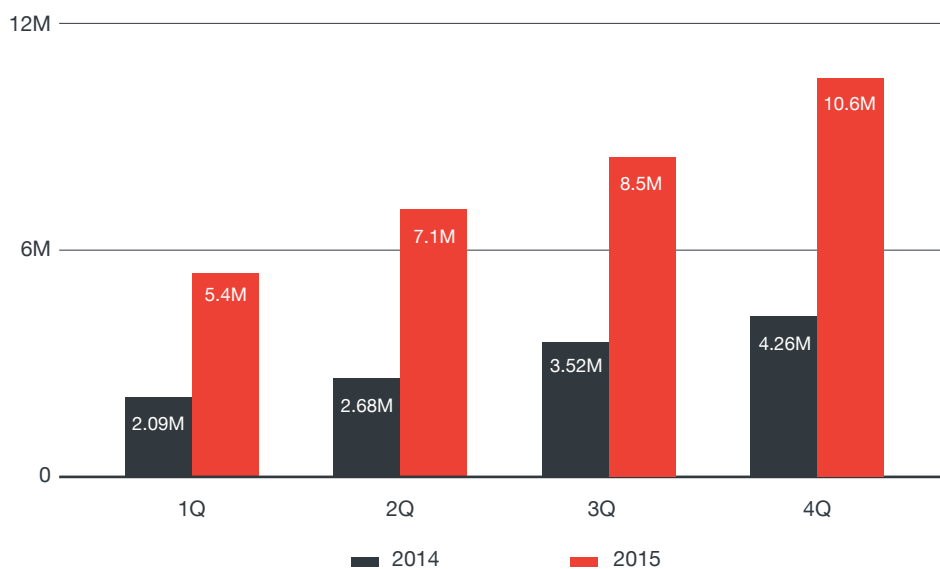
Compared to 2014 data, the number of Android malware doubled by the end of 2015.

Countries where the highest number of C&C servers were hosted in 2015

● US	28%
● Ukraine	10%
● Russia	8%
● Germany	5%
● China	5%
● Netherlands	4%
● France	3%
● South Korea	3%
● UK	3%
● Poland	2%
● Others	29%
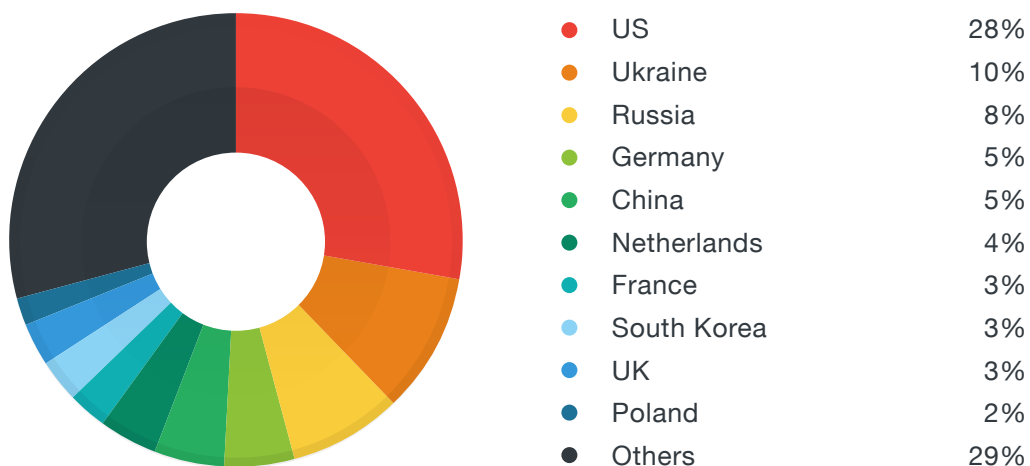
The top 3 C&C hosting countries were still the US, Ukraine, and Russia respectively in 2015.

Countries with the highest number of C&C server connections in 2015

●	US	34%
●	Japan	14%
●	India	7%
●	Australia	5%
●	Taiwan	4%
●	Germany	3%
●	France	2%
●	Turkey	2%
●	Canada	2%
●	Malaysia	2%
●	Others	25%
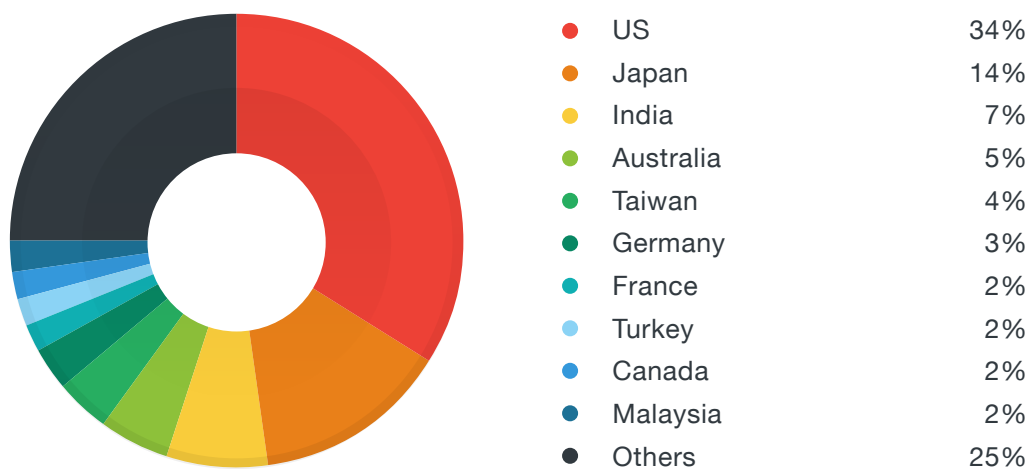
US had the most number of C&C connections in 2015.

References

1. Jonathan Leopando. (31 August 2015). *TrendLabs Security Intelligence Blog.* "Blackmail, Deletion Offers Hit Ashley Madison Users." Last accessed on 22 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/blackmail-deletion-offers-hit-ashley-madison-users/.

2. TrendLabs. (21 August 2015). *Trend Micro Security News.* "The Ashley Madison Breach Isn't Just About Infidelity."Last accessed on 14January 2016, http://www.trendmicro.com/vinfo/us/security/news/online-privacy/ashley-madison-breach-isnt-just-about-infidelity.

3. Christopher Budd. (20 July 2015). *TrendLabs Security Intelligence Blog.* "Impact Team to Ashley Madison – Shut down or Else!."Last accessed on 25January 2016, http://blog.trendmicro.com/impact-team-to-ashley-madison-shut-down-or-else/.

4. Trend Micro. (8 July 2015). *TrendLabs Security Intelligence Blog.* "Hacking Team Adobe Flash Zero-Day."Last accessed on 25January 2016, http://blog.trendmicro.com/hacking-team-adobe-flash-zero-day/.

5. Weimin Wu. (8 July 2015). *TrendLabs Security Intelligence Blog.* "Hacking Team Flash Zero-Day Tied To Attacks In Korea and Japan… on July 1."Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-tied-to-attacks-in-korea-and-japan-on-july-1/.

6. Christopher Budd. (17 March 2015). *TrendLabs Security Intelligence Blog.* "What You Need to Know About the Premera Data Breach."Last accessed on 27January 2016, http://blog.trendmicro.com/premera-databreach/.

7. Christopher Budd. (10 July 2015). *TrendLabs Security Intelligence Blog.* "The Latest on the OPM Hack: 21 Million Affected."Last accessed on 27January 2016, http://blog.trendmicro.com/the-latest-on-the-opm-hack-21-million-affected/.

8. U.S. Office of Personnel Management. *OPM.* "What Happened."Last accessed on 9 February2016, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

9. TrendLabs. (22 September 2015). *Trend Micro Security News.* "Follow the Data: Dissecting Data Breaches and Debunking the Myths." Last accessed on 26 January 2016, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data.

10. TrendLabs. (16 January 2016). *Trend Micro Security News.* "Operation P n Storm: Fast Facts and the Latest Developments."Last accessed on 27January 2016, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts.

11. Jack Tang. (17 July 2015). *TrendLabs Security Intelligence Blog.* "Analyzing the Pawn Storm Java Zero-Day – Old Techniques Reused."Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-the-pawn-storm-java-zero-day-old-techniques-reused/.

12. Trend Micro. (13 October 2015). *TrendLabs Security Intelligence Blog.* "New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries."Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/.

13. Peter Pi. (14 July 2015). *TrendLabs Security Intelligence Blog.* "'Gifts'From Hacking Team Continue, IE Zero-Day Added to Mix."Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/gifts-from-hacking-team-continue-ie-zero-day-added-to-mix/.

14. Peter Pi. (11 July 2015). *TrendLabs Security Intelligence Blog.* "Another Zero-Day Vulnerability Arises from Hacking Team Data Leak."Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/another-zero-day-vulnerability-arises-from-hacking-team-data-leak/.

15. Peter Pi. (11 July 2015). *Trendlabs Security Intelligence Blog.* "New Zero-Day Vulnerability (CVE-2015-5123) in Adobe Flash Emerges from Hacking Team Leak."Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/new-zero-day-vulnerability-cve-2015-5123-in-adobe-flash-emerges-from-hacking-team-leak/.

16. Brooks Li. (7 July 2015). *TrendLabs Security Intelligence Blog.* "Hacking Team Flash Zero-Day Integrated Into Exploit Kits."Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/.

17. Wish Wu. (17 August 2015). *TrendLabs Security Intelligence Blog.* "MediaServer Takes Another Hit with Latest Android Vulnerability."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/mediaserver-takes-another-hit-with-latest-android-vulnerability/.

18. Wish Wu. (4 August 2015). *TrendLabs Security Intelligence Blog.* "Android MediaServer Bug Traps Phones in Endless Reboots."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/android-mediaserver-bug-traps-phones-in-endless-reboots/.

19. Wish Wu. (29 July 2015). *Trendlabs Security Intelligence Blog.* "Trend Micro Discovers Vulnerability That Renders Android Devices Silent."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-vulnerability-that-renders-android-devices-silent/.

20. Simon Huang. (7 January 2015). *TrendLabs Security Intelligence Blog.* "Malformed AndroidManifest.xml in Apps Can Crash Mobile Devices."Last accessed on 22 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/malformed-androidmanifest-xml-in-apps-can-crash-mobile-devices/.

21. Wish Wu. (26 June 2015). *TrendLabs Security Intelligence Blog.* "Trend Micro Discovers Android Vulnerability that Can Lead to Exposure of Device Memory Content."Last accessed on 22 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-android-vulnerability-that-can-lead-to-exposure-of-device-memory-content/.

22. Gideon Hernandez. (6 April 2015). *TrendLabs Security Intelligence Blog.* "Android Installer Hijacking Bug Used as Lure for Malware."Last accessed on 22 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/android-installer-hijacking-bug-used-as-lure-for-malware/.

23. Trend Micro. (19 June 2015). *TrendLabs Security Intelligence Blog.* "The Samsung SwiftKey Vulnerability – What You Need To Know, And How To Protect Yourself."Last accessed on 22 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/the-samsung-swiftkey-vulnerability-what-you-need-to-know-and-how-to-protect-yourself/.

24. Trend Micro Incorporated. (19 June 2015). *TrendLabs Security Intelligence Blog.* "Samsung Swiftkey Vulnerability (CVE-2015-4641)."Last accessed on 22 January 2016, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/8652/samsung-swiftkey-vulnerability-cve20154641.

25. Seven Shen. (27 May 2015). *TrendLabs Security Intelligence Blog.* "Trend Micro Discovers Apache Cordova Vulnerability that Allows One-Click Modification of Android Apps."Last accessed on 22 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-apache-vulnerability-that-allows-one-click-modification-of-android-apps/.

26. Ju Zhu. (21 September 2015). *TrendLabs Security Intelligence Blog.* "The XcodeGhost Plague – How Did It Happen?."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/the-xcodeghost-plague-how-did-it-happen/.

27. Robert McArdle. (3 October 2013). *TrendLabs Security Intelligence Blog.* "Deep Web and Cybercrime – It Is Not Just the Silk Road."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/deepweb-and-cybercrime-it-is-not-just-the-silk-road/.

28. Lion Gu. (23 October 2015). *TrendLabs Security Intelligence Blog.* "Prototype Nation: Emerging Innovations in Cybercriminal China."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/prototype-nation-emerging-innovations-in-cybercriminal-china/.

29. Maxim Goncharov. (28 July 2015). *TrendLabs Security Intelligence Blog.* "The Russian Underground—Revamped."Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/the-russian-underground-revamped/.

30. Forward-Looking Threat Research Team.(10 January 2016). *TrendLabs Security Intelligence Blog.* "Think, Learn, Act – Training for Aspiring Cyber Criminals in the Brazilian Underground." Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/think-learn-act-training-for-aspiring-cyber-criminals-in-the-brazilian-underground/.

31. Akira Urano.(13 October 2015). *TrendLabs Security Intelligence Blog.* "Japanese Cybercriminals New Addition To Underground Arena." Last accessed on 27 January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/japanese-cybercriminals-new-addition-to-underground-arena/.

32. Trend Micro.(8 December 2015). *TrendLabs Security Intelligence Blog.* "The German Underground: Buying and Selling Goods via Droppers." Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/the-german-underground-buying-and-selling-goods-via-droppers/.

33. Stephen Hilt and Kyle Wilhoit.(7 December 2015). *TrendLabs Security Intelligence Blog.* "Out in the Open: Accessibility in the North American Underground." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/out-in-the-open-accessibility-in-the-north-american-underground/.

34. Kashmir Hill.(2 September 2015). *Fusion.* "Watch out, new parents—internet-connected baby monitors are easy to hack." Last accessed on 27January 2016, http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/.

35. Swati Khandelwal.(18 January 2014). *The Hacker News.* "100,000 Refrigerators and other home appliances hacked to perform cyber attack." Last accessed on 22January 2016, http://thehackernews.com/2014/01/100000-refrigerators-and-other-home.html.

36. Rainer Link.(28 July 2015). *TrendLabs Security Intelligence Blog.* "Is Your Car Broadcasting Too Much Information?." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/.

37. Andy Greenberg.(24 July 2013). *Forbes.* "Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)." Last accessed on 19January 2016, http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#4160e2455bf2.

38. Andy Greenberg.(21 July 2015). *Forbes.* "Hackers Remotely Kill a Jeep on the Highway—With Me in It." Last accessed on 26January 2016, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

39. Trend Micro.(5 August 2015). *TrendLabs Security Intelligence Blog.* "The GasPot Experiment: Hackers Target Gas Tanks." Last accessed on 26January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/the-gaspot-experiment-hackers-target-gas-tanks/.

40. TrendLabs.(27 October 2015). *Trend Micro Security News.* "2016 Trend Micro Security Predictions: The Fine Line." Last accessed on 26January 2016, http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2016.

41. Peter Pi.(2 February 2015). *TrendLabs Security Intelligence Blog.* "Trend Micro Discovers New Adobe Flash Zero-Day Exploit Used in Malvertisements." Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/.

42. Joseph C. Chen.(8 December 2015). *TrendLabs Security Intelligence Blog.* "Blog of News Site 'The Independent'Hacked, Leads to TeslaCrypt Ransomware." Last accessed on 25January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/blog-of-news-site-the-independent-hacked-leads-to-teslacrypto-ransomware/.

43. Joseph C. Chen.(30 September 2015). *TrendLabs Security Intelligence Blog.* "3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/3000-high-profile-japanese-sites-hit-by-massive-malvertising-campaign/.

44. Joseph C. Chen.(7 July 2015). *TrendLabs Security Intelligence Blog.* "Hacking Team Flash Zero-Day Integrated Into Exploit Kits." Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/.

45. Brooks Li and Joseph C. Chen.(3 November 2015). *TrendLabs Security Intelligence Blog.* "Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/angler-and-nuclear-exploit-kits-integrate-pawn-storm-flash-exploit/.

46. David Dunkel.(6 August 2015). *TrendLabs Security Intelligence Blog.* "Crypto-Ransomware Attacks: The New Form of Kidnapping." Last accessed on 22January 2016, http://blog.trendmicro.com/crypto-ransomware-attacks-the-new-form-of-kidnapping/.

47. Anthony Joe Melgarejo.(19 March 2015). *TrendLabs Security Intelligence Blog.* "CryptoWall 3.0 Ransomware Partners With FAREIT Spyware." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/.

48. Paul Pajares and Jon Oliver.(22 September 2015). *TrendLabs Security Intelligence Blog.* "Businesses Held for Ransom: TorrentLocker and CryptoWall Change Tactics." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics/.

49. Anthony Joe Melgarejo.(3 December 2015). *TrendLabs Security Intelligence Blog.* "Chimera Crypto-Ransomware Wants You (As the New Recruit)." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/chimera-crypto-ransomware-wants-you-as-the-new-recruit/.

50. Stephen Hilt and Kyle Wilhoit.(7 December 2015). *TrendLabs Security Intelligence Blog.* "North American Underground: The Glass Tank." Last accessed on 9 February2016, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf.

51. Forward-Looking Threat Research Team.(23 June 2015). *TrendLabs Security Intelligence Blog.* "Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015." Last accessed on 9 February2016, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-ascending-the-ranks.pdf.

52. Federal Bureau of Investigation.(10 January 2016). *Internet Crime Complaint Center.* "Criminals Continue to Defraud And Extort Funds from Victims Using Cryptowall Ransomware Schemes." Last accessed on 9 February2016, http://www.ic3.gov/media/2015/150623.aspx.

53. Trend Micro.(13 October 2015). *TrendLabs Security Intelligence Blog.* "FBI, Security Vendors Partner for DRIDEX Takedown." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/us-law-enforcement-takedown-dridex-botnet/.

54. Ryan Angelo Certeza.(13 October 2015). *TrendLabs Security Intelligence Blog.* "Dealing with the Mess of DRIDEX." Last accessed on 27January 2016, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3147/dealing-with-the-mess-of-dridex.

55. Rhena Inocencio.(5 November 2014). *TrendLabs Security Intelligence Blog.* "Banking Trojan DRIDEX Uses Macros for Infection." Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/banking-trojan-dridex-uses-macros-for-infection/.

56. Trend Micro.(6 November 2015). *TrendLabs Security Intelligence Blog.* "DRIDEX: Down, But Not Out." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/dridex-down-but-not-out/.

57. Ryan Flores.(25 November 2015). *TrendLabs Security Intelligence Blog.* "DRIDEX Spam Runs Resurface Against US Targets." Last accessed on 22January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/dridex-spam-runs-resurface-against-us-targets/.

58. Maxim Goncharov.(15 July 2015). *TrendLabs Security Intelligence Blog.* "Hideouts for Lease: The Silent Role of Bulletproof Hosting Services in Cybercriminal Operations." Last accessed on 27January 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/hideouts-for-lease-the-silent-role-of-bulletproof-hosting-services-in-cybercriminal-operations/.

Created by:

TrendLabs

The Global Technical Support & R&D Center of **TREND MICRO**

TREND MICRO™

Securing Your Journey
to the Cloud