



# Hazards Ahead

Current Vulnerabilities Prelude  
Impending Attacks

#### TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

# Contents

4

Data breach dumps fueled attacks and extortion

8

New attacks reiterated existing iOS and Android issues

11


Shotgun approach to PoS malware attacks affected more and more SMBs

14

This quarter's highlights

20

Threat landscape in review



We've reached a point where just about anything can be vulnerable to threats. The security incidents we saw this past quarter revealed just how big the existing cracks are in the mobile ecosystem, Internet-connected devices, and network infrastructures, among others. Similar to seismic readings signaling forthcoming earthquakes, these security gaps could be a prelude to massive events that we believe will greatly impact 2016.

We saw how severe data breaches have become more personal and lucrative. Attackers dumped incriminating confidential information in publicly accessible locations, damaging the reputation and destroying the credibility of both businesses and individuals. The data breaches we witnessed and their "aftershocks" or the chain of attacks that followed them were of a significant magnitude. The Hacking Team breach, for one, led to an outbreak of numerous security vulnerabilities. Extortion and blackmail ran rampant, as cybercriminals leveraged the Ashley Madison breach for their own nefarious gains. We're likely to see more breaches follow these attacks' footsteps. Attackers are bound to release more and more confidential and potentially destructive information to the public or sell what they know to the highest bidders in the Deep Web.

The "shotgun approach" will continue to be an effective means for attackers to gain new victims. Attacks targeting small and medium-sized businesses (SMBs) will continue to ensue because they have proven to be lucrative targets. Going after high-profile individuals, including politicians, will serve as a launchpad for the targeted attacks of the future.

Security loopholes present in mobile platforms and Internet-connected devices will continue to be exploited, posing risks not only to user privacy but also physical safety. Device manufacturers will need to collaborate with security experts if they wish to secure their creations and their users.

*NOTE: All mentions of "detections" within the text refer to instances when threats were found on users' devices and subsequently blocked by any Trend Micro security solution. Unless otherwise stated, the figures featured in this report came from data gathered by the Trend Micro™ Smart Protection Network™ cloud security infrastructure, which uses a combination of in-the-cloud technologies and client-based techniques to support on-premise products and hosted services.*

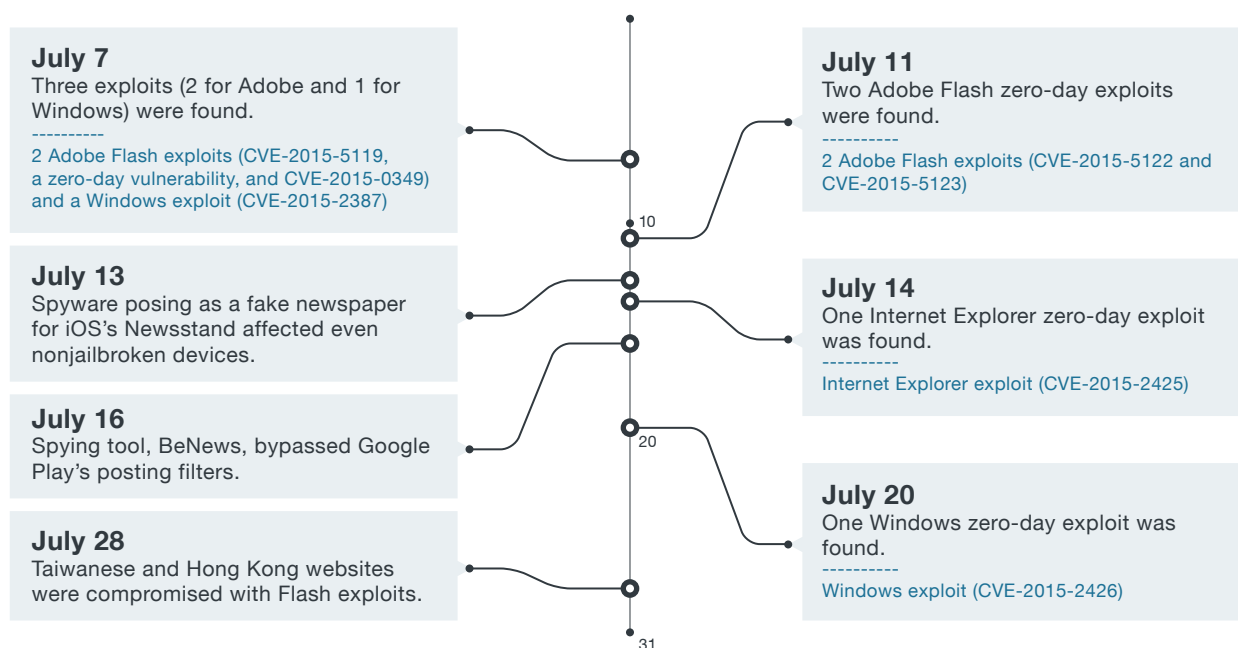
# Data breach dumps fueled attacks and extortion

The data breaches seen this quarter spurred a chain of attacks. The attacks of the future are likely to emulate the Ashley Madison and Hacking Team leaks—the inclusion of data breach tactics in cybercriminals’ usual arsenals. Dumping stolen confidential information in public domains can tarnish victims’ reputations and cause far greater damage than business disruptions that result from web defacement and distributed denial-of-service (DDoS) attacks.

## Hacking Team breach: A gold mine of vulnerabilities

Last July, Italian company, Hacking Team, said more than 400GB<sup>1</sup> of the confidential data it kept was leaked to the public. Proprietary company information was included in the data the attackers stole. The Hacking Team breach was particularly unique in that the information leaked could aid other attackers to exploit newly exposed security vulnerabilities in the company’s infrastructure.

### Hacking Team attack timeline



*Various zero-day and vulnerability exploits, along with a mobile spying tool, related to the Hacking Team breach surfaced throughout July. If successfully exploited, these could have disastrous repercussions. Several websites in Taiwan and Hong Kong were also compromised to deliver Adobe® Flash® exploits.*

Five vulnerabilities (three of which we identified) in Adobe Flash, Internet Explorer®, and Microsoft™ Windows® emerged as a result of the Hacking Team breach. As of this July, these have affected at least a billion connected devices<sup>2</sup> running affected Adobe Flash versions. The Windows exploits put around 78% of the overall desktop user base<sup>3</sup> (those running affected versions of the operating system [OS]) at risk. Some 27% of the desktop browser user base<sup>4</sup>, meanwhile, were affected by the related Internet Explorer 11 exploit. The Flash zero-day exploit targeting CVE-2015-5119<sup>5</sup> was integrated into the Angler and Nuclear Exploit Kits<sup>6</sup> and subsequently used to launch attacks against organizations in Korea and Japan<sup>7, 8</sup>. Government and media websites in Hong Kong and Taiwan<sup>9</sup> were also compromised with the help of the Flash vulnerabilities exposed as a by-product of the Hacking Team breach.

Part of the data dumped in relation to the Hacking Team leak was the source code of their spy app, Remote Control System Android (RCSAndroid), dubbed the “most professionally developed and sophisticated Android malware”<sup>10</sup> to date. RCSAndroid’s data-stealing routines include capturing screenshots and voice calls in real time, along with collecting passwords for and messages from apps like Facebook, Viber, and Skype.

The Hacking Team leak also left iPhones®, jailbroken or not, to a piece of spyware disguised as a newspaper that unknowing users could add to Newsstand<sup>11</sup>. It asks users to grant it permission to access all kinds of data stored on their devices. A similar app for Android™ devices called “BeNews”<sup>12</sup> followed soon after. BeNews could not just compromise affected devices’ security but also circumvent Google Play™’s standard security check.

## Ashley Madison breach: A story of sex, lies, and extortion

The Ashley Madison breach made waves primarily because of the website’s scandalous nature<sup>13</sup>. And hacktivist group, Impact Team, surely took advantage of the site members’ (cheaters’) vulnerability. The breach spelled catastrophe for both Avid Life Media (the site owner) and over 30 million of Ashley Madison’s users<sup>14</sup> whose reputations were dragged through the mud. Reports of victims committing suicide<sup>15</sup> even circulated.

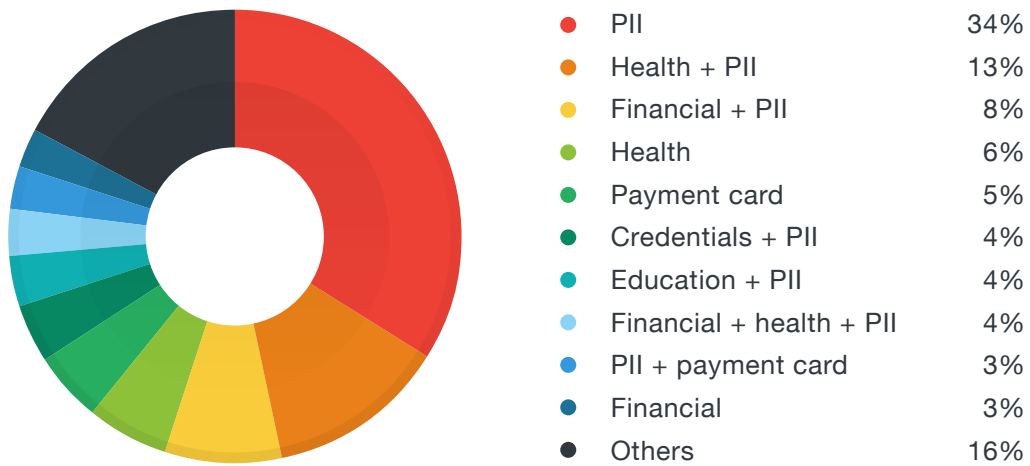
Attackers quickly leveraged the leak to launch extortion attacks<sup>16</sup>, blackmailing users to pay 1BTC (~US\$291)\* or their families and friends would know their dirty secret. Additionally, we found fake profiles tied to Trend Micro honeypot email accounts and Internet Protocol (IP) addresses that were among identified Ashley Madison users<sup>17</sup>.

Anyone is a potential data breach victim. Any information users put up online is at risk of getting stolen and misused. As the Ashley Madison leak showed, data breaches can be personal and lucrative at the same time.

\* Currency exchange rate as of 27 October 2015 was used (1 BTC = US\$291.31)

## Healthcare providers: Successful breach targets

Several healthcare providers were breached this September. Health insurer, Excellus BlueCross BlueShield (BCBS), was reportedly a target of a series of attacks spanning nearly two years<sup>18</sup>. The personal records of around 4.5 million patients were also compromised when attackers hit the UCLA Health System<sup>19</sup>. These two instances showed why the patient databases healthcare industry players keep made them viable breach targets<sup>20</sup>. The Trend Micro report, “Follow the Data: Analyzing Breaches by Industry,”<sup>21</sup> also revealed that combined health-and-personally-identifiable-information (PII) was the second-most stolen data type in breaches. This trend will likely continue in the future.



*Healthcare data (medical records, insurance data, etc.), along with PII, are stolen most in breaches.*

The Hacking Team and other breaches in the healthcare industry highlighted the critical role that vulnerability patch management plays. Organizations should always strive to protect their network and the data they keep from all kinds of exploits.

“Cyberspace has become more punitive. Attacks are not isolated cases. Enterprises must adjust their incident response plans to address the advent of secondary attack stages, which could either be secondary infections or using stolen data for extortion. Intrusion suppression will become the goal of incident response. It is imperative for enterprises to limit the ‘dwell time’ of adversaries. We must disrupt our adversaries’ capacity to gain a foothold on our hosts, thus inhibiting from instigating secondary infections. Virtual patching and integrating breach detection with security information and event management (SIEM) and file integrity monitoring systems will be key in mitigating the punitive attacks of 2016.”

**— Tom Kellermann**

*Chief Cybersecurity Officer*

# New attacks reiterated existing iOS and Android issues

The discovery of Mediaserver vulnerabilities in Android highlighted the need for a more integrated set of security strategies across Google, manufacturers, and carriers. Modified versions of app-creation tools like Xcode and Unity also dispelled the notion that Apple's walled garden approach to security can spare iOS from attacks. Attackers continued to take advantage of gaps in security to trail their sights on mobile device users, regardless of platform, thus furthering the already-exponential growth of mobile malware.

## Android's latest bane: Mediaserver vulnerabilities

Android's Mediaserver component, which handles media-related tasks, recently became and is likely to remain an active attack target. This past quarter alone, we've seen attackers exploit at least five vulnerabilities in the service.

Stagefright<sup>22</sup> (CVE-2015-3824), which allows attackers to install malware on affected devices by distributing malicious Multimedia Messaging Service (MMS) messages, reportedly put 94.1% of Android devices (as of this July) at risk. We also found a bug that could render Android phones silent and unable to make calls or send text messages<sup>23</sup>. Reports said more than 50% of Android devices (as of this July)<sup>24</sup> were vulnerable to this flaw. Another critical Mediaserver vulnerability (CVE-2015-3823)<sup>25</sup>, which could cause devices to endlessly reboot and allow attackers to remotely run arbitrary code, was also found. At that time, 89% of Android devices were susceptible to exploitation. CVE-2015-3842, which could allow remote code execution in Mediaserver's AudioEffect component, also figured in the landscape this August<sup>26</sup>.

In response to the recent spate of Android vulnerability discoveries, Google finally announced regular security updates<sup>27</sup> for the platform. We have yet to see how the platform's current state of fragmentation will affect this plan. Security patches may not be able to make their way to all devices without the support of manufacturers and carriers, rendering them vulnerable to exploitation.



## Tampered tools and bugs: Threats to iOS's walled garden

Apple is known for its walled garden approach, which then meant stricter app-posting policies and thus more secure apps. This belief was shattered though when several iOS apps on both the App Store and third-party stores were tainted with a malicious piece of code known as "XcodeGhost."<sup>28</sup> The malicious apps could be used to instigate fraud, phishing, and even data theft.

As it turned out, several Chinese iOS app developers downloaded a copy of Xcode from forums and used it to build apps. They didn't know that the code they used was malicious and so tainted their own creations. Smart Protection Network data revealed that China was most affected by the threat. Unity, a platform for two- (2D) and three-dimensional (3D) game creation, suffered the same unfortunate fate due to UnityGhost.

iOS's AirDrop<sup>®</sup> feature<sup>29</sup> also figured in the exploit landscape. The related bug affects even devices that aren't configured to accept files sent via AirDrop. Another iOS vulnerability, Quicksand<sup>30</sup>, was also found capable of leaking data sent to and from mobile-device-management (MDM)-enabled clients, putting not only personal but also corporate data in harm's way.

Apple was quick to address the issues that surfaced. It removed infected apps from its App Store. Given its growing mobile user base, we're likely to see more iOS threats in the future. Attackers will continue to find more ways to bypass Apple's strict policies and walled garden. Cross-platform threats like WireLurker<sup>31</sup> and Masque<sup>32</sup>, which put not just individuals but also businesses at risk, can also be expected.

“Apple’s increasing phone market share is tempting attackers to exert more effort to exploit iOS apps. Apple’s strict security policies on posting iOS apps are, however, pushing them to come up with cleverer tricks like infection via development tools and libraries to get the job done. We’re bound to see more ‘Ghost-like’ threats in the future. Attackers may also opt to abuse certificates and application programming interfaces (APIs) to distribute iOS malware. In response, Apple needs to constantly tighten its app-posting policies.”

**—Ju Zhu**

*Mobile Threat Researcher*

# Shotgun approach to PoS malware attacks affected more and more SMBs

SMBs proved lucrative and easy point-of-sale (PoS) malware attack targets<sup>33</sup> this quarter. This could be due to the extensive customer databases they keep with minimal to nonexistent security. We'll likely see more of such attacks in the future. The slow adoption of next-generation payment technologies like the Europay, MasterCard, and Visa (EMV)<sup>34</sup> and contactless Radio-Frequency-Identification (RFID)-enabled credit cards<sup>35</sup>, mobile wallets (Apple Pay<sup>®36</sup> and Android Pay<sup>™37</sup>), and new payment-processing architectures<sup>38</sup> could also adversely affect the security landscape.

## Shotgun approach: An effective PoS malware attack launcher

This quarter, attackers went after as many vulnerable PoS devices as possible in hopes of hitting the jackpot. They relied on tried-and-tested tactics like spamming as well as tools like macro malware, exploit kits, and botnets. They must have done something right because the PoS malware detection volume grew 66%. SMBs, which had poorer protections in place compared with large enterprises, suffered most.

A PoS random access memory (RAM) scraper made its way into devices aided by the Angler Exploit Kit<sup>39</sup>, which is known for using malvertisements and compromised sites as infection vector. A reconnaissance Trojan that sported fileless installation capabilities to evade detection was used to find and infect PoS devices. Fileless malware hide in locations that are not normally scanned for infection.

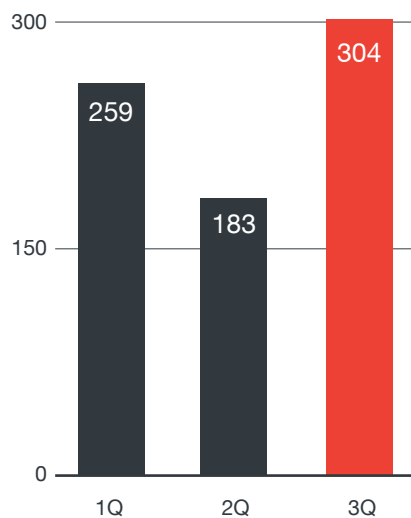
This July, a new GamaPOS variant<sup>40</sup> spread mayhem with the help of the Andromeda botnet and the “dynamite or blast fishing” approach. Blast fishing is the practice of using explosives to stun or kill schools of fish for easy collection. Attackers spammed practically every address they could get their hands on in hopes that the malware would make their way to PoS systems. Their emails came with macro malware attachments or links pointing to compromised websites. Our data revealed that the threat affected users in 13 United States (US) states and a city in Canada.

Kasidet<sup>41</sup> or Neutrino malware began sporting PoS-RAM-scraping capabilities this quarter. Kasidet, a commercially available builder, is known for its use in DDoS attacks. Kasidet most recently made its way into PoS systems via malware-laced spam. As a result, its latest iteration accounted for 12% of this quarter's total PoS malware detection volume.

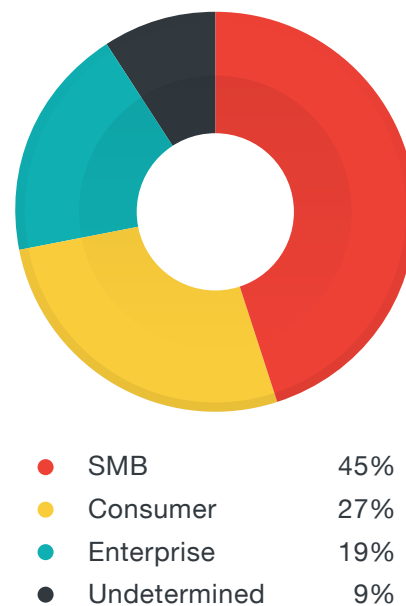
## SMBs: Favored PoS malware attack targets

Last quarter, we thought PoS RAM scrapers reached their saturation point due to the huge decline in detection volume<sup>42</sup>. This quarter proved otherwise, as the detection volume again rose, with SMBs as primary targets.

Number of PoS malware detections (1Q-3Q 2015)



PoS malware detection distribution by segment (3Q 2015)



*The PoS malware detection volume rose nearly 66%, most likely due to attackers' use of the shotgun approach, which allowed them to find what proved to be easier and more lucrative prey—SMBs.*

Attackers' choice to use age-old tactics this quarter could have been a last-ditch effort to gain more victims before US merchants were forced to adopt EMV credit cards, said to be more secure, at the start of October this year.

“PoS malware targeting SMBs are not new. We’ve been talking about them for a while now. What’s new is that cybercriminals have shifted from using targeted-attack-style to traditional mass-infection tools like spam, botnets, and exploit kits. What remain unchanged are the risks the malware pose to ordinary individuals making credit card payments. Casting a wider net is a risky strategy because malware can be more quickly detected and neutralized; but it’s also almost certain to uncover new victims. These new victims and their data, if successfully extracted, could allow cybercriminals to launch more targeted campaigns against them and even their contacts.”

**— Numaan Huq**

*Senior Threat Researcher*

# This quarter's highlights











## Political figures: Favored cyber-espionage targets

Pawn Storm<sup>43</sup>, an ongoing cyber-espionage operation known for targeting the US and its ally states, along with Russian dissidents<sup>44</sup>, targeted the MH17 investigation team<sup>45</sup>. Monitoring revealed that its targets included organizations in the government, media, military, and defense sectors. Earlier this July, the attackers ramped up their activities aided by the newest Java zero-day exploit (CVE-2015-2590)<sup>46, 47</sup> since 2013.

In an attack against the armed forces of a North Atlantic Treaty Organization (NATO) member country and a US defense organization, the spear-phishing domain, ausameetings.com (fake version of ausameetings.org, the Association of the US Army [AUSA]'s annual expo website) was used. Soon after we published our report of the incident, the Pawn Storm actors (most likely in retaliation), changed an exploit-hosting domain to redirect to a Trend Micro IP address<sup>48</sup>.

Apart from previously mentioned targets, the Pawn Storm actors also trailed their sights on the members of the rock band, Pussy Riot, along with media outfits that criticized the Russian regime. The CEO of a Russian encryption software manufacturer and a former Russian prime minister were not spared as well.

### Pawn Storm campaign targets

2011	April 2015	August 2015
 US military	 NATO country members	 Russian politicians
 US and its allies' embassies	 The White House	 Russian band, Pussy Riot
 US defense contractor personnel	 The German Parliament	 Russian media practitioners
		 Russian software manufacturer's CEO

*Politicians in the US and Russia constantly figured as Pawn Storm targets since 2011.*

### Pawn Storm's August 2015 US target distribution



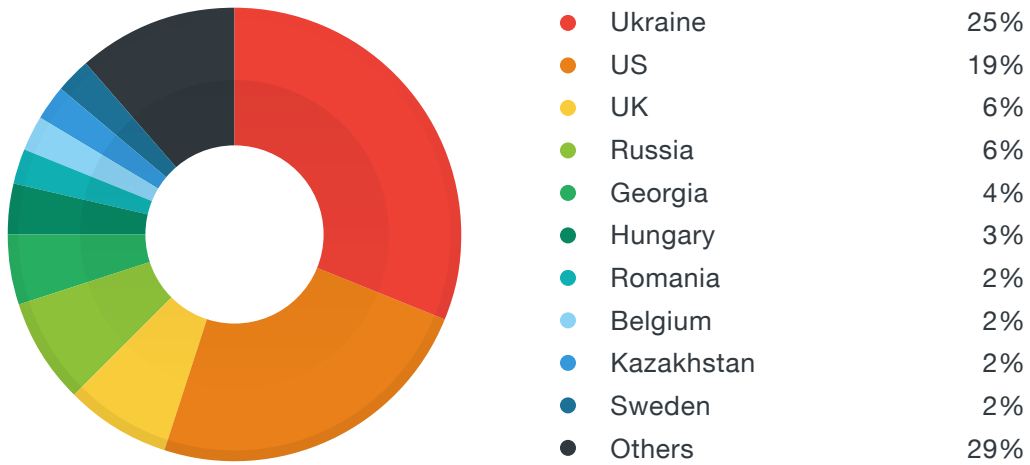
*Pawn Storm's top industry targets in the US were the military, defense, and government sectors.*

### Pawn Storm's August 2015 Ukrainian target distribution



*In the Ukraine, the Pawn Storm actors primarily set their sights on the military, media, and government sectors.*

### Pawn Storm's August 2015 top country target distribution



The Ukraine, the US, and the United Kingdom (UK) were Pawn Storm's top country targets this August.

Like Pawn Storm, Rocket Kitten<sup>49</sup> resurfaced this quarter. This time, its targets included a linguistics and pre-Islamic culture expert who assisted in ClearSky's Tamar Reservoir research. The researchers behind the report were not spared as well.

### Rocket Kitten's March and September 2015 targets

March	August 2015
Israeli civilian organizations	Middle Eastern policy researchers
Israeli academic institutions	Middle Eastern diplomatic facility personnel
German-speaking government agencies	Middle Eastern international affairs personnel
European government agencies	Middle Eastern defense and security personnel
Private European companies	Middle Eastern journalists

Most of Rocket Kitten's victims were diplomatic facility and international affairs personnel as well as policy researchers from the Middle East.

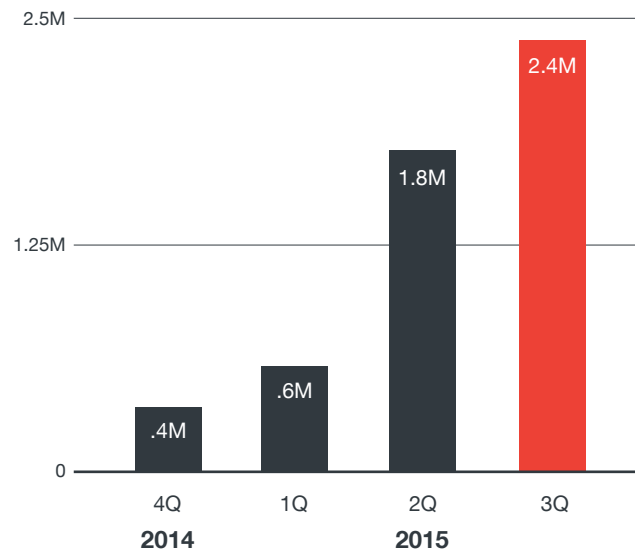
Given the recent state of affairs, we're bound to see further attacks against politicians that would serve as jump-off points for future campaigns.



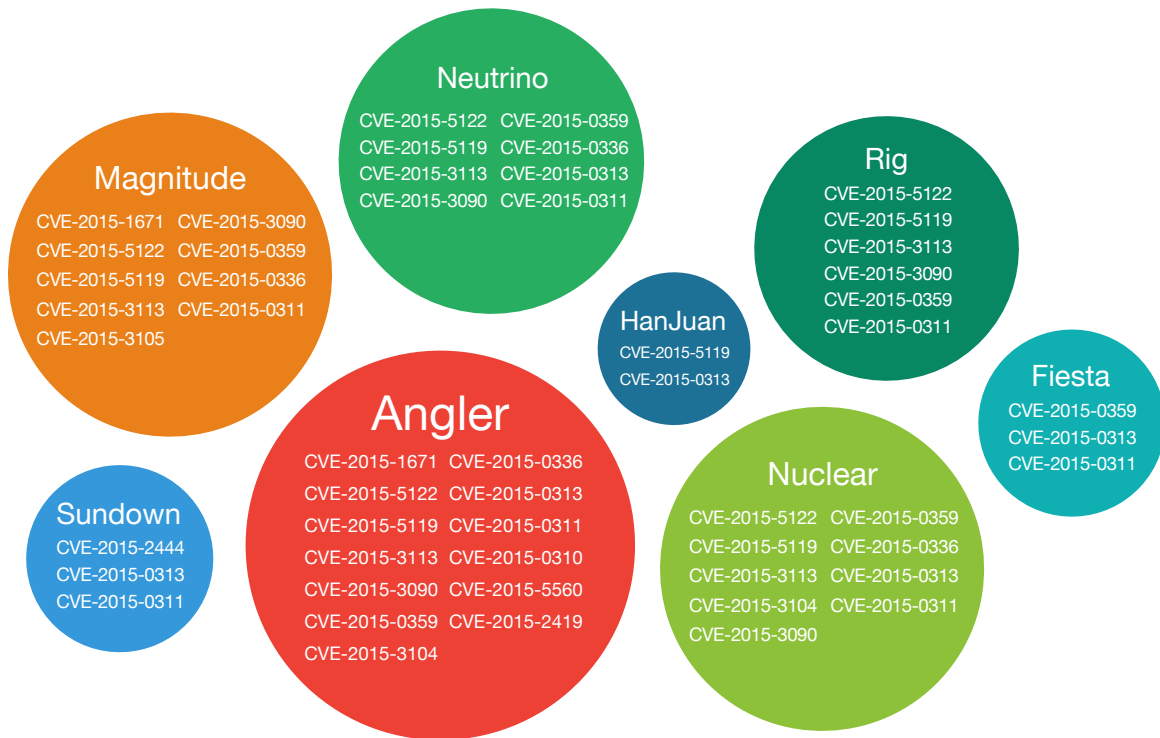
## Angler: Still the most widely used exploit kit

Angler Exploit Kit's creators didn't give in to complacency; they updated their arsenal this quarter. As such, it continued to be the most active exploit kit, posting a 34% quarter-on-quarter (QoQ) growth. We saw attackers use their creation to distribute malware. They didn't just go after PoS systems but also more traditional means—computers—to spread mayhem in search of as many victims as possible. The Adobe Flash zero-day exploit that resulted from the Hacking Team leak also made its way into Angler and contemporaries, Neutrino and Magnitude. Angler's creators, as we previously noted<sup>50</sup>, were indeed aggressively integrating as many Adobe Flash exploits as possible into their kit.

Number of Angler-Exploit-Kit-hosting URLs by quarter

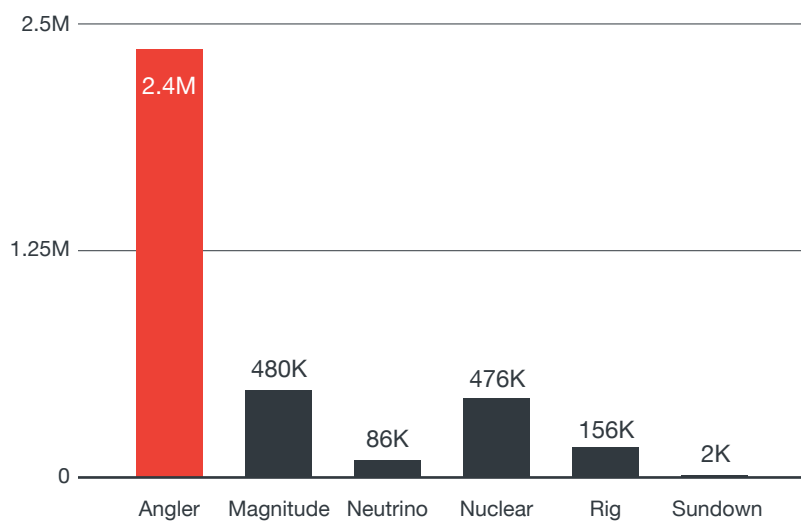


### Vulnerability exploits integrated into kits (1Q-3Q 2015)



*Angler was updated a lot more than its contemporaries were. It was the first kit to integrate the Hacking Team leak Adobe Flash zero-day exploits, making it the most active today.*

### Number of exploit-kit-hosting URLs seen (3Q 2015)



*The number of users who accessed Angler-hosting links increased from May to September this year. Website compromise incidents in Japan, zero-day vulnerability exploit attacks related to the Hacking Team breach, and widespread PoS malware distribution had ties to the Angler Exploit Kit as well.*

Around 3,000 high-profile Japanese websites were compromised to display malvertisements this September<sup>51</sup>, putting almost half a million users at risk. Malware-laced banners that were sure to appeal to tons of victims were used in attacks. Already-patched vulnerabilities in Internet Explorer (CVE-2015-2419)<sup>52</sup> and Adobe Flash (CVE-2015-5560)<sup>53</sup> were also used, again highlighting the need to always keep software and systems updated.

The constant updates that the Angler Exploit Kit received made it a security focus this quarter. The fact that Angler also has the ability to easily circumvent protection aided by the Diffie-Hellman protocol<sup>54</sup> also baffled and challenged security researchers. The Diffie-Hellman protocol, in a nutshell, is a means for two computer users to generate a shared private key with which they can then exchange information even across an insufficiently secured channel.

## Internet-ready devices: Plagued by security issues

The perils that online threats pose are now more palpable than ever. While connectivity has its benefits, it also introduces greater risks not only to the connected devices but their users as well.

Our researchers discovered attacks on gas-tank-monitoring systems via the GasPot experiment<sup>55</sup>. We saw attackers modify target tank information, which could have dire consequences for the general public<sup>56</sup>. What's worse is that gas tanks aren't the only Internet-connected devices exposed on the Web. SHODAN, a website for monitoring all such devices, lists insufficiently protected heating and surveillance systems as well as power plants. Given that these affect utilities and even entire economies, successful attacks against them could spell disastrous consequences for nations.

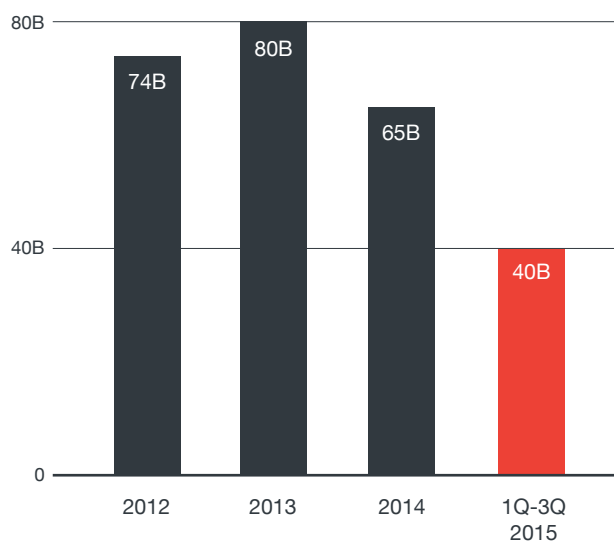
Car hacking, a far-fetched notion a few years back, is slowly becoming a reality. More and more manufacturers are launching connected and even self-driving cars, bringing a wide range of benefits, and unfortunately, threats to the fore. This quarter, Chris Valasek and Charlie Miller showed how any 3G-connected hacker could easily take control of the new Jeep Cherokee's critical systems (engine, brakes, etc.) and cause accidents that can cost even a driver's life<sup>57</sup>.

The recent emergence of numerous vulnerabilities in Internet-connected devices calls for stronger collaboration between manufacturers and security experts. Manufacturers don't necessarily keep security in mind when crafting their latest products. Security research can aid them in continuously ensuring their customers' safety while reaping the benefits that the most innovative technologies offer.

# Threat landscape in review

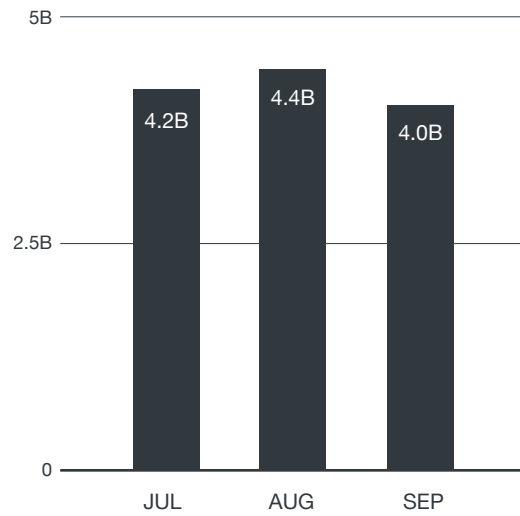
Based on Smart Protection Network data, the overall threat detection volume has been posting a nearly 20% decline since 2012. This could be due to the fact that prevalent threats like ransomware employed fileless infection routines. Also, despite a general affinity for the shotgun approach to threat distribution, other attackers still preferred to only go after well-chosen victims (mostly SMBs and large enterprises) that are sure to yield better results.

Total number of threats blocked (2012-2015)



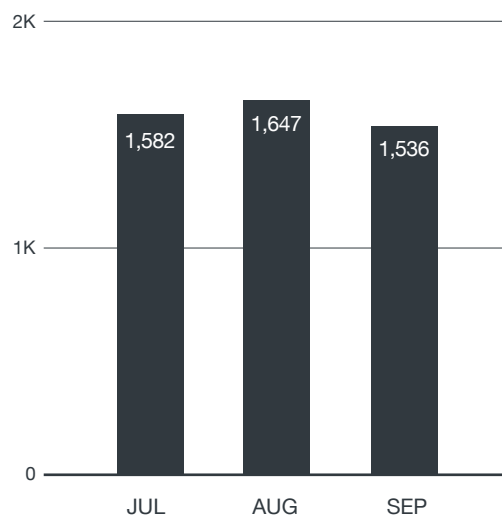
*We have been seeing a decline in the total number of threats blocked since 2014. This trend still holds true to date.*

### Total number of threats blocked (3Q 2015)



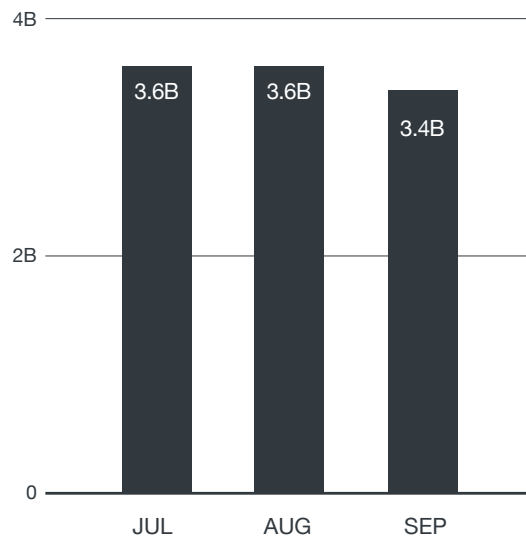
*As in the previous quarter, we blocked an average of 4.2 billion threats per month from July to September.*

### Trend Micro overall detection rate (3Q 2015)



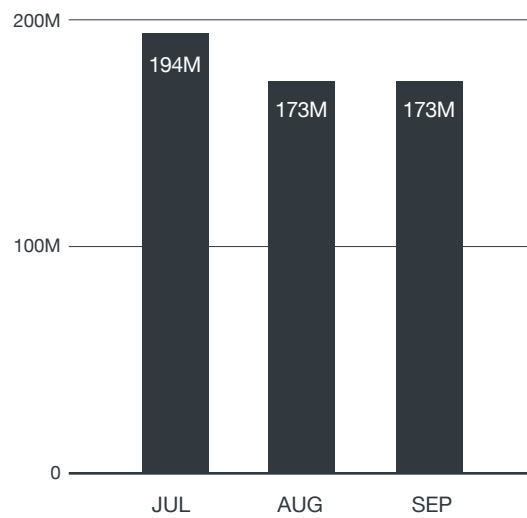
*We blocked an average of 1,588 threats per second this quarter.*

### Number of email reputation queries categorized as spam (3Q 2015)



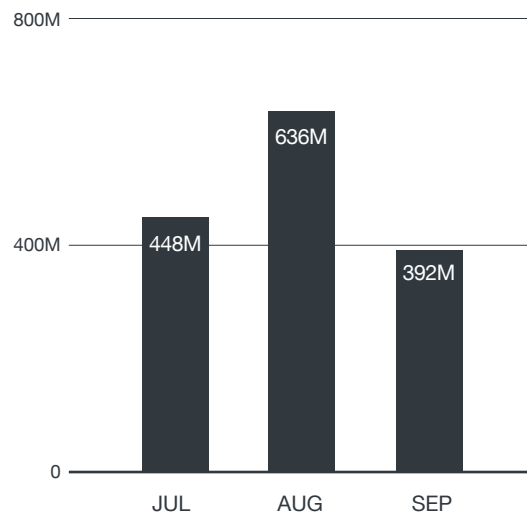
*We prevented a total of 10.6 billion emails from known spam-sending IP addresses from reaching users' inboxes. This indicates a slight increase from last quarter's 10.5 billion emails, which could be due to attackers' rejuvenated interest in spamming as a means to deliver threats.*

### Number of user visits to malicious sites blocked (3Q 2015)



*We prevented more than 540 million users from visiting malicious sites this quarter.*

### Number of malicious files blocked (3Q 2015)



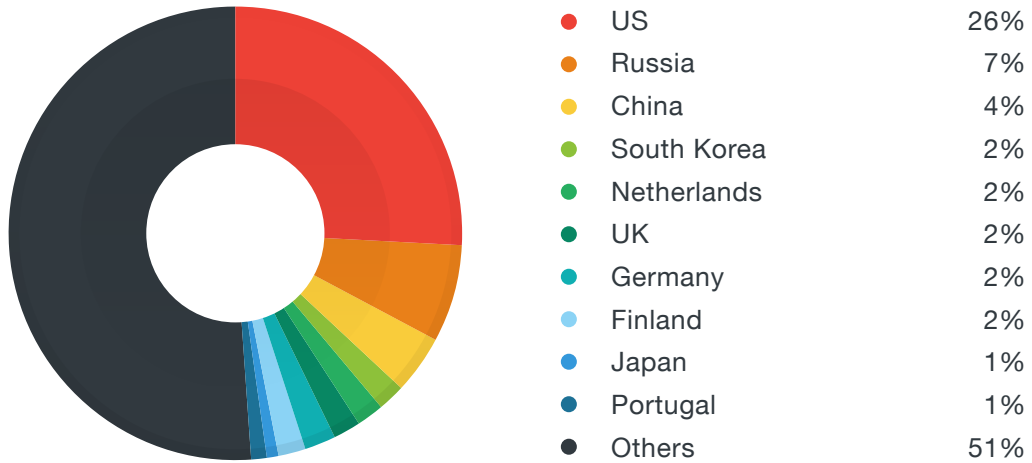
*We prevented more than a billion malicious files from infecting computers this quarter. Techniques like fileless installation contributed to the decrease in detection.*

### Top malicious domains users were prevented from visiting (3Q 2015)

Domain	Reason for blocking user access to
jsgnr.eshopcomp.com	Known browser hijacker
a020f0.com	Had ties to TROJ_POWELIKS
sso.anbtr.com	Served as a means for PE_SALITY.RL communication
cnfg.toolbar-services.com	Known adware related to browser toolbars
disorderstatus.ru	Known adware related to browser toolbars
differentia.ru	Had annoying pop-up pages or messages that redirected to malicious sites
sp-storage.spccint.com	Had ties to Conduit adware
allmodel-pro.com	Had ties to MultiPlug malware
bhinnekaonline.com	Had ties to Ransom-AZI Trojans
92vblljpl3fqub.ru	Had annoying pop-up pages or messages that redirected to malicious sites

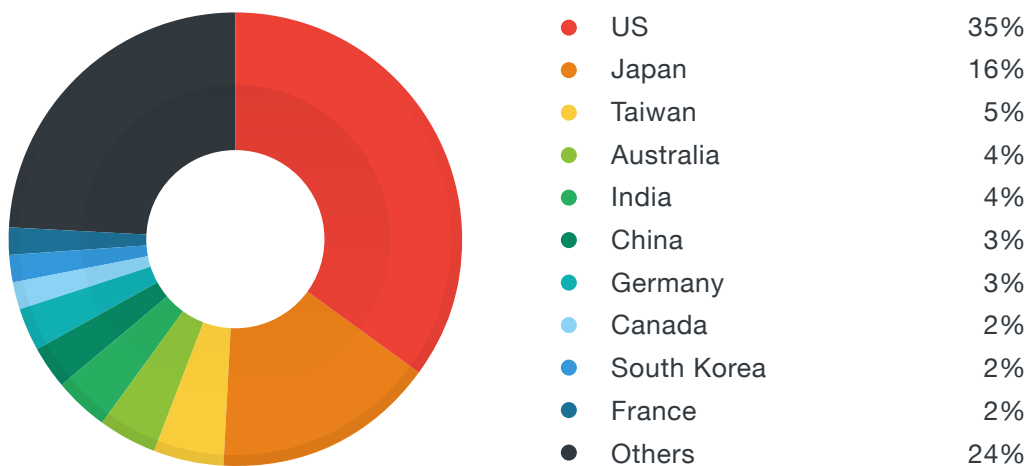
*Browser hijackers remained the most accessed malicious domains this quarter.*

### Countries that hosted the highest number of malicious URLs (3Q 2015)



*The US remained the top malicious-URL-hosting country from the previous quarter. China and Russia switched places while South Korea climbed a few notches, knocking Portugal off fourth place.*

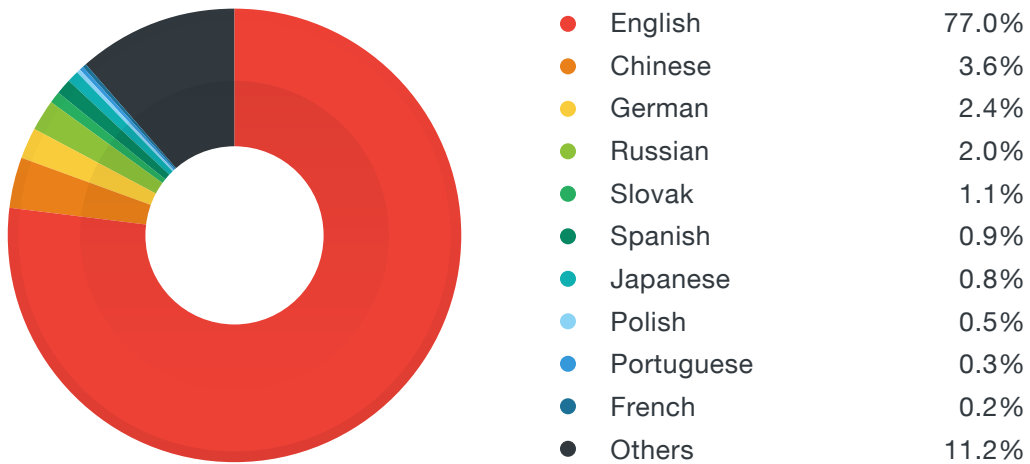
### Countries with the highest number of users who clicked malicious URLs (3Q 2015)



*No notable changes were observed in the list of countries where most users who clicked malicious URLs were from this quarter.*

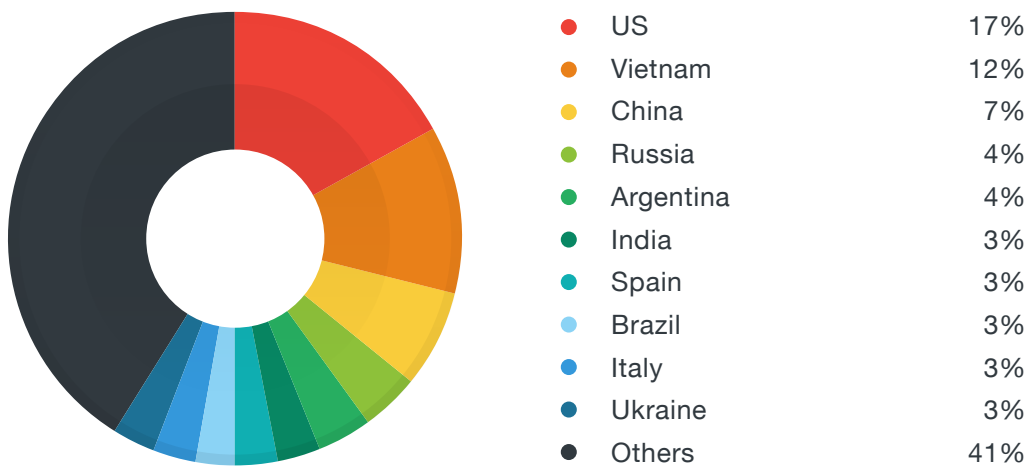


### Top spam languages (3Q 2015)



*English remained spammers' most preferred language. Slight decreases in the shares of Chinese and German compared with last quarter were also recorded.*

### Top spam-sending countries (3Q 2015)



*The US and China were the most active spam senders this quarter, retaining their top 1 and 3 posts, respectively. Vietnam, meanwhile, ousted Russia from the top 2 spot.*

### Top malware families (3Q 2015)

Family	Volume
SALITY	81K
DOWNAD	71K
BARTALEX	58K
GAMARUE	47K
DUNIHI	42K
VIRUX	38K
RAMNIT	36K
AUTORUN	26K
DLOADR	26K
SKEEYAH	24K

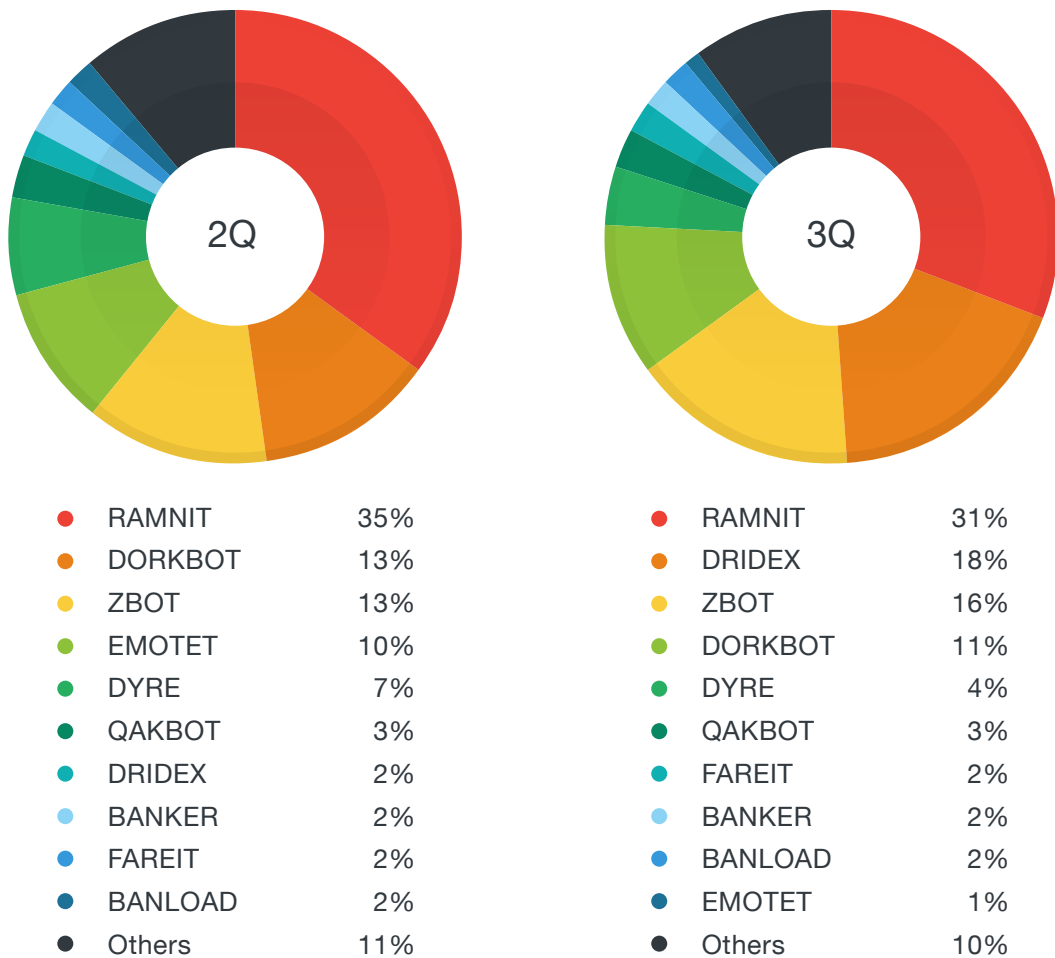
### Top malware families by segment (3Q 2015)

Segment	Family	Volume
Enterprise	DOWNAD	56K
	SALITY	33K
	DUNIHI	26K
SMB	BARTALEX	18K
	SKEEYAH	10K
	UPATRE	8K
Consumer	SALITY	28K
	GAMARUE	23K
	VIRUX	18K

*BARTALEX joined this quarter's list of top malware due to related macro-based malware attacks this July. BARTALEX typically use Microsoft Word® document attachments that function as UPATRE downloaders. DOWNAD still figured in the list of top malware, seven years after it first emerged<sup>58</sup>. This could be due to the fact that users (likely enterprises) still use old and unsupported Windows versions like XP that are vulnerable to the threat.*

DRIDEX<sup>59</sup> is a notable online banking malware family. It sports several data-stealing routines, including form grabbing, HTML injection, and browser screenshot capture. It targets European and US banks and financial institutions. Considered the GameOver ZeuS (GoZ) successor, DRIDEX uses an improved version of GoZ's peer-to-peer (P2P) architecture to secure its command-and-control (C&C) servers from security software detection.

### Top 10 online banking malware families (2Q-3Q 2015)



*RAMNIT remained the top online banking malware family despite registering a 4% decline in its share from the previous quarter. DRIDEX's share, meanwhile, rose from 2% last quarter to 18% this quarter, most likely due to its use of a botnet.*

### Top adware families (3Q 2015)

Family	Volume
OPENCANDY	495K
MYPCBACKUP	86K
MULTIPLUG	84K
ELEX	82K
TOMOS	65K
MONTIERA	62K
REGCLEANPRO	58K
DEALPLY	48K
PRICEGONG	40K
DOWNWARE	34K

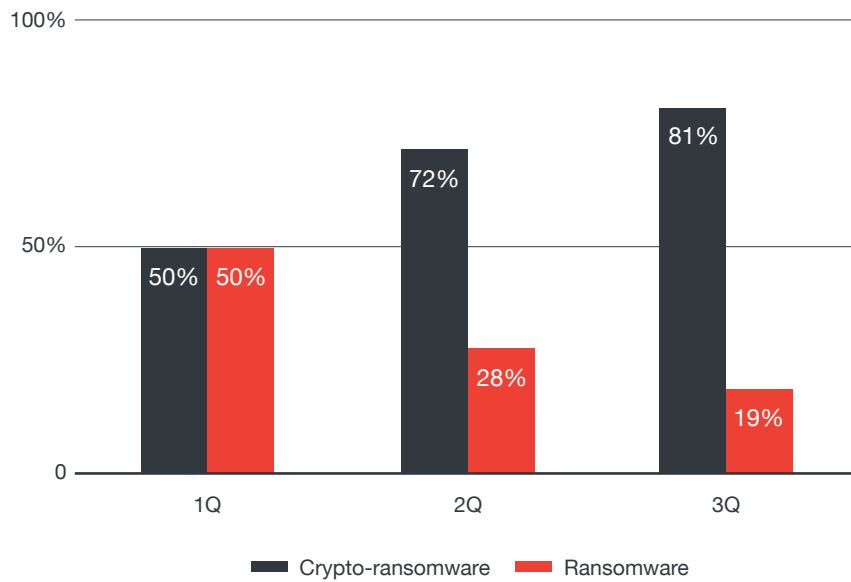
### Top adware families by segment (3Q 2015)

Segment	Family	Volume
Enterprise	OPENCANDY	46K
	MULTIPLUG	14K
	TOMOS	9K
SMB	OPENCANDY	17K
	MULTIPLUG	3K
	ELEX	3K
Consumer	OPENCANDY	398K
	FAKEGOOG	70K
	MYPCBACKUP	57K

*OPENCANDY and MYPCBACKUP, which generally came in the form of free software or toolbars, continued to be a nuisance for all kinds of users.*

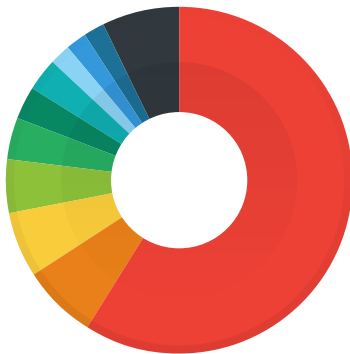
Crypto-ransomware have been predominantly figuring in the threat landscape since last quarter. It has since had a larger share compared with its less-destructive counterpart, ransomware, which could be attributed to CryptoWall-related spam outbreaks.

### Comparison of ransomware and crypto-ransomware shares (1Q-3Q 2015)



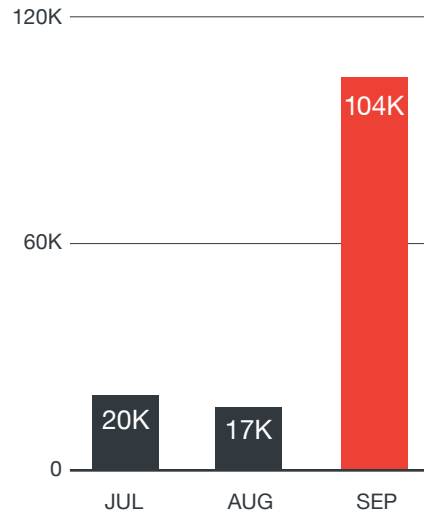
*Crypto-ransomware constantly outnumbered ransomware QoQ.*

### Top ransomware families (3Q 2015)



●	CRYPTOWALL	59%
●	CRILOCK	7%
●	REVETON	6%
●	RANSOM	5%
●	CRYPTESLA	4%
●	MATSNU	3%
●	KOVTER	3%
●	CRYPCTB	2%
●	CRYPDEF	2%
●	CRYPTWALL	2%
●	Others	7%

### CryptoWall-related spam volume (3Q 2015)



*Protecting users from ransomware starts by catching the threats before they run on computers. Continuous ransomware monitoring shows that CRILOCK or TorrentLocker and CRYPTOWALL can be caught as early as when they arrive via spam (either as attachments or embedded malicious links).*

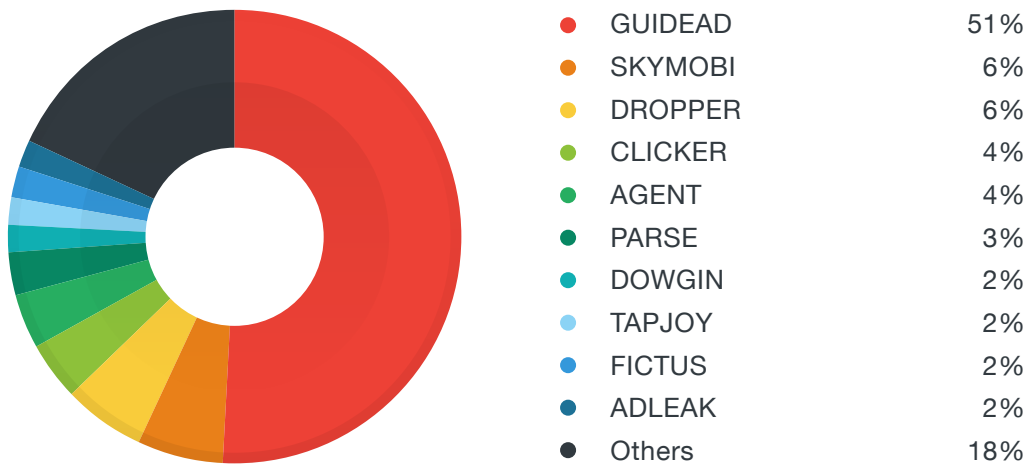
### Top Android malware families (3Q 2015)



●	ADULTPLAYER	14%
●	SYPAY	9%
●	FAKEINST	8%
●	SMSSNOW	6%
●	OPFAKE	5%
●	LINKSMSHIDER	4%
●	SMSREG	4%
●	SMSTHIEF	3%
●	SYSSERVICE	3%
●	SMSSPY	3%
●	Others	41%

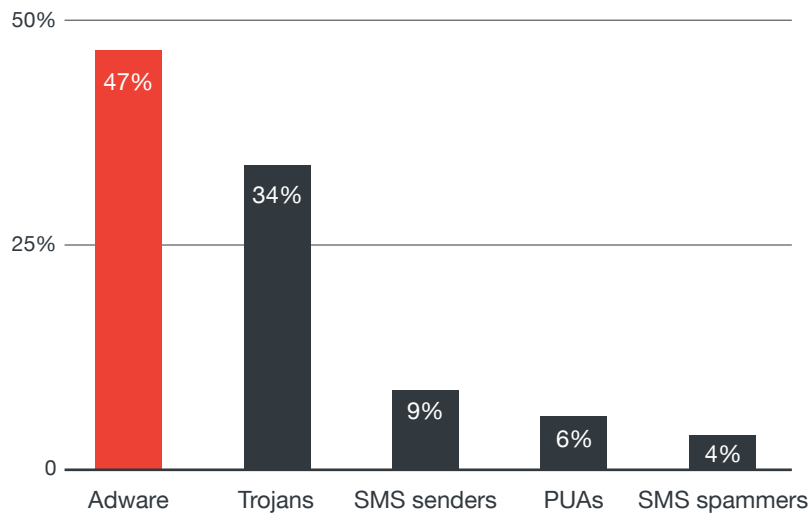
*ADULTPLAYER secretly takes photos of affected app users for later use in extortion scams.*

### Top Android adware families (3Q 2015)



*GUIDEAD, now classified as a potentially unwanted application (PUA), is a SkyMobi software development kit (SDK) that promotes the other apps the developer created much like spam annoys computer users with unwanted ads.*

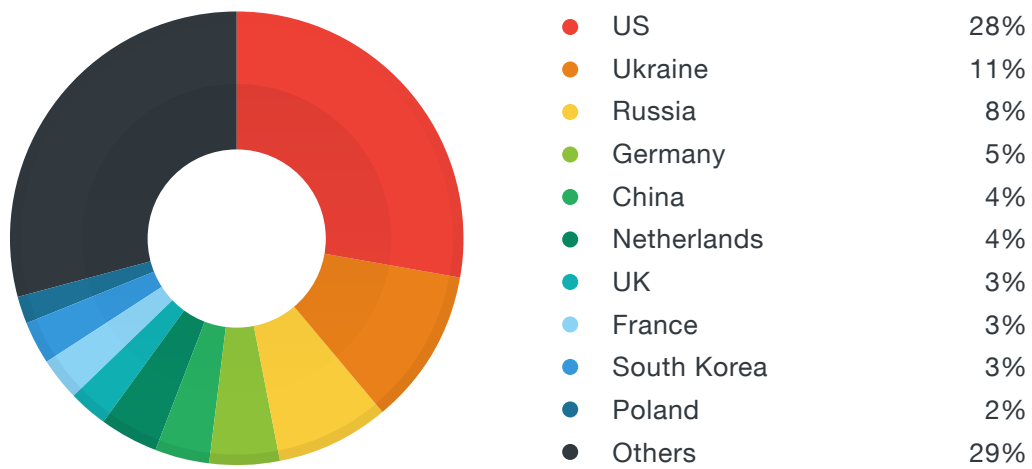
### Top Android threat types seen (3Q 2015)



*Nearly half of the Android threats seen this quarter were adware, pushing the type back to the top spot. SMS spammers joined the list of top Android threat types. These send content created with an automated tool in bulk and differ from SMS senders, which send messages without the user's authorization.*

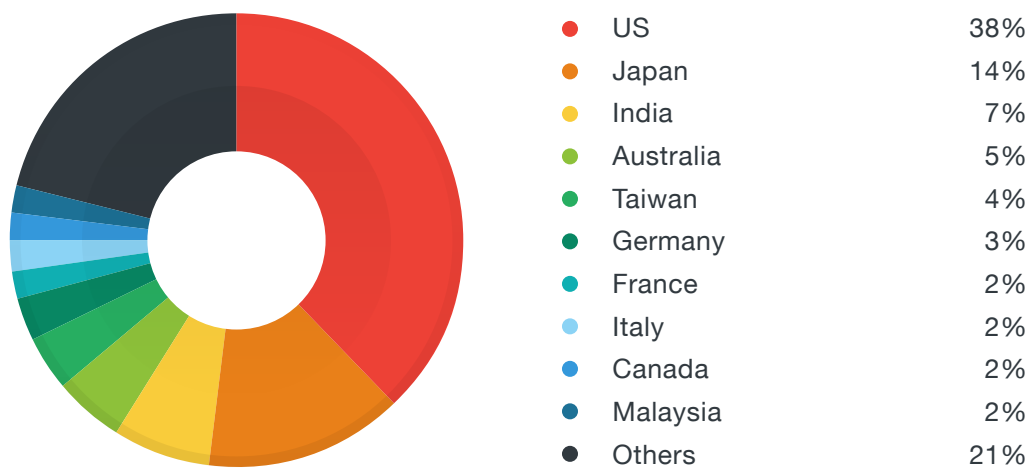
**Note:** A mobile threat family may exhibit the behaviors of more than one threat type.

### Countries where the highest number of C&C servers were hosted (3Q 2015)



*The top C&C-server country hosts remained the US, the Ukraine, and Russia this quarter. Note though that attackers don't necessarily have to reside in the countries where their C&C servers are located, as these can be remotely accessed.*

### Countries with the highest number of C&C server connections (3Q 2015)



*The US still dominated the list of countries with the highest number of C&C connections this quarter.*



## References

1. Steve Ragan. (5 July 2015). CSO. "Hacking Team Hacked, Attackers Claim 400GB in Dumped Data." Last accessed on 27 October 2015, <http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html>.
2. Adobe Systems Incorporated. (2015). *Adobe Flash Runtimes*. "Statistics." Last accessed on 30 October 2015, <http://www.adobe.com/products/flashruntimes/statistics.html>.
3. Net Applications.com. (2006–2015). *Net Marketshare*. "Desktop Operating System Market Share." Last accessed on 30 October 2015, <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpsp=198&qpn=1&qptimeframe=M>.
4. Net Applications.com. (2006–2015). *Net Marketshare*. "Desktop Browser Version Market Share." Last accessed on 30 October 2015, <https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0&qpsp=198&qpn=1&qptimeframe=M>.
5. Trend Micro Incorporated. (16 August 2015). *Threat Encyclopedia*. "Adobe Flash Player Vulnerability (CVE-2015-5119)." Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/6994/adobe-flash-player-vulnerability-cve20155119>.
6. Brooks Li. (7 July 2015). *TrendLabs Security Intelligence Blog*. "Hacking Team Flash Zero Day Integrated into Exploit Kits." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/>.
7. Peter Pi. (7 July 2015). *TrendLabs Security Intelligence Blog*. "Unpatched Flash Player Flaw, More PoCs Found in Hacking Team Leak." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/>.
8. Weimin Wu. (1 July 2015). *TrendLabs Security Intelligence Blog*. "Hacking Team Flash Zero Day Tied to Attacks in Korea and Japan... on July 1." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-tied-to-attacks-in-korea-and-japan-on-july-1/>.
9. Joseph C. Chen. (28 July 2015). *TrendLabs Security Intelligence Blog*. "Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIvy." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-attacks-spread-compromised-tv-and-government-sites-in-hong-kong-and-taiwan-lead-to-poisonivy/>.
10. Veo Zhang. (21 July 2015). *TrendLabs Security Intelligence Blog*. "Hacking Team RCSAndroid Spying Tool Listens to Calls; Roots Devices to Get In." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/>.
11. Danielle Walker. (13 July 2015). *SC Magazine*. "iPhones, Jailbroken and Not, Vulnerable to Hacking Team Spyware, Firm Finds." Last accessed on 27 October 2015, <http://www.scmagazine.com/ios-devices-dont-have-to-be-jailbroken-for-spyware-sold-by-hacking-team-to-be-installed/article/426137/>.
12. Wish Wu. (16 July 2015). *TrendLabs Security Intelligence Blog*. "Fake News App in Hacking Team Dump Designed to Bypass Google Play." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/fake-news-app-in-hacking-team-dump-designed-to-bypass-google-play/>.
13. Trend Micro. (20 August 2015). *TrendLabs Security Intelligence Blog*. "Ashley Madison: A Tale of Sex, Lies, and Data Breaches." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/ashley-madison-a-tale-of-sex-lies-and-data-breaches/>.
14. Matthew Herper. (1 September 2015). *Forbes*. "Were There 30 Million Cheaters on Ashley Madison, or 10? How Estimates Get Out of Hand." Last accessed on 27 October 2015, <http://www.forbes.com/sites/matthewherper/2015/09/01/were-there-30-million-cheaters-on-ashley-madison-or-10-how-estimates-get-out-of-hand/>.
15. Chris Baraniuk. (24 August 2015). *BBC News*. "Ashley Madison: 'Suicides' over Website Hack." Last accessed on 27 October 2015, <http://www.bbc.com/news/technology-34044506>.

16. Jonathan Leopando. (31 August 2015). *TrendLabs Security Intelligence Blog*. "Blackmail, Deletion Offers Hit Ashley Madison Users." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/blackmail-deletion-offers-hit-ashley-madison-users/>.
17. Ryan Flores. (8 September 2015). *TrendLabs Security Intelligence Blog*. "Ashley Madison, Why Do Our Honeypots Have Accounts on Your Website?" Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/ashley-madison-why-do-our-honeypots-have-accounts-on-your-website/>.
18. Andy Greenberg. (10 September 2015). *Wired*. "Hack Brief: Health Insurer Excellus Says Attackers Breached 10M Records." Last accessed on 27 October 2015, <http://www.wired.com/2015/09/hack-brief-health-insurance-firm-excellus-says-attackers-breached-10m-records>.
19. Chad Terhune. (17 July 2015). *Los Angeles Times*. "UCLA Health System Data Breach Affects 4.5 Million Patients." Last accessed on 27 October 2015, <http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html>.
20. TrendLabs. (14 August 2015). *Trend Micro Security News*. "Medical Data in the Crosshairs: Why Is Healthcare an Ideal Target?" Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/medical-data-in-the-crosshairs-why-is-healthcare-an-ideal-target>.
21. Numaan Huq. (22 September 2015). *Trend Micro Security News*. "Follow the Data: Analyzing Breaches by Industry." Last accessed on 3 November 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf>.
22. Wish Wu. (31 July 2015). *TrendLabs Security Intelligence Blog*. "MMS Not the Only Attack Vector for 'Stagefright.'" Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/mms-not-the-only-attack-vector-for-stagefright/>.
23. Wish Wu. (29 July 2015). *TrendLabs Security Intelligence Blog*. "Trend Micro Discovers Vulnerability That Renders Android Devices Silent." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-vulnerability-that-renders-android-devices-silent/>.
24. Android. *Developers*. "Dashboards." Last accessed on 27 October 2015, <http://developer.android.com/about/dashboards/index.html>.
25. Wish Wu. (26 August 2015). *TrendLabs Security Intelligence Blog*. "Revisiting CVE-2015-3823: Mediaserver Bug Leads to Heap Overflow, Too." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/revisiting-cve-2015-3823-mediaserver-bug-leads-to-heap-overflow-too/>.
26. Wish Wu. (17 August 2015). *TrendLabs Security Intelligence Blog*. "Mediaserver Takes Another Hit with Latest Android Vulnerability." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/mediaserver-takes-another-hit-with-latest-android-vulnerability/>.
27. Marshall Honorof. (5 August 2015). *Tom's Guide*. "Android Finally Getting Regular Security Updates." Last accessed on 27 October 2015, <http://www.tomsguide.com/us/android-monthly-security-updates,news-21432.html>.
28. Ju Zhu. (21 September 2015). *TrendLabs Security Intelligence Blog*. "The XcodeGhost Plague—How Did It Happen?" Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-xcodeghost-plague-how-did-it-happen/>.
29. Charlie Osborne. (17 September 2015). *ZDNet*. "Apple AirDrop Flaw Leaves Users Vulnerable to Exploit." Last accessed on 27 October 2015, <http://www.zdnet.com/article/apple-airdrop-flaw-leaves-users-vulnerable-to-exploit/>.
30. Allie Coyne. (21 August 2015). *IT News*. "Apple iOS 'Quicksand' Flaw Enables Enterprise Data Theft." Last accessed on 30 October 2015, <http://www.itnews.com.au/news/apple-ios-quicksand-flaw-enables-enterprise-data-theft-408202#ixzz3q2cWNI7a>.
31. Spencer Hsieh. (7 November 2014). *TrendLabs Security Intelligence Blog*. "Staying Safe from WireLurker: The Combined Mac/iOS Threat." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/staying-safe-from-wirelurker-the-combined-macios-threat/>.

32. Brooks Hong. (20 November 2014). *TrendLabs Security Intelligence Blog*. "The Other Side of Masque Attacks: Data Encryption Not Found in iOS Apps." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-other-side-of-masque-attacks-data-encryption-not-found-in-ios-apps/>.
33. Taylor Armerding. (12 January 2015). *CSO*. "Why Criminals Pick on Small Business." Last accessed on 27 October 2015, <http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html>.
34. TrendLabs. (1 August 2015). *Trend Micro Security News*. "Next-Gen Payment-Processing Tech: EMV Credit Cards." Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/security/news/security-technology/next-gen-payment-processing-tech-emv-credit-cards>.
35. TrendLabs. (1 August 2015). *Trend Micro Security News*. "Next-Gen Payment-Processing Tech: Contactless RFID Credit Cards." Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/security/news/security-technology/next-gen-payment-processing-tech-rfid-credit-cards>.
36. TrendLabs. (1 August 2015). *Trend Micro Security News*. "Mobile Payment Systems: How Apple Pay Works." Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/mobile-payment-systems-apple-pay>.
37. TrendLabs. (1 August 2015). *Trend Micro Security News*. "Mobile Payment Systems: How Android Pay Works." Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/mobile-payment-systems-android-pay>.
38. TrendLabs. (1 August 2015). *Trend Micro Security News*. "Next-Gen Payment-Processing Architectures." Last accessed on 27 October 2015, <http://www.trendmicro.com/vinfo/us/security/news/security-technology/next-gen-payment-processing-architectures>.
39. Anthony Joe Melgarejo. (27 July 2015). *TrendLabs Security Intelligence Blog*. "Angler Exploit Kit Used to Find and Infect PoS Systems." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/angler-exploit-kit-used-to-find-and-infect-pos-systems/>.
40. Jay Yaneza. (16 July 2015). *TrendLabs Security Intelligence Blog*. "New GamaPoS Malware Piggybacks on Andromeda Botnet; Spreads in 13 US States." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-gamapos-threat-spreads-in-the-us-via-andromeda-botnet/>.
41. Trend Micro. (24 September 2015). *TrendLabs Security Intelligence Blog*. "Credit-Card-Scraping Kasidet Builder Leads to Spike in Detections." Last accessed on 27 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/>.
42. TrendLabs. (August 2015). *Trend Micro Security Intelligence Blog*. "A Rising Tide: New Hacks Threaten Public Technologies." Last accessed on 27 October 2015, [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt\\_a\\_rising\\_tide.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_a_rising_tide.pdf).
43. Feike Hacquebord. (16 April 2015). *TrendLabs Security Intelligence Blog*. "Operation Pawn Storm Ramps Up Its Activities; Targets NATO, White House." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/>.
44. Feike Hacquebord. (18 August 2015). *TrendLabs Security Intelligence Blog*. "Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/>.
45. Feike Hacquebord. (22 October 2015). *TrendLabs Security Intelligence Blog*. "Pawn Storm Targets MH17 Investigation Team." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/>.
46. Trend Micro. (11 July 2015). *TrendLabs Security Intelligence Blog*. "Pawn Storm Update: Trend Micro Discovers New Java Zero-Day Exploit." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/>.
47. Trend Micro. (14 July 2015). *TrendLabs Security Intelligence Blog*. "An In-Depth Look at How Pawn Storm's Java Zero Day Was Used." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/an-in-depth-look-at-how-pawn-storms-java-zero-day-was-used/>.

48. Trend Micro. (15 July 2015). *TrendLabs Security Intelligence Blog*. "Pawn Storm C&C Redirects to Trend Micro IP Address." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-cc-redirects-to-trend-micro-ip-address/>.
49. Cedric Pernet. (1 September 2015). *TrendLabs Security Intelligence Blog*. "Rocket Kitten Spies Target Iranian Lecturer and InfoSec Researchers in New Modus." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-spy-kittens-are-back-an-update-to-rocket-kitten/>.
50. TrendLabs. (18 August 2015). *Trend Micro Security News*. "A Rising Tide: New Hacks Threaten Public Technologies." Last accessed on 28 October 2015, <http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup>.
51. Joseph C. Chen. (30 September 2015). *TrendLabs Security Intelligence Blog*. "3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/3000-high-profile-japanese-sites-hit-by-massive-malvertising-campaign/>.
52. Trend Micro. (30 July 2015). *Threat Encyclopedia*. "July 2015—Microsoft Releases 14 Security Advisories." Last accessed on 28 October 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/3833/july-2015-microsoft-releases-14-security-advisories>.
53. Trend Micro. (12 October 2015). *Threat Encyclopedia*. "Adobe Flash Player Integer Overflow Vulnerability (CVE-2015-5560)." Last accessed on 28 October 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/8859/adobe-flash-player-integer-overflow-vulnerability-cve20155560>.
54. Whitfield Diffie and Martin. E. Hellman. (November 1976). *IEEE*. "New Directions in Cryptography." Last accessed on 28 October 2015, <https://ee.stanford.edu/~hellman/publications/24.pdf>.
55. Trend Micro. (5 August 2015). *TrendLabs Security Intelligence Blog*. "The GasPot Experiment: Hackers Target Gas Tanks." Last accessed on 28 October 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-gaspot-experiment-hackers-target-gas-tanks/>.
56. Arthur Brice. (17 November 2009). *CNN*. "Puerto Rico Fire Linked to Faulty Gas-Tank-Monitoring System." Last accessed on 28 October 2015, <http://edition.cnn.com/2009/US/11/17/puerto.rico.fire.investigation/index.html>.
57. Iain Thomson. (21 July 2015). *The Register*. "Jeep Drivers Can Be Hacked to Death: All You Need Is the Car's IP Address." Last accessed on 28 October 2015, [http://www.theregister.co.uk/2015/07/21/jeep\\_patch/](http://www.theregister.co.uk/2015/07/21/jeep_patch/).
58. Arman Capili. (30 November 2008). *TrendLabs Security Intelligence Blog*. "DOWNAD: Gearing Up for a Botnet." Last accessed on 3 November 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/downad-gearing-up-for-a-botnet/>.
59. Ryan Angelo Certeza. (6 December 2014). *Threat Encyclopedia*. "Dealing with the Mess of DRIDEX." Last accessed on 28 October 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3147/dealing-with-the-mess-of-dridex>.



Created by:

**TrendLabs**

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

#### TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit [www.trendmicro.com](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud