Setting the Stage:
Landscape Shifts Dictate Future Threat Response Strategies
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 Dissecting Breaches
7 Pawn Storm Zero-Days and Other Vulnerabilities
10 Deep Web and Underground Explorations
13 Smart Technology Nightmares
15 Angler, the King of Exploit Kits
18 Data Held Hostage
21 Takedowns versus DRIDEX
23 Threat Landscape in Review
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’ 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,” 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)

UCLA Health System
May 5
4.5M records (personal information and medical records)

IRS Washington DC
May 26
100K records (financial data)

OPM
June 4
21.5M records (personal information)

Ashley Madison
July 21
37M records (personal information)

Systema Software
September 21
1.5M records (medical records)

Experian
October 1
15M records (personal information)

Vtech
November 30
6.4M records (email addresses)

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

CareFirst BlueCross BlueShield
May 20
1.1M records (personal information)

Japan Pension Service
June 1
1M records (personal information)

Hacking Team
July 7
Undetermined number (trade secrets)

Excellsus BlueCross BlueShield
September 10
10M records (personal information and financial data)

Scottrade
October 1
4.6M records (personal information)

Secretary of State Brian Kemps
November 18
6M records (personal information)

---

2015’s biggest data breaches

5 | Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies
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, 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. 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.

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), two Flash Player zero-day vulnerabilities (CVE-2015-5122 and CVE-2015-5123), and one particular Flash zero-day that was used in limited attacks in Japan and Korea. This said zero-day (CVE-2015-5119) 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.
TrendLabs 2015 Annual Security Roundup

2015 in vulnerabilities

* Discovered by Trend Micro

PC | Mobile

Zero-day | Used in Operation PawnStorm

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

May 27
CVE-2015-1835

June 19
CVE-2015-3113

June 26
CVE-2015-5119

July 7
CVE-2015-8122

August 4
CVE-2015-3823

August 11
CVE-2015-3839

October 13
CVE-2015-7645

October 15
CVE-2015-6600

November 1

2015 in vulnerabilities

8 | Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies
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.\textsuperscript{17,18} It can also be used to render Android devices silent and unable to make calls due to unresponsive screens.\textsuperscript{19} A vulnerability in Android’s manifest file may also cause devices to experience constant rebooting, making the device totally useless.\textsuperscript{20}

Some other Android vulnerabilities include the Android debugger Debuggered vulnerability\textsuperscript{21} we discovered in June. It can be utilized to expose a device’s memory content. The Android Installer Hijacking vulnerability,\textsuperscript{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\textsuperscript{23} (CVE-2015-4640 and CVE-2015-4641\textsuperscript{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\textsuperscript{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\textsuperscript{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—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. 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.

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. 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. 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.
 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\textsuperscript{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.\textsuperscript{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\textsuperscript{34} and smart refrigerators,\textsuperscript{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\textsuperscript{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\textsuperscript{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\textsuperscript{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.\textsuperscript{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.
One of the challenges we noted in our 2016 security predictions\(^4\) 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, 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.

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.

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

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.
Anger-exploit-kit-hosting URLs were the most accessed in 2015. SweetOrange, Hanjuan, Fiesta, and Sundown exploit kits were rarely updated in 2015.

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 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, 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.

\[\text{Compared to last year’s data, this year’s crypto-ransomware numbers steadily rose up to the end of 2015 and even overtook ransomware.}\]

In 2015, we saw more incidents involving the crypto-ransomware variant called Cryptowall. 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.

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.
The ransomware family Chimera\textsuperscript{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.\textsuperscript{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.\textsuperscript{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)\textsuperscript{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.
Reports of a ransomware that archives files using a password lock surfaced. Victims had to pay $300 in exchange for the password.

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

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

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

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

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

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

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

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

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.

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

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.
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. DRIDEX is an advanced information-stealing malware that targets users’ online banking data. The malware is spread via spam that contain malicious file attachments that use macros.

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 the number of DRIDEX detections within the US, but the threat still persisted in other countries. 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 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). 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.
English remained the most-used spam language in 2015.
The number of spam doubled in the US in 2015. China and Russia moved up the ranks, while Japan joined the top 10.
Top malicious domains users were prevented from visiting in 2015

<table>
<thead>
<tr>
<th>Malicious URL Blocked</th>
<th>Reason for blocking access to</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.adnetworkperformance.com">www.adnetworkperformance.com</a></td>
<td>Known browser hijacker</td>
</tr>
<tr>
<td>jsgnr.eshopcomp.com</td>
<td>Hosts potentially malicious hijacking browsers</td>
</tr>
<tr>
<td>facebook.tbc.cint.com</td>
<td>Known to host malware</td>
</tr>
<tr>
<td>sso.anbtr.com</td>
<td>Known to host malware</td>
</tr>
<tr>
<td>bugreport.yac.mx</td>
<td>Known to host unwanted applications</td>
</tr>
<tr>
<td>sp-storage.spccint.com</td>
<td>Known to host unwanted applications</td>
</tr>
<tr>
<td>checkver.dsiteproducts.com</td>
<td>Known to host unwanted applications</td>
</tr>
<tr>
<td>a020f0.com</td>
<td>Related to TROJ_POWELIKS</td>
</tr>
<tr>
<td>ffb6c1.com</td>
<td>Known to produce multiple website pop-ups</td>
</tr>
<tr>
<td>dda0dd.com</td>
<td>Known to produce continuous website pop-ups</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SALITY</td>
<td>325K</td>
</tr>
<tr>
<td>DOWNAD</td>
<td>298K</td>
</tr>
<tr>
<td>GAMARUE</td>
<td>207K</td>
</tr>
</tbody>
</table>

Top malware families of 2015 by segment

<table>
<thead>
<tr>
<th>Segment</th>
<th>Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>DOWNAD</td>
<td>231K</td>
</tr>
<tr>
<td></td>
<td>SALITY</td>
<td>132K</td>
</tr>
<tr>
<td></td>
<td>DUNIHI</td>
<td>111K</td>
</tr>
<tr>
<td>SMB</td>
<td>DOWNAD</td>
<td>37.2K</td>
</tr>
<tr>
<td></td>
<td>DLOADR</td>
<td>36.1K</td>
</tr>
<tr>
<td></td>
<td>DRIDEX</td>
<td>35.6K</td>
</tr>
<tr>
<td>Consumer</td>
<td>SALITY</td>
<td>123K</td>
</tr>
<tr>
<td></td>
<td>GAMARUE</td>
<td>112K</td>
</tr>
<tr>
<td></td>
<td>Virux</td>
<td>74K</td>
</tr>
</tbody>
</table>

*DOWNAD, SALITY, and GAMARUE continue to be the top infectors in 2015.*
Top 10 online banking malware families of 2015

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® documents were the most used for macro malware in 2015.
Top adware families for 2015

<table>
<thead>
<tr>
<th>Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPENCANDY</td>
<td>1.9M</td>
</tr>
<tr>
<td>MYPCBACKUP</td>
<td>504K</td>
</tr>
<tr>
<td>DEALPLY</td>
<td>407K</td>
</tr>
</tbody>
</table>

Top adware families in 2015 by segment

<table>
<thead>
<tr>
<th>Segment</th>
<th>Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>OPENCANDY</td>
<td>223K</td>
</tr>
<tr>
<td></td>
<td>DEALPLY</td>
<td>76K</td>
</tr>
<tr>
<td></td>
<td>TOMOS</td>
<td>45K</td>
</tr>
<tr>
<td>SMB</td>
<td>OPENCANDY</td>
<td>81K</td>
</tr>
<tr>
<td></td>
<td>DEALPLY</td>
<td>34K</td>
</tr>
<tr>
<td></td>
<td>VPAYD</td>
<td>25K</td>
</tr>
<tr>
<td>Consumer</td>
<td>OPENCANDY</td>
<td>1.5M</td>
</tr>
<tr>
<td></td>
<td>FakeGooG</td>
<td>386K</td>
</tr>
<tr>
<td></td>
<td>MYPCBACKUP</td>
<td>264K</td>
</tr>
</tbody>
</table>

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

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


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

©2016 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Created by:
TrendLabs
The Global Technical Support & R&D Center of TREND MICRO