Magnified Losses, Amplified Need for Cyber-Attack Preparedness

TrendLabs℠ 2014 Annual Security Roundup

Contents

2014 showed how destructive attacks could be to individuals and companies alike. Effects of losing massive amounts of confidential data to attackers such as substantive financial losses and irreparable reputation damage ran rampant throughout the year. The severity of the attacks and their effects revealed one thing—the risks of becoming the next victim of a cyber attack have gone higher.

Various companies suffered financial, legal, operational, and productivity losses after getting hit by massive data breaches. Breaches across industries aided by point-of-sale (PoS) RAM scrapers, for one, increased in number in 2014. The year was not solely marred by the biggest breaches seen to date though, as attacks targeting vulnerabilities like Heartbleed and Shellshock in widely used, previously considered secure open source software as well as FakeID and Same Origin Policy (SOP) Bypass in mobile devices and platforms were also seen. Established processes like two-factor authentication also proved vulnerable to threats, as evidenced by attacks instigated by the criminals behind Operation Emmental.

As years pass, we are bound to see more crippling attacks against both likely and unlikely targets. Attackers will always trail their sights on one thing—profit. They will continue to indiscriminately hit data gold mines because peddling stolen information is a lucrative business, as evidenced by the thriving cybercriminal underground economy.

Merely dealing with threats as they surface is no longer enough, acting on risk assessment results prior to security incidents is actually more beneficial. Organizations need to rethink their current cybersecurity investments so they can easily respond to and mitigate attacks. Planning ahead so they can instantly take action if they need to is critical because these kinds of cyber attacks can happen to companies in any industry and of whatever size.

"

All in all, it's a combination of identifying what's most important, deploying the right technologies, and educating users. It is everybody's job—not just that of IT professionals—to ensure that the company's core data stays safe.

—Raimund Genes
Trend Micro CTO

"

"

Strengthening trust at all levels is crucial in today's hyper-connected world. In this increasingly complex innovation-driven ecosystem, however, a change in mindset is necessary. It's not just the big global multinationals, but also new start-ups and SMEs who will play a prime role in forging the path towards a safer and converged environment. ITU is committed to support building global trust, including by facilitating information sharing that is crucial to combating cyber-threats.

—Houlin ZHAO,
Secretary General, ITU

"

Scale of Impact and Losses Due to Cyber Attacks Intensified

Massive data breach disclosures came one after another in 2014 in much more rapid succession than past years. The Sony Pictures breach illustrated the wide spectrum of losses that can hit a company that has failed to secure its network.

As expected, major data breach incidents were reported as 2014 wore on.[1] Retailers, banks, public utilities, and numerous organizations lost millions of customer data to attackers. Companies across industries succumbed to breaches that not only cost them financially but also brought significant brand damage.[2] In the second quarter of 2014, for instance, source code repository Code Spaces went out of business after an attacker deleted its client databases and backups.[3] P.F. Chang's had to go back to using manual credit-card-imprinting devices after a breach. Outside of the United States, an educational company for children in Japan, Benesse, suffered a major data breach, where a former employee of a third-party partner leaked at least 28.95 million customer records to advertisers. As a result, the company had to apologize and allocate part of its ¥20-billion fund (almost US$169 million) to establish the Benesse Children's Fund.[4]

Among the cyber attacks seen in 2014 though, the "Sony Pictures hack" probably best showed how much a company could lose as an aftermath of a security breach. The company was forced to temporarily shut its network down after it was compromised by the so-called Guardians of Peace (GOP).[5] It reportedly lost 100TB of confidential data as a result.[6] While Sony Pictures has not declared the cost of the breach, cybersecurity experts from the Center of Strategic and International Studies pegged the loss to reach US$100 million.[7–9] Other companies under the Sony banner have fallen victim to massive attacks.[10] A company executive was quoted in 2007 as saying he would not invest US$10 million on security technologies to avoid a US$1-million incident.[11]

> "In order to detect anomalies, however, IT administrators will need to know first what to look out for. Since attacks are commonly designed to leave little to no tracks at all, it is important to know where possible indicators of a compromise can be found."
>
> **—Ziv Chang**
> *Director of Cybersafety Solutions*

> "Attackers spend much time during reconnaissance to understand the target company—its IT environment and security defenses—and IT administrators need to adopt this mentality in terms of their security strategy. All networks are different. This means that each one will need to be configured differently. IT administrators need to fully understand the network and implement the necessary defense measures to fit their environment."
>
> **—Spencer Hsieh**
> *Targeted Attack Threat Researcher*

All of the reports on who were responsible for the Sony Pictures hack have so far been inconclusive. Some believe it was an insider job akin to the Amtrak incident motivated by reasons like money, ideology, coercion, or ego.[12–13] Others, meanwhile, chose to lay the blame on hacktivists. At the end of the day though, it does not matter who was at fault. Had the conglomerate learned from past incidents and protected its network from possible intrusions, it could have spared itself from this situation.[14]

Even if the truth about how hackers breached Sony Pictures's defenses remains unknown, our own analysis of WIPALL, the destructive malware the FBI warned businesses against following the Sony Pictures hack, revealed it was not as sophisticated as other classes of malware the likes of STUXNET.[15–17] However, there may be other components of the attack not made public.

Behavior Comparison of Selected Malware

	WIPALL	STUXNET	BlackPOS	ZeuS/ZBOT	MBR Wiper in South Korea Attacks
Malware components	Several backdoors and malicious .SYS files	A worm, an .LNK file, and a rootkit	Main Trojan scrapes and exfiltrates data	Trojan spyware and a configuration file	Dropper drops the main Trojan
Arrival and/ or autostart mechanism	*Not enough information*	Arrives via USB drives; the .LNK file executes copies of the worm	Exploits four vulnerabilities	Uses social engineering and registry keys	Uses a link in spear-phishing emails; exploits a Hangul Word Processor vulnerability
Stealth mechanism	Disables a system's real-time scanner	Uses exploits and a rootkit component	Mimics security software to evade detection	Varied	Mimics legitimate Windows services
Lateral movement	Uses predefined credentials to hack network shares	Installs client and server components to execute network commands	*Not enough information*	Not applicable	Checks saved SSH credentials for accounts with root access
Information stolen	*Not enough information*	Allows attackers to view and alter the project database and information from the WinCC server	Steals credit card credentials of customers stored in infected (PoS) systems	Logs keystrokes to steal user credentials to bank login pages	Leaks confidential information (in a South Korean nuclear power plant's case)
Purpose	File deletion from systems and fixed and remote drives	Control programmable logic controllers (PLCs)	Payment card data theft	Banking credential theft	Sabotage

Different weak points contributed to the breaches. In the Code Spaces case, attackers gained access to employee credentials to get inside the company's network. This could have been prevented through stronger password management policies and employee awareness training. Home Depot claimed that the attackers broke in using credentials stolen from a vendor. This finding highlights the importance of vetting the security practices of partner entities.[18] For Sony, custom defense could have given security defenders a means to detect an intrusion early on, as files are being accessed and deleted or sent outside the network.[19] To do that though, they should first know their baseline. They should know how their networks are configured and what the systems that comprise them contain so they can spot irregularities or clues of lateral movement.[20]

2014 Was the "Year of PoS RAM Scrapers"

PoS RAM scrapers came close to becoming a mainstream threat in 2014, as several high-profile targets lost millions of customer data to attackers.

High-profile targets across a wide variety of industries were hit by attacks aided by PoS RAM scrapers that allowed cybercriminals to get their hands on millions of customer data. Retailers were no longer the sole PoS system breach targets, as attackers also trailed their sights on hotels, restaurants, and parking lots, among others.[21–35]

Trend Micro data shows that the number of infected PoS systems in 2014 increased throughout the year. The infections were evenly distributed across countries as well.

Number of Systems Where PoS Malware Were Found in 2014
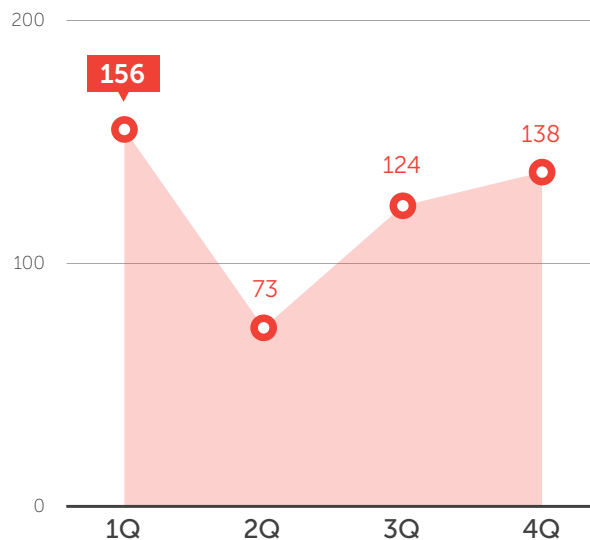
Country Distribution of Systems Where PoS Malware Were Found in 2014

● United States	29.77%
● Canada	6.71%
● United Kingdom	6.50%
● Australia	5.87%
● Philippines	5.66%
● Taiwan	3.98%
● France	3.14%
● Italy	3.14%
● Brazil	2.94%
● Japan	2.31%
● Others	29.98%
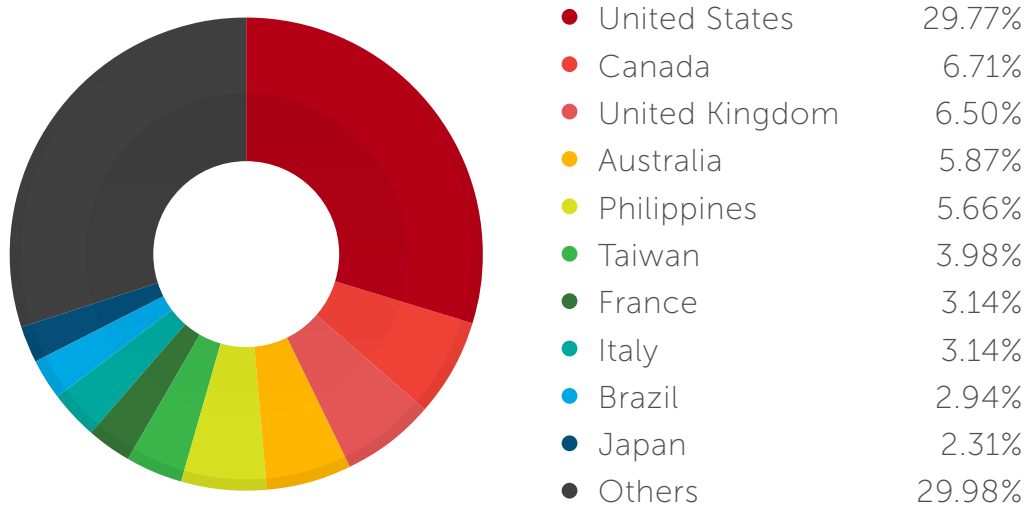
PoS Malware Family Distribution, 2013 Versus 2014

2014

2013

● Alina	55.39%
● Rdasrv	43.63%
● VSkimmer	0.98%
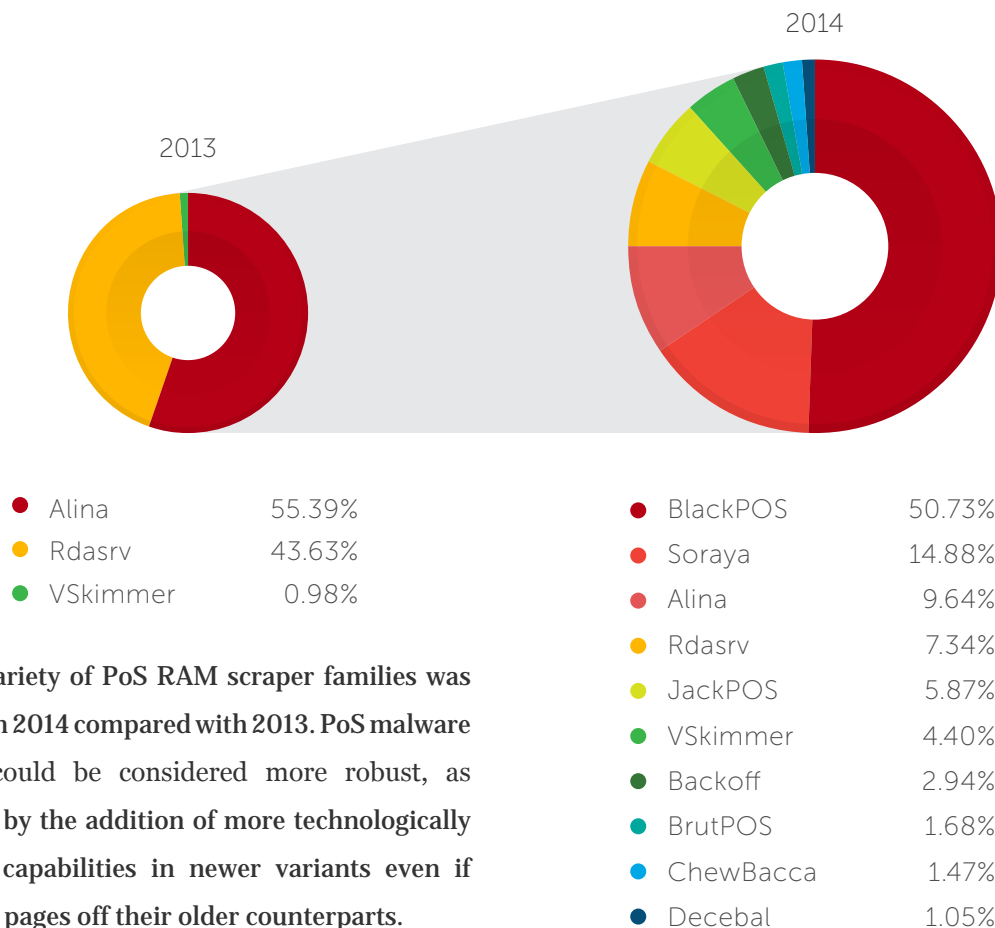
A wider variety of PoS RAM scraper families was also seen in 2014 compared with 2013. PoS malware creation could be considered more robust, as evidenced by the addition of more technologically advanced capabilities in newer variants even if these took pages off their older counterparts.

● BlackPOS	50.73%
● Soraya	14.88%
● Alina	9.64%
● Rdasrv	7.34%
● JackPOS	5.87%
● VSkimmer	4.40%
● Backoff	2.94%
● BrutPOS	1.68%
● ChewBacca	1.47%
● Decebal	1.05%

Timeline of PoS-RAM-Scraping Incidents in 2014, Including Damage

RETAIL
Payment card credentials of up to 40M customers

RETAIL
Credit card credentials of 350,000 customers, 9,200 of which were fraudulently used

HOTEL
Payment card numbers with security codes and expiration dates

BEAUTY
Track 2 payment card data with CVV numbers of <25,000 customers

RETAIL
Payment card credentials of approximately 2.6M customers

RESTAURANTS
Payment card credentials

RETAIL
Payment card information of customers from 335 shops

COURIER
Payment card data of customers from 51 locations

RETAIL
Payment card credentials

RETAIL
Payment card credentials of 56M and email addresses of 53M customers

RESTAURANTS
Payment card credentials of customers from 216 stores

RESTAURANTS
Payment card credentials of customers from 395 stores

RETAIL
Payment card numbers

PARKING
Payment card details of customers of 17 parking facilities

RETAIL
Payment card credentials of 1.16M customers

PARKING
Credit card credentials

RETAIL
Credit card credentials

RESTAURANTS
Payment card credentials

PARKING
Payment card credentials

Timeline labels: DEC 2013, JAN 2014, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC, JAN 2015

Cybercriminal underground markets across regions also proved that selling stolen data was indeed a lucrative business. Development kits specifically for PoS RAM scrapers, in fact, were seen in underground markets, most likely due to the success of PoS-malware-related attacks.[36–37]

Timeline of PoS RAM Scraper Emergence, Including Relationships with Other Versions

RawPOS	2009	Rdasrv
Alina	2010	BlackPOS
Dexter	2011	VSkimmer
Soraya	2012	ChewBacca
LusyPOS	2013	Decebal
JackPOS	2014	BlackPOS 2
Backoff	2015	BrutPOS
NewPoSThings		GetMyPass
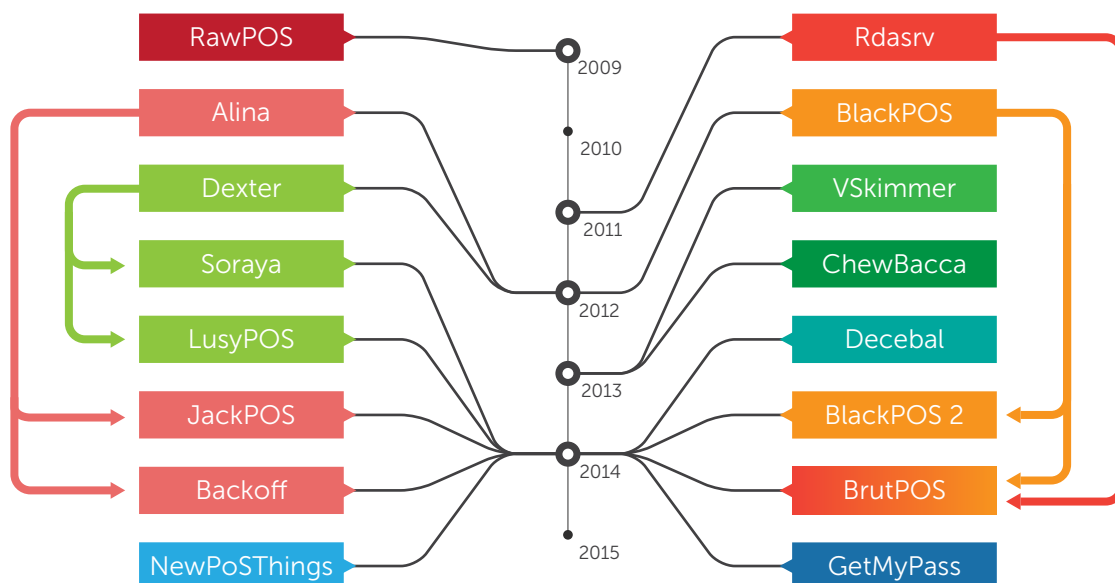
As cybercriminals prospered, however, businesses continued to suffer the consequences brought on by PoS malware attacks. Companies whose networks were successfully breached spent millions of dollars to rid their systems of the threat and, ultimately, regain their customers' trust. Though individuals and businesses in the United States suffered most from PoS threats, those from other countries like Canada and the United Kingdom were not spared as well. The United States is at particular risk of credit card fraud due to the low adoption of EMV technology within the country.

In response, the biggest financial institutions worldwide, including American Express, Visa, MasterCard, and Discover, have started shifting the liability from fraudulent transaction theft to merchants if these merchants do not adopt EMV payment terminals. Solutions like shifting to chip-and-pin or EMV cards, along with other reforms, have also been suggested. Properly implemented, EMV usage can make credit card fraud significantly harder to monetize.

Single-purpose systems like PoS devices were not readily thought to be targets by cybercriminals and threat actors but proved to be massively profitable if attacks against them succeed. This can signal increased interest in similar standalone equipment like industrial control systems (ICS) and SCADA-related devices as well.[38–41]

For retailers, hotels, restaurants, and other service providers that heavily rely on PoS systems in their day-to-day business, it will be worth examining the possible entry points that attackers can take advantage of. This also means that not only should these companies lock down PoS security through application control technology in order to limit the execution of programs to only those that PoS systems should be using, but companies should also look at the different parts of the entire network that attackers can breach. Technologies that provide advanced network security threat detection and real-time intelligence can increase the chances of detecting intrusions.
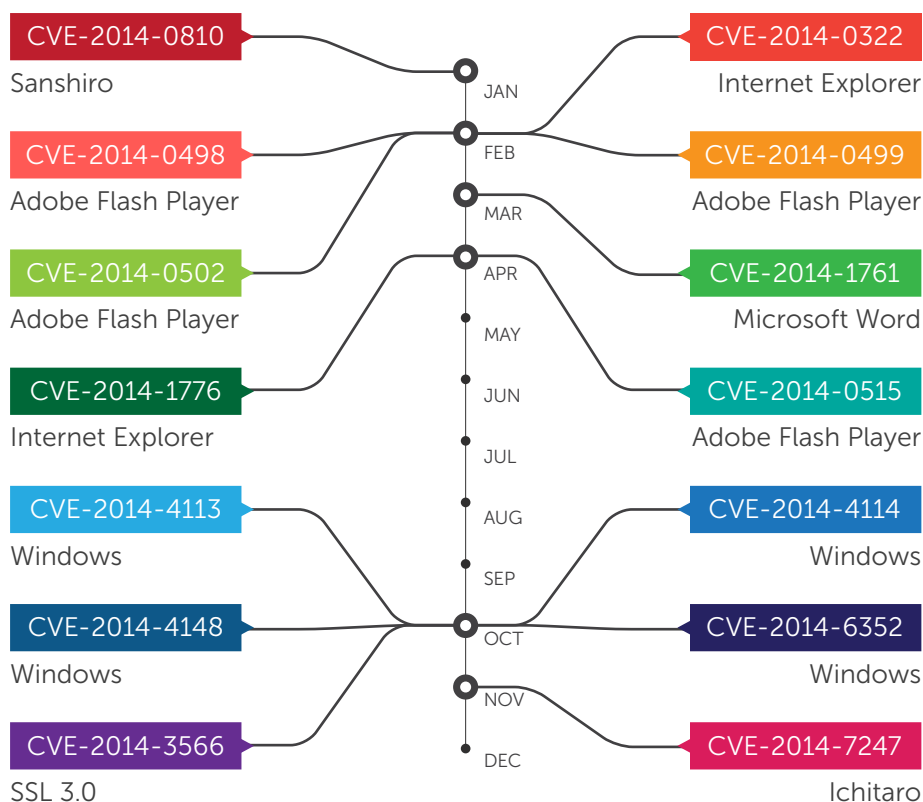
Heartbleed and Shellshock Proved That No Application Was Invulnerable

Software and platforms previously considered secure proved otherwise in 2014.

Though it was true that the number of major zero-day exploits declined in 2014 compared with previous years, the severity of the threats that surfaced did not diminish.[42] Gaping security holes that were left unpatched in widely used software and platforms continued to be exploited to instigate attacks that rendered targets defenseless.

Timeline of Major Zero-Day Vulnerabilities in 2014

CVE-2014-0810 Sanshiro	JAN	CVE-2014-0322 Internet Explorer
CVE-2014-0498 Adobe Flash Player	FEB	CVE-2014-0499 Adobe Flash Player
	MAR	
CVE-2014-0502 Adobe Flash Player	APR	CVE-2014-1761 Microsoft Word
	MAY	
CVE-2014-1776 Internet Explorer	JUN	CVE-2014-0515 Adobe Flash Player
	JUL	
CVE-2014-4113 Windows	AUG	CVE-2014-4114 Windows
	SEP	
CVE-2014-4148 Windows	OCT	CVE-2014-6352 Windows
	NOV	
CVE-2014-3566 SSL 3.0	DEC	CVE-2014-7247 Ichitaro

> *"No matter how many zero days or Heartbleed-/Shellshock-type vulnerabilities we may see, we should never forget that the fundamental vulnerabilities in Web applications such as SQL injection, cross-site scripting (XSS), broken authentication, etc., are still very prevalent. They are, quite often, the reason behind the big data breaches that occur. Also, we should never forget the best practices on controlling access to data, encrypting it as much as we can, ensuring the right security products are in place, quickly shielding against vulnerabilities."*
>
> **—Pawan Kinger**
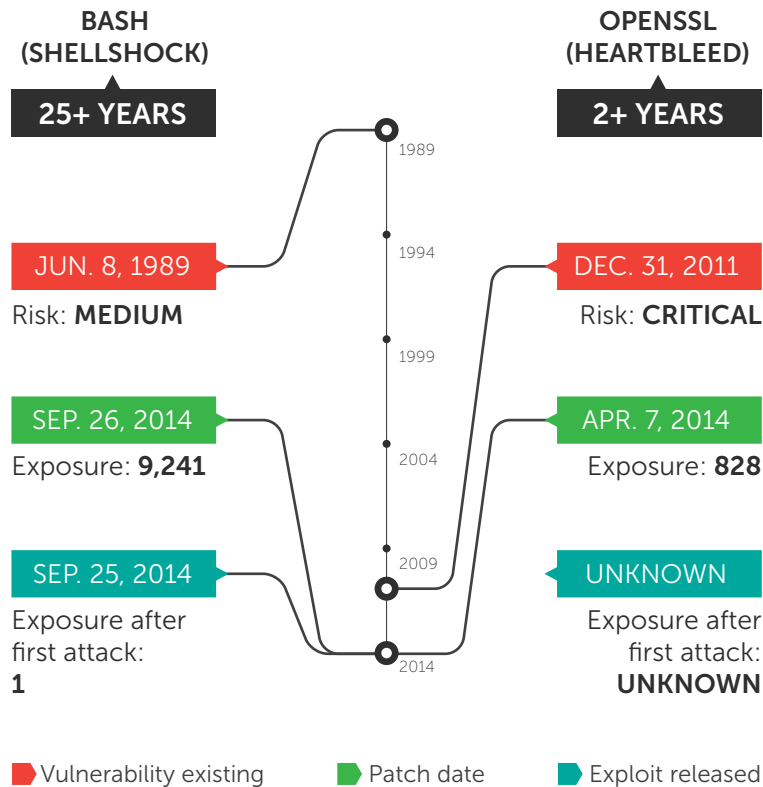> *Director of Deep Security Labs*

Applications initially thought more secure than those commonly exploited remained unpatched for years until two of the biggest exploits seen to date came to the fore.[43] Heartbleed and Shellshock proved that even open source applications, which were believed more secure than their commercial counterparts (e.g., Windows®, Adobe®, and Java™), were vulnerable to threats.[44] They particularly affected systems running Linux, which is concerning given that 67.7% of websites use UNIX. An overwhelming majority of supercomputers, which are primarily used by research facilities, academia, and other sectors that require ultra-fast computing power, use Linux as well.[45–46]

The fact that Linux is widely used as a server platform means Heartbleed and Shellshock put massive amounts of data at risk. If these servers are attacked, their owners could suffer crippling effects. Affected server owners would have to spend a lot of money paying staff to patch vulnerable systems. Patching could also cause system downtime, which could translate to revenue loss.

Open source initiatives can greatly benefit from a more stringent review process in keeping with quality assurance as part of a good software development life cycle. Because of the pervasive impact of these kinds of vulnerabilities, affected companies and individuals should consider vulnerability protection technologies that can provide virtual patches for vulnerable software before a vendor does so.

Comparison of Windows of Exposure of High-Profile Vulnerabilities Disclosed in 2014

BASH (SHELLSHOCK)

25+ YEARS

OPENSSL (HEARTBLEED)

2+ YEARS

1989

JUN. 8, 1989
Risk: **MEDIUM**

1994

DEC. 31, 2011
Risk: **CRITICAL**

1999

SEP. 26, 2014
Exposure: **9,241**

2004

APR. 7, 2014
Exposure: **828**

SEP. 25, 2014
Exposure after first attack:
1

2009

UNKNOWN
Exposure after first attack:
UNKNOWN

2014

■ Vulnerability existing   ■ Patch date   ■ Exploit released

# Online and Mobile Banking Faced Bigger Security Challenges

Operation Emmental proved that two-factor authentication was no longer enough to secure sensitive transactions, while online banking Trojans and malicious mobile apps continued to be a problem.

Online and mobile banking took off worldwide, especially in technologically advanced countries though steps to secure transactions were not able to keep pace.[47] Multifactor authentication has not yet been widely adopted.[48] Even users have yet to fully grasp the concept of securing their financial transactions. They still fall for social engineering lures cleverly crafted to trick them into giving out sensitive information like their account numbers, usernames, or passwords.

The convenience that online and mobile banking offers comes with risks. In fact, cybercriminals continuously devise ways to try to steal from bank customers. Those behind one particular operation we have dubbed "Emmental" have, in fact, even proven that two-factor authentication could be circumvented.[49]

Incremental increases month over month were seen in the number of online banking malware throughout the last quarter of 2014. Notorious online banking malware like ZeuS/ZBOT continuously lined cybercriminals' pockets with millions of dollars in stolen cash.[50] They have constantly been enhanced throughout the years to keep up with online banking security improvements. And this fact is not expected to change because online and mobile banking users, individuals and companies alike, constantly prove to be lucrative cybercrime targets.

## Number of Computers Where Online Banking Malware Were Found in 2014
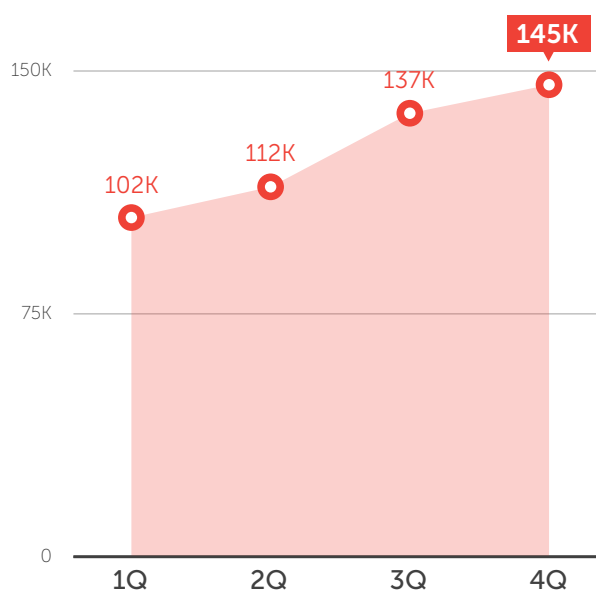
> "The malware that the attackers used revealed a weakness in single-session token protection strategies. Banks and other organizations that continue to use these are exposing themselves and their customers to rogue mobile apps. More advanced defenses, which include the use of multiple transaction authentication numbers (TANs), photo-TANs, and card readers, should be considered."

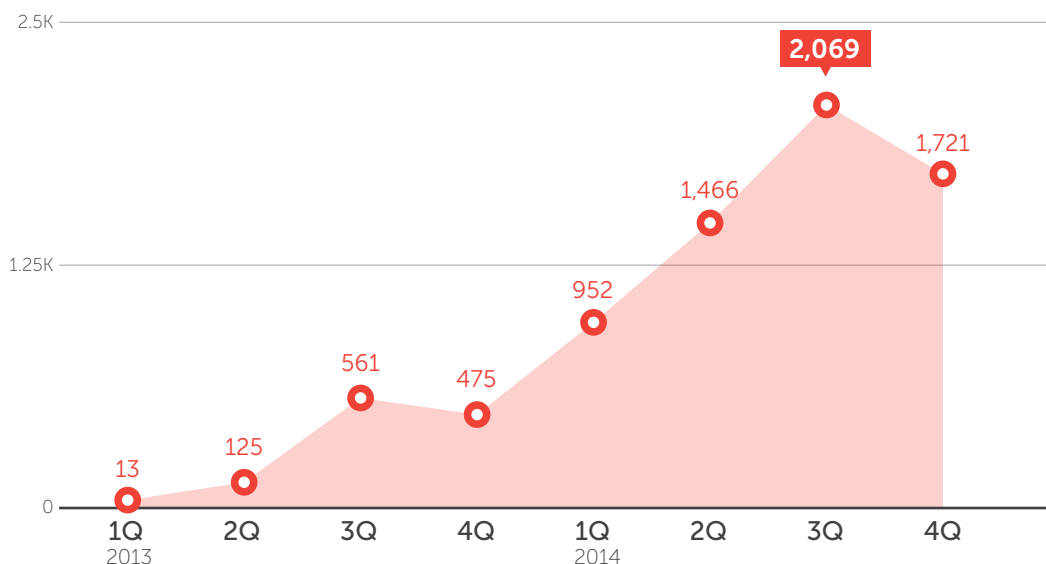**—David Sancho, Feike Hacquebord, and Rainer Link**

Senior Threat Researchers

Threats that ran on computers were not the only ones online and mobile banking users worried about though. They also had to stay protected from mobile malware and high-risk apps. Along with the increased adoption of mobile banking came more fake banking apps that aimed to steal not just users' banking credentials but also the money saved in their accounts. Case in point, the number of Android™ malware and high-risk apps continuously increased throughout 2014. A fourfold increase in the number of banking- or finance-related malware for the Android platform alone was also seen.

Cumulative Number of Android Malware in 2014

	1Q	2Q	3Q	4Q
	2.09M	2.68M	3.52M	4.26M
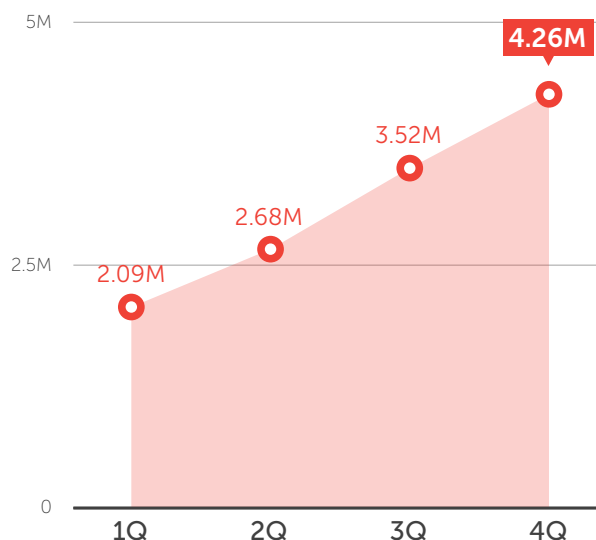
Number of Mobile Banking/Financial Malware

	1Q 2013	2Q	3Q	4Q	1Q 2014	2Q	3Q	4Q
	13	125	561	475	952	1,466	2,069	1,721

Note: *Banking-/Finance-related mobile apps refer to malicious apps that aim to steal victims' financial information. Examples of these are fake banking apps.*

Android users were not the only ones at risk though, as iOS threats also surfaced last year. Some examples of these were WireLurker and Masque, which could infect even nonjailbroken devices.

iOS Malware Count
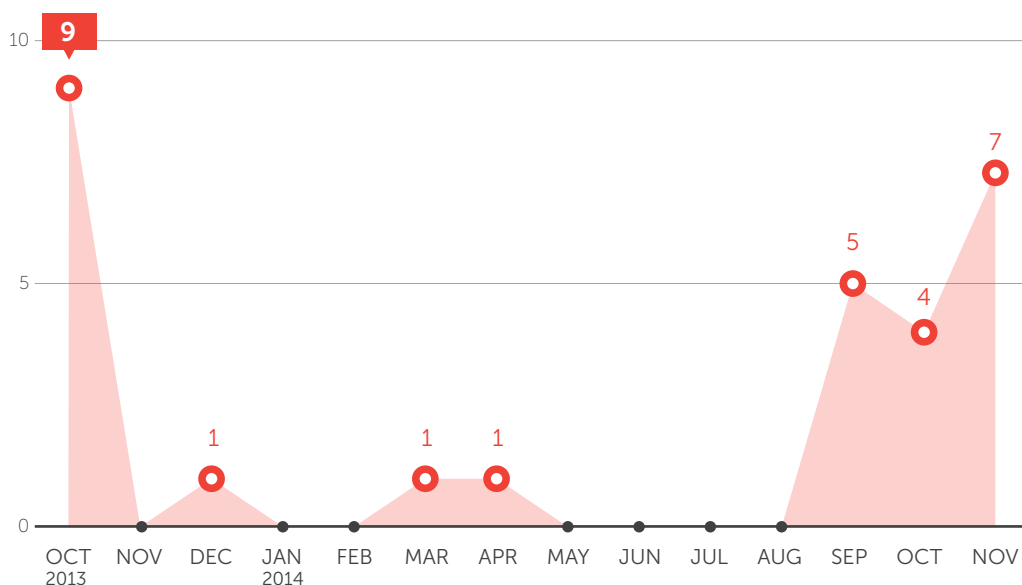
New mobile vulnerabilities like FakeID and SOP also caused security woes in 2014.[51–52] Bugs like FakeID could pass off malicious mobile banking apps as legitimate, which could lead to disastrous consequences.

Companies that end up as banking fraud victims stand to lose a lot of money if made to reimburse customers' stolen money in cases of qualified fraud. Even worse, they could lose their customers' trust if the latter do not feel they are as protected as they should be.[53]

Banks and other financial institutions should consider multifactor authentication in order to set more roadblocks against cybercriminals meaning to intercept bank-to-customer communication. Companies at risk should also be proactive in informing customers on how to improve their computer security—through the use of security software and good password management practices—if they have knowledge of attacks that are victimizing their or other banks' account holders.

As to users of mobile devices, only download applications from official app stores, and even then, take the time to check out the developer and read app reviews prior to download, whether the device used runs on Android or iOS.

Ransomware Became a Bigger and More Sophisticated Threat

Ransomware spread more malice across regions and segments. And unlike older variants, they no longer just issue empty threats but actually encrypt files.
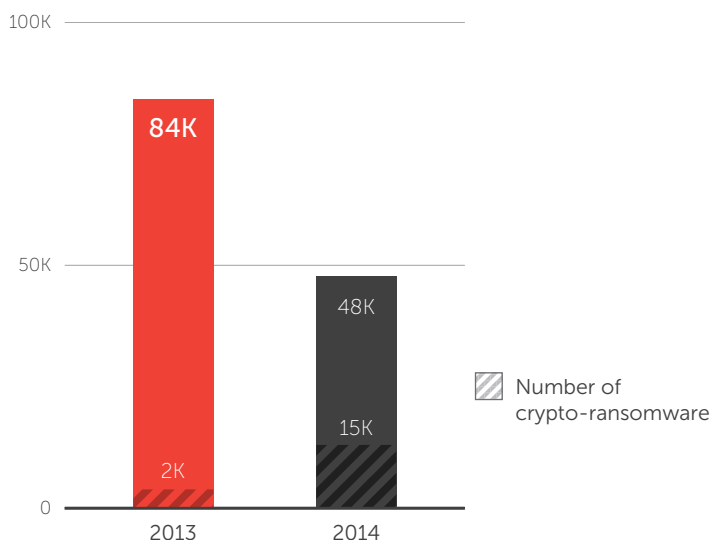
Ransomware, now capable of actually encrypting files held for ransom instead of just issuing empty threats, have crossed borders.[54–57] **They can now be found in Australia and New Zealand (ANZ) after spreading mayhem in Europe, the Middle East, and Africa as well as Japan. More recent variants of the threat have moved beyond focusing on a single segment as well, as perpetrators victimized consumers and small businesses alike.**

Although the number of detected ransomware declined from 2013 to 2014, related infections remained destructive. And while traditional ransomware like REVETON and RANSOM dominated 2013 with a 97% share, crypto-ransomware took the stage in 2014, as their share increased 27.35%.
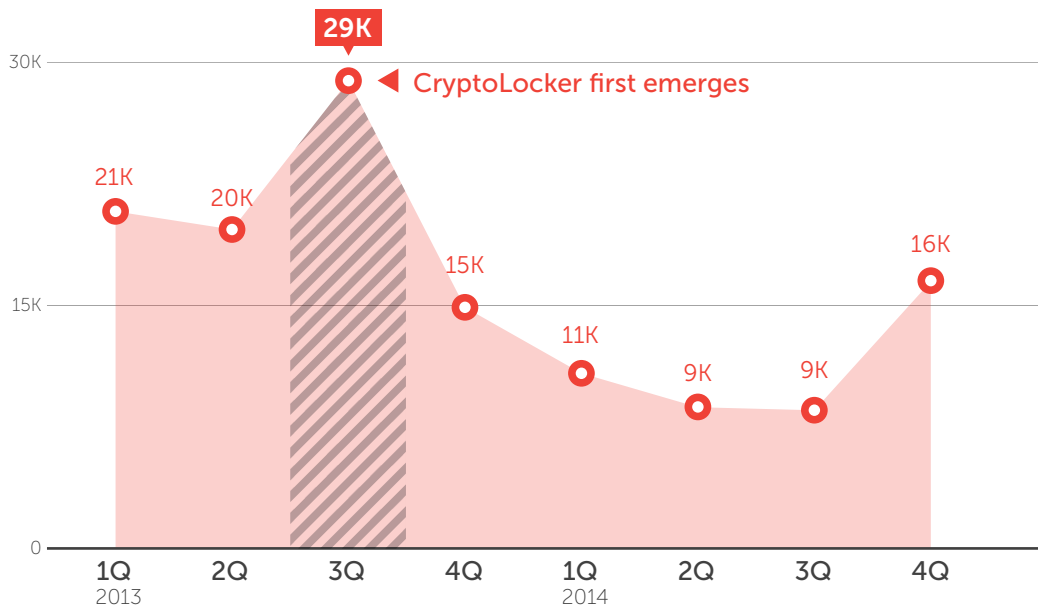
> *"While not presenting anything new to the table, CryptoLocker has taken the scare tactics effectively used before by ransomware and fake antivirus attacks to a new level. Most users rely nowadays on good antimalware, but it is important to note that user education, regular software updates, and strict computer usage policies are crucial in defending against CryptoLocker and similar threats."*
>
> **—Jay Yaneza**
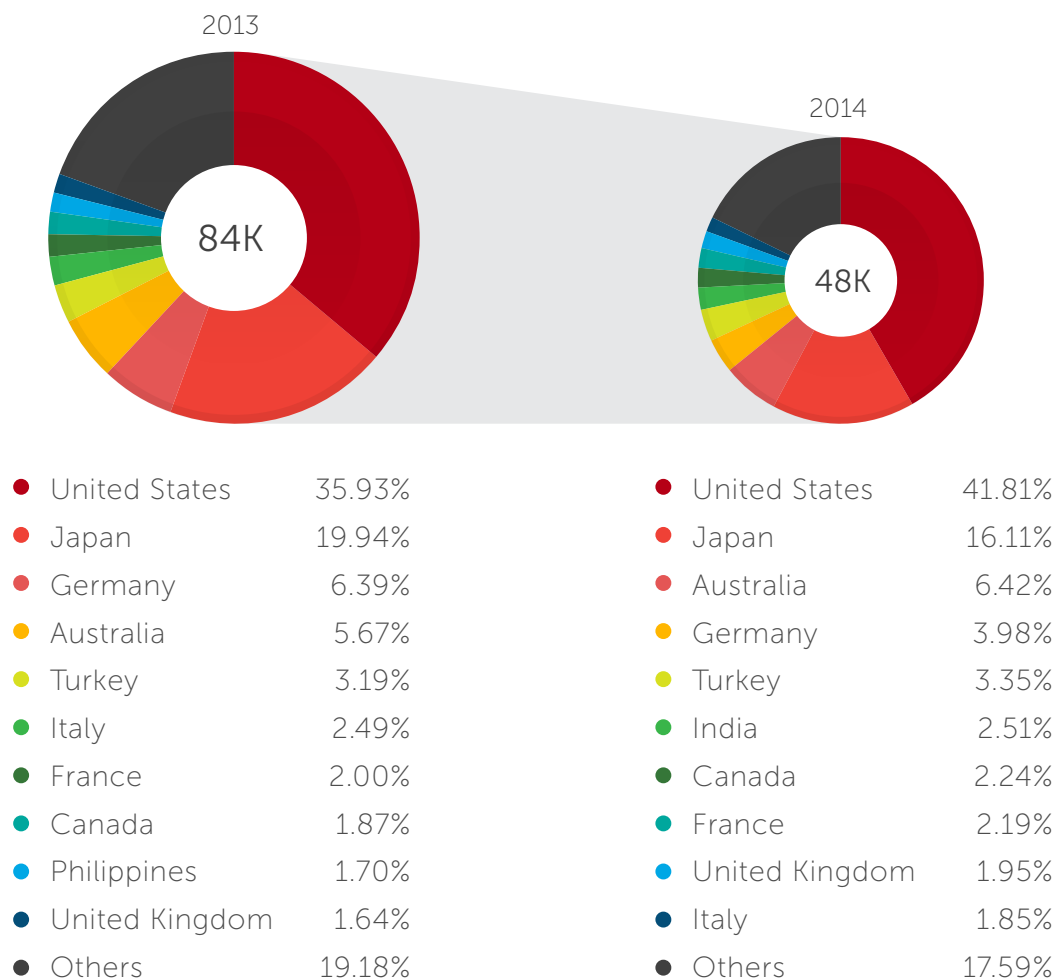> *Threat Analyst*

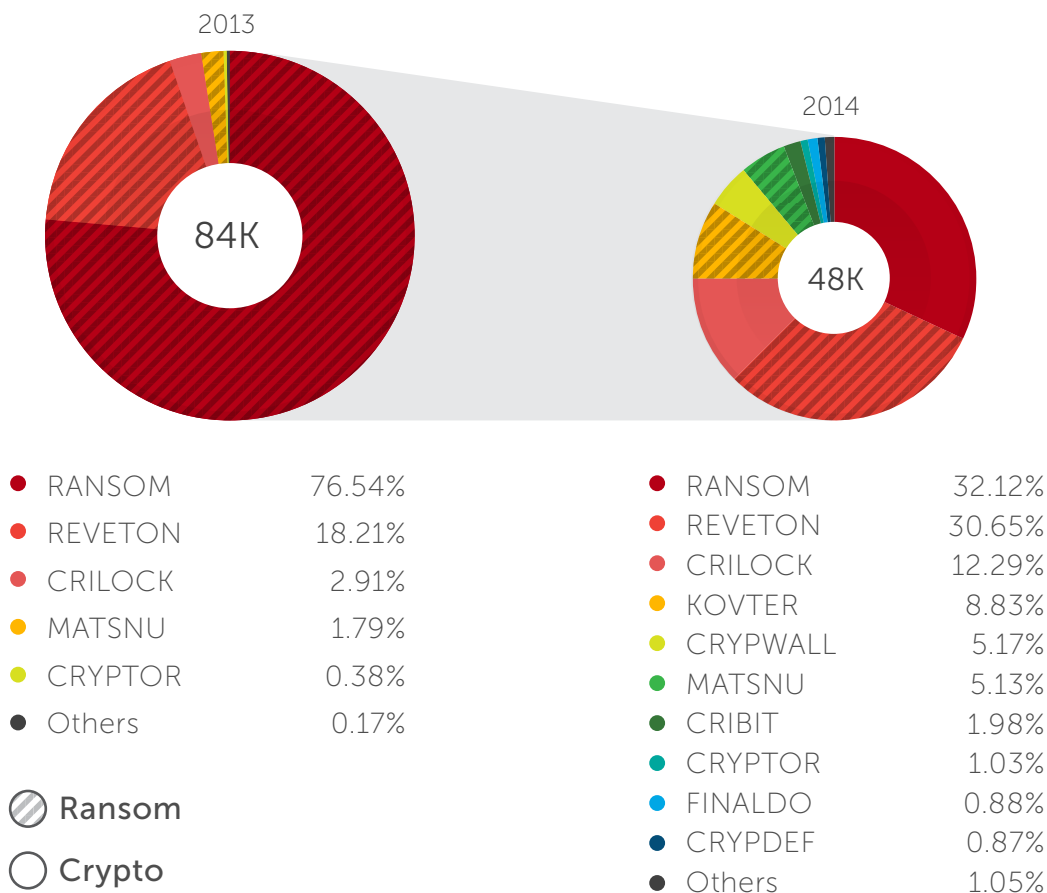## Number of Computers Where Ransomware Were Found, 2013 Versus 2014

Bar chart showing 2013: 84K total, 2K crypto-ransomware; 2014: 48K total, 15K crypto-ransomware. Legend: Number of crypto-ransomware.

Number of Computers Where Ransomware Were Found by Quarter

29K

CryptoLocker first emerges

30K
21K
20K
15K
16K
15K
11K
9K
9K
0

| 1Q | 2Q | 3Q | 4Q | 1Q | 2Q | 3Q | 4Q |
2013
2014

Country Distribution of Ransomware Detections, 2013 Versus 2014

2013

84K

2014

48K

United States	35.93%		United States	41.81%
Japan	19.94%		Japan	16.11%
Germany	6.39%		Australia	6.42%
Australia	5.67%		Germany	3.98%
Turkey	3.19%		Turkey	3.35%
Italy	2.49%		India	2.51%
France	2.00%		Canada	2.24%
Canada	1.87%		France	2.19%
Philippines	1.70%		United Kingdom	1.95%
United Kingdom	1.64%		Italy	1.85%
Others	19.18%		Others	17.59%

Ransomware Family Distribution, 2013 Versus 2014

2013

84K

2014

48K

● RANSOM	76.54%		● RANSOM	32.12%
● REVETON	18.21%		● REVETON	30.65%
● CRILOCK	2.91%		● CRILOCK	12.29%
● MATSNU	1.79%		● KOVTER	8.83%
● CRYPTOR	0.38%		● CRYPWALL	5.17%
● Others	0.17%		● MATSNU	5.13%
			● CRIBIT	1.98%
⊘ Ransom			● CRYPTOR	1.03%
○ Crypto			● FINALDO	0.88%
			● CRYPDEF	0.87%
			● Others	1.05%

The share of ransomware-infected systems in the United States, Australia, Turkey, India, Canada, France, and the United Kingdom increased from 2013 to 2014.

Comparison of Country Distribution of Ransomware Detections, 2013 Versus 2014

Country	2013	Country	2014	Change in Share
United States	35.93%	United States	41.81%	↑
Japan	19.94%	Japan	16.11%	↓
Germany	6.39%	Australia	6.42%	↑
Australia	5.67%	Germany	3.98%	↓
Turkey	3.19%	Turkey	3.35%	↑
Italy	2.49%	India	2.51%	↑
France	2.00%	Canada	2.24%	↑
Canada	1.87%	France	2.19%	↑
Philippines	1.70%	United Kingdom	1.95%	↑
United Kingdom	1.64%	Italy	1.85%	↓
Others	19.18%	Others	17.58%	Varies

(Australia)

(Spain)

CryptoLocker Acheter decryptage Decrypter un Fincher ^{gratuit} FAQ Soutien

Acheter decryptage et restaurer tous vos fichiers

Acheter decryptage pour **399 EUR** avant le **2014-11-30 2:49:10 AM**

OU acheter plus tard avec le prix de **799 EUR**

Temps restant avant augmentation de prix: **0**

Vos fichiers chiffres au total: **33976**

Prix actual: **2.98826 BTC (environ 799 EUR)**

Paye: **0 BTC (environ 0 EUR)**

Restant a payer: **2.98826 (environ 799 EUR)**

ACHETEZ-LE MAINTENANT! Garantie de 100% de la restauration de fichiers ✔

Acheter Decryptage avec ₿bitcoin

1 **Creer bitcoin portefeuille**

Vous devez vous inscrire Bitcoin portefeuille, svoir les intructions faciles ou regarder des video sur YouTube.

(France)

CryptoLocker Acquista decrittografia Decrittografare File ^{libero} FAQ Supporto

Acquista derittazione e ripristinare i file

Acquista decrittazione per **398 EUR** prima **2014-11-30 2:45:35 AM**

O acquistare in un secondo momento con il prezzo di **798EUR**

Tempo rimasto prima aumento dei prezzi: **0**

Numero di file crittografati: **16147**

Prezzo corrente: **2.98452 BTC (circa 798 EUR)**

Pagato: **0 BTC (environ 0 EUR)**

Rimanendo a pagare: **2.98452 (circa 798 EUR)**

Compralo Subito! 100% garanzia di ripristinare 1 file ✔

Acquista decifratura con ₿bitcoin

1 **Registrati bitcoin wallet**

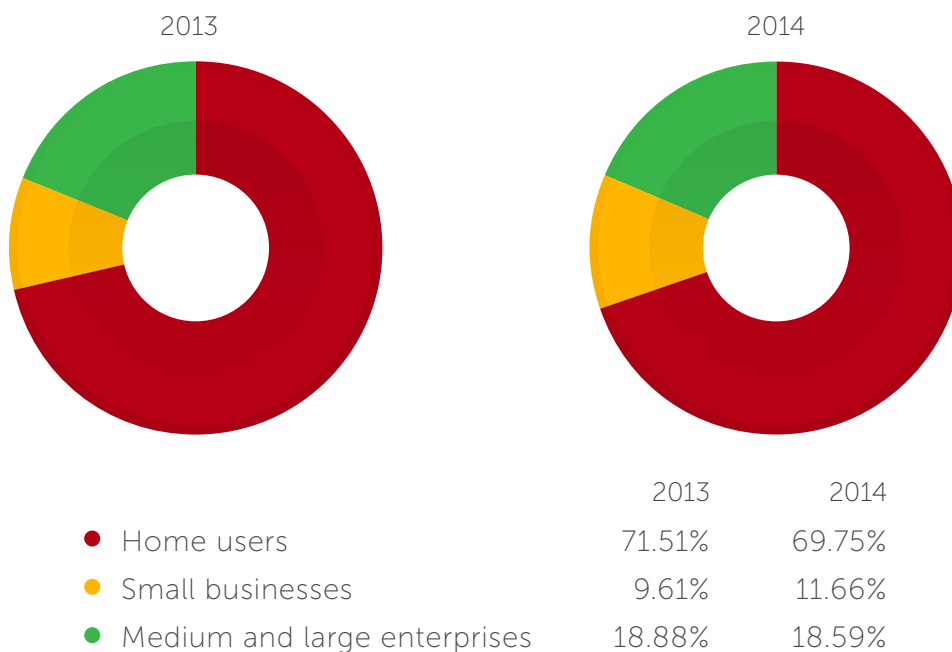Si dovrebbe registrare Bitcoin waller, vedi semplici istruzioni o gurdare i video su YouTube.

(Italy)

**CryptoLocker**   Acquista decrittografia   Decrittografare File ^libero^   FAQ   Supporto

kaufen entschlusselung und wiederherstellung ihrer dateien

Kaufen Entschlusselung fur **398 EUR** bevor **2014-11-30 2:45:35 AM**
oder kaufen Sie es spater mit dem Preis von **798EUR**

Verbleibende Zeit bis sum Preisansrieg: **0**

Anzhal von verschlusselten Dateien: **16147**

Aktueller Preis: **2.89674 BTC (rund 798 EUR)**

Bezhalt: **0 BTC (rund 0 EUR)**

Verbleibende zu zahlen: **2.89674 (rund 798 EUR)**

KAUFE ES JETZT! 100% Garantie der Wiederherstellung von Datein ✓

Kaufen Entschlusselung mit ₿ **bitcoin**

① **Registrieren Bitcoin Wallet**

Sie solten Bitcoin Wallet registrieren, siehe einfachen Anweisungen oder Videos absielen auf YouTube.

(Germany)

Ransomware Segment Distribution, 2013 Versus 2014

2013   2014

	2013	2014
● Home users	71.51%	69.75%
● Small businesses	9.61%	11.66%
● Medium and large enterprises	18.88%	18.59%

A similar increase, specifically toward the end of 2014, in the number of ransomware infections was seen in the mobile landscape. Apart from widening their target base, ransomware also evolved to ensure the anonymity of their operators by requiring victims to pay in Bitcoins and other cryptocurrencies.

Mobile Ransomware Count
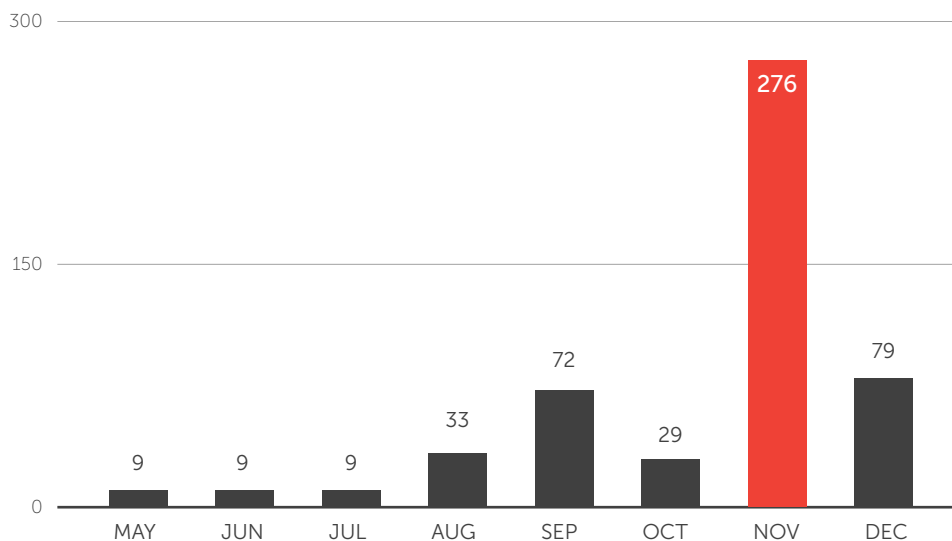
Unfortunately for home users and employees who encounter ransomware, prevention is the best route that will save them from having to pay ransom. It is important to keep the following tips in mind:

• Avoid clicking suspicious links.

• Back up important data using the 3-2-1 rule.[58]

• Check the email sender.

• Double-check the message content.

• Ensure that security software is updated.

Threat Actors and Cybercriminal Economies Continued to Thrive Worldwide

Threat actors are no longer associated with a single country, as evidenced by targeted attacks like Operation Pawn Storm.

We have been tracking developments in the cybercriminal underground economy to better understand cybercrime motivations. Unsurprisingly, financial profit is the biggest if not the sole driver of the different cybercriminal hubs springing up around the world. Like any developing real-world economy, the cybercriminal underground thrives on constantly improving specializations and activities related to setting up and running cybercriminal operations.

On one hand are suppliers of products and services—blackhat developers of Trojan builders and distributed denial-of-service (DDoS) tools as well as owners of massive credit card dumps—while on the other are buyers with specific needs who can choose from among different vendors. Throughout the years, the prices of different underground products and services have been influenced by market forces—as the supply increases, prices decrease.

Credit Card Prices in the Russian Cybercriminal Underground by Year
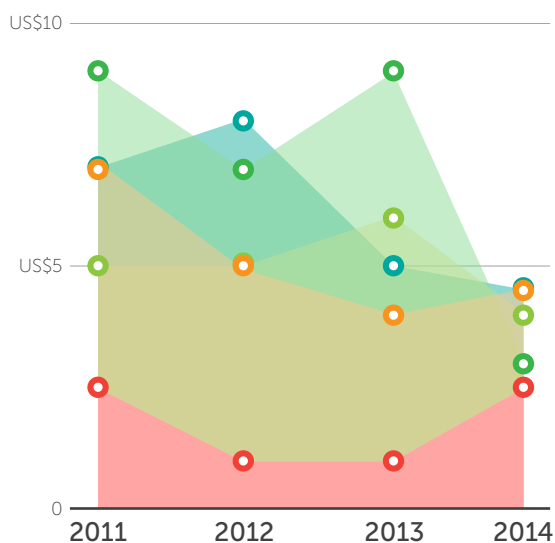
	2011	2012	2013	2014
USA	US$2.50	US$1.00	US$1.00	US$2.50
AUS	US$7.00	US$5.00	US$4.00	US$4.50
CAN	US$5.00	US$5.00	US$6.00	US$4.00
GER	US$9.00	US$7.00	US$9.00	US$3.00
UK	US$7.00	US$8.00	US$5.00	US$4.50

While several commonalities among regional cybercriminal underground markets exist, each tends to develop in slightly different ways. The Russian underground, for instance, is notorious for trading traffic direction systems (TDSs) and pay-per-install services—business models that drive the volume of grayware and adware in victims' computers upward, alongside commissions. The Chinese cybercriminal underground, meanwhile, is much more fixated on mobile fraud, with hardware setups that can send SMS spam to thousands of potential victims in under an hour. Finally, the Brazilian underground is known for phishing banks and, more notably, a 10-module training course for cybercriminal newbies on how to commit fraud.

Most of the cybercriminal communications on the surface Web are relatively well-hidden through the use of forums or encrypted social media posts. However, anonymity is such a key factor in a cybercriminal's longevity in the business that the use of darknets in the Deep Web has become significant as well. After the Silkroad takedown in 2013, in fact, a lot of players were expected to try and take the place of Dread Pirate Roberts. Different marketplaces emerged in 2014 while law enforcement played cat and mouse with unsearchable websites as in an operation called "Operation Onymous," which brought down 17 alleged operators.[59] Cryptocurrencies also play a large role in the Deep Web, and in 2014 we saw

a new cryptocurrency called "Cloakcoins," which, unlike Bitcoins, offer complete untraceability of the transaction chain.[60]

Even in the clandestine world of targeted attack campaigns launched by a different breed of threat actors, the emergence of international players was evident. While cybercriminals primarily pursued monetary profit, threat actors worldwide realized the value of stealing corporate data, intellectual property, and other trade secrets. The diversity of targets and locations of targeted-attack-related command-and-control (C&C) servers do not suggest a single dominant player when it comes to espionage. Targets as diverse as telecommunications companies, manufacturing firms, governments, and media outfits continued to be seen. Campaigns like Regin targeted victims in Belgium; Operation Pawn Storm in the United States, Hungary, and Austria; and Plead in Taiwan.

Companies assessing their risk levels should take into account all kinds of possible intruders, including those who target them across the planet. As cybercrime becomes more attractive to the unscrupulous and as targeted attack campaigns become much easier to mount, the pressure to reassess the breadth and quality of cybersecurity investments must only intensify.

> *"Operation Pawn Storm used next-level spear-phishing tactics to obtain the email credentials of primarily military, embassy, and defense contractor personnel from the United States and its allies. The threat actors used a mix of spear-phishing emails and specially crafted Webmail service phishing websites to gain access to victims' inboxes in hopes of getting better footholds inside target organizations."*
>
> **—Loucif Kharouni, Feike Hacquebord, Numaan Huq, Jim Gogolinski, Fernando Mercês, Alfred Remorin, and Douglas Otis**
>
> *Senior Threat Researchers*

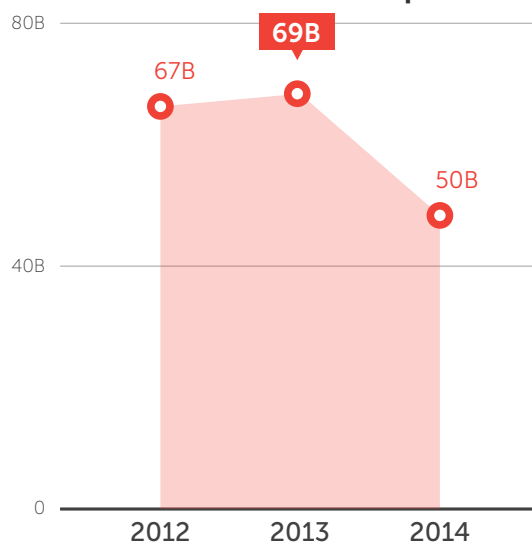# Overall Threat Volumes Decrease, but Phishing Almost Doubles

Trend Micro Smart Protection Network telemetry showed a general decrease in the volume of threat components like malicious domains and spam, but malware continued to be important tools in cybercriminal operations. Phishing sites almost doubled in number this year.

Quality over quantity was a resounding theme in the 2014 threat landscape, reflected in part by the overall volume of malicious components we identified and blocked throughout the year. **Web threats largely remained multicomponent in nature.** However, as security events proved, attackers continued to fine-tune their strategies even if these were not original to obtain not just **more victims but more desirable ones.**

### Number of Email Reputation Queries Blocked as Spam

Blocking spam-sending IP addresses is a crucial step in breaking infection chains. Emails haphazardly sent to huge mailing lists remained part of the threat landscape, albeit as white noise. Trend Micro spam filters were able to easily weed them out though, as we detected 50 billion **email reputation queries—slightly lower than the numbers seen in 2012 and 2013 but still fairly significant**—as spam.

Volume of Spam Blocked by Messaging Products

We were also able to block spam based on content, **alongside the reputation of the sender. Based on** data from Trend Micro messaging products, the volume of spam tended to be stable, with a slight **uptick in the third quarter of 2014.**
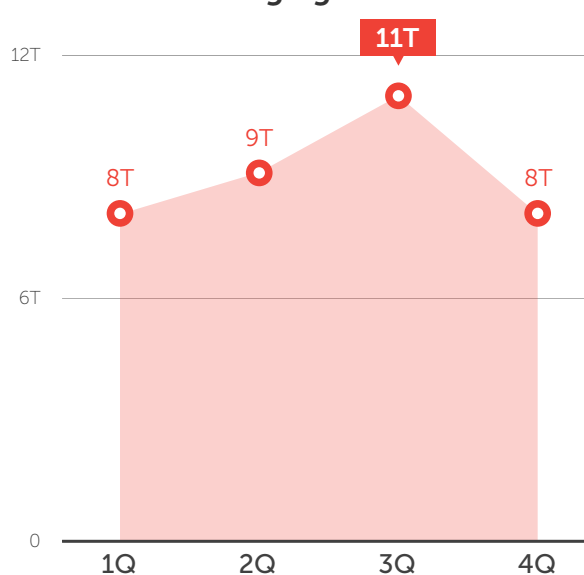
Note: This data set is from Trend Micro messaging product feedback.

Top 10 Spam Languages in 2013 and 2014

2013

2014
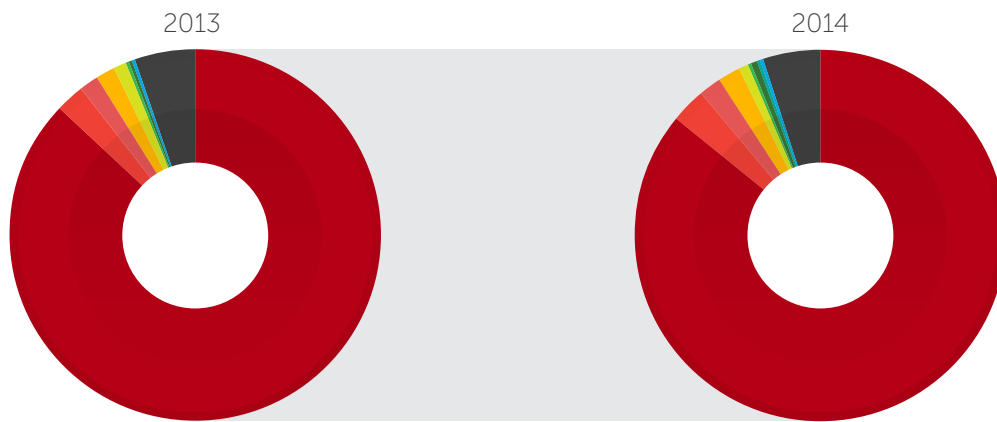
	English	87.14%
	Chinese	2.36%
	Japanese	1.84%
	German	1.48%
	Russian	1.20%
	Portuguese	0.28%
	Spanish	0.21%
	Icelandic	0.12%
	Italian	0.10%
	French	0.10%
	Others	5.17%

	English	85.84%
	German	3.29%
	Japanese	1.87%
	Chinese	1.84%
	Russian	0.85%
	Portuguese	0.41%
	Polish	0.37%
	Spanish	0.32%
	French	0.29%
	Italian	0.12%
	Others	4.80%

English remained spammers' most preferred language even though its overall share decreased from 2013's 87.14%. This means we saw slightly more non-English spam in 2014. Among the non-English spam, those written in German topped the list, toppling Chinese and Japanese.

Top Spam-Sending Countries, 2013 Versus 2014

2013

2014
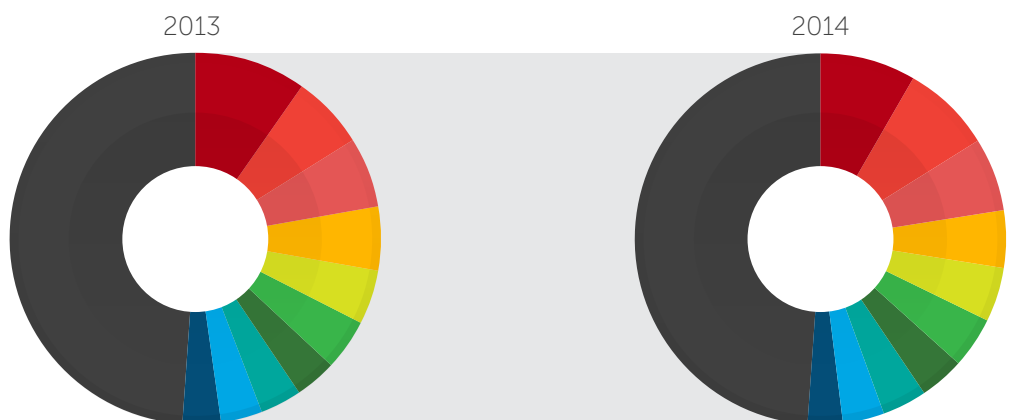
United States	9.91%
Spain	6.29%
India	6.26%
Argentina	5.37%
Italy	4.87%
Taiwan	4.38%
Colombia	3.69%
China	3.53%
Peru	3.53%
Mexico	3.29%
Others	48.88%

| United States	8.37%
Spain	7.89%
Argentina	6.35%
Italy	5.00%
Germany	4.84%
Vietnam	4.27%
Iran	3.95%
China	3.90%
Russia	3.58%
Colombia	3.19%
Others	48.66%

The United States and Spain were the most active spam senders, as in 2013, despite posting relatively smaller shares. A spike in the salad spam volume was seen in Spain, Germany, Italy, and Iran, which could have further contributed to the 2014 spam language distribution.[61]

Spammers also made full use of other channels like social networking sites in 2014 with the same end goal—to get as many valuable clicks as possible. For instance, in our investigation of Twitter abuse, we saw how attackers can use social platforms to lure people.[62] Webmail clients also helped spammers slip through spam filters because network communications were likely encrypted.

This is precisely why the ability to block malicious URLs, IP addresses, and domains is critical to an enterprise's security arsenal. Should a spam slip through or use social media or Webmail, URL-blocking technology should be able to catch a user's wayward click before it accesses a malicious remote location.

URLs can serve as phishing landing pages, redirectors, malware download locations, and thus are the lifeblood of any cybercriminal operation. In 2014, we were able to block close to 4 billion user queries from accessing malicious sites, or up to 7,000 clicks per minute.
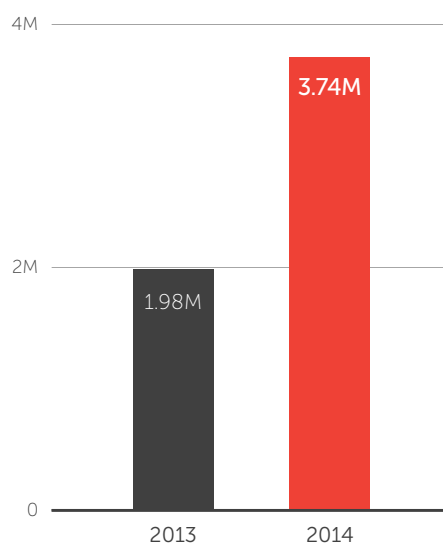
User Visits Blocked from Accessing Malicious Sites
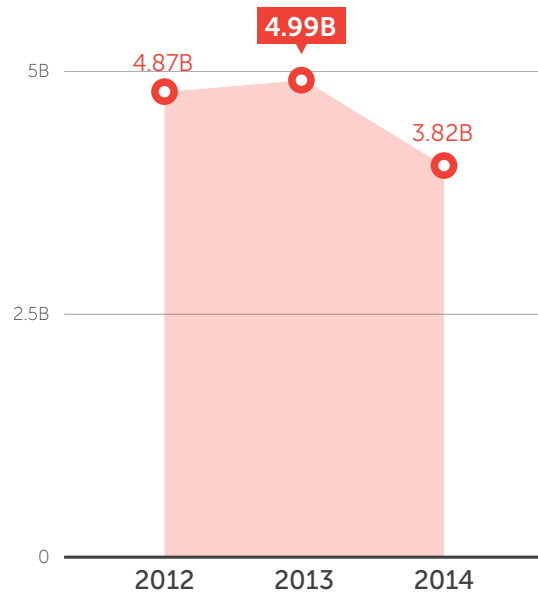
Despite what appears to be a decline in the number of malicious sites, the volume of phishing sites continued to grow. We observed an 88.65% increase in the number of phishing sites in 2014. Bulk creation of new domains with one-year registration was easy and as cheap or even cheaper than renewal. Website -creation or ready-made website templates were also available underground.

Volume of Phishing Sources, 2013 Versus 2014

Of the malicious URLs we blocked, the top ones were related to malicious sites known for serving malware.

Top Malicious Domains Users Were Blocked from Visiting in 2014

Malicious URL Blocked	Reason for Blocking
ads.alpha00001.com:80/cgi-bin/advert/getads.cgi	Has multiple records related to malware-download/spam sites
ody.cc:80/vip48.html	Has multiple records related to malware-download/spam sites
interyield.jmp9.com:80/interyield/bindevent.do	Exhibits malicious behaviors
directxex.com:80/uploads/698118324.server.exe	Related to WORM_AUTORUN.BMC
flyclick.biz:80/click	Used in exploit kits
sp-storage.spccint.com:80/autoupdate/2.11.11.7/autoupdate.zip	Exhibits malicious behaviors
upload.mobogenie.com:80/mu/release/mobogenie2.2.1.zip	Detected as ADW_NEXTLIVE
www. advconversion.com:80/ads-conversiontrack/conversion/set.do	Exhibits malicious behaviors
ads.alpha00001.com:80/cgi-bin/advert/getkws.cgi	Exhibits malicious behaviors
ody.cc:80/vip53.html	Exhibits malicious behaviors

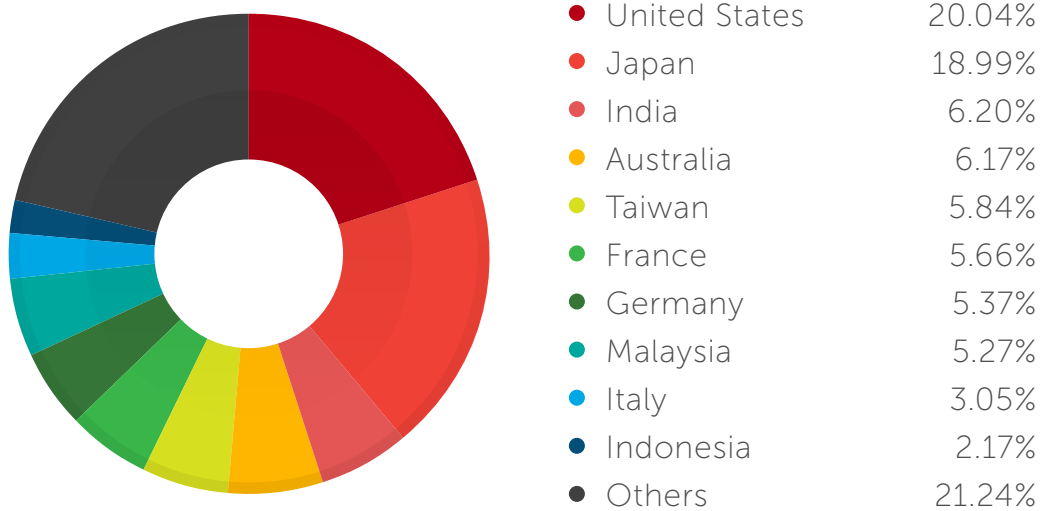As in 2013, the United States had the highest number of C&C servers related to botnet activities, followed by the United Kingdom and India. Note, however, that the threat actors or attackers did not **necessarily reside in the said countries because C&C servers can be remotely managed.**

Country Distribution of C&C Servers in 2014
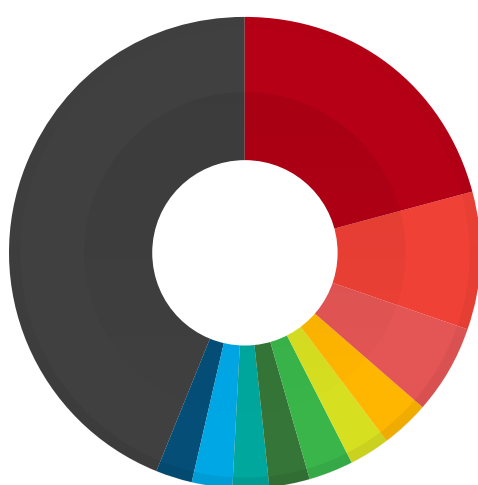
● United States	21.08%
● United Kingdom	9.45%
● India	6.11%
● Brazil	3.14%
● Iran	2.94%
● Germany	2.86%
● Russia	2.85%
● Ukraine	2.63%
● Netherlands	2.60%
● Romania	2.47%
● Others	43.87%

Country Distribution of C&C Connections in 2014

|		
●	United States	20.04%
●	Japan	18.99%
●	India	6.20%
●	Australia	6.17%
●	Taiwan	5.84%
●	France	5.66%
●	Germany	5.37%
●	Malaysia	5.27%
●	Italy	3.05%
●	Indonesia	2.17%
●	Others	21.24%

Zombie computers were broadly distributed across countries though the United States, Japan, and India topped the list.

Should spam and URL filters fail to block threats, **security solutions should be able to identify** whether an unknown file is likely to be malicious or not based on its source's reputation or its content and behaviors. In 2014, Trend Micro blocked 10 billion requests to access or download malicious files, almost twice the number recorded in 2013. Around 21,000 file reputation queries per minute turned out to be malicious.

Number of Malicious Files Blocked
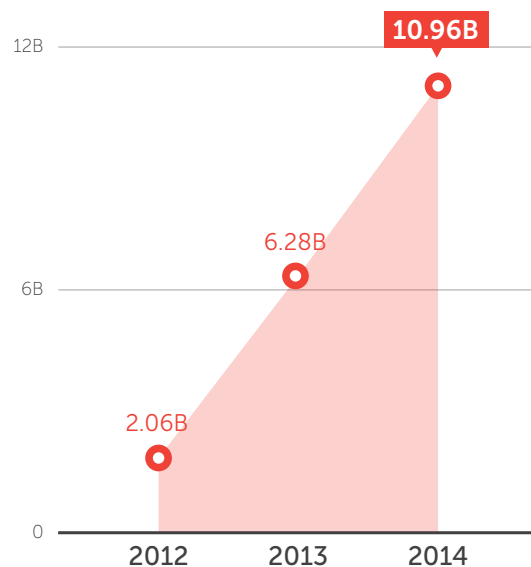
DOWNAD continued to be the top enterprise infector. This could be att ributed to the fact several companies still use Windows® XP, which is vulnerable to this threat, especially since Microsoft has ceased supporting the OS.

As attacks and attacker tools and tactics continue to improve, enterprises must ensure they use multilayer solutions that can better catch threats before these reach user endpoints.
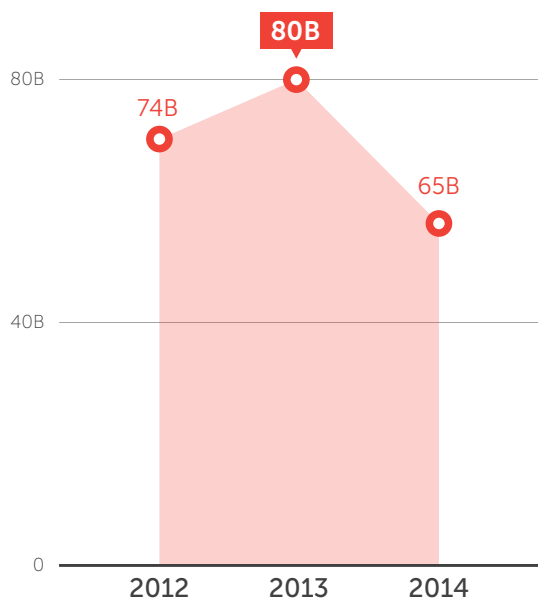
Top Malware and Adware in 4Q 2014
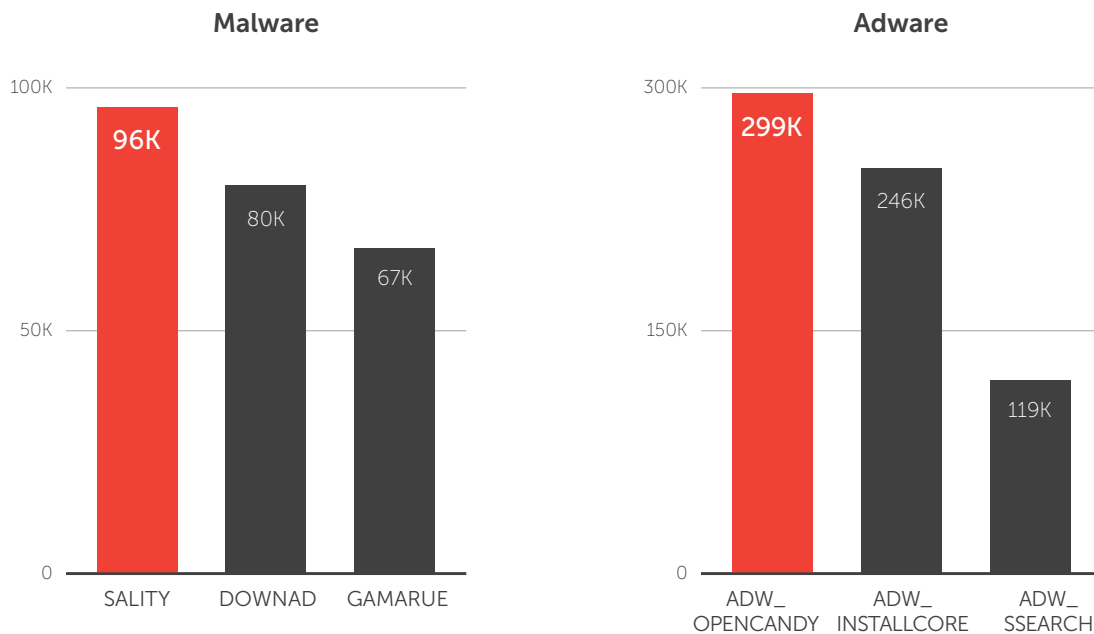
Malware

Adware


Computers Affected by Malware

Medium and Large Enterprise

Small Business

Home
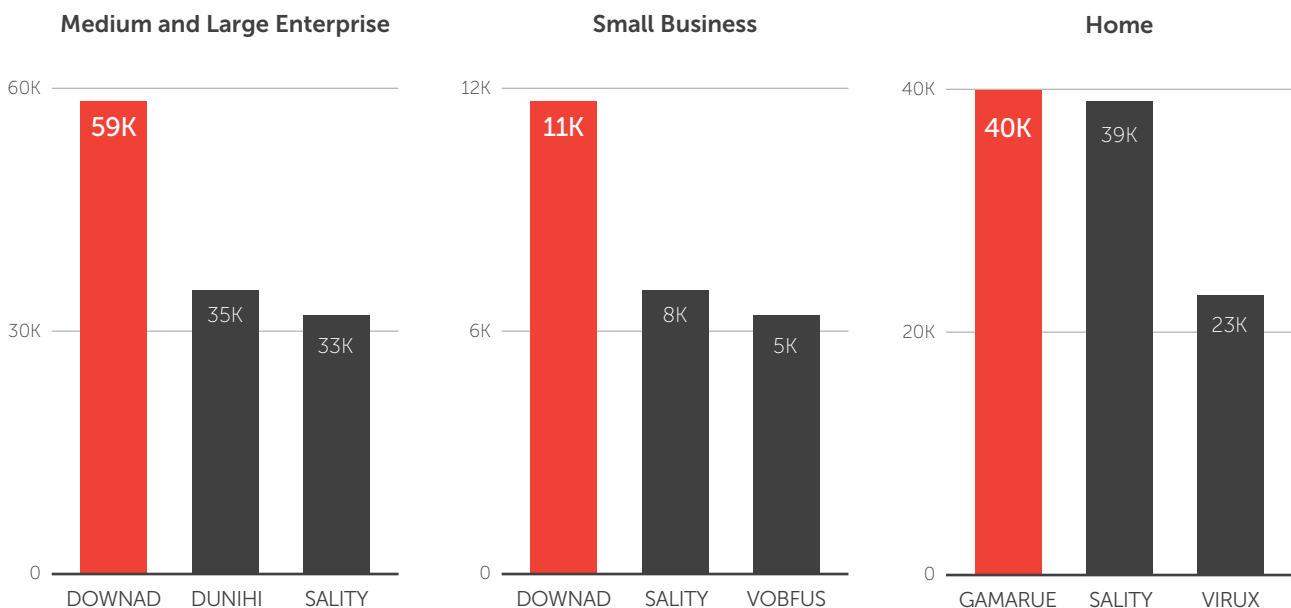
MALWARE/ADWARE FAMILY	BEHAVIOR	DAMAGE POTENTIAL
ADW_INSTALLCORE	Freeware-bundled toolbars	Medium
ADW_OPENCANDY	Adware that comes bundled with third-party application installers	Medium
ADW_SSEARCH	Bundled with malware packages as a component	Low
DOWNAD	Worm with multiple routines to spread, blocks access to security vendor sites, downloads malware	Critical
DUNIHI	Worm that arrives via spam or malicious sites, turns computers into bots	Medium
GAMARUE	Worm, turns computers into bots, spreads through link files, hides files	Medium
SALITY	File infector, spreads by infecting. EXE and .SCR files and removable drives, downloader	High
VIRUX	File infector downloaded from crack-download sites, spreads by infecting various file types, downloads FAKEAV, etc.	High
VOBFUS	Worm, uses autorun to infect drives, downloads FAKEAV, etc., polymorphic	High

Total Number of Threats Blocked

80B
74B
65B
80B
40B
0
2012 2013 2014

Annual Detection Rates

2,546
2,337
2,065
2,600/s
1,300/s
0
2012 2013 2014
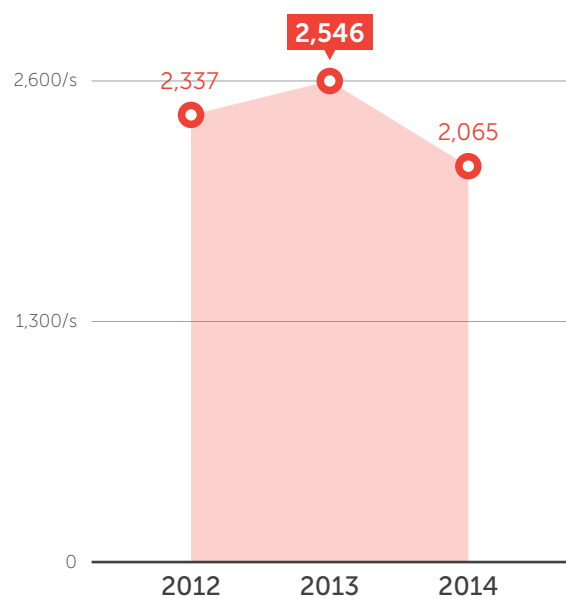
References

1. Trend Micro Incorporated. (2013). *Trend Micro Security News.*
    "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed on 29 January 2015,
    http://about-threats.trendmicro.com/us/security-predictions/2014/blurring-boundaries/.

2. Lewis Morgan. (23 December 2014). *IT Governance.*
    "List of Cyber Attacks and Data Breaches in 2014." Last accessed on 29 January 2015,
    http://www.itgovernance.co.uk/blog/list-of-the-hacks-and-breaches-in-2014/.

3. Trend Micro Incorporated. (2014) *Trend Micro Security News.*
    "Turning the Tables on Cyber Attacks." Last accessed on 9 February 2015,
    http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf.

4. "Report and Response Regarding Leakage of Customers' Personal Information." (10 September 2014). Last accessed on 17 February 2015,
    http://blog.benesse.ne.jp/bh/en/ir_news/m/2014/09/10/uploads/news_20140910_en.pdf.

5. Trend Micro Incorporated. (8 December 2014). *Trend Micro Security News.*
    "The Hack of Sony Pictures: What We Know and What You Need to Know." Last accessed on 29 January 2015,
    http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know.

6. Reuters. (9 December 2014). *Fortune.*
    "Cyber Attack Could Cost Sony Studio as Much as $100 Million." Last accessed on 29 January 2015,
    http://fortune.com/2014/12/09/cyber-attack-could-cost-sony-studio-as-much-as-100-million/.

7. Steve Tobak. (18 December 2014). *Fox Business.*
    "3 Revelations from the Sony Hack." Last accessed on 29 January 2015,
    http://www.foxbusiness.com/technology/2014/12/18/revelations-from-sony-hack/.

8. Andrea Peterson. (5 December 2014). *The Washington Post.*
    "Why It's So Hard to Calculate the Cost of the Sony Pictures Hack." Last accessed on 29 January 2015,
    http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack/.

9. The Associated Press and Bloomberg. (18 December 2014). *TheStar.com.*
    "Sony Hacker Attack Will Cost Company Tens of Millions of Dollars." Last accessed on 29 January 2015,
    http://www.thestar.com/business/2014/12/18/sony_hacker_attack_will_cost_company_tens_of_millions_of_dollars.html.

10. Adam Clark Estes. (9 December 2014). *Gizmodo.*
    "Why Sony Keeps Getting Hacked." Last accessed on 29 January 2015,
    http://gizmodo.com/why-sony-keeps-getting-hacked-1667259233.

11. Trend Micro Incorporated. (22 December 2014). *Simply Security.*
    "The Reality of the Sony Pictures Breach." Last accessed on 29 January 2015,
    http://blog.trendmicro.com/reality-sony-pictures-breach/.

12. Masayoshi Someya. (18 August 2014). *TrendLabs Security Intelligence Blog*.
    "Risks from Within: Learning from the Amtrak Breach." Last accessed on 29 January 2015,
    http://blog.trendmicro.com/trendlabs-security-intelligence/risks-from-within-learning-from-the-amtrak-data-breach/.

13. Jim Gogolinski. (9 December 2014). *TrendLabs Security Intelligence Blog*.
    "Insider Threats 101: The Threat Within." Last accessed on 29 January 2015,
    http://blog.trendmicro.com/trendlabs-security-intelligence/insider-threats-101-the-threat-within/.

14. Rich Trenholm. (8 December 2014). *CNET.*
    "Sony Hacked Again, This Time the PlayStation Network." Last accessed on 29 January 2015,
    http://www.cnet.com/uk/news/sony-hacked-again-this-time-the-playstation-store/.

15. Trend Micro Incorporated. (5 December 2014). *TrendLabs Security Intelligence Blog*. "WIPALL Malware Leads to #GOP Warning in Sony Hack." Last accessed on 29 January 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/wipall-malware-leads-to-gop-warning-in-sony-hack/.

16. Trend Micro Incorporated. (23 December 2014). *TrendLabs Security Intelligence Blog*. "MBR Wiper Attacks Strike Korean Power Plant." Last accessed on 29 January 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiper-attacks-strike-korean-power-plant/.

17. Trend Micro Incorporated. (25 September 2014). *Trend Micro Security News*. "Utilizing Island Hopping in Targeted Attacks." Last accessed on 17 February 2015, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/utilizing-island-hopping-in-targeted-attacks.

18. Trend Micro Incorporated. (3 December 2014). *TrendLabs Security Intelligence Blog*. "An Analysis of the 'Destructive' Malware Behind FBI Warnings." Last accessed on 29 January 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-the-destructive-malware-behind-fbi-warnings/.

19. Bryant Tan. (14 September 2014). *TrendLabs Security Intelligence Blog*. "The Easy-to-Miss Basics of Network Defense." Last accessed on 30 January 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-easy-to-miss-basics-of-network-defense/.

20. Ziv Chang. (14 August 2014). *TrendLabs Security Intelligence Blog*. "7 Places to Check for Signs of a Targeted Attack in Your Network." Last accessed on 30 January 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/7-places-to-check-for-signs-of-a-targeted-attack-in-your-network/.

21. Target Brands, Inc. (10 January 2014). *Target.com*. "Target Provides Update on Data Breach and Financial Performance." Last accessed on 30 January 2015, http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

22. Karen Katz. (15 June 2014). *Nieman Marcus*. "To Our Loyal Nieman Marcus Group Customers." Last accessed on 30 January 2015, http://www.neimanmarcus.com/en-tw/NM/Security-Info/cat49570732/c.cat.

23. White Lodging Services, Inc. (3 February 2014). *White Lodging*. "Resources and Information for Guests." Last accessed on 30 January 2015, http://www.whitelodging.com/about/payment-card-issues.

24. Sally Beauty Holdings, Inc. (17 March 2014). *Sally Beauty Holdings, Inc.* "Sally Beauty Data Incident." Last accessed on 30 January 2015, https://sallybeautyholdings.com/questions-and-answers.aspx.

25. Chuck Rubin. (17 April 2014). *Michaels*. "A Letter from Our CEO." Last accessed on 30 January 30, 2015, http://www.michaels.com/payment-card-notice-ceo-letter/payment-card-notice-CEO.html.

26. P.F. Chang's. (4 August 2014). *P.F. Chang's*. "P.F. Chang's Security Compromise Update." Last accessed on 30 January 2015, http://pfchangs.com/security/.

27. Charlene Sarmiento. (2 September 2014). *Goodwill*. "Goodwill Provides on Data Security Issue." Last accessed on 30 January 2015, http://www.goodwill.org/press-releases/goodwill-provides-update-on-data-security-issue/.

28. Homer TLC, Inc. (6 November 2014). *The Home Depot*. "The Home Depot Reports Findings in Payment Data Breach Investigation." Last accessed on 30 January 30, 2015, https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

29. Jimmy John's. (24 September 2014). *Jimmy John's*. "Jimmy John's Notifies Customers of Payment Card Security Incident." Last accessed on 30 January 30, 2015, https://www.jimmyjohns.com/datasecurityincident/index.html.

30. Alasdair James. (10 October 2014). *Kmart*. "Kmart Investigating Payment System Breach." Last accessed on 30 January 2015, http://www.kmart.com/en_us/dap/statement1010140.html.

31. John Gainor. (9 October 2014). *DQ.*
"Data Security Incident." Last accessed on 30 January 2015,
http://www.dq.com/us-en/datasecurityincident/?localechange=1&.

32. SP Plus Corporation. (28 November 2014). *SP+.*
"SP+ Acts to Block Payment Card Security Incident." Last accessed on 30 January 2015,
http://www.spplus.com/sp-acts-block-payment-card-security-incident/.

33. Brian Krebs. (4 December 2014). *Krebs on Security.*
"Banks: Credit Card Breach at Bebe Stores." Last accessed on 30 January 2015,
http://krebsonsecurity.com/2014/12/banks-credit-card-breach-at-bebe-stores/.

34. Park 'n Fly. (13 January 2015). *Park 'n Fly.*
"Park 'n Fly Notifies Customers of Data Security Compromise." Last accessed on 30 January 2015,
http://www.pnf.com/security-update/.

35. CFA Properties, Inc. (2 January 2015). *Chik-fil-A.*
"Information and Resources Related to Investigation of Potential Data Breach at Chick-fil-A." Last accessed on 30 January 2015,
http://press.chick-fil-a.com/Pressroom/LatestNews/PressDetail/databreach.

36. Trend Micro Incorporated. (2014) *Trend Micro Security News.*
"PoS RAM Scraper Malware: Past, Present, and Future." Last accessed 9 February 9 2015,
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf.

37. Trend Micro Incorporated. (2014). *Trend Micro Security News.*
"The Evolution of PoS Malware." Last accessed on 30 January 2015,
http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware.

38. American Express Company. (29 June 2012). *American Express.*
"American Express Announces U.S. EMV Roadmap to Advance Contact, Contactless, and Mobile Payments." Last accessed on 30 January 2015,
http://about.americanexpress.com/news/pr/2012/emv_roadmap.aspx.

39. Visa. (9 August 2011). *Visa.*
"Visa Announces U.S. Participation in Global Point-of-Sale Counterfeit Liability Shift." Last accessed on 30 January 2015,
http://usa.visa.com/download/merchants/bulletin-us-participation-liability-shift-080911.pdf.

40. MasterCard. (2015). *MasterCard.*
"The Next Generation of Payments Comes to the United States." Last accessed on 30 January 2015,
http://www.mastercard.us/mchip-emv.html.

41. DFS Services LLC. (12 November 2012). *Discover.*
"Discover Announces Next Steps for EMV Deployment Across the Globe." Last accessed on 30 January 2015,
http://blog.discovernetwork.com/stories/news/discover-announces-next-steps-for-emv-deployment-across-the-globe/.

42. Pawan Kinger. (14 January 2015). *TrendLabs Security Intelligence Blog.*
"Remembering the Vulnerabilities of 2014." Last accessed on 30 January 30, 2015,
http://blog.trendmicro.com/trendlabs-security-intelligence/remembering-the-vulnerabilities-of-2014/.

43. Pavan Thorat and Pawan Kinger. (25 September 2014). *TrendLabs Security Intelligence Blog.* "Bash Vulnerability Leads to Shellshock: What It Is, How It Affects You." Last accessed on 30 January 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/shell-attack-on-your-server-bash-bug-cve-2014-7169-and-cve-2014-6271/.

44. Pawan Kinger. (8 April 2014). *TrendLabs Security Intelligence Blog.*
"Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability." Last accessed on 30 January 2015,
http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability/.

45. W3TECHS.com. (29 January 2015). *W3 Techs.*
"Usage of Operating Systems for Websites." Last accessed on 30 January 2015,
http://w3techs.com/technologies/overview/operating_system/all.

46. TOP500.org. (29 January 2015). *Top 500.*
"Development Over Time." Last accessed on 30 January 2015,
http://www.top500.org/statistics/overtime/.

47. MEF. (24 January 2014). *MEF Minute.*
     "Mobile Payments Driving Global M-Commerce Adoption." Last accessed on 30 January 2015,
     http://mefminute.com/2014/01/24/mobile-payments-driving-global-m-commerce-adoption/.

48. Martin C. Libicki, Edward Balkovich, Brian A. Jackson, Rena Rudavsky, and Katharine Watkins Webb. (2015). *RAND Corporation.*
     "Influences on the Adoption of Multifactor Authentication." Last accessed on 30 January 2015,
     http://www.rand.org/pubs/technical_reports/TR937.html.

49. David Sancho. (22 July 2014). *TrendLabs Security Intelligence Blog.*
     "Finding Holes in Banking Security: Operation Emmental." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/finding-holes-operation-emmental/.

50. Brian Krebs. (2 June 2014). *Krebs on Security.*
     "'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge." Last accessed on 30 January 2015,
     http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.

51. Simon Huang. (12 August 2014). *TrendLabs Security Intelligence Blog.*
     "The Dangers of the Android FakeID Vulnerability." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/the-dangers-of-the-android-fakeid-vulnerability/.

52. Simon Huang. (26 December 2014). *TrendLabs Security Intelligence Blog.*
     "Facebook Users Targeted by Android Same Origin Policy Exploit." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/facebook-users-targeted-by-android-same-origin-policy-exploit/.

53. EY. (2014). *EY.*
     "Global Commercial Banking Survey 2014: Advancing Service in a Digital Age." Last accessed on 30 January 2015,
     http://www.ey.com/Publication/vwLUAssets/EY-global-commercial-banking-survey-2014/$FILE/EY-global-commercial-banking-survey-2014.pdf.

54. Luis Raul Parra. (5 December 2014). *TrendLabs Security Intelligence Blog.*
     "Crypto-Ransomware Goes Local in EMEA Region." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/crypto-ransomware-goes-local-in-emea-region/

55. Joseph C. Chen. (21 October 2014). *TrendLabs Security Intelligence Blog.*
     "TorrentLocker Run Hits Italian Targets." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/torrentlocker-run-hits-italian-targets/.

56. Paul Pajares and Christopher Ke. (11 January 2015). *TrendLabs Security Intelligence Blog.*
     "TorrentLocker Ransomware Hits ANZ Region." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/torrentlocker-ransomware-hits-anz-region/.

57. Rhena Inocencio. (24 March 2014). *TrendLabs Security Intelligence Blog.*
     "Ransomware and Bitcoin Theft Combine in BitCrypt." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/.

58. Jonathan Leopando. (2 April 2014). *TrendLabs Security Intelligence Blog.*
     "World Backup Day: The 3-2-1 Rule." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/.

59. Caleb Chen. (6 November 2014). *Cryptocoinsnews.*
     "Operation "ONYMOUS" Also Shut Down Dark Net Markets Cloud 9 Hydra and Maybe More." Last accessed on 30 January 2015,
     https://www.cryptocoinsnews.com/operation-onymous-also-shut-down-deep-net-markets-cloud-9-hydra-and-more/.

60. Cloakcoin.com (30 November 2014). *Cloakcoin.*
     Last accessed on 30 January 2015,
     http://www.cloakcoin.com/.

61. Michael Casayuran. (1 October 2014). *TrendLabs Security Intelligence Blog.*
     "KELIHOS Spambot Highlights Security Risks in SPF Records." Last accessed on 5 February 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/kelihos-spambot-highlights-security-risk-in-spf-records/.

62. Jon Oliver. (14 October 2014). *TrendLabs Security Intelligence Blog.*
     "Investigating Twitter Abuse, Part 3." Last accessed on 30 January 2015,
     http://blog.trendmicro.com/trendlabs-security-intelligence/investigating-twitter-abuse-part-3/.

Created by:

TrendLabs

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

TREND MICRO ™

Securing Your Journey
to the Cloud