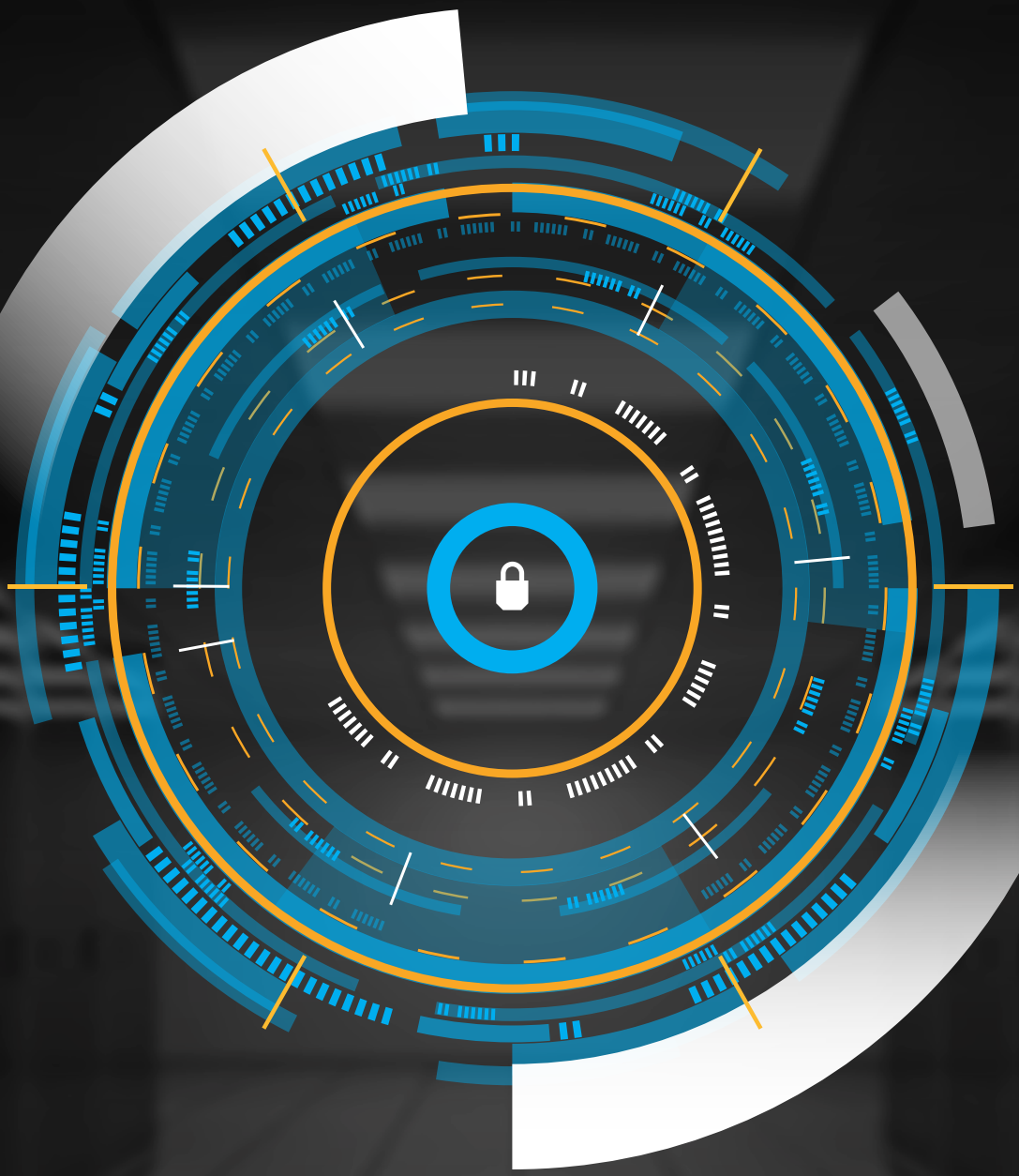


ISTR

Internet Security Threat Report

VOLUME 21, APRIL 2016

Symantec

CONTENTS

CHARTS & TABLES

INTRODUCTION

Symantec has established one of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 63.8 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services, such as Symantec DeepSight™ Intelligence, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 74,180 recorded vulnerabilities (spanning more than two decades) from over 23,980 vendors representing over 71,470 products.

Spam, phishing, and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than five million decoy accounts, Symantec.cloud, and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before they reach customers' networks. Over nine billion email messages are processed each month and more than 1.8 billion web requests filtered each day across 13 data centers. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 52 million consumers and 175 million endpoints.

Symantec Website Security secures more than one million web servers worldwide with 100 percent availability since 2004. The validation infrastructure processes over six billion Online Certificate Status Protocol (OCSP) look-ups per day, which are used for obtaining the revocation status of X.509 digital certificates around the world. The Norton™ Secured Seal is displayed almost one billion times per day on websites in 170 countries and in search results on enabled browsers.

These resources give Symantec analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.

EXECUTIVE SUMMARY

Introduction

Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36 percent from the year before. Perhaps what is most remarkable is that these numbers no longer surprise us. As real life and online become indistinguishable from each other, cybercrime has become a part of our daily lives. Attacks against businesses and nations hit the headlines with such regularity that we've become numb to the sheer volume and acceleration of cyber threats.

Most threat reports only scratch the surface of the threat landscape, whereas the breadth of Symantec's data enables the Internet Security Threat Report (ISTR) to examine multiple facets, including targeted attacks, smartphone threats, social media scams, and Internet of Things (IoT) vulnerabilities, as well as attackers' tactics, motivations, and behaviors. While there is much to be learned from this comprehensive view into the threat landscape, the following are six key findings and trends from 2015.

A New Zero-Day Vulnerability Was Discovered on Average Each Week in 2015

Advanced attack groups continue to profit from previously undiscovered flaws in browsers and website plugins

In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125 percent increase from the year before. Or put another way, a new zero-day vulnerability was found every week (on average) in 2015. In 2013, the number of zero-day vulnerabilities (23) doubled from the year before. In 2014, the number held relatively steady at 24, leading us to conclude that we had reached a plateau. That theory was short-lived. The 2015 explosion in zero-day discoveries reaffirms the critical role they play in lucrative targeted attacks.

Given the value of these vulnerabilities, it's not surprising that a market has evolved to meet demand. In fact, at the rate that zero-day vulnerabilities are being discovered, they may become a commodity product. Targeted attack groups exploit the vulnerabilities until they are publicly exposed, then toss them aside for newly discovered vulnerabilities. When The Hacking Team was exposed in 2015 as having at least six zero-days in its portfolio, it confirmed our characterization of the hunt for zero days as being professionalized.

Vulnerabilities can appear in almost any type of software, but the most attractive to targeted attackers is software that is widely used. Again and again, the majority of these vulnerabilities are discovered in software such as Internet Explorer and Adobe Flash, which are used on a daily basis by a vast number of consumers and professionals. Four of the five most exploited zero-day vulnerabilities in 2015 were Adobe Flash. Once discovered, the zero days are quickly added to cybercriminal toolkits and exploited. At this point, millions will be attacked and hundreds of thousands infected if a patch is not available, or if people have not moved quickly enough to apply the patch.

Over Half a Billion Personal Records Were Stolen or Lost in 2015

More companies than ever are not reporting the full extent of their data breaches

At the close of 2015, the world experienced the largest data breach ever publicly reported. An astounding 191 million records were exposed. It may have been the largest mega-breach, but it wasn't alone. In 2015, a record-setting total of nine mega-breaches were reported. (A mega-breach is defined as a breach of more than 10 million records.)

The total reported number of exposed identities jumped 23 percent to 429 million. But this number hides a bigger story. In 2015, more and more companies chose not to reveal the full extent of the breaches they experienced. Companies choosing not to report the number of records lost increased by 85 percent. A conservative estimate by Symantec of those unreported breaches pushes the real number of records lost to more than half a billion.

The fact that companies are increasingly choosing to hold back critical details after a breach is a disturbing trend. Transparency is critical to security. While numerous data sharing initiatives are underway in the security industry, helping all of us improve our security products and postures, some of this data is getting harder to collect.

Major Security Vulnerabilities in Three Quarters of Popular Websites Put Us All at Risk

Web administrators still struggle to stay current on patches

There were over one million web attacks against people each and every day in 2015. Many people believe that keeping to well-known, legitimate websites will keep them safe from online crime. This is not true. Cybercriminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. More than 75 percent of all legitimate websites have unpatched vulnerabilities. Fifteen percent of legitimate websites have vulnerabilities deemed 'critical,' which means it takes trivial effort for cybercriminals to gain access and manipulate these sites for their own purposes. It's time for website administrators to step up and address the risks more aggressively.

Spear-Phishing Campaigns Targeting Employees Increased 55 Percent in 2015

Cyber attackers are playing the long game against large companies

In 2015, a government organization or a financial company targeted for attack once was most likely to be targeted again at least three more times throughout the year. Overall, large businesses that experienced a cyber attack saw an average of 3.6 successful attacks each.

In the last five years, we have observed a steady increase in attacks targeting businesses with less than 250 employees, with 43 percent of all attacks targeted at small businesses in 2015, proving that companies of all sizes are at risk.

It's not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target. In one example, an organization of 35 employees was the victim of a cyber attack by a competitor. The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage. This serves as a clear warning that all businesses are potentially vulnerable to targeted attacks. In fact, spear-phishing campaigns targeting employees increased 55 percent in 2015. No business is without risk. Attackers motivated purely by profit can be just as technically sophisticated and well-organized as any nation state-sponsored attackers. Take, for example, the Butterfly gang, who steal information to use in stock manipulation.

Ransomware Increased 35 Percent in 2015

Cyber criminals are using encryption as a weapon to hold companies' and individuals' critical data hostage

Ransomware continues to evolve. Last year, we saw Crypto-ransomware (encrypting files) push the less damaging locker-style ransomware (locking the computer screen) out of the picture. Crypto-style ransomware grew 35 percent in 2015. An extremely profitable type of attack, ransomware will continue to ensnare PC users and expand to any network-connected device that can be held hostage for a profit. In 2015, ransomware found new targets and moved beyond its focus on PCs to smart phones, Mac, and Linux systems. Symantec even demonstrated proof-of-concept attacks against smart watches and televisions in 2015.

Symantec Blocked 100 Million Fake Technical Support Scams in 2015

Cyber scammers now make you call them to hand over your cash

While ransomware continues to grow as a threat, it is not the only threat that people face. As people conduct more of their lives online, attackers are finding new ways to lure victims. Fake technical support scams, first reported by Symantec in 2010, have evolved from cold-calling unsuspecting victims to the attacker fooling victims into calling them directly. Attackers trick people with pop-ups that alert them to a serious error or problem, thus steering the victim to an 800 number, where a "technical support representative" attempts to sell the victim worthless services. In 2015, Symantec blocked 100 million of these types of attacks.

Attackers continue to find ways to profit from what can be stolen online. Last year, Netflix expanded into new countries, attracting the attention of attackers. Symantec researchers discovered logins and passwords to legitimate Netflix accounts being sold on the black market. The account access information was stolen via phishing or malware. Of course, reselling account access on the black market is not a new phenomenon. Symantec continues to see stolen hotel loyalty, airline frequent flyer, and gaming accounts advertised for sale on the black market.

BIG NUMBERS

BREACHES

Total Breaches

2013	2014	2015
253	312	305
–	+23%	-2%

Breaches With More Than 10 Million Identities Exposed

2013	2014	2015
8	4	9
–	-50%	+125%

Total Identities Exposed

2013	2014	2015
552M	348M	429M
–	-37%	+23%

Average Identities Exposed per Breach

2013	2014	2015
2.2M	1.1M	1.3M
–	-49%	+21%

Median Identities Exposed per Breach

2013	2014	2015
6,777	7,000	4,885
–	+3%	-30%

EMAIL THREATS, MALWARE AND BOTS

Overall Email Spam Rate

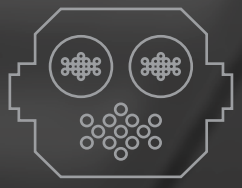
2013	2014	2015
66%	60%	53%
–	-6%pts	-7%pts

Email Phishing Rate (Not Spear Phishing)

2013	2014	2015
1 in 392	1 in 965	1 in 1,846

Email Malware Rate (Overall)

2013	2014	2015
1 in 196	1 in 244	1 in 220



Number of Bots

2013	2014	2015
2.3M	1.9M	1.1M
–	-18%	-42%

New Malware Variants (Added in Each Year)

2014	2015
317M	431M
–	+36%

Crypto-Ransomware Total

2014	2015
269K	362K
–	+35%
Average Per Day	Average Per Day
737	992

MOBILE

New Mobile Vulnerabilities

2013	2014	2015
127	168	528
–	+32%	+214%

New Android Mobile Malware Families

2013	2014	2015
57	46	18
–	-19%	-61%

New Android Mobile Malware Variants

2013	2014	2015
3,262	2,227	3,944
–	-32%	+77%

VULNERABILITIES

New Vulnerabilities

2013	2014	2015
6,787	6,549	5,585
–	-4%	-15%

Zero-day Vulnerabilities

2013	2014	2015
23	24	54
–	+4%	+125%

WEB

Web Attacks Blocked per Day

2013	2014	2015
569K	493K	1.1M
–	-13%	+117%

Scanned Websites with Vulnerabilities ...

2013	2014	2015
77%	76%	78%
–	-1% pts	+2% pts

... Percentage of Which Were Critical

2013	2014	2015
16%	20%	15%
–	+4% pts	-5% pts

Websites Found with Malware

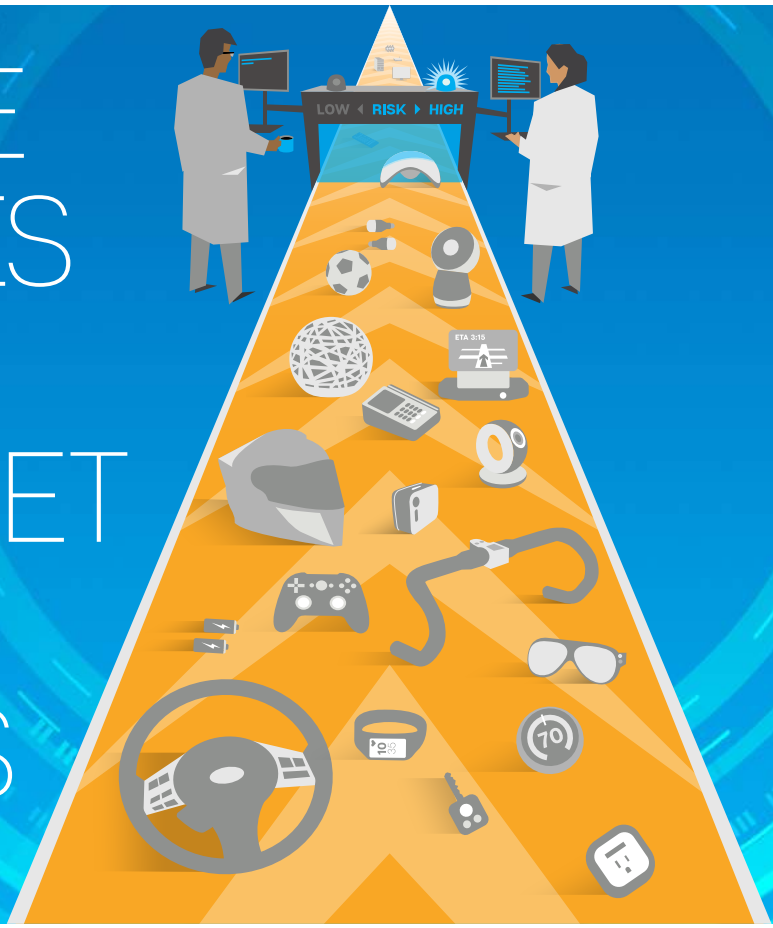
2013	2014	2015
1 in 566	1 in 1,126	1 in 3,172

SPEAR-PHISHING (EMAIL TARGETED ATTACKS)

Spear-Phishing Emails per Day

2013	2014	2015
83	73	46
–	-12%	+37%

MOBILE DEVICES & THE INTERNET OF THINGS



SMARTPHONES AND MOBILE DEVICES

Smartphones are an increasingly attractive target for online criminals. As a result, they are investing in more sophisticated attacks that are effective at stealing valuable personal data or extorting money from victims. Although Android users remain the main target, 2015 saw effective attacks on Apple devices as well, and iOS devices did not need to be jail-broken to be compromised.

One Phone Per Person

The world bought more than 1.4 billion smartphones in 2015, up 10 percent from the 1.3 billion units sold in the previous year, according to IDC's Worldwide Quarterly Mobile Phone Tracker (January 27, 2016). Five out of six new phones were running Android, with one in seven running Apple's iOS operating system (Smartphone OS Market Share, 2015, Q2). One mobile manufacturer, Ericsson, predicts there could be as many as 6.4 billion smartphone subscriptions by the end of 2020, almost one per person.

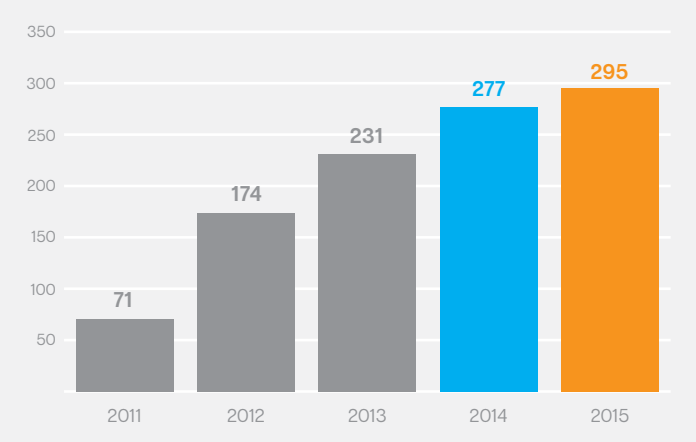
At the same time, high-end phones and tablets have powerful processors and with 4G network, they have high-bandwidth connectivity. They also contain valuable personal information. In 2015, Apple Pay launched in more countries around the world. With Samsung Pay and Android Pay also competing to manage the cards in your wallet, other mobile payment systems are likely to follow. All of this makes smartphones very attractive to criminals.

Cross-Over Threats

With many app stores, users are able to browse, purchase, and remotely install apps from their desktop, providing a unique opportunity for a cross-over of threats. In one example with Google Play, customers can browse the Play Store from their computer using a normal web browser, installing apps directly onto their phone. Recent examples of some Windows malware have exploited this by stealing browser cookies for Google Play sessions from the infected desktop computer and using these stolen cookies (essentially the users' credentials), impersonating the user to remotely install apps onto the victims' phones and tablets without their knowledge or consent.

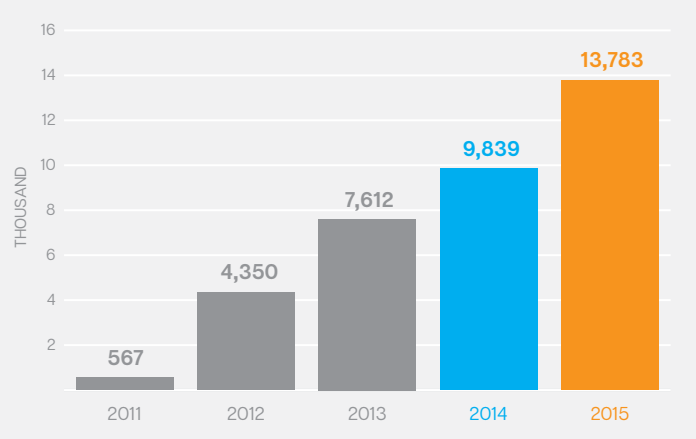
Cumulative Android Mobile Malware Families

▶ *The number of Android malware families added in 2015 grew by 6 percent, compared with the 20 percent growth in 2014.*



Cumulative Android Mobile Malware Variants

▶ *The volume of Android variants increased by 40 percent in 2015, compared with 29 percent growth in the previous year.*



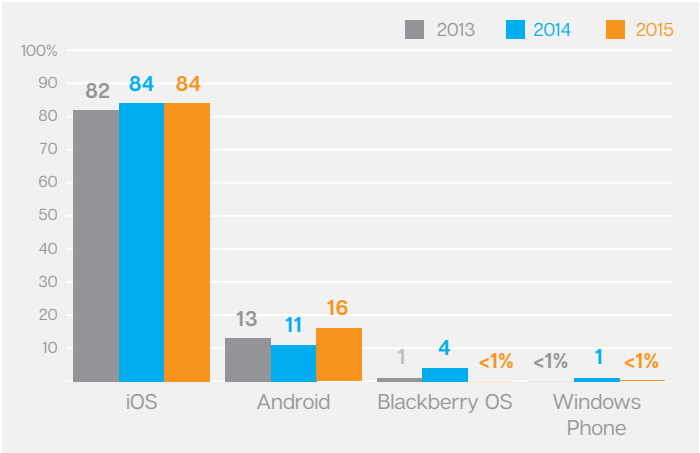
The number of mobile vulnerabilities has increased every year over the past three years. Unlike Android devices, iOS vulnerabilities have been a critical part of gaining access to an iOS device, especially for jail-breaking. Jail-breaking enables a user to install apps that are not authorized on the Apple Store and bypasses the integral security of iOS. It is much more difficult to compromise a non-jailbroken device, as this typically requires an app to be installed by downloading it from the Apple Store. Apple is well-known for its stringent screening processes, which is why the number of malicious iOS apps is so much smaller than for Android.

In 2012, IOS.Finfish had been the first example of a malicious iOS app to be discovered in the Apple Store. Finfish was able to steal information from a compromised device. OSX.Wirelurker emerged in 2014, which used an attack involving USB connections to a Mac or PC, potentially enabling apps to be installed on non-jailbroken iOS devices.

However, in 2015, attacks using XcodeGhost and YiSpecter were revealed not to require vulnerabilities, or to be jail-broken, in order to compromise an iOS device. We will be taking a closer look at these and other mobile threats later in this section.

Mobile Vulnerabilities by Operating System

▶ *Vulnerabilities on the iOS platform have accounted for the greatest number of mobile vulnerabilities in recent years, with research often fueled by the interest to jail-break devices or gain unauthorized access to install malware.*



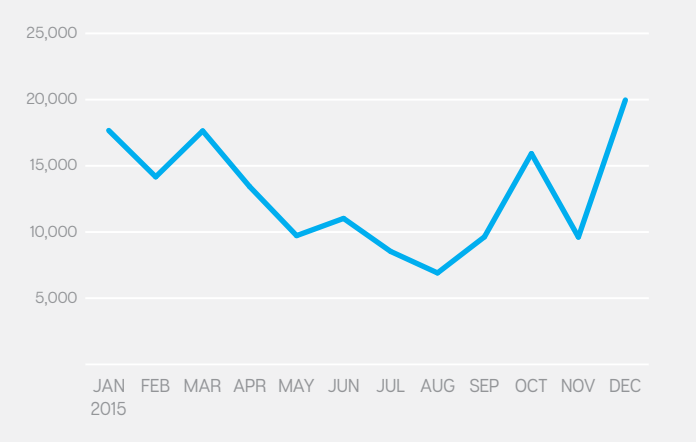
Android Attacks Become More Stealthy

Android malware is becoming stealthier. For example, malware authors started to obfuscate code to bypass signature-based security software. Additionally, before they begin their attacks, some malware can now check to see if it is running on real phones or the kind of emulators or sandboxes that security researchers use.

The number of malware attacks against Android fluctuated during 2015. In Q1, Symantec blocked approximately 550 attacks each day, the highest period of the year. This fell to approximately 272 per day by Q3, rising again to 495 by the end of Q4.

Android Malware Volume

- *There were more than three times as many Android apps classified as containing malware in 2015 than in 2014, an increase of 230 percent.*



Top Ten Android Malware

- *Thirty-seven percent of Android malware blocked by Symantec in 2015 related to variants of Android.Lotoor, which is generic detection for hacking tools that can exploit vulnerabilities in Android in order to gain root privilege access on compromised Android devices.*

Rank	Malware	Percentage
1	Android.Lotoor	36.8%
2	Android.RevMob	10.0%
3	Android.Malapp	6.1%
4	Android.Fakebank.B	5.4%
5	Android.Generisk	5.2%
6	Android.AdMob	3.3%
7	Android.Iconosis	3.1%
8	Android.Opfake	2.7%
9	Android.Premiumtext	2.0%
10	Android.Basebridge	1.7%

How Malicious Video Messages Could Lead to Stagefright and Stagefright 2.0

No matter how quickly Google patches critical vulnerabilities in the Android OS, the speed at which end-users receive updates is dependent on their device manufacturers, and sometimes this can take longer. This was highlighted when on July 2015, seven vulnerabilities were patched that could allow attackers to compromise affected devices by simply sending them a malicious multimedia message (MMS); all the intended victim had to do was to look at the malicious message, triggering an exploit.

The seven vulnerabilities involved were collectively known as the "Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities," (CVE-2015-1538, CVE-2015-1539, CVE-2015-3824, CVE-2015-3826, CVE-2015-3827, CVE-2015-3828 and CVE-2015-3829), and all were related to an Android component known as libStageFright, which handled media playback. Joshua Drake, from Zimperium zLabs, reported the vulnerabilities to Google in April and May 2015, raising further concerns that while Google had provided patches to its partners, many manufacturers took much longer providing patches to protect their customers. The severity of these vulnerabilities was compounded by the fact that despite the availability of a patch from Google, users remained at risk until carriers and manufacturers rolled out their own patches. This can often take weeks or months, and many older devices may never have a patch pushed out to them at all.

However, Google was keen to point out that devices with Android 4.0 and higher (approximately 95% of active Android devices), have protection against a buffer overflow attack built-in, using a technology called Address Space Layout Randomization, (ASLR). Additionally, Android users were able to turn-off the automatic retrieval of multimedia messages through the built-in Messaging application, as well as through Google Hangouts.

Whilst this afforded partial mitigation, it could not prevent the vulnerabilities from being exploited if a malformed or malicious multimedia message was downloaded and opened.

In October 2015, two more Android vulnerabilities (CVE-2015-6602 and CVE-2015-3876), similar to the original Stagefright bug, were disclosed. Again, if exploited they could allow an attacker to gain control of a compromised device, this time when the intended victim viewed a preview of an .mp3 or .mp4 file. By creating malicious audio or video files, attackers could entice a user to preview a song or video on an unpatched Android device.

Google had previously patched the libStageFright library so it no longer automatically processed such messages; however, it remained possible for attackers to exploit libStageFright through the mobile browser. Dubbed Stagefright 2.0, these new vulnerabilities could also be exploited through man-in-the-middle attacks and through third-party applications that still used Stagefright. Discovered and reported in August, the patches for these new vulnerabilities were included in Google's October Monthly Security Update.

Android Users under Fire with Phishing and Ransomware

Besides familiar tricks such as hiding malicious code inside ostensibly legitimate apps, or being disguised as something more useful, attackers are using more sophisticated techniques to make money from their victims. For example, Symantec researchers uncovered a new Android phishing Trojan that tricks users into entering their banking credentials by popping up a fake login page on top of legitimate banking apps. Similarly, the latest Android ransomware copies Google's design style to make it appear more legitimate and intimidating when it displays fake FBI warnings on users' lockscreens. We have also seen phone ransomware start to encrypt files, such as pictures, rather than simply change the phone's access PIN.

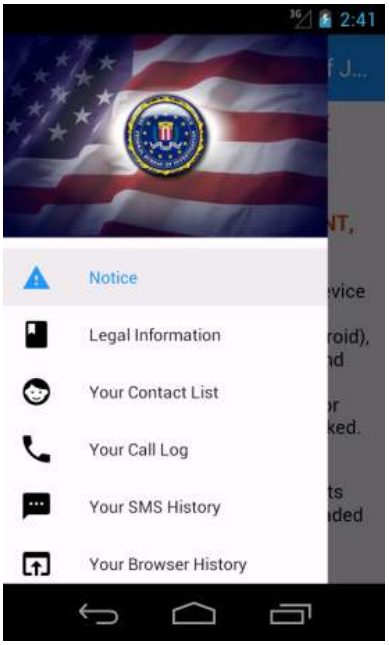
Apple iOS Users Now More at Risk than Ever

Thanks to Apple's tight control over its app store and operating system, threats to iPhones and iPads have been infrequent and limited in scale. This changed in 2015.

- In 2015, we identified nine new iOS threat families, compared to four in total previously.
- Bootlegged developer software, known as XcodeGhost, infected as many as 4,000 apps.
- The YiSpecter malware bypassed the app store altogether by using the enterprise app provisioning framework.
- Researchers found Youmi embedded in 256 iOS apps. This software is used in apps to display advertising, but also sends personal information to a remote location without users' consent.
- Vulnerabilities in Apple's AirDrop wireless file transfer system could allow an attacker to install malware on an Apple device.

Ransomware Goes Mobile

- *Imagine the frustration of a user who downloads a cool new app to their phone only to find the device locked with an FBI warning on the home screen when they try to log in.*
- *They have two options: pay a 'fine' and hope that the attackers unlock the phone or give up access to precious photos, contacts, and memories.*



iOS App Developers Haunted by XcodeGhost

As Apple sells more and more iPads and iPhones, we believe that criminals will increasingly target them, drawn in part by the higher disposable income (on average) of their owners. However, owners and Apple users should no longer assume that Apple devices are immune from attack. In September 2015, malware was discovered in a number of iOS applications in China and was discovered in a number of legitimate Apple Store apps, including WeChat, a popular IM application. The problem was that these apps were not specifically designed to be malicious, but rather their developers had been compromised with malware that was embedded into the apps they were developing.

The malicious code, known as XcodeGhost (detected as OSX.Codgost), had been discovered in certain unofficial versions of Apple's integrated development environment, Xcode. Developers of iOS applications that used these infected versions of Xcode were unknowingly allowing malicious code to be inserted into their own official iOS applications, putting their own users at risk.

If a user downloads and installs an infected app, XcodeGhost uploads information about the device to its command and control (C&C) server. The attacker would then be able to issue commands through the C&C server to perform actions including:

- Creating fake phishing alerts to steal the victim's username and password
- Reading and writing data on the device's clipboard, which could be used to uncover passwords copied from a password management tool
- Hijacking the browser to open specific URLs, which could lead to further exploits

It has been estimated that hundreds of iOS apps on the Apple App Store were infected, potentially affecting hundreds of thousands of users, particularly in China, where the WeChat app is particularly popular.

This threat did not require a jailbroken iOS device, as with other iOS threats previously, making it a new and rather worrying development in the mobile threat landscape. Symantec blocked 33 attacks in 2015, between September and December. Moreover, it wasn't just Apple's iOS that came under fire in 2015. Mac OS X, the company's popular desktop operating system, also saw a rise in vulnerabilities, exploits, and threats during the year.

YiSpecter Shows How Attackers Now Have iOS Firmly in Their Sights

In 2015, we saw an escalation in threats targeting the iOS platform, including YiSpecter (detected as IOS.Specter), which was also discovered in October 2015. YiSpecter was specifically designed to target Chinese speakers and has affected mainly users in East Asia, including China and Taiwan.

YiSpecter is a Trojan horse that is able to exploit both jailbroken and non-jailbroken iOS devices; it essentially provides a back door onto the compromised device and installs adware. The Trojan allows an attacker to accomplish a range of tasks, including uninstalling apps, downloading new fraudulent apps, and forcing other apps to display adverts.

Targeting Non-Jailbroken iOS Devices and Certificate Abuse

YiSpecter was the first iOS threat that took advantage of Apple's enterprise app provisioning framework to compromise non-jailbroken devices. The framework is used by many businesses to legitimately deploy private apps to their workforce without having to make them publicly available on the official App Store. Apps are built and signed with enterprise certificates, and do not need to be vetted by Apple before being distributed outside of the App Store. This also affords more scope for businesses to develop apps with features that would otherwise be rejected by Apple, but could still be signed and deployed legitimately through the framework.

However, as demonstrated with YiSpecter, iOS enterprise certificates can also be used to package and sign their malware. It's not known exactly how the attackers gained access to certificates, but it's possible that they registered with Apple as an enterprise, paying the necessary fees and following the vetting procedure. Alternatively, they may have been able to steal legitimate certificates from an already-registered developer or by partnering with one.

Once the attackers had access to a valid enterprise certificate, they were able to create, sign, and distribute their malicious apps, potentially to any iOS device, without any further intervention from Apple. Of course, when Apple learns of the misuse of any enterprise certificate, it can be instantly revoked, rendering any apps signed by it useless. Enterprise-signed apps can generally only be installed once the user accepts the request to trust the app or developer. From experience, we know that asking the user whether they trust an app or developer is rarely an effective security measure, but it is one last line of defense that needs to be crossed before the malware can be installed.

Exploiting Apple's Private APIs

One of the reasons that YiSpecter included more advanced functionality was because it also used Apple's own private APIs to perform activities that standard iOS apps cannot. These "private APIs" are reserved for Apple's own apps to be able to perform a range of system-level actions. Other iOS developers are not supposed to use these APIs in their apps, and any third-party apps that do so are rejected from the Apple App Store. Of course, YiSpecter is able to circumvent the official App Store, instead relying on unofficial distribution channels to spread the malware. As a result, the threat is able to take advantage of the private APIs for its own purposes.

Cross-Platform Youmi Madware Pilfers Personal Data on iOS and Android

In October 2015, Apple pulled as many as 256 apps from its App Store for apparently violating the company's privacy guidelines. The apps had used third-party advertising technology from a company called Youmi (detected as Android.Youmi), which was secretly being used to access private information, including Apple ID email addresses and International Mobile Station Equipment Identity (IMEI) numbers.

Soon after this, the same advertising library was discovered in a number of Android apps, where it was being used to perform a range of actions that could also compromise the user's privacy, including harvesting their GPS location and phone number, as well as downloading additional, potentially unwanted applications.

Distinguishing Madware

Adware and its mobile counterpart, mobile Adware (or madware), has been around for many years and is a popular way of financing free apps, where the app developer is paid a fee for each of the adverts presented to their users. Many people are happy relinquish a small area of the screen for advertising in exchange for a free app; however, this may sometimes happen without consent

or be particularly aggressive. Symantec recorded a 77 percent rise in apps containing unwanted madware.

Ad-blocking tools have grown in popularity as a way to avoid this, and by blocking mobile ads, they also help to reduce mobile data costs incurred with madware traffic and minimize the number of on-screen ads. Furthermore, such software can also help to improve the security posture of a device by blocking potentially unwanted madware that may be installed without the user's permission or knowledge.

App Analysis by Symantec's Norton Mobile Insight

- *Symantec analyzed 71 percent more apps in 2015 and more than three times as many (230 percent) more were classified as malicious. A 30 percent rise in grayware was owing in large part to a 77 percent rise in apps containing unwanted madware.*

	2013	2014	2015
Total Apps Analyzed	6.1 Million	6.3 Million	10.8 Million
Total Apps Classified as Malware	0.7 Million	1.1 Million	3.3 Million
Total Apps Classified as Grayware	2.2 Million	2.3 Million	3.0 Million
Total Grayware Further Classified as Madware	1.2 Million	1.3 Million	2.3 Million
Malware Definition	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.		
Grayware Definition	Programs that do not contain viruses and that are not obviously malicious, but that can be annoying or even harmful to the user, (for example, hacking tools, accessware, spyware, adware, dialers, and joke programs).		
Madware Definition	Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.		

Protecting Mobile Devices

We recommend that people and employers treat mobile devices like the small, powerful computers that they are and protect them accordingly, including:

- Access control, including biometrics where possible.
- Data loss prevention, such as on-device encryption.
- Automated device backup.
- Remote find and wipe tools, in the event of a lost device.
- Regular updating. For example, the latest version of Android, codenamed Marshmallow (version 6.0), was launched in October and includes a number of features designed specifically to thwart attackers. According to Statista, in October 2015, KitKat (version 4.4) was still the most widely used version of Android at 38.9 percent, and Lollipop (version 5.0) accounted for 15.6 percent.
- Refrain from downloading apps from unfamiliar sites and only install apps from trusted sources.
- Don't jailbreak devices. Jailbroken devices are often more susceptible to security issues.
- Pay particular attention to permissions requested by an app.
- Update apps as often as possible, or if a suspicious app is identified, delete it and wait for a new version to be made available.
- Change your Apple ID password, or your Google Play password, if you suspect your account has been compromised. This advice extends to safeguarding account credentials on any third-party app store.
- Watch out for any suspicious emails or push notifications to your device asking for your credentials, or any other personally identifying information.
- Until a patch is applied, proceed cautiously when using your mobile browser to preview unsolicited audio and video files.
- Android users are advised to apply any security updates issued by their carrier or device manufacturer as they become available.
- Additional mobile security solutions can also help safeguard against malicious software, and enterprises should consider mobility management tools that can help secure and control mobile devices within an organization.

Looking Ahead

We predict that mobile threats will continue to proliferate in 2016. We may soon see PC-like exploit kits for phones commercialized on the black market.

At the same time, Apple and Google are working hard to secure their operating systems and wider ecosystems. In particular, we anticipate improvements in the techniques used to validate and sign applications, as well as in application delivery. Phone users will become accustomed to frequent on-by-default application and operating system updates, and the need for security software on their mobile devices.

This is perhaps an indicator of progress, rather than a cause for despair. It suggests that security researchers, operating system, developers, and app writers are, in fact, paying more attention to mobile security by identifying and fixing more problems. Although we expect mobile devices to come under growing attack over the next year, there is also hope that with the right preventative measures and continuing investment in security, users can achieve a high level of protection against them.

THE INTERNET OF THINGS

Internet-connected things are multiplying rapidly. We saw many proof-of-concept and real-world attacks in 2015, identifying serious vulnerabilities in cars, medical devices, and more. Manufacturers need to prioritize security to reduce the risk of serious personal, economic, and social consequences.

Billions and Billions of Things

The Internet of Things has already arrived. We only have to look around at our own environment to see the impact it is having on our everyday lives. The average smart phone now has more computing power than the Space Shuttle; a smartwatch now downloads updates from the Internet; the point-of-sale terminals at a coffee shop are all connected to the company's central financial system; many cars now have satellite navigation and Bluetooth connections; an Internet-connected thermostat can control the temperature in our homes.

In the USA, for example, there are 25 online devices per 100 inhabitants, and that is just the beginning. Gartner forecasts that 6.4 billion connected things will be in use worldwide in 2016, and will reach 20.8 billion by 2020 (Gartner, Inc., press release, November 10, 2015).

If the Internet of Things is to deliver the promised $2 trillion economic benefit, designers and manufacturers have to address fundamental security challenges. The prospects, however, are not good.

The Insecurity of Things

Over the last year, Symantec has seen an increase in proof-of-concept attacks and growing numbers of IoT attacks in the wild. In numerous cases, the vulnerabilities were obvious and all too easy to exploit. IoT devices often lack stringent security measures, and some attacks are able to exploit vulnerabilities in the underlying Linux-based operating systems found in several IoT devices and routers. Many issues stem from how securely vendors implemented mechanisms for authentication and encryption (or not). Here are some examples:

- **Cars.** Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. In the UK, thieves hacked keyless entry systems to steal cars.
- **Smart home devices.** Millions of homes are vulnerable to cyberattacks. Symantec research found multiple vulnerabilities in 50 commercially available devices, including a 'smart' door lock that could be opened remotely online without a password.
- **Medical devices.** Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps, x-ray systems, CT-scanners, medical refrigerators, and implantable defibrillators.
- **Smart TVs.** Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft, and even ransomware, according to Symantec research.
- **Embedded devices.** Thousands of everyday devices, including routers, webcams, and Internet phones, share the same hard-coded SSH and HTTPS server certificates, leaving more than 4 million devices vulnerable to interception and unauthorised access.

We expect to see more stories like this in the coming year. If a device can be hacked, it likely will be. In addition, where there are proof-of-concept attacks, real attacks invariably follow. We may even expect to see IoT devices as the preferred route for attacking an organization, and potentially the most difficult for incident response staff to recognize and remove.

Given the present poor state of security on connected devices, they will present an increasingly attractive target to criminals who look for easy targets in the same way that burglars prefer houses without alarms or resident dogs.

Peek into the Future: The Risk of Things

Internet-connected things

[1] **20.8 billion** (predicted)

20 Numbers in billions
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1

The insecurity of things

Medical devices. Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators.

Smart TVs. Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft and even ransomware, according to Symantec research.

Cars. Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. **In the UK, thieves hacked keyless entry systems to steal cars.**

[1] Today in the USA, there are **25 connected devices per 100 inhabitants**

[1] **6.4 billion**

[1] **4.9 billion**

[1] **3.9 billion**

2014 2015 2016 2020

1 Source: gartner.com/newsroom/id/3165317

Home Automation to Reach a Tipping Point by 2020

Despite the increased attention and rapid development, the Internet of Things has not reached a critical mass when it comes to home automation. Perhaps one of the final hurdles holding IoT dominance back has to do with standardized communication protocols. So far, we have seen plenty of growth with interconnected IoT devices using well-established protocols, such as Wi-Fi and Bluetooth®. Devices that utilize 802.11b/g/n/ac wireless protocols, including Smart TVs, intelligent thermostats, IP cameras, and other devices, are cropping up everywhere. Devices that employ Bluetooth 4.0, such as fitness trackers, smart watches, and other wearables, have also helped IoT gain significant traction in that market.

However, these communication protocols fall flat in many home automation cases. The latest Wi-Fi technologies work great for quick and efficient wireless connections, but have power requirements that can put a strain on smaller devices. Bluetooth does operate better in this scenario, but its short range does not make it ideal for communication from more than a few feet away. That's not to say that it cannot be done. It just has not been possible to do it cheaply enough to bring the technology to ubiquity.

A number of vendors have stepped in to address these communications challenges, though none has yet to dominate the market. This has resulted in a fragmented market of competing wireless communication specifications tied to specific vendors or vendor groups. What may finally open the gates for small, low powered IoT devices is Wi-Fi HaLow™ (IEEE 802.11ah), a new communications protocol for IoT and wearable devices, slated to be finalized and certified between 2016 and 2018. Once released, router manufacturers could quickly incorporate the protocol to their products, as with other communications protocols like 802.11ac, and in so doing, open the doors for consumers to automate their homes more easily and cheaply.

Of course, when introducing any new technology, the attack surface expands, which presents a variety of new problems from a security standpoint. Proprietary IoT networks have already been found with multiple security vulnerabilities, some trivial and some serious. The fundamental question regarding IoT and home automation is not, "How do we do this?" It is, "How do we do this securely?"

With the adoption of common standards, it is likely that older proprietary protocols will fall by the wayside, paving the way for potentially greater consolidation in the marketplace. While larger, well-known brand names will continue to release their own products, smaller, innovative IoT companies will become attractive targets for organizations seeking to quickly expand their portfolios into those areas. However, cybersecurity must be at the core for the adoption of this new breed of IoT technology to succeed. As more homes become connected, it will be difficult for consumers to ignore the benefits that this new technology will promise.

It is always important to weigh the convenience of remote control, automation, ease of use, and the benefits they can bring, against the potential risks introduced that could lead to hackers opening IoT locks, disabling IoT burglar alarms, or generally wreaking havoc with IoT devices.

How to Protect Connected Devices

Protecting the Internet of things requires the same holistic approach as other areas of IT security. Unfortunately, both Industrial IoT ecosystems, like the Industrial Internet Consortium (IIC), and consumer IoT ecosystems, such as the AllSeen Alliance, are still very early in defining standards for this rapidly evolving area. To address this, Symantec published its Security Reference Architecture, and contributed to the IIC and AllSeen efforts, along with the Online Trust Alliance (OTA) IoT Trust Framework, and the US Department of Homeland Security (DHS) Security Tenets for Life Critical Embedded Systems.

Effective security requires layers of security built into devices and the infrastructure that manages them, including authentication, code signing, and on-device security (such as Embedded Critical System Protection technology). Analytics, auditing, and alerting are also key to understanding the nature of threats emerging in this area. Finally, strong SSL/TLS encryption technology plays a crucial role in authentication and data protection.

Towards a Secure, Connected Future

As with other aspects of Internet security, some threats are more dangerous than others are, and while a hacked fitness monitor may be an inconvenience, a vulnerability in millions of cars may present a more serious danger. Similarly, a backdoor in a medical device may give thieves access to medical records, albeit on a relatively small-scale, or it may lead to serious injury or potentially even death.

The remedies are well-understood, but manufacturers need to prioritize security and find the right balance between innovation, ease-of-use, and time-to-market constraints. Fundamentally, companies and consumers need to be assured that suppliers are building security into the IoT devices they are buying. ■

WEB THREATS

WEB ATTACKS, TOOLKITS, AND EXPLOITING VULNERABILITIES ONLINE

If web servers are vulnerable, then so are the websites they host and the people who visit them. Attackers are exploiting any vulnerability they can to compromise websites and commandeer their host servers. The ease of use and wide availability of web attack toolkits is feeding the number of web attacks, which doubled in 2015.

Website owners still aren't patching and updating their websites and servers as often as perhaps they should. This is like leaving a window open through which cybercriminals can climb through and take advantage of whatever they find.

Over the past three years, more than three quarters of websites scanned contained unpatched vulnerabilities, one in seven (15 percent) of which were deemed critical in 2015.

Scanned Websites with Vulnerabilities

A critical vulnerability is one which, if exploited, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.

2013	2014	2015
		
77%	76%	78%
	-1% pts	+2% pts

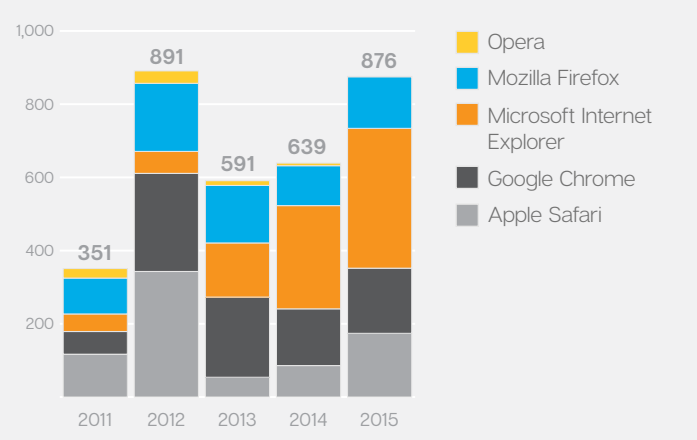
Percentage of Vulnerabilities Which Were Critical

2013	2014	2015
		
16%	20%	15%
	+4% pts	-5% pts

Problematic Plugins

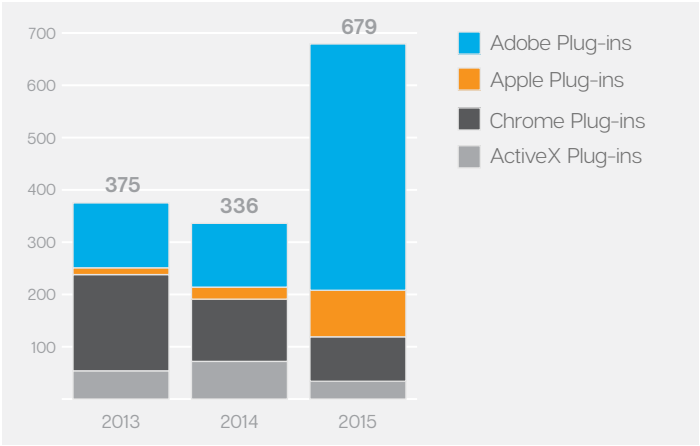
It's not just the operating systems making web servers vulnerable. While many of the major content management system providers have improved security and implemented automatic updates in recent years, the security of plugins for these systems is still a big problem.

Browser Vulnerabilities



Annual Plugin Vulnerabilities

The number of vulnerabilities in Adobe plugins has grown in 2015, an indication that attackers are seeking to exploit plugins that are not only cross-platform, but also ubiquitous. Most Adobe vulnerabilities are related to Adobe Flash Player (also known as Shockwave Flash).



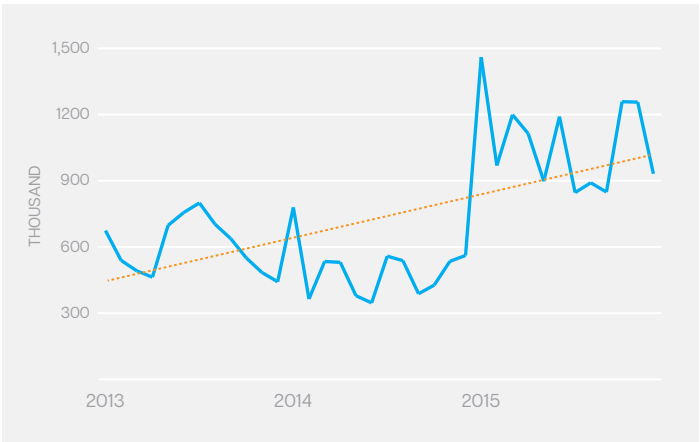
The End Is Nigh for Flash

Adobe Flash Player has continually been the subject of malicious exploitation over the years and accounted for 10 vulnerabilities that were classified as zero days in 2015 (17 percent) compared with 12 in 2014 (50 percent), and five in 2013 (22 percent). With such rich pickings, it's clear to see why attackers are partial to exploiting Flash. Apple, Google, and Mozilla have all expressed their concerns with the Flash plugin, and Google recently announced that Flash will no longer be supported natively in Chrome. Mozilla continues to support Flash within Firefox as an exception to the general plugin policy.

From a security perspective, we expect Adobe Flash will gradually fall out of common usage over the next year.

Web Attacks Blocked per Month

The chart shows the number of web attacks blocked each day on average since 2013. An average of one million web attacks was blocked each day in 2015, an increase of 117 percent (more than double) compared with 2014.



Exploiting Plugins for Web Servers

It's not only plugins for web browsers that are vulnerable and exploited. Take WordPress, which now powers a quarter of the world's websites, for example. Anyone can write a WordPress plugin—and they often do. Plugins range from the useful to the completely ridiculous, such as Logout Roulette: "on every admin page load, there's a 1 in 10 chance you'll be logged out."

The problem is, some plugins are shockingly insecure. Windows attracts many exploits because of its large user base, and the same applies to WordPress plugins. Vulnerable plugins found on WordPress sites can and will be exploited.

Plugins, whether for browsers or servers, need to be updated regularly as they are vulnerable to security flaws, and out-of-date versions should be avoided where possible.

Minimize Risk from Plugins

- *Update plugins regularly.*
- *Watch the media and security lists for warnings.*
- *Be very selective about the plugins used to reduce your attack surface.*

Infection by Injection

In 2015, Symantec also saw the return of Team GhostShell, which claims to have hacked a significant number of websites. Earlier this year, the Symantec Security Response team reported:

"From first appearances, the recently released list of hacked websites seems to be random and there is no indication that any particular country or sector is being targeted. The group is more than likely hacking websites based on their vulnerability.

In keeping with its previous modus operandi, it is likely that the group compromised the databases by way of SQL injection attacks and poorly configured PHP scripts."

Again, these are hacks that most likely could have been prevented with better website and server management. SQL injection is a long-established attack method, which continues to work because of an unnecessary weakness in the parameters administrators establish for search queries.

Web Attack Exploit Toolkits

It is difficult to defend against new and unknown vulnerabilities, particularly zero-day vulnerabilities for which there may be no patch, and attackers are trying hard to exploit them faster than vendors can roll out patches.

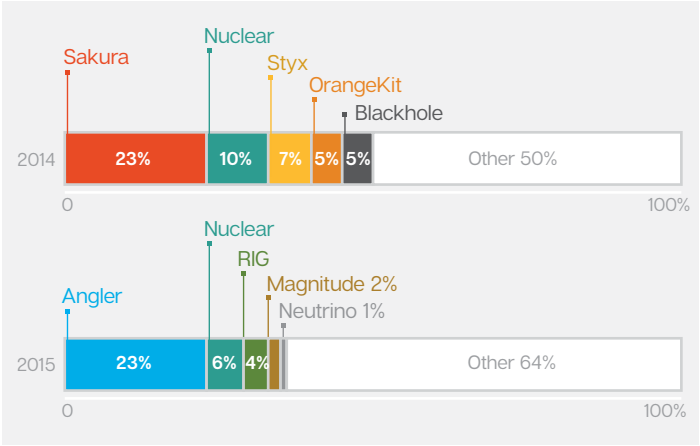
In 2015, following the breach of Hacking Team, an Italy-based company, previously unknown zero-day exploits were made public by the attackers. Exploits for zero-day vulnerabilities were shared, and within hours, integrated into exploit toolkits.

Angling for Malicious Ads

The Angler exploit kit, first seen in 2013, is arguably among the most sophisticated exploit kits available today, and has pioneered many technical advances that other exploit kits have often followed, including the use of anti-cybersecurity countermeasures. For example, Angler is able to download and execute malware from memory, without needing to write any files to disk, in an attempt to evade detection by traditional security technology. Additionally, one significant factor in Angler's incredible growth in 2015 is that it has been very fast at integrating the growing number of new zero-day exploits into its arsenal.

Top Five Web Attack Toolkits

- *The Angler exploit kit was the most common exploit kit in use during 2015, and accounted for 23 percent of all exploit-kit web attacks. It has grown considerably in the last year and was not featured in the top five for 2014.*



Angler was the most active exploit kit in 2015, and hundreds of thousands of attacks by this kit were blocked by Symantec on a daily basis. In total, the number of Angler-based attacks blocked numbered over 19.5 million. Angler's favorite delivery mechanism was malvertisments, favoring exploited Adobe Flash vulnerabilities. Windows was the preferred target for Angler in 2015. Windows 7 in particular accounted for 64 percent of Angler attacks, and Windows 8.1 accounted for 24 percent. Moreover, Mac OS X did not appear to be in the firing line for attackers using the Angler toolkit in 2015, but this is expected to change as cybercriminals seek to exploit the Apple ecosystem.

Tech Support Scams Go Nuclear, Spreading Ransomware

In 2015, Symantec recorded an increase in tech support scams, equivalent to a 200 percent rise compared to the previous year.

Tech support scams are not a new tactic, and hundreds of thousands of people worldwide are targeted on a daily basis. The earliest types of tech support scams involved call center workers cold-calling users, trying to sell them technical support packages to resolve non-existent problems on their intended victims' computers.

These scams have evolved over time, and more recent examples may display seemingly endless fake warning messages, urging the intended victims to call a toll-free number for help. On calling the number, seemingly professional-sounding call center staff try to convince their intended victims to install malware and other unwanted applications onto their computers, while claiming it will fix their problems.

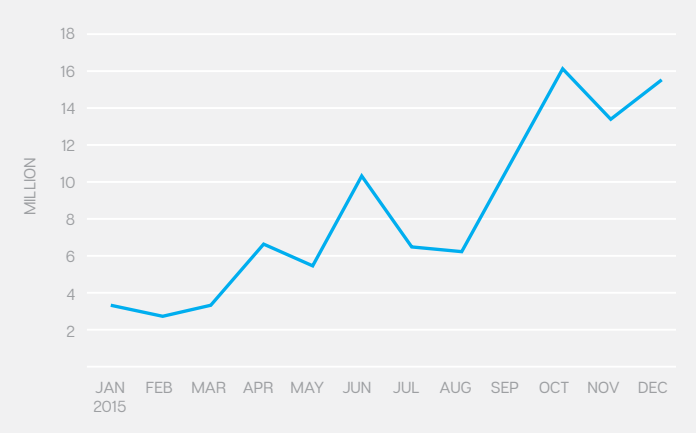
In the latest twist, tech support scammers were found using the Nuclear exploit kit to drop ransomware onto its intended victims' computers. The scammers could distract the user while the ransomware encrypts files on their computer, perhaps increasing their chances of earning money from the victim.

While this wasn't the first time tech support scammers have been discovered installing ransomware, the most recent examples include a malicious HTML iframe on their website, redirecting visitors to a server hosting the Nuclear exploit kit. The exploit kit was found to be taking advantage of the recent Adobe Flash Player Unspecified Remote Code Execution Vulnerability (CVE-2015-7645), among other vulnerabilities. On success, it either dropped Trojan.Cryptowall (ransomware) or Trojan.Miuref.B (an information-stealing Trojan).

This was the first time Symantec has seen tech support scams used in parallel with the Nuclear exploit kit to deliver ransomware, and if this proves to be an effective combination, this trend is set to continue. While it may be quite plausible that tech support scammers and exploit kit attackers have joined forces, it is possible that the tech support scammers' own web servers were compromised by a separate group who are using the Nuclear exploit kit.

Blocked Tech Support Scams

- *In total, Symantec blocked more than 100 million malware or exploit-kit attacks relating to tech support scams in 2015.*
- *The countries targeted the most by tech support scams were the US, UK, France, Australia, and Germany.*



Malvertising

The middle of 2015 was filled with accounts of malvertising affecting almost every segment of the ad-supported Internet. One possible explanation is that malvertising is simply an easier way to infect site visitors than spamming out links to infected websites. It's much easier for an attacker to try and compromise a popular site or seek to host malicious ads on popular, high-traffic websites because it means they don't need to consider the complex nuancing of social engineering, eliminating one more step in the bad guys' "pipeline."

Ad companies often don't request a lot of information from people submitting ads, making it easy for criminals to masquerade as legitimate businesses and upload malicious ads, which can appear on any number of sites.

Thanks to the use of cookies, malware authors can also tailor their malicious code or redirects to target almost any subset of users, by geography, time of day, company, interests, or recent Internet activity.

Classification of Most Frequently Exploited Websites

- *Technology and business related websites were the most popular for hosting malicious content and malvertising in 2015.*

	2015 Top 10 Most Frequently Exploited Categories of Websites	2015 Percentage of Total Number of infected Websites	2014 Top 10	2014 %
1	Technology	23.2%	Technology	21.5%
2	Business	8.1%	Hosting	7.3%
3	Search	7.5%	Blogging	7.1%
4	Blogging	7.0%	Business	6.0%
5	Dynamic	6.4%	Anonymizer	5.0%
6	Educational	4.0%	Entertainment	2.6%
7	Domain Parking	3.2%	Shopping	2.5%
8	Entertainment	2.6%	Illegal	2.4%
9	Shopping	2.4%	Domain Parking	2.2%
10	Illegal	2.1%	Virtual Community	1.8%

Unfortunately, malvertising is notoriously difficult to track and criminals have become increasingly clever, removing the malicious code from their ads after an hour or two, making it almost invisible. Since it is powerful, effective, and hard to analyze, we expect the use of malvertising to continue to grow. Consequently, an increased demand for ad-blockers may in turn help to reduce the negative impact of malvertising.

CYBERSECURITY CHALLENGES FOR WEBSITE OWNERS

Whether it's the way we shop, work, or pay our tax bill, trust and confidence in online services has become critical to our way of life. Thankfully, changes are coming to the way we use and secure the Internet to reinforce trust in online privacy, security, and transactions.

Website security encompasses more than the information in transit between a server and visitors to a website. Organizations need to think about their websites as parts of an entire ecosystem that needs constant care and attention if they want to retain people's trust and confidence.

The consequences of failing to bolster website security are likely to extend beyond the costs to an individual company: it will damage consumer confidence and the wider economic fallout could be huge.

Put Your Money Where Your Mouse Is

The scales finally tipped during the 2015 Thanksgiving holiday weekend in the US, as the number of consumers shopping online exceeded those shopping in store, according to the National Retail Foundation.

E-commerce is big business, and Ecommerce Europe reported that global business-to-consumer ecommerce turnover grew by 24 percent, reaching $1.9 billion in 2014. However, that may seem small compared to the $6.7 trillion that Frost & Sullivan estimates the business-to-business e-commerce market will be worth by 2020. Frost & Sullivan's forecast includes all forms of electronic commerce including using Internet and electronic data interchange systems.

Even governments are becoming increasingly dependent on digital services to keep their books balanced. The British government, for example, recently revealed that it had saved £1.7 billion through digital and technology transformation in 2014.

While SSL/TLS certificates, trust marks, and good website security all help maintain the online economy, all this economic activity could be at risk if people lose trust and confidence in the security foundations of the online economy.

Websites Are Still Vulnerable to Attacks Leading to Malware and Data Breaches

Websites are a critical element in major attacks: they are a way into the network, they are a way into sensitive data, and they are a way to reach customers and partners.

For example, the rise in malware aimed at Linux web servers—including website hosts—proves that criminals have realized that the infrastructure behind websites is as valuable, if not more so, than the information encrypted by SSL/TLS certificates.

Many attacks against website infrastructure could be prevented with regular maintenance and patching, but the numbers suggest that website owners just aren't managing to keep up. Three quarters of the websites Symantec scanned in 2015 had vulnerabilities—a number that hasn't shifted in years.

Cybercriminals continued to find vulnerabilities in the underlying infrastructure of website security in 2015, including FREAK, which allowed attackers intercepting a secure connection to force the server to downgrade to encryption an easier-to-crack protocol.

Distributed-denial-of-service (DDoS) attacks have also continued to prove disruptive to businesses 2015. While large-scale attacks such as the one that hit the BBC at the end of 2015 tend to grab headlines, businesses of every size are a target for attack and often smaller sites can suffer as part of the collateral damage when a host has to shut down a server, taking multiple sites offline, because of an attack on just one of its clients.

Mitigation tactics and tools exist to defend against DDoS attacks, but website managers need to take the time to understand and deploy them if they are to keep their websites safe.

Moving to Stronger Authentication

It's not all bad news. There have been several advances in both the strength and adoption of SSL/TLS certificates in 2015 as well as initiatives by Certificate Authorities (CAs) to make issuing SSL/TLS certificates more transparent.

Crucially, nearly 40 percent of all downstream Internet traffic in the US is now encrypted, according to research from Sandvine, and this is expected to grow to more than 70 percent of the world's Internet traffic over the coming year.

Unfortunately, in a world where everything is encrypted, consumers have a false sense of security that whenever they see HTTPS in the browser, the website that they are on has been validated and authenticated and must therefore be genuine. In reality, online fraud has historically occurred on Domain

Validated (DV) sites, which offer no validation of the organization behind the site.

With DV certificates, the CA will verify that a contact at the domain in question approves the certificate request, usually via email or telephone, and this is often automated. Consequently, DV certificates are usually cheaper than the more rigorous Extended Validation (EV) SSL certificates, which require more vetting and validation.

While DV certificates verify the consent of a domain owner, they make no attempt to verify who the domain owner really is, making it ideal for both phishing and MITM (man-in-the-middle) attacks. Symantec expects to see a move by organisations, particularly those driven by PCI compliance, to strengthen the requirements for stronger authentication, and the adoption of EV SSL certificates providing greater levels of assurance.

Encryption of SSL/TLS will also become stronger with the shift from SHA-1 to SHA-2. Historically, SHA1 is a very popular one-way hashing function, where each hash generated from a source is intended to be unique. There should be no "collision" where two different sources will generate the same hash; however, the first weaknesses were identified as early as 2005. This came to a head in 2014 when Google announced it would soon no longer support sites using SHA1 and will display security warnings to visitors trying to access sites with SHA-1 certificates expiring after 1st January 2017. Several other browser vendors followed suit, spelling the inevitable end for SHA-1.

The security community is making great progress, and there is a real opportunity to significantly reduce the number of successful website attacks, but it will only happen if website owners step up and take action too.

Accelerating to Always-On Encryption

Nearly 40 percent of all downstream Internet traffic in the US is now encrypted, according to research from Sandvine, and this is expected to grow to more than 70 percent of the world's Internet traffic over the year. This sudden upsurge is down to a number of factors:

- **Big company commitment.** Some of the biggest names on the Internet have already adopted HTTPS, including Facebook, Twitter and, more recently, Netflix.
- **Search engine preference.** Google announced in 2014 that the adoption of 'HTTPS everywhere' would have a positive impact on search rankings, encouraging site owners to adopt it to get an edge in search engine rankings.
- **HTTP upgrade.** The Internet Engineering Task Force (IETF), the organization in charge of creating standards for the Internet, published a new version of the Hypertext Transfer Protocol in 2015. Dubbed HTTP/2, it will likely be adopted as standard in the near future and, as the draft states, HTTP/2 enables a "more efficient use of network resources," meaning HTTP/2 is designed to deliver better, faster responsive performance for websites out of the box. And every major browser has said its support for HTTP/2 is only going to be over SSL/TLS. In effect, this makes encryption mandatory for sites using this new standard.

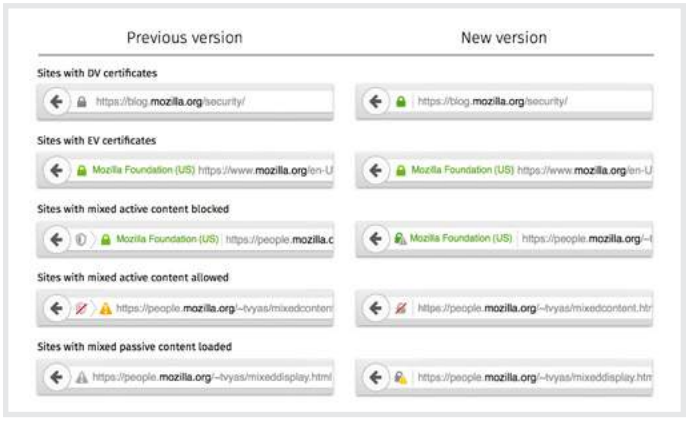
The hope is that within the next few years, every page on the Internet will have an SSL/TLS certificate. Symantec is already working with web hosting providers to help them provide encryption as part of their service to website owners.

Reinforced Reassurance

Several major browsers are also changing their security indicators—the colours and symbols used in the address bar to indicate to visitors how safe a site is—to make it clear when an SSL/TLS-secured web page includes unsecured content that is vulnerable to man-in-the-middle tampering. In other words, this will make it clearer when a site fails to achieve always-on encryption and the danger this poses.

This is just one example of the drive to offer added reassurance to websites visitors and online shoppers, which also includes trust marks and shopping guarantees, which help to allay the fears many shoppers have when they shop online and can't see the store owner in person or hold the goods they're buying in their hands.

Taken from Mozilla's Security Blog



Websites Need to Become Harder to Attack

Organizations need to be more proactive around SSL/TLS implementation. It's not a one-and-done task. Tools that automate and streamline the process are essential.

Updates are released regularly for SSL/TLS protocol libraries, such as OpenSSL, to protect against such vulnerabilities, but website owners still have to install them. The move from SHA-1 certificates to the much stronger SHA-2 is also accelerating, but again organizations have to deploy the new certificates properly for the change to be effective.

Rather than thinking solely about protection, website managers need to think about protection, detection, and response. They need to use automation tools to monitor their websites continually for signs of vulnerability or attack, block those attacks, and then report, update, and patch accordingly.

SSL/TLS AND THE INDUSTRY'S RESPONSE

SSL/TLS remains at the heart of online privacy, authentication, and encryption, but around them is an infrastructure of trust that requires maintenance and vigilance if it is to remain effective. The industry must learn and adapt.

The Evolution of Encryption

On August 11, 1994, Daniel Kohn sold a CD to a friend in Philadelphia. His friend used his credit card to spend $12.48, plus shipping costs, in a transaction that, for the first time ever, was protected by encryption technology. The site Daniel ran at the time required customers to download a special browser to conduct secure transactions, which employed the PGP encryption standard that his website relied on.

Reporting the next day, the New York Times commented:

> *"Alarmed by increasing reports of security breaches on the Internet, many people and businesses are reluctant to transmit sensitive information, including credit cards numbers, sales information, or private electronic mail messages, on the network."*

Twenty years later, people's concerns remain the same, although their behaviour suggests they're willing to take the risk of relying on their bank for help if something goes wrong. Without a consistent and secure SSL/TLS infrastructure, however, this fragile state of trust will crumble and ecommerce simply won't be able to function.

Strength in Numbers

The strength of SSL/TLS has come a long way since 1994, and this year saw the switch from SHA-1 to SHA-2 as the industry standard moving forward.

As computing power has increased, so has a hacker's ability to break hashing algorithms through sheer brute force. Many experts predict that SHA-1 will become vulnerable in the very near future. That's why the major browsers have agreed to stop supporting SHA-1 certificates during the next two years so that any visitors trying to access a site continuing to use them will see a security warning.

"The current plan is to [stop accepting SHA-1 certificates] on January 1, 2017. However, in light of recent attacks on SHA-1, we are also considering the feasibility of having a cut-off date as early as July 1, 2016," says Mozilla, and there has been discussion of bringing those dates even further forward to accelerate the change.

Symantec offers a free upgrade service, but large organizations need to ensure they have a full migration plan in place to update any devices and applications that may not currently recognize SHA-2.

Time to freak out?

- *The vulnerability known as FREAK was discovered back in March 2015. Attackers who intercepted the setting up of a secure connection between an affected server and client could force them to use 'export-grade' encryption, a much weaker form of encryption than is usually used today, therefore making the transacted message easy to break with the computing resources available today.*
- *It's estimated that servers supporting 9.6 percent of the top one million website domains were initially vulnerable to attack and nine months later, 8.5 percent remain so.*

Slipping through the Cracks

Despite encryption getting stronger, many of the attacks aimed at SSL/TLS this year have focused on weaknesses in the wider SSL/TLS ecosystem.

Symantec has seen a much greater focus in the last year on the code libraries related to SSL/TLS implementations, and as a result, we have seen a regular stream of vulnerability updates and fixes.

That's the good news. But the most common unpatched vulnerabilities on web servers in the last year reveal that website owners aren't keeping up with the releases. It's vital that website managers maintain the integrity of their SSL/TLS implementations. It's not a fit-and-forget task.

Top 10 Vulnerabilities Found Unpatched on Scanned Web Servers

- *POODLE (Padding Oracle On Downgraded Legacy Encryption) exploited an outdated form of encryption (SSL 3.0) instead of TLS.*

	Name
1	SSL/TLS POODLE Vulnerability
2	Missing X-Content-Type-Options Header
3	Missing X-Frame-Options Header
4	SSL Certificate Signed using Weak Hashing Algorithm
5	Cross Site Scripting Vulnerability
6	Missing Strict-Transport-Security Header
7	SSL v2 support detected
8	Missing Secure Attribute in an Encrypted Session (SSL) Cookie
9	SSL Weak Cipher Suites Supported
10	SSL and TLS protocols renegotiation vulnerability

Although we didn't see any vulnerabilities as potentially dangerous as 2014's Heartbleed, OpenSSL released several updates and patches throughout 2015. OpenSSL is one of the most widely-used implementations of the SSL and TLS cryptographic protocols and is used on two-thirds of all web servers.

The updates it released were for vulnerabilities that ranged from low risk to high severity and which could allow attackers to carry out man-in-the-middle attacks to eavesdrop on secure communications or to launch denial-of-service attacks.

Checks and Balances

In order to strengthen the SSL/TLS ecosystem, Symantec has pushed for the widespread adoption of DNS Certification Authority Authorization (CAA). This allows an organization, or DNS owner, to specify which certificate authority (CA) it will buy SSL/TLS certificates from. If a malicious actor, or an employee who doesn't know company policy, tries to purchase a certificate from a CA not on the approved list, that CA can check the CAA and alert the DNS owner of the request.

This reduces the risk of rogue certificates being issued in a legitimate organization's name without its knowledge, which in turn would reduce the risk of criminals being able to set up certified phishing sites.

In an effort to better spot rogue certificates, Symantec is also complying with Google's request to log all EV certificates we issue on its Certificate Transparency log. As of March 2016, Symantec is also logging OV and DV certificates. Along with software that can monitor and audit certificates and their use, this creates, as its authors say, "an open framework that lets anyone observe and verify newly issued and existing SSL certificates in nearly real time."

Trust Services, Electronic Identification (eID), and Electronic Trust Services (eTS)

In September 2015, the European Commission completed the adoption of all the implementing acts required for adoption of the new eIDAS Regulation. This regulation marks a major change in the regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities across Europe.

Moreover, it is also an important step forward in promoting greater security requirements for Certificate Authorities (CAs) with the implementation of an EU Trust Mark for Qualified Trust Services. The new trust mark will help in clearly differentiating qualified trust services from others in the market, fostering greater transparency and confidence in such essential online services. ■

SOCIAL MEDIA, SCAMS, & EMAIL THREATS

SOCIAL ENGINEERING AND EXPLOITING THE INDIVIDUAL

The sophistication and ruthlessness of some of the attacks and tactics used by cybercriminals in 2015 have demonstrated how vulnerable individuals are online and chipped away at public confidence in online security. Data breaches, government surveillance, and good old-fashioned scams came together to further encroach on personal privacy, whether it is personal photos, login credential or medical histories. Personal data is anything but private.

Trust No One

In 2015, Symantec saw plenty of traditional scams and malware attacks intended to gather personal information. For example, one scam promised large numbers of followers for free on Instagram, while seeking to fool people into revealing their passwords. Some attacks impersonated tax officials in an attempt to trick people into downloading malicious email attachments.

In their simplest form, many scams still rely on the poor security habits of the general public to succeed. However, we have also seen how poor website security can expose customer data. In the latter example, it doesn't matter how strong a password may be if the website is vulnerable to a data breach.

More concerning are attacks in 2015 that made use of sophisticated social engineering to bypass the two-factor authentication systems designed to safeguard users.

By going through a legitimate password-reset process and posing as Google via SMS, however, one scam was able exploit the public's trust in a reputable brand to gain access to email accounts without raising the victims' suspicions.

How the Gmail Scam Works

An attacker obtains a victim's **email address** and **phone number**—both of which are usually publicly available.

The attacker poses as the victim and requests a password reset from Google.

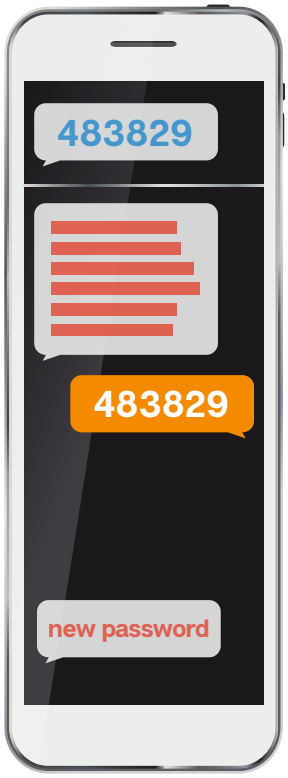
3

Google sends the code to the victim.

4

The attacker then texts the victim with a message similar to:

"Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity."



5

The victim therefore expects the password-reset verification code that Google sends out and passes it on to the attacker.

6

The attacker can then reset the password and once they have what they want or have set up forwarding, can inform the victim—again posing as Google—of their new temporary password, leaving the victim none the wiser.

Secrets and Lies

While traditional scams continued, 2015 also saw more salacious scams and threats to privacy.

Online 'sextortion' has been around for years, and more recent examples, particularly prevalent in Asia, have turned to malicious Android apps. These scammers, using an attractive avatar or profile picture, encourage the intended victim to share sexually-explicit videos. The criminals then encourage the victim to "continue the liaison" using an Android app, which also gathers the victim's phone number, account details, and all of their contacts.

Now with an incriminating video, and a list of the victim's friends and family, the gang threatens to send the sexually explicit content to the victim's entire contact list unless they pay up. Because of the sensitive nature of the threat, victims often find it difficult to go to the authorities and end up sending hundreds, if not thousands, of dollars to the attacker.

In the wake of the Ashley Madison attack, a spike in spam messages with subject lines like "How to Check if You Were Exposed in Ashley Madison Hack" or "Ashley Madison hacked, is your spouse cheating?" were reported. The hack was perhaps more unusual in that its ramifications went well beyond the financial sphere to affect people's personal relationships and reputations.

Social Engineering Using Social Media

Social media remains a favored target of scammers, as criminals seek to leverage the trust people have in their own social circles to spread scams, fake links, and phishing. To succeed, the social engineering involved must be convincing, and so we see more progressive and ingenious tactics to dupe potential victims.

One scam in particular went to great lengths to create an entire family tree of hundreds of thousands of fake Twitter accounts, each branch boosting the credibility of the one above, to gain followers, and retweets from genuine Twitter users. At the top of the family tree were accounts impersonating news outlets and celebrities, even curating real tweets from the genuine accounts to make them seem more credible.

Through the discovery of these imposter accounts, we identified three account types that were being used:

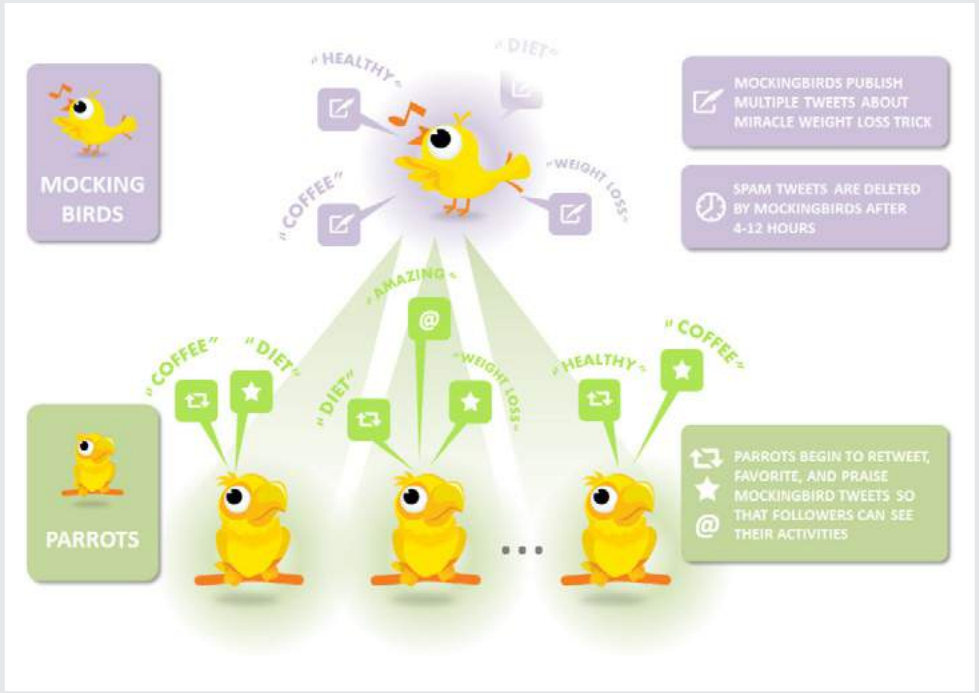
- 'Mockingbird' accounts: use brand and celebrity imagery for impersonation
- 'Parrot' accounts: fake accounts using stolen tweets and photographs of real women
- 'Egg' accounts: act like new users with no tweets and use the default "egg" avatar

Each tweet from a Mockingbird account received nearly 1,000 retweets and 500 favorites, which were not genuine, as they originated from a secondary account, which we called the Parrot. In turn, Parrot accounts, follow anyone and everyone in the hope that genuine Twitter users will follow them back, a remarkably effective tactic.

If these Parrot accounts only retweeted spam from the Mockingbird accounts, they would quickly be spotted, which is why they also posted other tweets too, typically copying tweets and retweeting memes from genuine Twitter users.

On the other hand, the majority of Egg accounts never composed a single tweet. Instead, they would simply be used to bolster the number of followers of the Parrot accounts in the hundreds.

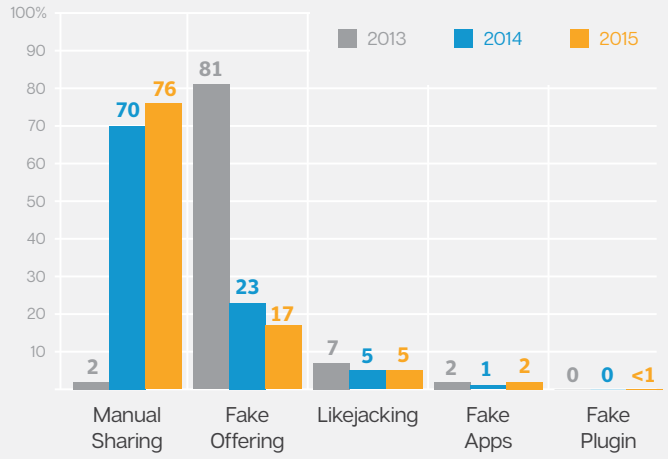
This complex operation centered on weight-loss spam. The operators went to great lengths to avoid anti-spam measures and were able to operate for a long time.



Graphic showing how the spam operation works. Taken from white paper.

Social networking scams require some form of interaction, and manual sharing remained the main route for social media attacks in 2015, expanding on the technique that had snowballed in the previous year.

Social Media



- **Manual Sharing** – *These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers, or messages that they share with their friends.*
- **Fake Offering** – *These scams invite social network users to join a fake event or group with incentives, such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.*
- **Likejacking** – *Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.*
- **Fake Apps** – *Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described, and may be used to steal credentials or harvest other personal data.*
- **Fake Plugin** – *Users are invited to install a plugin to view a video, but the plugin is malicious and may spread by re-posting the fake video message to a victim's profile page without permission. Examples include installing a fake YouTube premium browser extension to view the video, or noticing that a DivX plugin is required, and the fake plugin masquerades as such. For more information visit: http://www.symantec.com/connect/blogs/fake-browser-plug-new-vehicle-scammers*

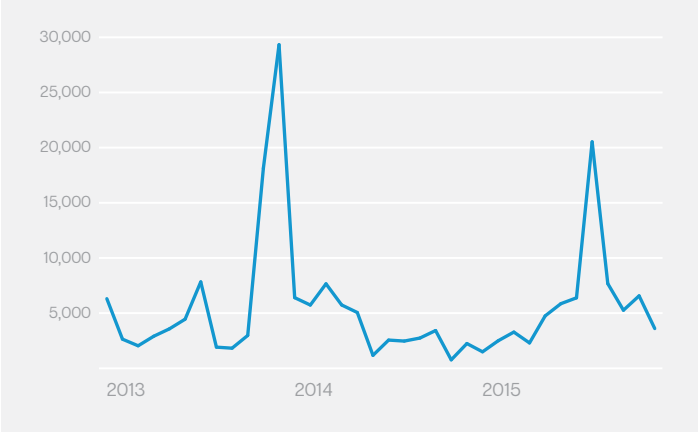
Language and Location Is No Barrier

Other forms of attack seen in 2015 also prove just how sophisticated and ruthless criminals are willing to be to make a profit. Wherever you live or whatever language you speak, you could still be under threat from cyber attackers. Take Boleto, a payment system used in Brazil for example. Boleto may be considered a niche, very local system, and yet in 2015, three malware families emerged specifically targeting it.

Similar localized attacks around the world show that cybercriminals are putting in the effort to manipulate victims no matter the location or the language. Adapting phishing scams using phishing toolkits makes it extremely easy to conduct a campaign against a target in one country, change the templates, and quickly target another elsewhere. Often the language used in such localized attacks has been automatically translated through the templates and may appear convincing to a non-native speaker.

Number of Phishing URLs on Social Media

- *The chart shows how social media has played a crucial role in the social engineering of attacks in the past. In recent years, these sites have clamped-down on such abuses, and made it much harder for the attackers to exploit them.*



Safeguarding Against Social Engineering

Cybercrime costs the global economy up to US$575 billion annually according to BofA Merrill Lynch Global Research, whose report goes on to say that in a potential worst-case 2020 'Cybergeddon' scenario, cybercrime could extract up to a fifth of the value created by the Internet.

It is everyone's responsibility to do all they can to prevent that from happening.

For consumers, it's time kick bad habits. Many people know the basics of good cybersecurity, yet people continue to share their passwords. In fact more than a third of people who share passwords in the United States have shared the password to their online banking account. People need to start taking more responsibility for shoring up their online security.

Users should more wary of who they follow on social media. Bots can appear more and more like a real person, and are sometimes difficult to spot. When choosing who to trust on social media, consider the following advice:

- **Be skeptical of new followers.** If a random person follows you, do not automatically follow them back. Look at their tweets. Are they retweeting content that looks like spam? If they are, they are most likely a bot.
- **Numbers can lie.** Even if these random followers have tens of thousands of followers, those numbers can easily be faked. Do not base your decision to follow them back based on how many people follow them.
- **Look for the "verified" badge.** Twitter users should always check to see if a well-known brand or famous celebrity has been verified by Twitter before following. The blue verified badge denotes that Twitter has authenticated the true owner of an account.

Taking risks with cybersecurity is not acceptable, and we should reject the misconception that privacy no longer exists. Privacy is something precious, and should be protected carefully.

For businesses, this means approaching security in terms of education, cybersecurity awareness training, and good digital hygiene. Every employee should be part of the effort to stay digitally healthy. CIOs and IT managers need to be aware of just how many risks they face and start proactively monitoring for symptoms so that they can diagnose digital diseases before putting customer data and customer confidence at risk.

EMAIL AND COMMUNICATIONS THREATS

IT systems continue to come under attack from rapidly evolving malware. Email remains the medium of choice for cybercriminals and email volumes continue to grow, as phishing and spam decline—the latter of which accounted for more than half of inbound email traffic. Phishing attacks were more targeted and malicious emails grew in number and complexity, highlighting how email remains an effective medium for cybercriminals.

Email Abuse

Email continues to dominate digital communications, regardless of the rising popularity of instant messaging technology for both business and consumer use. Symantec estimates there were approximately 190 billion emails in circulation each day in 2015, a number that we predict to grow by as much as 4 percent by the end of 2016. On average, each business user sent and received 42 emails each day, and a growing number of individuals were reading email on mobile devices. For cybercriminals who want to reach the largest number of people electronically, email is still the favored way to do it.

No wonder it is still widely used by Internet criminals for spam, phishing, and email malware. In 2015, Symantec saw email threats decline. Email-based attacks from phishing and malware are categorized as spam, and accounted for approximately one percent of all spam email. Symantec provides further analysis of spam classified as malware and phishing, as these threats have potentially significant, harmful consequences.

Symantec scans a significant proportion of the global business email traffic, giving us a unique insight into this medium and the security threats it poses. Many business emails will never be sent outside of an organization, with approximately three quarters of external business email traffic being inbound, more than half of which was spam.

Spam Trends

More than half of inbound business email traffic was spam in 2015, despite a gradual decline over recent years. In 2015, spam reached its lowest level since 2003. However, the spam problem is not going away. Spammers are finding other ways to reach their audiences, including the use of social networking and instant messaging, two of the most popular types of applications found on mobile devices. In exploiting them in addition to email, spammers continually seek to evolve their tactics.

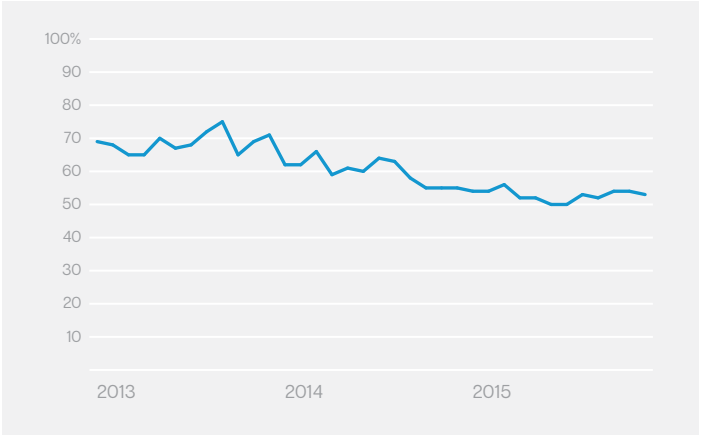
In addition, Symantec has observed an increase in what is commonly known as "snowshoe spam." As an analogy, snowshoes are designed to spread the wearer's weight across a wide area, and snowshoe spamming distributes large volumes of spam across a wide range of IP addresses. As the name implies, this technique seeks to circumvent anti-spam technology, such as propagation latency and IP address reputation, by sending large volumes of spam messages in very short bursts. By also quickly rotating domains and recirculating IP addresses, this can make them more difficult to block quickly.

Overall Email Spam Rate

2013	2014	2015
		
66%	60%	53%
	-6% pts	-7% pts

Estimated Global Email Spam Rate per Day

In June, spam fell below 50 percent for the first time since 2003.



Percentage of Spam in Email by Industry

Some industry sectors receive more spam than others, but the range is only approximately 5 percent.

Industry Detail	Percentage of Email as Spam
Mining	56.3%
Manufacturing	54.2%
Construction	53.7%
Services	53.0%
Agriculture, Forestry, & Fishing	52.9%
Retail Trade	52.7%
Nonclassifiable Establishments	52.6%
Wholesale Trade	52.5%
Public Administration	52.2%
Finance, Insurance, & Real Estate	52.1%
Transportation & Public Utilities	51.8%
Non SIC Related Industries	
Healthcare	54.1%
Energy	53.0%

Spam by Company Size

No particular company size received significantly more spam than any other did, with a range of only 1.5 percent.

Company Size	Spam % in Email
1-250	52.9%
251-500	53.3%
501-1000	53.3%
1001-1500	51.9%
1501-2500	52.6%
2501+	52.5%

Phishing Trends

Over the years, phishing campaigns have become much easier to operate, thanks to the evolving cybercriminal marketplace. Attackers will cooperate, with some specializing in phishing kits, and others selling them on to other scammers who want to conduct phishing campaigns.

These kits often trade for between US$2 and $10, and their users do not require much in the way of technical skills to operate them or customize their webpages to suit their needs. Scammers may use the data stolen from these attacks for their own purposes, or sell it on underground marketplaces for a profit.

Symantec has reported a concerning increase in the number and sophistication of phishing attempts, targeting specific departments within organizations. While some phishing attempts may seem obvious, such as a fake delivery tracking emails, the Legal and Finance departments at some company were targeted with well-crafted phishing attacks.

Some of these included wire transfer attempts, and while it may seem surprising, some companies have lost millions of dollars because employees were fooled into believing wire transfer requests and other phishing attacks were genuine. The social engineering involved in these phishing attacks is more sophisticated and targeted. They not only send generic scams to large numbers of people, but seek to develop ongoing relationships, validate access to company information, and build trust.

Social engineering requires research and reconnaissance, reviewing social media profiles, and the online activity of potential targets to learn about their job, their co-workers, and the organizational structure. With this information so easily obtained online, phishing emails are more personalized, and convincing—displaying an understanding of the business and knowledge of key executives and work processes.

Many businesses are a prime target, and an assumption that technology can provide automatic protection is a false one. While leveraging sophisticated controls and technology for protection, organizations still rely on the capability of its employees to detect advanced and targeted phishing campaigns.

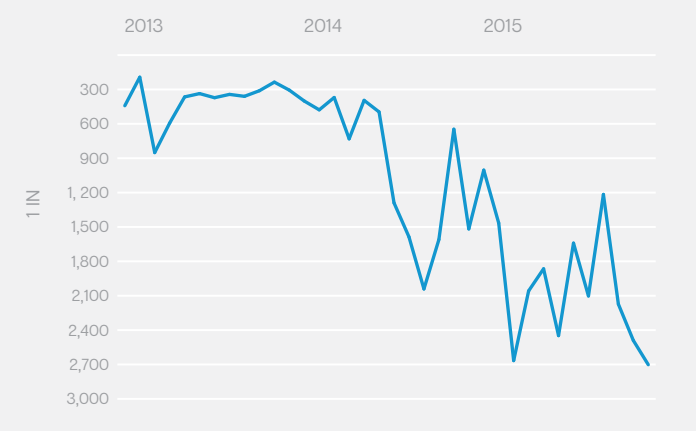
One successful attempt can do serious harm to a company's reputation and credibility.

Email Phishing Rate (Not Spear Phishing)

2013	2014	2015
1 in 392	1 in 965	1 in 1,846

Phishing Rate

▶ *Phishing numbers in 2015 continued to fluctuate, but remained in gradual decline throughout the year.*



Phishing Ratio in Email by Industry

▶ *Retail was the industry sector most heavily exposed to phishing attacks in 2015.*

Industry Detail	Phish Email Ratio
Retail Trade	1 in 690
Public Administration	1 in 1,198
Agriculture, Forestry, & Fishing	1 in 1,229
Nonclassifiable Establishments	1 in 1,708
Services	1 in 1,717
Manufacturing	1 in 1,999
Finance, Insurance, & Real Estate	1 in 2,200
Mining	1 in 2,225
Wholesale Trade	1 in 2,226
Construction	1 in 2,349
Transportation & Public Utilities	1 in 2,948
Non SIC Related Industries	
Energy	1 in 2,525
Healthcare	1 in 2,711

Phishing Rate in Email

▶ *No particular company size received significantly more spam than any other did, with a range of only 1.5 percent.*

Company Size	Phishing Rate in Email
1-250	1 in 1,548
251-500	1 in 758
501-1000	1 in 1,734
1001-1500	1 in 2,212
1501-2500	1 in 1,601
2501+	1 in 2,862

Email Malware Trends

As with phishing fraud, malware distributed in emails requires social engineering to convince its recipient to open the attachment or to click on a link. Attachments can be disguised as fake invoices, office documents, or other files, and often exploits an unpatched vulnerability in the software application used to open that type of file. Malicious links may direct the user to a compromised website using a web attack toolkit to drop something malicious onto their computer.

Threats like Dridex exclusively use spam email campaigns, and incorporate real company names in the sender address and in the email body. The vast majority of Dridex spam masquerades as financial emails, such as invoices, receipts, and orders. The emails include malicious Word or Excel attachments with a payload that drops the actual malware designed to target online banking information.

The cybercriminal group behind this particular attack has used many different techniques for sending spam and malware: from simple malware attachments, hyperlinks in the message body that point to an exploit kit landing page, malicious PDF attachments, and document macros.

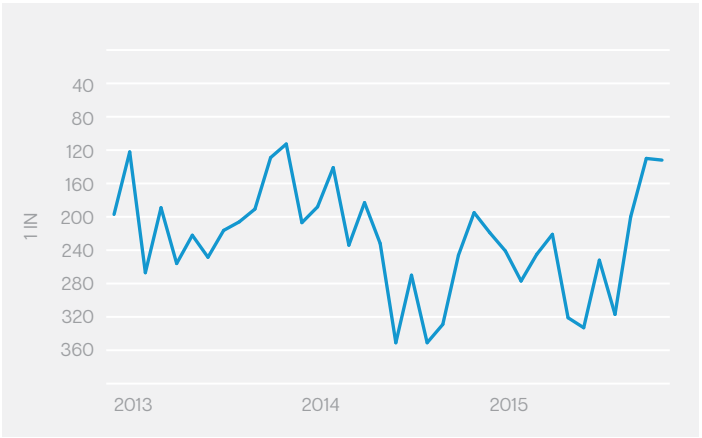
Email malware has not been in decline in the same way as general spam, and because of its relatively low volume in comparison, it is more subject to fluctuation. Spikes occur when large campaigns are undertaken.

Email Malware Rate (Overall)

2013	2014	2015
1 in 196	1 in 244	1 in 220

Proportion of Email Traffic in Which Virus Was Detected

▶ *The overall email malware rate for 2015 increased since 2014. Email remains an effective medium for cybercriminals.*



Malicious File Attachments in Email

▶ *In 2015, Office documents were the most popular attachment type, with executable files becoming less popular. Overall 1.3 percent of attachment types were executable, including .exe, .com, .pif, .bat and others.*

Rank	File Extension	Blocked in Emails
1	.doc	55.8%
2	.xls	15.0%
3	.zip	8.7%
4	.htm	7.9%
5	.docm	2.4%
6	.js	2.2%
7	.mso	1.9%
8	.html	1.6%
9	.exe	0.9%
10	.png	0.8%

Virus Ratio in Email by Industry

- *The retail sector had the highest rate of malware-borne malware in 2015, with more than one percent of email classified as malicious.*

Industry Detail	Ratio of Malware in Email
Retail Trade	1 in 74
Public Administration	1 in 151
Agriculture, Forestry, & Fishing	1 in 187
Services	1 in 199
Wholesale Trade	1 in 234
Construction	1 in 240
Manufacturing	1 in 243
Nonclassifiable Establishments	1 in 277
Mining	1 in 304
Finance, Insurance, & Real Estate	1 in 310
Transportation & Public Utilities	1 in 338
Non SIC Related Industries	
Energy	1 in 319
Healthcare	1 in 396

Ratio of Malware in Email Traffic by Company Size

- *The highest rate of malware in email traffic was in the 251-1000 company size grouping. The range was 0.4 percent.*

Company Size	Malware Rate in Email
1-250	1 in 184
251-500	1 in 82
501-1000	1 in 189
1001-1500	1 in 312
1501-2500	1 in 168
2501+	1 in 352

Communications Attacks

We saw a succession of attacks and vulnerabilities in the underlying encryption used to secure email transmissions. For example, the Logjam attack exploits a weakness in the key exchange mechanism that begins any encrypted exchange.

- *Customers can check their domains for Logjam, and other major vulnerabilities, using Symantec's SSL Toolbox.*
- *Use this free tool to check for major issues, such as POODLE or Heartbleed, as well as potential errors in your SSL/TLS certificate(s) installation.*

Email Encryption

Email encryption is valuable because it protects the privacy of messages and can help to authenticate senders. It is under threat because of vulnerabilities in the underlying technology (see above) but also because it is not widely used.

Although webmail systems such as Microsoft's Outlook.com and Google Mail use encryption on the clients, and almost all email systems prioritize encrypted transmission, a surprising proportion of email is sent in the clear using unencrypted SMTP transfers. Google reports that in 2015, around 57 percent of inbound emails were encrypted compared with 51 percent the year before. The number of outbound encrypted emails rose from 65 percent to 80 percent in the same period. It isn't unusual for some spam to be sent using encryption. As long ago as 2010, the Rustock botnet used TLS encryption as a means to disguise the spam it was sending.

Good desktop and gateway email encryption tools do exist, including Symantec's own, but companies need to make better use of the technology available to them to protect email in transit and at rest.

Email Security Advice

Organizations and individuals need to realize that even if they do not think they are an obvious target for cybercriminals, it does not mean they are immune.

On a personal level, this means remaining vigilant by:

- Not opening emails from unknown senders
- Looking for the padlock and checking the encryption certificate on any sites where you enter sensitive data
- Not using unsecure networks when accessing sensitive data

For organizations to remain vigilant by:

- Deploying email encryption where possible
- Ensuring that email is scanned for malware, spam, and phishing
- Using web security systems to block access to known phishing sites

Looking Ahead

With a continual three-year decline, we expect phishing attacks to remain at least at current levels, if not decline further. Phishing attacks have become more targeted, and less scattergun. Many attacks have shifted towards social media, adding to the decline in email numbers. Some parts of the world suffer more from email phishing attacks than others—with the greatest decline in many English-speaking countries, North America and parts of Western Europe.

People will continue to do more and more online, and because Internet access and online transactions are growing in popularity among developing countries, we may even see growth in phishing attacks in these areas. For example, paying utility bills, booking doctors' appointments, applying to a university, managing frequent flyer accounts, and taking out insurance all provide fruitful inspiration for phishing attacks.

As organizations deliver more services online they need to be mindful of the need for security, and they have to work with customers to educate them further and build trust. In addition, they may need to consider two-factor authentication to ensure customer confidence and reduce the cost of phishing fraud.

As we have noted, cybercriminals are increasingly moving towards more complex email threats, where malware authors, ransomware creators, phishers, and scammers will seek to exploit what they perceive to be the weakest link in the chain—humans. Social engineering, or "head hacking," is a vital ingredient to any would-be attacker that is trying to gain access to systems that hold potentially valuable information. ■

TARGETED ATTACKS

TARGETED ATTACKS, SPEAR PHISHING, AND INTELLECTUAL PROPERTY THEFT

Widespread, persistent, and sophisticated attacks against government organizations and businesses of all sizes pose greater risks to national security and the economy. The number of zero-day vulnerabilities grew, and evidence of them being weaponized for use in cyberattacks was revealed. Spear-phishing campaigns became stealthier, targeting fewer individuals within a smaller number of select organizations.

Persistent Attacks

In February 2015, 78 million patient records were exposed in a major data breach at Anthem, the second largest healthcare provider in the US. Symantec traced the attack to a well-funded attack group, named Black Vine, that has associations with a China-based IT security organization, called Topsec. Black Vine is responsible for carrying out cyberespionage campaigns against multiple industries, including energy and aerospace, using advanced, custom-developed malware.

Other high-profile targets of cyberespionage in 2015 included the White House, the Pentagon, the German Bundestag, and the US Government's Office of Personnel Management, which lost 21.5 million personnel files, including sensitive information such as health and financial history, arrest records, and even fingerprint data.

These attacks are part of a rising tide of sophisticated, well-resourced, and persistent cyberespionage attacks around the world. Targets include state secrets, intellectual property such as designs, patents, and plans, and as evidenced by recent data breaches, personal information.

Symantec's continuing investigation into the Regin Trojan gives us a further glimpse into the technical capabilities of state-sponsored attackers. It revealed 49 new modules, each of which adds new capabilities, such keylogging, email and file

access, and an extensive command-and-control infrastructure. Symantec analysts commented that the level of sophistication and complexity of Regin suggests that the development of this threat could have taken well-resourced teams of developers many months or years to develop.

Currently, spear-phishing and watering-hole attacks that exploit compromised websites are the favored avenues for targeted attacks. However, as additional layers of technology are introduced to an organization, its attack surface expands. With businesses turning more to cloud technology and the prevalence of IoT devices, we expect to see targeted attacks seeking to exploit vulnerabilities in these systems within the next year or two. Cloud services particularly vulnerable to exploits, such as SQL injection flaws, will likely be targeted first. Spear-phishing campaigns exploiting misconfiguration and poor security by users, rather than cloud service providers, will bear low-hanging fruit for the attackers.

In order to remain below the radar, spear-phishing campaigns have increased in number, but have become smaller with fewer individuals targeted in each campaign. We expect spear-phishing campaigns will soon consist of just a single target, or a few select individuals at the same organization. Moreover, the larger spear-phishing campaigns will likely all be conducted using web-based watering hole attacks, with compromised websites exploiting highly-coveted zero-day vulnerabilities.

Zero-Day Vulnerabilities and Watering Holes

Zero-day vulnerabilities are particularly valuable to attackers. Indeed, because zero-day vulnerabilities are such a seemingly rare commodity, attackers will closely guard their exploits so that they may be used for longer and remain undetected.

Sophisticated watering-hole attacks, using compromised websites, activate only when a visitor to that website originates from a particular IP address. Reducing collateral damage in this way makes it less likely that the covert attack is discovered. Moreover, this approach also makes it more difficult for security researchers who may visit the website from a different location. Once an exploit is disclosed publically by the relevant vendor, these watering-hole sites will often switch to using another unpublished exploit for a different zero-day vulnerability in order to remain hidden.

The breach of Hacking Team in 2015 stood out because the attackers weren't after money or identities; they were after cyberweapons, such as zero-day exploits. Hacking Team is an Italian outfit that specializes in covert surveillance and espionage software marketed at government users. Previously unknown zero-day exploits were uncovered in the attack and made public by the attackers. Details of weaponized zero-day vulnerabilities and numerous Trojans used by the group were shared within days on public forums, and within hours, exploit kit authors had integrated them into their exploit toolkits.

Diversity in Zero Days

There was an unprecedented 54 zero-day vulnerabilities found throughout 2015, more than doubling the number found in the previous year. Discovering unknown vulnerabilities and figuring out how to exploit them has clearly become a go-to technique for advanced attackers, and there is no sign of this trend changing.

Zero-Day Vulnerabilities

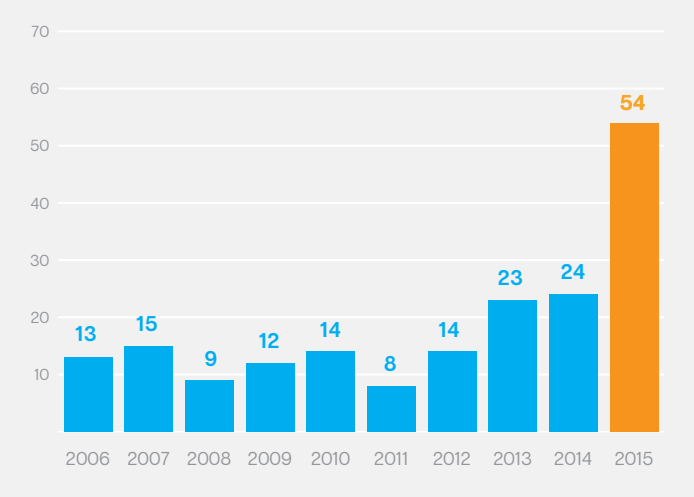
▶ *Zero-day vulnerabilities command high prices on the black market. Because of this, and because of their very nature we believe that the number of zero-day vulnerabilities yet to be discovered is much higher.*

2013	Change	2014	Change	2015
23	+4%	24	+125%	54

Most of the zero days seen in 2015 target old, "faithful" technologies that have been targeted for years. Attackers racked up 10 individual zero-day vulnerabilities against Adobe's Flash Player during the year. Microsoft received equal attention from malicious zero-day developers, though the 10 zero day vulnerabilities found targeting their software was distributed across Microsoft Windows (6x), Internet Explorer (2x), and Microsoft Office (2x). The Android operating system was also targeted through four zero-day vulnerabilities during 2015.

Zero-Day Vulnerabilities, Annual Total

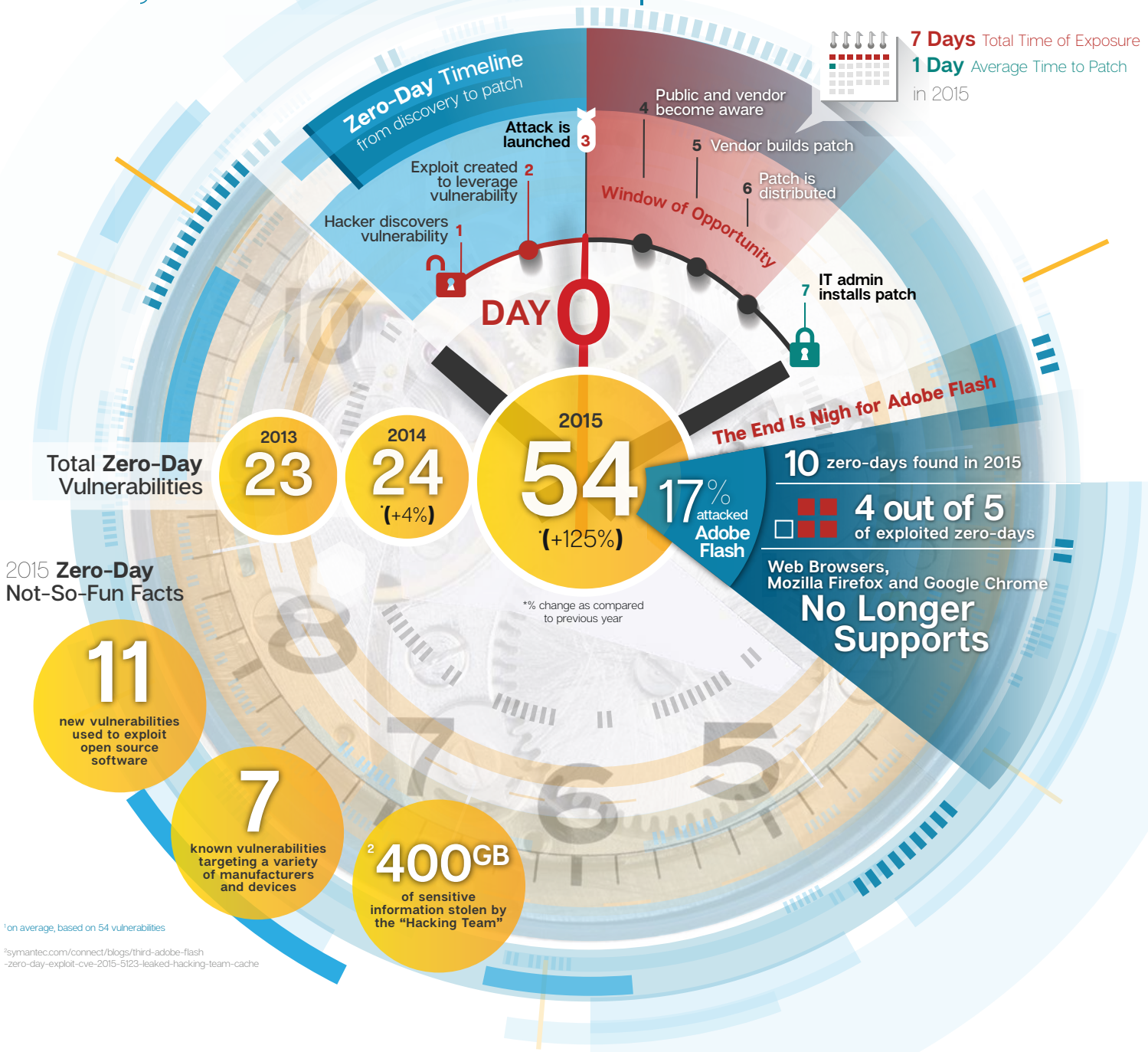
▶ *The highest number of zero-day vulnerabilities was disclosed in 2015, evidence of the maturing market for research in this area.*



A New Zero-Day Vulnerability Discovered [1] Every Week in 2015

Advanced attack groups continue to profit from previously undiscovered flaws in browsers and website plugins.

In 2015, 54 zero-day vulnerabilities were discovered.



[1] on average, based on 54 vulnerabilities

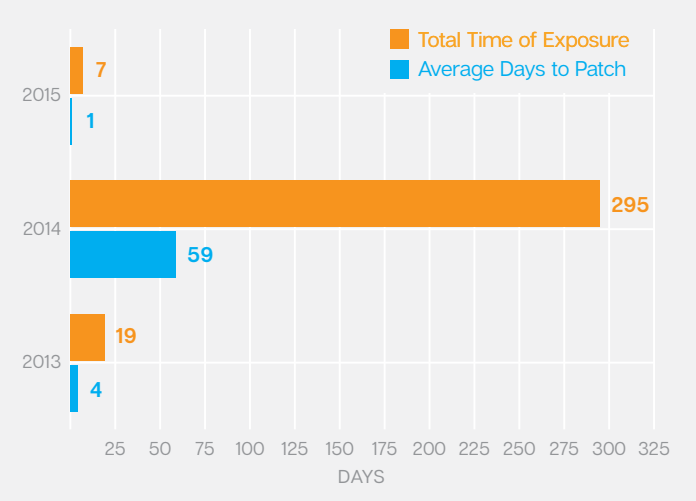
[2] symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache

What is concerning, though not surprising, is that there were 11 zero-day vulnerabilities that were used to exploit open source software. Some exploits targeted common libraries and packages, while others went after open source web development tools, like content management systems and e-commerce platforms. Networking protocols were also highly targeted, with continued attacks against OpenSSL, as well as Samba.

However, what should give most people cause for concern is that attackers appear to be discovering and exploiting zero-day vulnerabilities in industrial control systems (ICSs)—devices used to control things ranging from industrial manufacturing to power plants. There were six known zero-day vulnerabilities during 2015 targeting a variety of different manufacturers and different devices.

Top 5 Zero-Day Vulnerabilities, Patch and Signature Duration

▶ *While there were more zero-day vulnerabilities disclosed in 2015, some were proof-of-concept, but vendors were generally quicker to provide fixes in 2015 than in 2014..*



The motivations behind such attacks are not clear, and could range from geopolitical disputes to ransom-related attacks. Regardless, if not monitored carefully, such attacks could have serious consequences in the future, and it doesn't look likely to go away anytime soon.

Top 5 Most Frequently Exploited Zero-Day Vulnerabilities

▶ *With the exception of CVE-2015-0235, the most frequently targeted zero-day exploits were related to vulnerabilities in Adobe's Flash Player.*

	2015 Exploit	2015	2014 Exploit	2014
1	Adobe Flash Player CVE-2015-0313	81%	Microsoft ActiveX Control CVE-2013-7331	81%
2	Adobe Flash Player CVE-2015-5119	14%	Microsoft Internet Explorer CVE-2014-0322	10%
3	Adobe Flash Player CVE-2015-5122	5%	Adobe Flash Player CVE-2014-0515	7%
4	Heap-Based Buffer Overflow aka 'Ghost' CVE-2015-0235	<1%	Adobe Flash Player CVE-2014-0497	2%
5	Adobe Flash Player CVE-2015-3113	<1%	Microsoft Windows CVE-2014-4114 OLE	<1%

In the case of CVE-2015-5119, Symantec already had signatures that were able to detect exploits four days before the vulnerability was publically disclosed. Sometimes, existing signatures can be successful in blocking attacks exploiting new vulnerabilities, and signatures are frequently updated to block more attacks even where protection exists beforehand. Additionally, this vulnerability was among those exposed in the breach against Hacking Team.

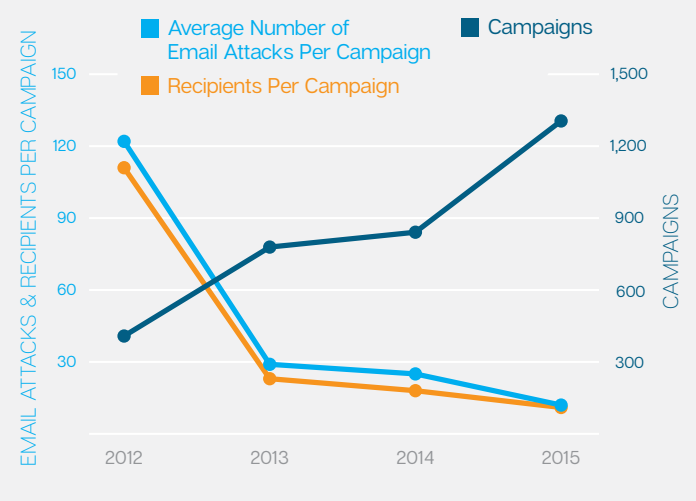
Spear Phishing

It's not only websites that may contain hidden exploits. A previously-unknown vulnerability may be exploited to attack an organization using an infected document attached in an email. Such an attack is known as spear phishing, and relies heavily on very good social engineering in order to dress-up the email to appear convincing.

Spear-phishing emails are sent in waves, or campaigns, to a very small group of people, often not all at once, but individually or where more than one person in an organization may be targeted. Over time, different exploits may be used against the same people, should these attacks prove ineffective. However, in recent years attackers quickly switch tactics after a few failed attempts in order to remain undetected. In previous years, they were more likely to continue with different exploits or by targeting different individuals within the organization.

Spear-Phishing Email Campaigns

In 2015, the number of campaigns increased, while the number of attacks and the number of recipients within each campaign continued to fall. With the length of time shortening, it's clear that these types of attacks are becoming stealthier.



	2013	2014	2015
Campaigns	779 +91%	841 +8%	1,305 +55%
Recipients per Campaign	23 -81%	18 -20%	11 -39%
Average Number of Email Attacks per Campaign	29 -76%	25 -14%	12 -52%
Average Duration of a Campaign	8 Days +173%	9 Days +13%	6 Days -33%

Spear-phishing attacks are less likely to arouse suspicion with campaigns that are smaller, shorter, and target fewer recipients. A few years ago, a targeted attack campaign may have been directed to a hundred or more individuals, any one of whom may become suspicious and raise the alarm. With fewer people, this probability is greatly reduced.

In 2015, the Finance sector was the most targeted, with 34.9 percent of all spear-phishing email directed at an organization in that industry, 15 percentage points higher than the previous year. The likelihood of an organization in this sector being targeted at least once in the year was 8.7 percent (approximately 1 in 11). With so many attacks destined for this sector, some businesses were being targeted more aggressively than others. Typically, such an organization may expect to be targeted at least four times during the year. The attackers only have to succeed once, whereas the businesses must thwart each and every attack to remain secure. Businesses should already be thinking about what to do *when* (not *if*) such a breach occurs.

Top Industries Targeted in Spear-Phishing Attacks

In 2015, we combined the Services groups (previously, "Services, Professional" and "Services, Non-Traditional") into one group. We have also identified some of the most frequently targeted sub-sectors, including the Energy sector, which includes some mining industries, and Healthcare, which is part of the Services category.

**The Risk in Group figure is a measure of the likelihood of an organization in that industry being attacked at least once during the year. For example, if there are 100 customers in a group and 10 of them were targeted, that would indicate a risk of 10 percent.*

Industry Detail	Distribution	Attacks per Org	% Risk in Group*
Finance, Insurance, & Real Estate	35%	4.1	8.7%
Services	22%	2.1	2.5%
Manufacturing	14%	1.8	8.0%
Transportation & Public Utilities	13%	2.7	10.7%
Wholesale Trade	9%	1.9	6.9%
Retail Trade	3%	2.1	2.4%
Public Administration	2%	4.7	3.2%
Non-Classifiable Establishments	2%	1.7	3.4%
Mining	1%	3.0	10.3%
Construction	<1%	1.7	1.1%
Agriculture, Forestry, & Fishing	<1%	1.4	2.0%
Non SIC Related Industries			
Energy	2%	2.0	8.4%
Healthcare	<1%	2.0	1.1%

Industries Targeted in Spear-Phishing Attacks by Group – Healthcare

▶ *Healthcare falls under the Services SIC group, but we have called it out here for clarity.*

Industry Detail	Distribution	Attacks per Org	% Risk in Group*
Health Services	<1%	2.0	1%

Industries Targeted in Spear-Phishing Attacks by Group – Energy

▶ *Energy companies are classified in the Mining category or the Transportation and Utilities category, depending on the nature of their business. We have called these out here for clarity.*

Industry Detail	Distribution	Attacks per Org	% Risk in Group*
Energy	1.8%	2.0	8.4%
Oil & Gas Extraction	1.4%	3.4	12.3%
Electric, Gas, & Sanitary Services	<1%	1.6	5.7%
Coal Mining	<1%	1.0	8.1%

Industries Targeted in Spear-Phishing Attacks by Group – Finance, Insurance, & Real Estate

▶ *Depository Institutions include organizations in the retail banking sector.*

Industry Detail	Distribution	Attacks per Org	% Risk in Group*
Finance, Insurance, & Real Estate	34.9%	4.1	8.7%
Depository Institutions	18.9%	5.9	31.3%
Holding & Other Investment Offices	8.3%	2.9	11.0%
Nondepository Institutions	3.7%	6.7	5.3%
Real Estate	1.4%	2.4	2.2%
Insurance Agents, Brokers, & Service	<1%	2.1	4.0%
Insurance Carriers	<1%	1.6	10.1%
Security & Commodity Brokers	<1%	2.2	3.7%

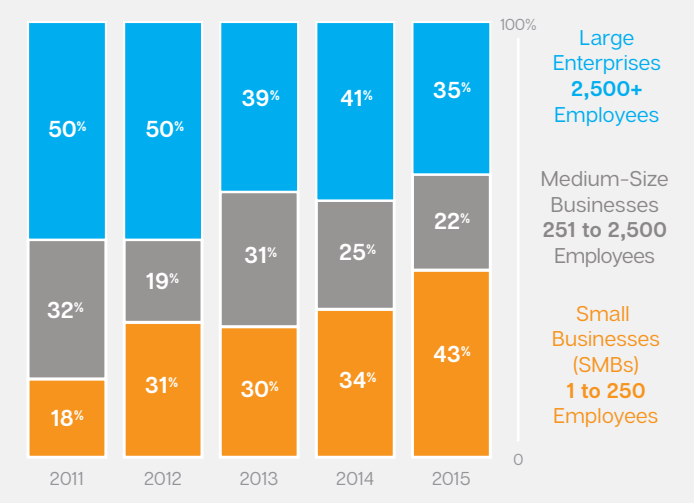
Industries Targeted in Spear-Phishing Attacks by Group – Public Administration

▶ *The Public Administration sector includes both national, central government agencies as well as local government.*

Industry Detail	Distribution	Attacks per Org	% Risk in Group*
Public Administration	2.0%	4.7	3.2%
Executive, Legislative, & General	1.8%	5.7	3.6%
Justice, Public Order, & Safety	<1%	4.3	1.1%
Administration of Economic Programs	<1%	1.1	7.3%
National Security & International Affairs	<1%	2.5	3.5%
Administration of Human Resources	<1%	1.0	2.0%

Spear-Phishing Attacks by Size of Targeted Organization

- *Attacks against small businesses continued to grow in 2015, although many of these attacks were directed to fewer organizations, increasing by 9 percentage points.*



Risk Ratio of Spear-Phishing Attacks by Organization Size

- *Small businesses had a 1 in 40 (3 percent) chance of being targeted, indicating a convergence of attacks on fewer organizations. Large enterprises had a 1 in 2.7 (38 percent) chance, suggesting a much broader focus in attacks, with a higher frequency.*

Industry Detail	2015 Risk Ratio	2015 Risk Ratio as %	Attacks per Org
Large Enterprises 2,500+ Employees	1 in 2.7	38%	3.6
Medium Business 251–2,500	1 in 6.8	15%	2.2
Small Business (SMB) 1–250	1 in 40.5	3%	2.1

Analysis of Spear-Phishing Emails Used in Targeted Attacks

- *Office documents, such as Word and Excel, remain popular as a delivery mechanism for exploits that drop malware onto a targeted computer. Perhaps surprisingly, executable file types are still popular, however, accounting for at least 36 percent of the spear-phishing attachments in 2015. In non-targeted email malware, executable file attachment accounted for approximately 1.3 percent of malicious attachments.*

Rank	Attachment Type	2015 Overall Percentage	Attachment Type	2014 Overall Percentage
1	.doc	40.4%	.doc	38.7%
2	.exe	16.9%	.exe	22.6%
3	.scr	13.7%	.scr	9.2%
4	.xls	6.2%	.au3	8.2%
5	.bin	5.4%	.jpg	4.6%
6	.js	4.2%	.class	3.4%
7	.class	2.6%	.pdf	3.1%
8	.ace	1.7%	.bin	1.9%
9	.xml	1.6%	.txt	1.4%
10	.rtf	1.4%	.dmp	1.0%

Active Attack Groups in 2015

Some of the more notable targeted attack groups that were active in 2015 included the following:

- Black Vine – Attacks associated with an IT security organization Topsec, primarily targeting aerospace and healthcare, including Anthem, in search of intellectual property and identities
- Advanced Threat Group 9 (ATG9, a.k.a. Rocket Kitten) – Iran based state-sponsored espionage attacks on journalists, human rights activists, and scientists
- Cadelle and Chafer – Iran-based and attacking mainly airlines, energy, and telcos in the Middle East, and one company in the US
- Duke and Seaduke – State-sponsored attacks against mainly European government agencies, high-profile individuals, and international policy and private research organizations; believed to have been around since 2010

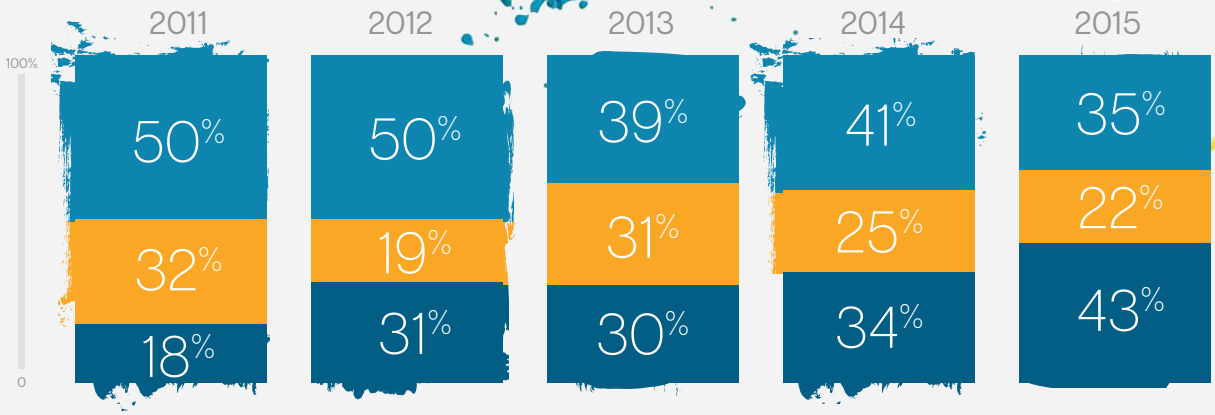
Attackers Target Both Large and Small Businesses

Like thrown paint on a blank canvas, attacks against businesses–both large and small–are indiscriminate. **If there is profit to be made, attackers strike at will.**

The last five years have shown a steady increase in attacks targeting **businesses with less than 250 employees.**

Number of Employees
- Large Enterprises **2,500+**
- Medium-Size Businesses **251 to 2,500**
- Small Businesses (SMBs) **1 to 250**

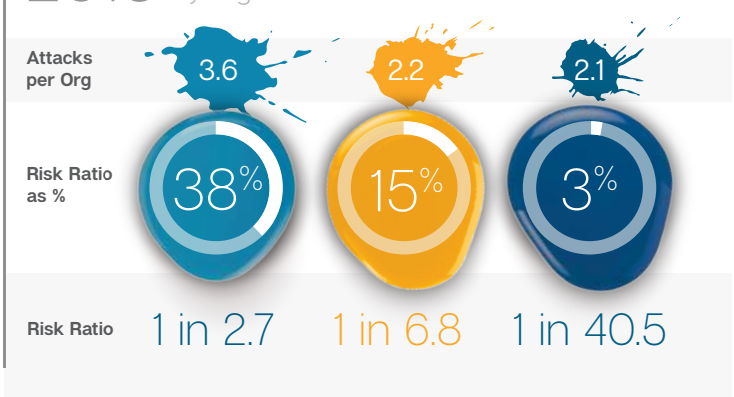
Spear-Phishing Attacks by Size of Targeted Organization



Cyber attackers are playing the long game against large companies, but all businesses of all sizes are vulnerable to targeted attacks. **In fact, spear-phishing campaigns targeting employees increased 55% in 2015.**

2013	2014	2015
779	841	**1,305**
+91%	+8%	+55%

2015 Risk Ratio of Spear-Phishing Attacks by Organization Size



- Advanced Threat Group 8 (ATG9, a.k.a. Emissary Panda) – Attacks against financial, aerospace, intelligence, telecommunications, energy, and nuclear engineering industries in search of intellectual property; notable for exploiting CVE-2015-5119, a zero-day exploit revealed in the Hacking Team breach
- Waterbug and Turla – Russia-based espionage spear-phishing and watering-hole attacks against government institutions and embassies; believed to have been active since 2005
- Butterfly – Attacks against multi-billion dollar corporations in IT, pharmaceuticals, commodities, including Facebook and Apple for insider trading

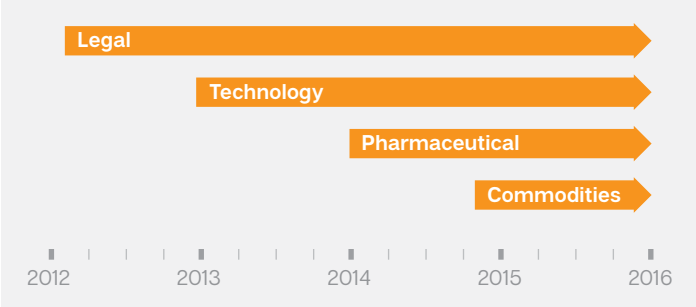
Profiting from High-Level Corporate Attacks and the Butterfly Effect

Butterfly is a group of extremely well-organized, highly-capable hackers who are spying on companies with a view to profiting on the stock market by selling market-sensitive information to the highest-bidder. The types of information the attackers potentially had access to included emails, legal documents, policy documents, training materials, product descriptions, and data harvested from specialist security systems. Stolen materials such as these could also be valuable for insider-trading purposes.

Symantec first saw these attacks in 2012 and 2013 when they compromised some well-known companies including Apple, Microsoft, and Facebook. However, they also employ sophisticated counter-measures to cover their tracks, including encrypted virtual command and control servers.

Timeline of Butterfly Attacks Against Industry Sectors

- *The Butterfly group has been active for a number of years, targeting a variety of organizations, including those linked to extracting natural resources.*
- *Their use of zero-day vulnerabilities in attacks reveals a level of sophistication that we have not seen before in commercially-motivated attacks.*
- *The graphic shows a timeline of when Butterfly attacks began against different industry sectors.*



Cybersecurity, Cybersabotage, and Coping with Black Swan Events

A Black Swan event is an event that was unprecedented and unexpected at the time it occurred; however, after further analysis, experts sometimes conclude that it could have been predicted. The term originates from the belief that all swans were white, until in 1697, black swans were discovered in Australia. If advanced cyberespionage is so common, it is perhaps curious that cybersabotage is not. The capabilities required to inflict physical damage are similar to those needed for cyberespionage, and the target set is growing thanks to the proliferation of Internet-connected devices, including industrial control systems.

The British Government's 2015 security and defense review sums up the challenges neatly:

> *"The range of cyber actors threatening the UK has grown. The threat is increasingly asymmetric and global. Reliable, consistent cyber defense typically requires advanced skills and substantial investment. But growing numbers of states, with state-level resources, are developing advanced capabilities which are potentially deployable in conflicts, including against CNI [Critical National Infrastructure], and government institutions. And non-state actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes."*

The Stuxnet cyberattack on the Iranian nuclear program is the best-known example of an Internet attack on physical infrastructure. It may be that other successful attacks have occurred in the shadows or that infections are in place, but haven't been activated yet. It seems unlikely that the world's critical infrastructure is immune. An attack at the end of 2014 on a German steel mill is a warning of potentially more serious attacks to come.

Speculations about possible cybersabotage continued into 2015 with the discovery of an information-stealing threat named Trojan.Laziok. This particular threat appears to have been designed for reconnaissance style attacks aimed at the energy sector, particularly in the Middle East. Laziok wasn't implicitly designed to attack and bring down critical infrastructure, but rather to gather information about the systems it compromised. As we discussed in ISTR 20, these attacks can be just as potent as direct attacks against critical systems, improving an attacker's ability to press further into an environment simply by learning more about the types of systems they are traversing. Simply put, if an attacker knows what types of computers he or she has or can compromise, they can decide how to proceed in order to carry out their malicious goals.

Cybersabotage and the Threat of "Hybrid Warfare"

The notion of hybrid threats has been around for a long time in cybersecurity, traditionally referring to malware that has many different attack vectors—such as dropping malicious Trojan code onto an infected device and infecting other code on the system, while spreading itself through email or some other means. The term "hybrid warfare," however refers to a type of warfare that is a combination of conventional and unconventional information and cyber warfare. According to NATO, "the term appeared at least as early as 2005 and was subsequently used to describe the strategy used by the Hezbollah in the 2006 Lebanon War."

It wasn't until the end of 2015 where speculations about cybersabotage turned into real indications of one such attack. On December 23, a power failure hit the Ivano-Frankivisk region in western Ukraine. Details emerged over the coming days and weeks of a multi-pronged cyber attack that not only disabled power in eight provinces in the region, but also masked the activity of the attackers and made it difficult to assess the extent of the outage.

The malware behind the attack appears to be a potent combination of the BlackEnergy Trojan (Backdoor.Lancafdo) and Trojan.Disakil. In order to carry out the attack, the BlackEnergy Trojan was most likely used to traverse the network, allowing the attackers to gather information about the computers they compromised until they reached the critical systems that allowed them to disconnect breakers, resulting in the loss of electricity in the region. However, it doesn't appear as though the Trojan itself disconnected the power. Rather, it allowed the attackers to discover the critical systems and then gain full control of them, after which they could use the original software on these systems to take down the power grid.

While noteworthy to this point, the attackers responsible appear to have planned the attack to such an extent that they were able to prolong the outage beyond the point it was pinpointed as an actual cyberattack. One way they were able to do this was by performing a telephone denial-of-service (TDoS) attack against the power supplier's call center, preventing customers from calling in, and leaving operators in the dark as to the extent of the outage.

However, the one-two punch in the attack appears to be tied to the use of Trojan.Disakil in the attack. A highly destructive Trojan, Disakil was likely used to overwrite system files and wipe master boot records on computers that operators would turn to in order to bring the power back online. So not only was the power taken down, so too were the systems used to restore it, forcing operators to manually restore power in circumstances they normally would be able to do so through available software.

As with any cyber attack, attribution can be difficult to determine. Based on circumstantial evidence and current geopolitical disputes, it is fairly easy to draw conclusions; however, there is no smoking gun in this case. What is known is that the group behind the BlackEnergy Trojan has been active for many years and has targeted multiple organizations in the Ukraine, as well as Western European countries, NATO, and others. Around the time of these attacks, this group was also discovered attacking media organizations in the Ukraine. It is likely this won't be the last we hear of them.

The cybersabotage attacks in Ukraine generated much debate about the use and effectiveness of hybrid warfare, and it is likely this won't be the last we hear of these types of attacks, particularly as international tensions remain high in some parts of the world, and managing the risks from cyberterrorism moves up the agenda for many national governments.

Small Business and the Dirty Linen Attack

Of course, small businesses have smaller IT budgets, and consequently spend less on cybersecurity than their large enterprise counterparts. However, this trend has continued for years, in spite evidence that shows a greater proportion of targeted spear-phishing attacks each year are intended for small businesses.

In 2015, 43 percent of targeted spear-phishing blocked by Symantec were destined for small businesses, compared with 34 percent in 2014. Additionally, the attackers focus narrowed, concentrating on fewer companies, and approximately 3 percent of small businesses were targeted in 2015, compared with 45 percent in the previous year. On average, these organizations were targeted at least twice during the year. This shift from a scattergun approach of more widely dispersed attacks in 2014, to a more sniper-style line of attack converging on fewer targets in 2015 also helps to keep these attacks below the radar.

One of the most difficult challenges is knowing when your organization is in the sights of cyber attackers, particularly when most cybersecurity headlines focus on nation states vying for company secrets, and the tens of millions of credit card details and other personal data exposed in breaches. It's all too easy to believe that a targeted attack only happens to other companies. However, no business is too small or too obscure to become a target and one good example that shows this is the Dirty Linen Attack.

Perhaps an unlikely target, General Linens Service, Inc. is a very small company, with only one location and 35 employees. They provide a linen service to restaurants and the hospitality industry, including uniforms and carpet cleaning. As unlikely a targeted as it would seem for a nation state, it was a competitor, General Linen Services, LLC. that had been hidden in their network for two years. Perhaps the similar choice of company name was deliberate, because for two years they were able to steal customers by accessing the targeted company's invoices, allowing them to see how much they were charging, giving them a significant advantage. The question was how they achieved this; a small business conducting cyberattacks on a rival seemed

extreme. However, it transpired that the attackers noticed that both companies used the same software for their web portal, and the targeted company had not changed the default administration password. This enabled the attackers to access their data 157 times. The good news is that General Linen Services, LLC was caught and convicted, and General Linens Service, Inc. discovered the importance of following security best practices.

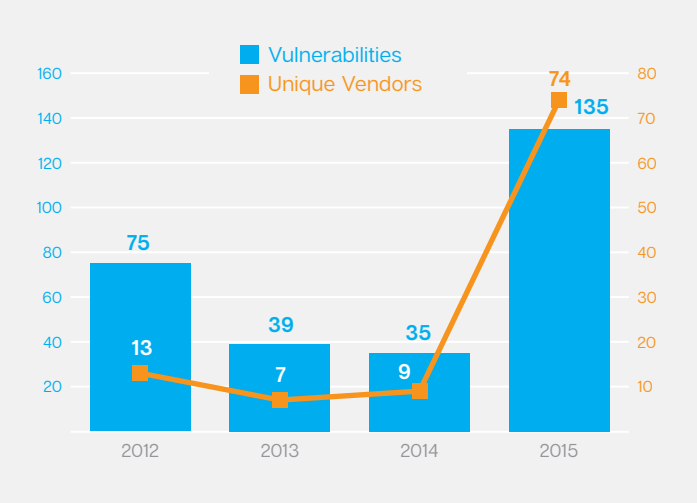
Industrial Control Systems Vulnerable to Attacks

Industrial control systems (ICSs) are found in many areas of industrial production and utility services worldwide, and are routinely connected to the Internet for remote monitoring and control. Uncovering vulnerabilities in these systems is a major area of research, emphasized by the growth in the numbers of these vulnerabilities in 2015.

The actual number of vulnerabilities affecting ICSs is estimated to be much higher, since many organizations standardize their platforms by using commercial off-the-shelf (COTS) products, such as Windows or Linux that are also subject to vulnerabilities, but which are not counted here. Furthermore, ICS management systems connected with enterprise networks can increase the potential exposure to threats more typically associated with these operating systems.

Vulnerabilities Disclosed in Industrial Control Systems

▶ *At least seven zero-day vulnerabilities directly related to a variety of different ICS manufacturers and devices in 2015.*



Obscurity is No Defense

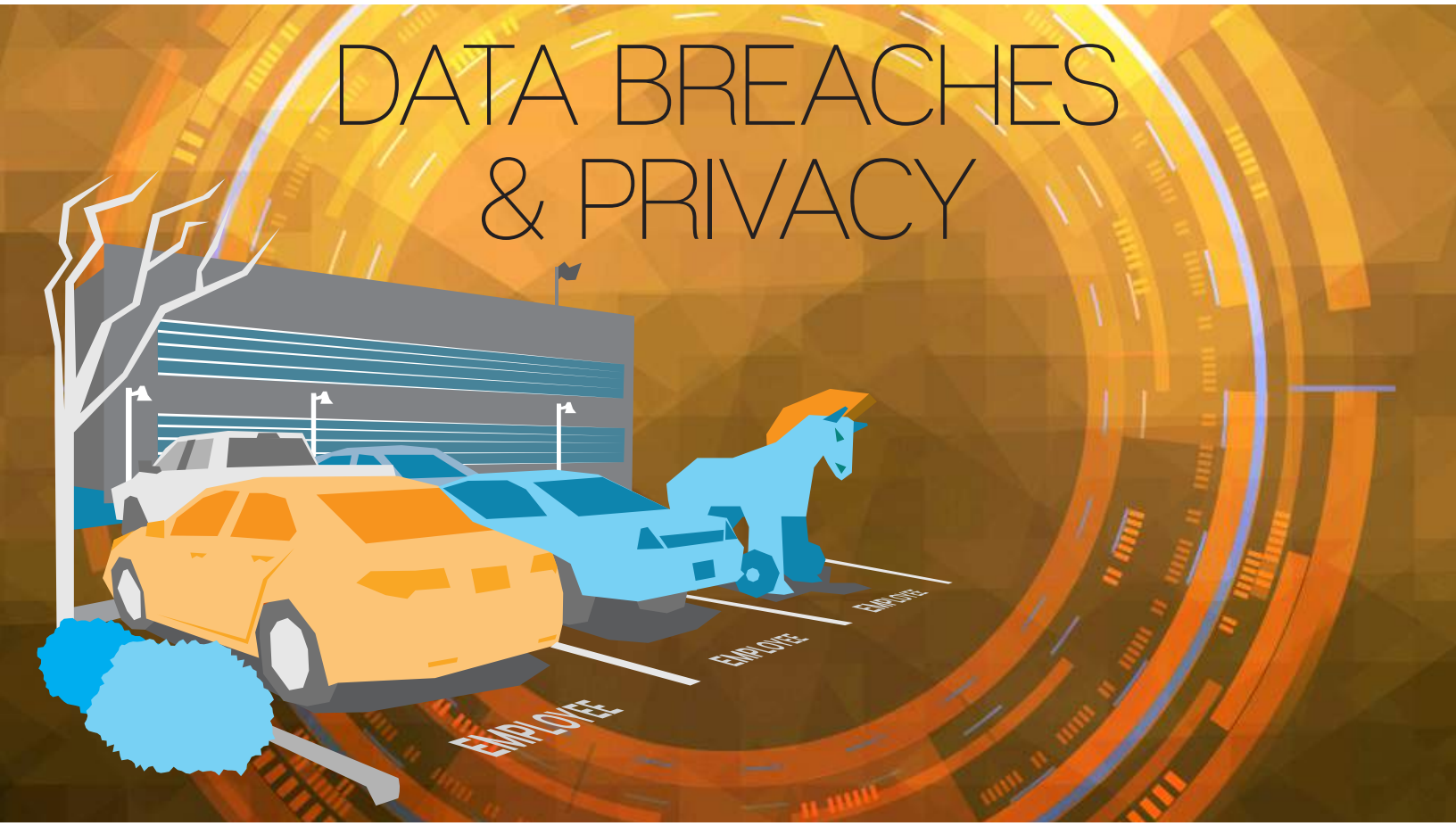
The most valuable form of protection against cyberespionage is simply to be aware that it is possible. All businesses are potentially vulnerable to targeted attacks using techniques such as watering hole attacks and spear phishing. Small size and obscurity are no protection.

Indeed, in 2015 small businesses accounted for a greater proportion (43 percent) of spear-phishing attacks, but the likelihood of being targeted diminished. While more attacks were destined for that group, they were focused on a smaller, more discreet number of businesses (3 percent).

Contrast this with large enterprises, which accounted for 35 percent of the spear-phishing attacks, and 1 in 2.7 (38 percent) were targeted at least once. This suggests a much more extensive scale where campaigns were more scattergun in their approach.

Having acknowledged the risk, organizations can take steps to protect themselves by reviewing their security and incident response plans, getting advice and help if required, updating the technical defenses, putting good personnel policies and training in place, and staying up to date with the latest information. ■

DATA BREACHES & PRIVACY



DATA BREACHES LARGE AND SMALL

Whether an insider attack, or criminal fraud focused on websites and point-of-sale devices, data breaches continued in 2015, costing victims more than ever. The number of mega-breaches climbed to the highest level since 2013. The number of breaches where the full extent of a breach was not revealed, increased; fewer companies declined to publish the numbers, unless required to do so by law.

The State of Play

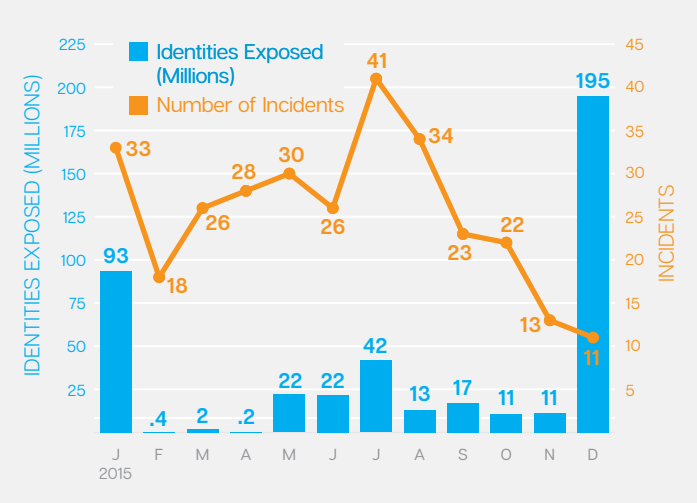
Symantec figures show the total number of breaches has risen slightly by 2 percent in 2015. The year also saw nine mega-breaches, surpassing 2013's record of eight breaches containing more than 10 million identities each. Another new record was set near the end of the year when 191 million identities were exposed, surpassing the previous record for the largest single data beach.

Helped in no small part by this massive breach, the overall total number of identities exposed has jumped 23 percent to 429 million. What's more concerning is that this number is likely much higher due to the increasing tendency of organizations to limit the information released about the extent of the breaches they suffer. In 2015, the number of breaches reported that did not include a figure for identities exposed increased by 85 percent, from 61 to 113. Symantec estimates the total number of identities exposed, had these breaches been fully reported, is likely to be at least half a billion.

It's a staggering number, but also one full of speculation based on incomplete data. The median number of identities exposed per breach has decreased by around a third to 4,885 identities per breach. However, this does not lessen the cause for concern, but rather suggests the data stolen across breaches is more valuable and the impact to the business greater than in previous years.

Timeline of Data Breaches

A massive breach in December 2015 helped to set a new record for identities exposed in a year. At 41, the month of July also saw the highest-ever number of breaches in a month.



A massive breach in December 2015 helped to set a new record for identities exposed in a year. At 41, the month of July also saw the highest-ever number of breaches in a month.

As a result, cyber insurance claims are becoming more common. This year's NetDiligence Cyber Claims study saw claims ranging up to US$15 million, while typical claims ranged from US$30,000 to US$263,000. But the cost of insuring digital assets is on the rise, contributing further to the rising overall cost of data breaches.

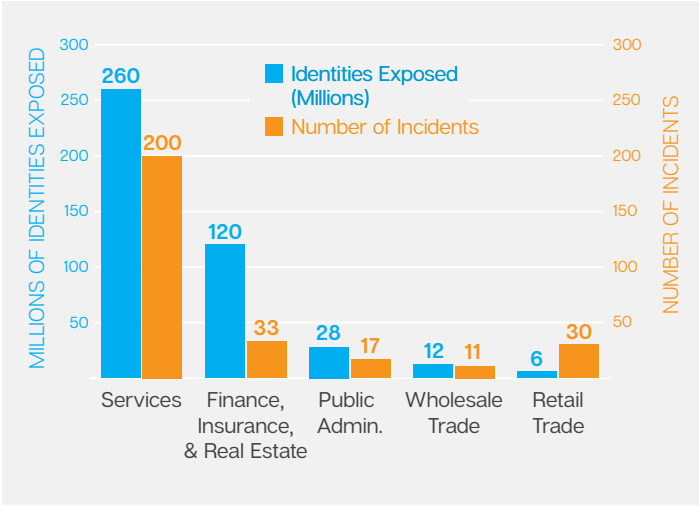
Average premiums for retailers surged 32 percent in the first half of 2015, and the healthcare sector saw some premiums triple. Reuters also reports that higher deductibles are now common and even the biggest insurers will not write policies for more than $100 million for risky customers.

Looking at industries across the broadest of categories, the Services sector was impacted by more data breaches than any other industry, both in terms of the number of incidents and the number of identities exposed. However, the reasons in each case differs when looking at the sub-sectors contained within these high-level classifications.

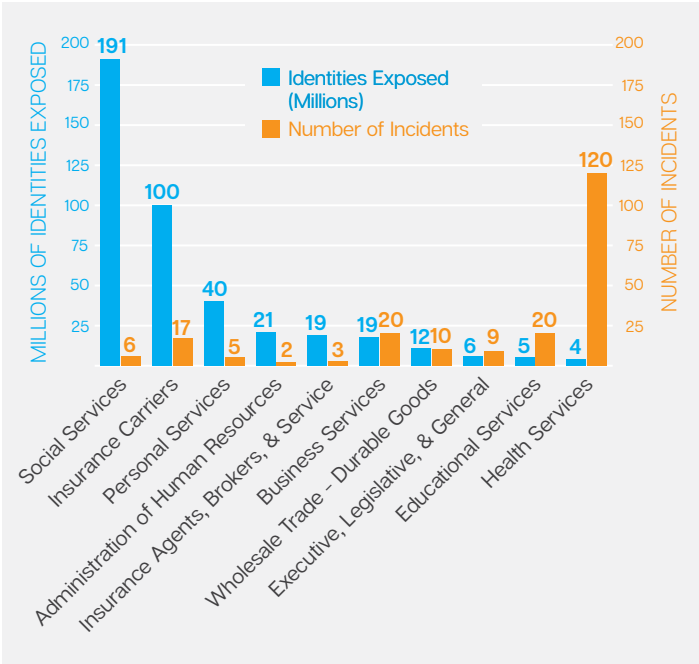
The largest number of breaches took place within the Health Services sub-sector, which actually comprised 39 percent of all breaches in the year. This comes as no surprise, given the strict rules within the healthcare industry regarding reporting of data breaches. However, the number of identities exposed is relatively small in this industry. Such a high number of breaches with low numbers of identities tends to show that the data itself is quite valuable to warrant so many small breaches.

The sub-sector responsible for the most identities exposed was Social Services. However, this is largely due to the record-breaking data breach responsible for 191 million identities exposed. Removing this one breach drops Social Services to the bottom of the list. (Coincidentally, this is where it falls within the list of sectors for number of breaches.)

Top 5 High Level Sectors Breached by Number of Identities Exposed and Incidents



Top Sub Level Sectors Breached by Number of Identities Exposed and Incidents



Facts about the Attack on Anthem

On January 26, 2015

78 Million

patient records were exposed.

The breach is believed to be the work of a well-resourced cyberespionage group, which Symantec calls **Black Vine.** They appear to have access to a wide variety of resources to let it conduct multiple, simultaneous attacks over a sustained period of time. **They used:**

- **attacker-owned infrastructure**
- **zero-day exploits**
- **custom-developed malware**

Three variants are named:

1) **Hurix,** 2) **Sakurel, and** 3) **Mivast**

detected as Trojan.Sakurel — Backdoor.Mivast

All variants have the following capabilities:

- Open a pipe back door
- Execute files & commands
- Delete, modify, and create registry keys
- Gather and transmit information about the infected computer

Top 10 Sub-Sectors Breached by Number of Incidents

Healthcare	120	Wholesale Trade	10
Business	20	Eating and Drinking Places	9
Education	20	Executive, Legislative, & General	9
Insurance	**17**	Depository Institutions	8
Hotels	14	Social Services	6

Top 10 Sectors Breached by Number of Incidents

- *Health Services is denoted as a sub-sector within the Services industry, and 120 of the 200 breaches that occurred within the Services sector were attributed to Healthcare.*

	Sector	Number of Incidents	% of Incidents
1	Services	200	65.6%
2	Finance, Insurance, & Real Estate	33	10.8%
3	Retail Trade	30	9.8%
4	Public Administration	17	5.6%
5	Wholesale Trade	11	3.6%
6	Manufacturing	7	2.3%
7	Transportation & Public Utilities	6	2.0%
8	Construction	1	<1%

Top 10 Sectors Breached by Number of Identities Exposed

- *The Services sector accounted for 60 percent of identities exposed, the majority of which were within the Social Services sub-sector.*

	Sector	Number of Incidents	% of Incidents
1	Services	259,893,565	60.6%
2	Finance, Insurance, & Real Estate	120,124,214	28.0%
3	Public Administration	27,857,169	6.5%
4	Wholesale Trade	11,787,795	2.7%
5	Retail Trade	5,823,654	1.4%
6	Manufacturing	3,169,627	<1%
7	Transportation & Public Utilities	156,959	<1%
8	Construction	3,700	<1%

Top 10 Sub-Sectors Breached by Number of Incidents

	Sector	Number of Incidents	% of Incidents
1	Health Services	120	39.3%
2	Business Services	20	6.6%
3	Educational Services	20	6.6%
4	Insurance Carriers	17	5.6%
5	Hotels & Other Lodging Places	14	4.6%
6	Wholesale Trade - Durable Goods	10	3.3%
7	Eating & Drinking Places	9	3.0%
8	Executive, Legislative, & General	9	3.0%
9	Depository Institutions	8	2.6%
10	Social Services	6	2.0%

Top 10 Sub-Sectors Breached by Number of Identities Exposed

	Sector	Number of Incidents	% of Incidents
1	Social Services	191,035,533	44.5%
2	Insurance Carriers	100,436,696	23.4%
3	Personal Services	40,500,000	9.4%
4	Administration of Human Resources	21,501,622	5.0%
5	Insurance Agents, Brokers, & Service	19,600,000	4.6%
6	Business Services	18,519,941	4.3%
7	Wholesale Trade - Durable Goods	11,787,795	2.7%
8	Executive, Legislative, & General	6,017,518	1.4%
9	Educational Services	5,012,300	1.2%
10	Health Services	4,154,226	1.0%

This calls into question how risk factors into a data breach. An industry may suffer a large number of data breaches or expose a large number of identities, but does this mean that the data itself is being used for nefarious purposes?

For instance, 48 percent of data breaches were caused by data accidentally being exposed. Personal data in these cases were indeed exposed, be it by a company sharing data with the wrong people or a misconfigured website that inadvertently made private records public. But was this data obtained by people with malicious intentions? In many cases, it's likely that it was not. A retired grandmother who accidentally receives someone else's healthcare record by email is unlikely to flip this information for identity theft. That's not to say it never happens—just that a large majority of such data breaches are of a lower risk.

What is a much higher risk are cases where either hackers or insider theft was the cause of a breach. These are instances where the motive was very likely to steal data. To that end, here are some examples of high risk industries.

Top Sectors Filtered for Incidents, Caused by Hacking and Insider Theft

	Industry Sector	Number of Incidents
1	Health Services	53
2	Hotels & Other Lodging Places	14
3	Business Services	14
4	Wholesale Trade - Durable Goods	9
5	Educational Services	9

The Health Services sub-sector still tops the list for number of incidences, but it is now followed by the Hotels & Other Lodging Places sub-sector. Interestingly, 100 percent of breaches in this particular sub-sector included credit card information, but only seven percent actually reported the number of identities stolen. The Business Services sector dropped from second to third place when looking at high-risk causes. The companies breached in this sector are primarily dominated by online businesses and software manufacturers.

Top Sectors Filtered for Identities Exposed, Caused by Hacking and Insider Theft

	Industry Sector	Identities Exposed
1	Insurance Carriers	100,301,173
2	Personal Services	40,500,000
3	Administration of Human Resources	21,500,000
4	Insurance Agents, Brokers, & Service	19,600,000
5	Business Services	18,405,914

In terms of identities exposed in high-risk breaches, the Insurance Carriers and the Insurance Agents, Brokers, & Service sub-sectors both appear in the top five. Between these two sub-sectors lie almost half the mega-breaches seen in 2015. This presents one other interesting item: of the insurance-related breaches, almost 40 percent of them also contained healthcare records. Given the overlap between healthcare costs and insurance companies that cover such costs, this isn't too surprising. What is concerning here is that attackers may have figured out that this highly prized data is available in insurance-related sectors, and in much bigger numbers than found in small hospitals or private practices.

By Any Other Name

The more details someone has about an individual, the easier it is to commit identity fraud. Criminals are targeting insurance, government, and healthcare organizations to get more complete profiles of individuals.

The types of information that thieves are persuing has not changed in 2015, save some minor changes in ranking. Real names are still the most common type of information exposed, present in over 78 percent of all data breaches. Home addresses, birth dates, Government IDs (like SSN), medical records, and financial information all appear in the 40 to 30 percent range, as in 2014, though their order of appearance has changes slightly. Rounding out the top 10, email addresses, phone numbers, insurance information, and user names/passwords again appear in 10 to 20 percent range.

This isn't to say credit card data isn't still a common target. Its black market value isn't especially high on a per-card basis, since credit card companies are quick to spot anomalous spending patterns (as are credit card owners) and stolen card data and other financial information has a limited shelf life. However, there is still an evergreen market for stolen credit card data.

Top 10 Types of Information Exposed

▶ *Financial information includes stolen credit card details and other financial credentials.*

	2015 Type	2015 %	2014 Type	2014 %
1	Real Names	78%	Real Names	69%
2	Home Addresses	44%	Gov. ID Numbers (e.g., SSN)	45%
3	Birth Dates	41%	Home Addresses	43%
4	Gov. ID Numbers (e.g., SSN)	38%	Financial Information	36%
5	Medical Records	36%	Birth Dates	35%
6	Financial Information	33%	Medical Records	34%
7	Email Addresses	21%	Phone Numbers	21%
8	Phone Numbers	19%	Email Addresses	20%
9	Insurance	13%	User Names & Passwords	13%
10	User Names & Passwords	11%	Insurance	11%

Retail remains a lucrative sector for criminals, although the introduction of the EMV standard, or 'chip-and-PIN' payment technology, in the US means the information criminals will be able to scrape from point-of-sale (POS) devices will be less valuable. EMV is a global standard for cards equipped with microchips, and the technology has been in use in some countries since 1990s and early 2000s. EMV is used to authenticate chip-and-PIN transactions, and following numerous large-scale data breaches in recent years, and increasing rates of credit card fraud, credit card issuers in the US are migrating to this technology in a bid to reduce the impact of such fraud.

Previously, criminals could get hold of 'Track 2' data, which is shorthand for some of the data stored on a card's magnetic strip. This made it easier to clone credit cards and use them in stores, or even in ATMs, if they had the PIN. Track 1 stores more information than Track 2, and contains the cardholder's name, as well as account number and other discretionary data. Track 1 is sometimes used by airlines when securing reservations with a credit card. The value of this data is reflected in the online black market sale prices, with Track 2 data costing up to US$100 per card.

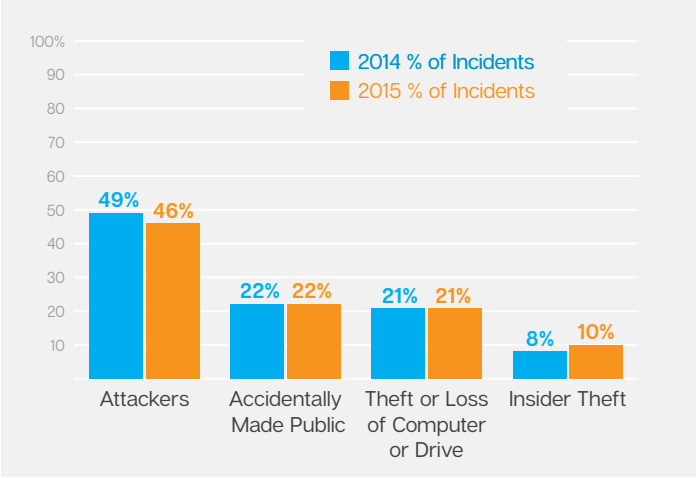
As of October 2015, 40 percent of US consumers have EMV cards, and 25 percent of merchants are estimated to be EMV compliant. With the move to the EMV standard, credit cards are much more difficult to clone, as they necessitate the use of a PIN in order to use them. And while the transition might take a few years to fully implement, alongside other improvements in POS security, it should make large-scale POS thefts more difficult and certainly less profitable for criminals.

The Insider Threat

While insider theft only accounted for around 10 percent of data breaches in 2015, the NetDiligence Cyber Claims study reported that there was insider involvement in 32 percent of the claims submitted in 2015. According to its CEO, a disgruntled insider was alleged to have been responsible for one of the most publicized data breaches of the year, at Ashley Madison. Although this has not been confirmed, if true, it highlights the potential damage a malicious insider can inflict.

Top Causes of Data Breach by Incidents

▶ *The proportion of incidents involving insider theft grew from less than one percent in 2014 to 10 percent in 2015.*



Over Half a Billion Personal Information Records Stolen or Lost in 2015

and more companies than ever not reporting the full extent of their data breaches

36% of information exposed were medical records

The largest number of breaches took place within the Health Services sub-sector, which actually comprised 39 percent of all breaches in the year. This comes as no surprise, given the strict rules within the healthcare industry regarding reporting of data breaches.

39%

120 Incidents

4 Million Identities Exposed

Most of an iceberg is submerged underwater, hiding a great ice mass. The number of reported identities exposed in data breaches are just the tip of the iceberg. What remains hidden?

REPORTED IDENTITIES EXPOSED

78 million **patient records were exposed at Anthem**

22 million **personal records were exposed at Office of Personnel Management**

UNREPORTED IDENTITIES EXPOSED

Despite companies' choice not to report the true number of records exposed, hundreds of millions more people may have been compromised.

2015 Stats

Total Reported Identities Exposed

numbers in millions

2015	429	+23%
2014	348	-37%
2013	552	

These numbers are likely higher, as many companies are choosing not to reveal the full extent of their data breaches.

2014: **61**

2015: **113** (+85%)

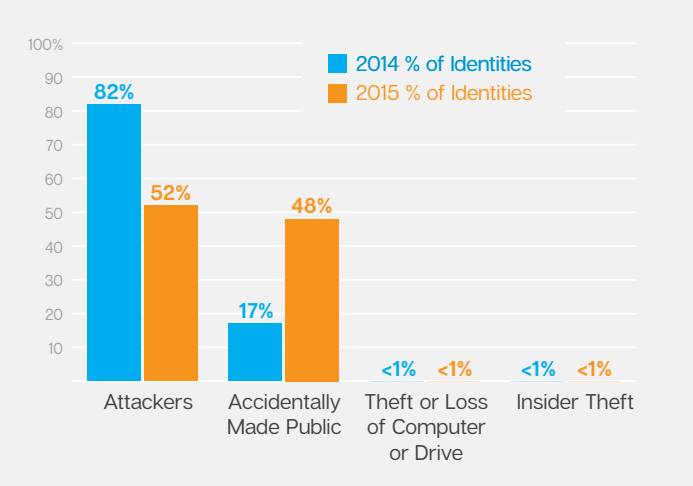
Incidents that did not report identities exposed in 2015

Given the facts, it is possible that ***500 Million** identities were exposed

*estimated

Top Causes of Data Breach by Identities Exposed

- *The proportion of identities exposed that was accidentally made public increased to 48 percent from 22 percent in 2014.*



The proportion of identities exposed that was accidentally made public increased to 48 percent from 22 percent in 2014.

Insider threats have always been a hot topic in cybersecurity, but in 2015, government bodies not only started to take notice—and take action.

- More than three-quarters of US government agencies surveyed in the MeriTalk Federal Insider Threat Report say their agency is more focused on combating insider threats today than one year ago.
- The UK's Centre for Defence Enterprise sponsored several projects in 2015 aimed at monitoring employee digital behaviour to predict and identify insider threats in real time, as well as learning simulators to help people spot risk.

Privacy Regulation and the Value of Personal Data

Cybercriminals are not only interested in 'who can hack,' but also 'who can leak.' Whether data may be stolen in a data breach, accidentally leaked, or even posted online legitimately in the past, personal data has a value in the underground shadow economy. Until relatively recently, many people did not recognize the potential value in personally identifiable information, and often were very lackadaisical in safeguarding it. The advent of social media in the last decade has enabled more people to share more personal data than at any time in history, and privacy controls were not at the forefront of many social networking applications.

Personal data can and will be used to commit crimes, whether to conduct identity fraud, or to enhance the social engineering in phishing scams, or even as part of the reconnaissance in the prelude to a targeted attack. The recognition of the potential value of this data in the wrong hands has resulted in social networking services enhancing and tightening their privacy controls, and more people regarding their personal data with greater respect. For example, the European Court of Justice's "right to be forgotten" ruling rippled through the data-gathering community in May 2014 and by the end of 2015, Google had received 348,085 requests to delist specific search results.

While many thought this would only be of benefit to those wanting to hide scandal or avoid incrimination, according to Google's FAQ, some of the most common cases for removal are sites that contain personal contact or address information or "content that relates solely to information about someone's health, sexual orientation, race, ethnicity, religion, political affiliation and trade-union status".

And the European Court of Justice sharpened the public's focus on privacy again this year when it ruled the 2000 "Safe Harbor" agreement to be invalid. As Monique Goyens, director general of the European Consumer Organisation explained, the ruling confirms that "an agreement which allows US companies to merely declare that they adhere to EU data protection rules without any authority screening this claim is clearly not worth the paper it is written on." As The Guardian newspaper commented at the time, it may "help stop the US government from being able to gain access to user data from the EU" and "may open the door to further probes, complaints, and lawsuits from users and data regulators."

However, in February 2016, The European Commission and the US agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield. The new framework was designed to address the requirements set out by the European Court of Justice after ruling the old Safe Harbor framework invalid. The press release states, "The new arrangement will provide stronger obligations on companies in the US to protect the personal data of Europeans and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities."

Surveying seven thousand people across Europe, Symantec's 2015 State of Privacy Report shows that in the UK alone, 49 percent of consumers are worried their data is not safe. And across the EU, technology companies (22 percent), retailers (20 percent) and social media companies (10 percent), were the least trusted. Symantec sees the lack of trust in these companies as a reputational issue, possibly stemming from recent high-profile data breach incidents.

We expect that reluctance to share personal information will grow and begin to change online behavior among consumers. One of the major reasons data privacy is becoming such a concern is because there is now a clear understanding amongst consumers that their data holds value. Providers of technology services should take heed when it comes to data privacy, because until the technology sector can be trusted to do the right thing by its consumers to safeguard that data, more work will need

to be done in the coming years to build and sustain the level of trust needed.

As data breaches proliferate and people's lives increasingly move online, we expect to see more regulation and more judicial interest in the protection of individual privacy in 2016 and beyond. Businesses need to be more transparent with customers on how they are keeping data secure. Security needs to be embedded into a company's value chain, but it should also be viewed internally as a customer-winning requirement, and not just a cost.

Ilias Chantzos, senior director in government affairs at Symantec commented, "There is a real consistency emerging that privacy is a competitive advantage for businesses and that privacy concerns also determine consumers' behaviour. It is critical to ensure consumers are empowered to understand what their data is being used for and how it is protected."

Reducing the Risk

While these are important steps, a large number of data breaches could also have been prevented with basic common sense, including:

- Patching vulnerabilities
- Maintaining good software hygiene
- Deploying effective email filters
- Using intrusion prevention and detection software
- Restricting third-party access to company data
- Employing encryption where appropriate to secure confidential data
- Implementing data loss prevention (DLP) technology

Of course, all of these relate to preventing outsider attacks. When it comes to mitigating the risk of malicious or accidental insider threats, organizations need to focus on employee education and data loss prevention.

Basic security hygiene should be drilled into employees the same way the public are told to cover our mouths when we cough or sanitize our hands in hospitals. Organizations should also be making use of data loss prevention technology to locate, monitor, and protect their data—wherever it is within the organization—so that they know who is doing what, with what data, in real time. DLP can block certain types of data from leaving an organization, such as credit card numbers and other confidential documentation.

Security should be an essential part of operations and employee behavior, rather than an add-on or something to appease auditors. Data breaches are unlikely to stop any time soon, but the scale and impact of them could certainly be reduced if organizations recognized that security goes well beyond the bounds of the CIO or the IT manager. Security is in every employee's hands. ■

E-CRIME & MALWARE

THE UNDERGROUND ECONOMY AND LAW ENFORCEMENT

The underground economy is booming and cybercrime is growing fast, but as we have seen with the growing number of high-profile arrests and takedowns in 2015, wherever the cybercriminals may be, law enforcement is now catching-up with them much more quickly. Ransomware attacks may have diminished, but they have also diversified, including targeting Linux web servers.

Business in the Cyber Shadows

Cybercriminals are more professional and are much bolder, not only in the targets they go after, but also the sums of money they seek. These criminal enterprises see themselves as a fully-functioning business, covering a multitude of areas, each with their own speciality. Just as legitimate businesses have partners, associates, resellers, and vendors, so do those enterprises operating in the shadows.

While prices for email addresses on the black market have dropped in recent years, credit card prices have remained relatively low but stable. However, if they come with 'luxury' data—verification that the seller's accounts are still active or that a credit card has not yet been blocked—they now fetch a premium price.

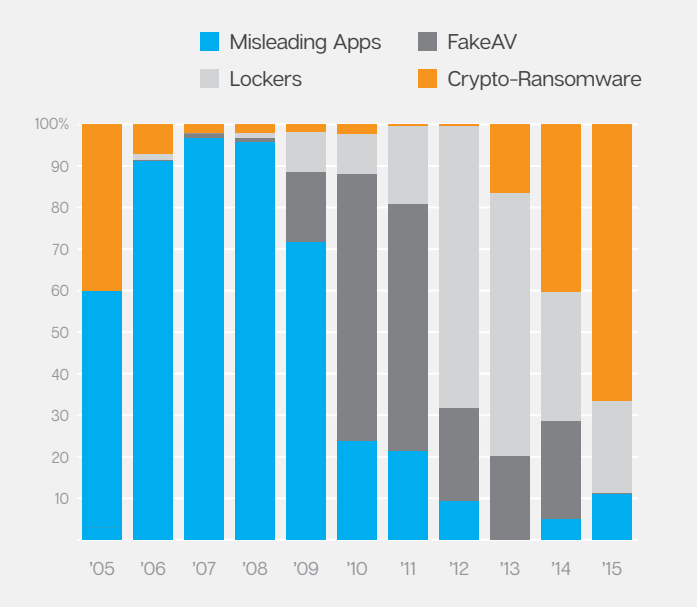
At the other end of the market, a drive-by download web toolkit, which includes updates and 24x7 support, can be rented for between US$100 and US$700 per week, while distributed denial-of-service (DDoS) attacks can be ordered from US$10 to US$1,000 per day. And at the top of the market, a zero-day vulnerability can sell for hundreds of thousands of dollars. Moreover, these figures have changes very little since 2014.

Stand and Deliver

Ransomware has become increasingly dominant in recent years and in 2014 many expected to see this trend continue. However, while we have seen ransomware attacks diversify, the growth in volume has not been seen. Attacks have moved to mobile devices, encrypting files, and anything else an owner will pay to recover.

Growing Dominance of Crypto-Ransomware

Percentage of new families of misleading apps, fake security software (Fake AV), locker ransomware and crypto ransomware identified between 2005 and 2015.



In 2015, one Symantec researcher demonstrated that smart TVs were potentially vulnerable to ransomware, although this has not yet been observed in the wild.

Some ransomware now also threatens to publish the victim's files online unless they pay—an interesting and sinister twist, which is likely to increase since the traditional advice of keeping effective backups, does not help in this scenario.

Never before in the history of human kind have people across the world been subjected to extortion on a massive scale as they are today. But why are criminals favoring ransomware, especially crypto-ransomware? With the glut of stolen information on the black market and the introduction of the more secure EMV standard (chip-and-PIN) payment cards for card payments in the US, the potential profit criminals can gain by exploiting stolen credit card details had reduced.

Credit card fraud involves several people to conduct, and consumer legislation ensures the victim's financial loss is minimized. In contrast, an attacker can obtain a ransomware toolkit from an underground source, and target their intended victims, who may have few alternatives but to pay-up. There are no middlemen for the criminal to pay and nothing to mitigate the losses to the victim, thus maximizing the profits.

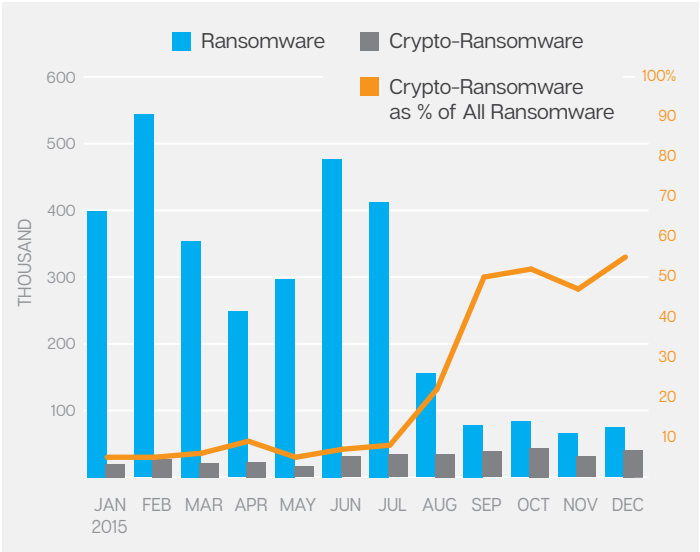
One crypto-ransomware tactic that seeks to increase the pressure on victims to pay-up, threatens to destroy the only copy of the secret key after a certain time, with the encrypted data potentially lost forever.

Crypto-Ransomware Over Time

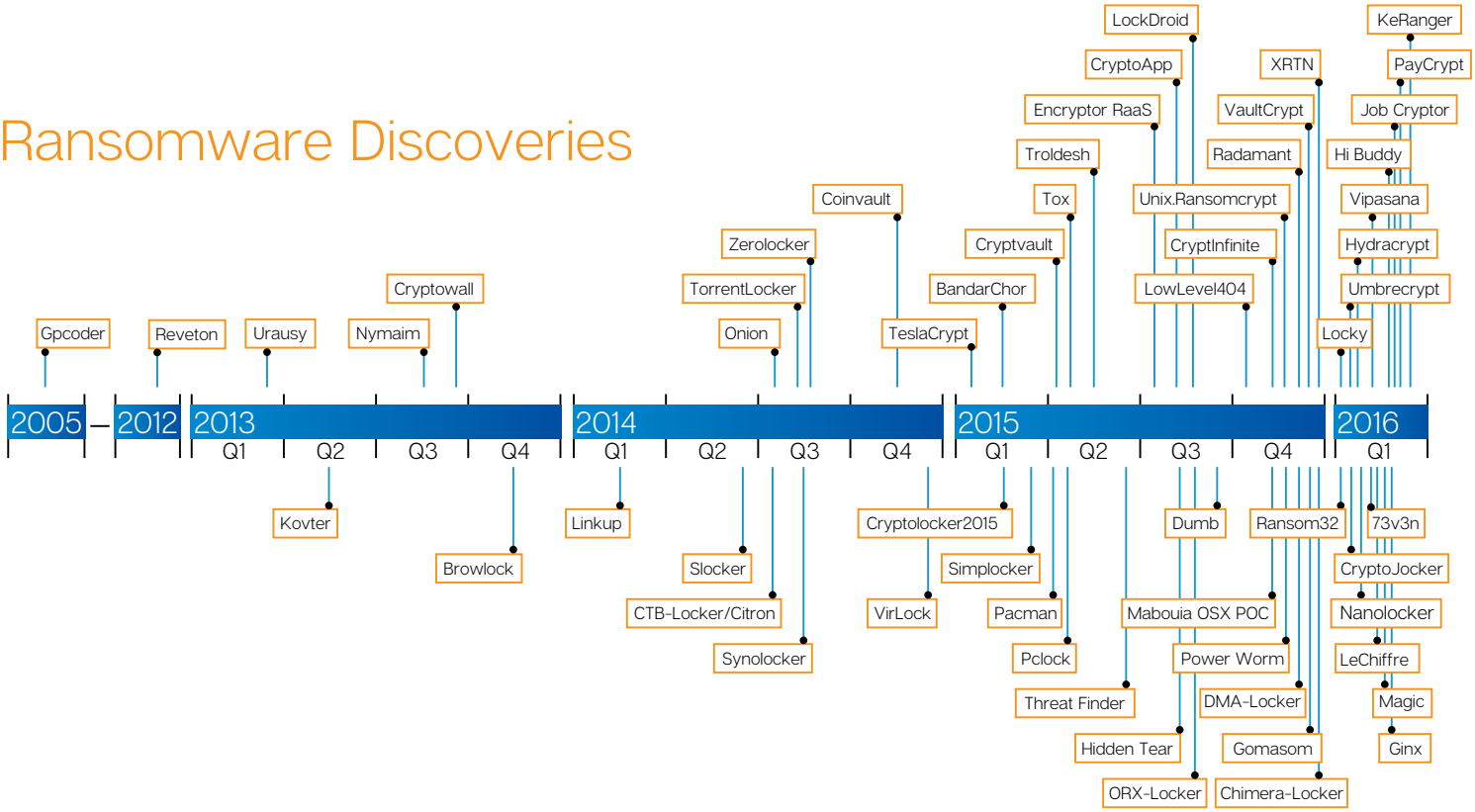
While more traditional locker-style ransomware is showing a rapid decline, crypto-ransomware continues to grow. Crypto-ransomware employs very strong, ostensibly unbreakable key-based cryptography to hold a victim's personal files to ransom by encrypting them with a key that only the criminals have access to.

Crypto-Ransomware as Percentage of All Ransomware

Although the chart indicates a steady decline in traditional ransomware in 2015, crypto-ransomware now accounts for the majority of all ransomware.



Ransomware Discoveries



Ransomware also targeted Linux web servers in 2015, encrypting files associated with web applications, archives, and back-ups. The evolution of Linux ransomware has also mirrored that of Windows ransomware: initial versions were basic, and often used poor encryption, making it relatively simple to recover encrypted files. However, just like with Windows ransomware, we can expect the criminals behind this new trend to quickly learn from their mistakes, and become more sophisticated in the future.

Global Issues, Local Attacks

With the build up to the presidential elections in the US, spam that leads to malware has been circulating that uses the US presidential primaries as bait. Spammers know how to play into visceral, emotive themes, like global events, the refugee crisis in the Middle East, immigration, and foreign policy issues, the economy, and even terrorism.

In January 2015, the Twitter and YouTube accounts of the US military command were hacked by self-styled supporters of the jihadist terrorist group, ISIS (a.k.a. IS, ISIL or Daesh). US Central Command commented that it was, "cyber-vandalism" rather than a serious data breach.

However, in April 2015, French television network TV5 Monde reported that it had been hacked by a group claiming to belong to the terrorist group, ISIS. According to reports, its TV station was brought to a standstill, and its website and social media pages were also disrupted in the attack. The hackers posted documents that purported to be the identity cards, and CVs of relatives of French soldiers involved in anti-ISIS operations in Iraq and Syria.

Both examples highlight a clear-cut case of terrorists using cyberthreats as an instrument to amplify their messages. The Internet has become not only tool only for online radicalization, but also for communication between terrorist groups, and for financing their operations. As a consequence, the calls for law enforcement to break encryption protocols are likely to have a wider and long-lasting impact on the technological integrity of Internet communications as a whole.

In a refereence to terrorism, one recent email campaign impersonated local law enforcement officials in the Middle East and Canada, tricking people into downloading malware by posing as security tips that would keep the intended victim safe from potential terror attacks in their location. The email spoofed the addresses of law enforcement agencies and included the names of officials who were all still in office at the time of the campaign. The subject lines in the emails often reflected the name of an employee who worked within the targeted company.

To make this type of attack convincing requires some degree of research, and here we have seen that this group did so before sending these phishing emails. Furthermore, without any

employee information, they would email other people in the company as an entry point, such as customer services or IT personnel.

This level of research and localisation indicates a growing professionalism, and is becoming increasingly common in botnet scams. The underground economy isn't just about selling stolen goods: it's an entire industry with the talented professionals and organisations you would expect in a legitimate business sector.

Botnets and the Rise of the Zombies

As with many other industries, up and coming economies, such as China in particular, has become a favoured as target for cybercrime in 2015. One significant factor has been a growth in broadband adoption in the last year. In 2013, the Chinese Government announced plans to expand broadband coverage for both rural and urban areas by 2020. One of the milestones for the multi-pronged strategy aimed to bring fixed broadband connections to 400 million Chinese households by 2015. In addition, prices have been kept low as broadband speeds have increased. All of this make the country an attractive target for cybercriminals seeking to compromise a fresh source of high-speed, internet-connected computers.

Malicious Activity by Source: Bots

▶ *China was the origin of much more bot activity in 2015, seeing a sharp rise of 84 percent in bot-related activity in that country. Bot activity in the US by contrast, fell by 67%. Successful law enforcement activity against cybercriminals, and heightened cybersecurity awareness are both contributing factors in the decline of bots in general.*

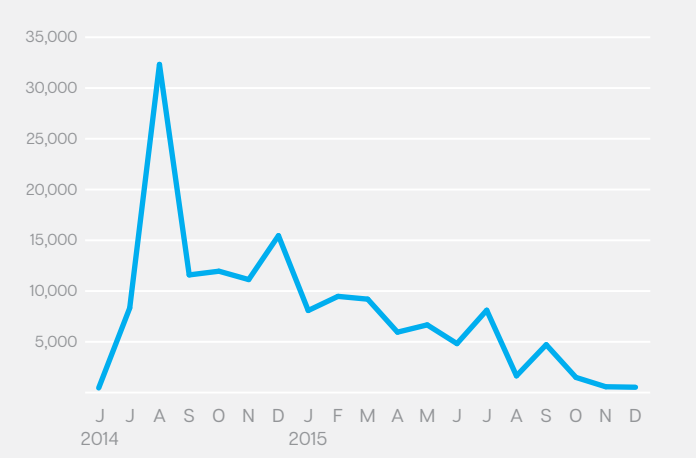
	2015 Country/ Region	2015 Bots % of Global	Percent Change Bots in Country/ Region	2014 Country/ Region	2014 Bots Percentage of Global
1	China	46.1%	+84.0%	China	16.5%
2	United States	8.0%	-67.4%	United States	16.1%
3	Taiwan	5.8%	-54.8%	Taiwan	8.5%
4	Turkey	4.5%	+29.2%	Italy	5.5%
5	Italy	2.4%	-71.2%	Hungary	4.9%
6	Hungary	2.2%	-69.7%	Brazil	4.3%
7	Germany	2.0%	-58.0%	Japan	3.4%
8	Brazil	2.0%	-70.1%	Germany	3.1%
9	France	1.7%	-57.9%	Canada	3.0%
10	Spain	1.7%	-44.5%	Poland	2.8%

The Dyre Consequences and Law Enforcement

After police shut down several major financial botnets in 2014, Dyre stepped up to take their place. Not only could Dyre hijack common web browsers and intercept Internet banking sessions to steal information, it could also download additional malware to the victim's computer, binding it to the perpetrator's network of botnet computers.

Dyre Detections Over Time

▶ *The chart shows a decline in Dyre malware activity long before the botnet was disrupted in November 2015. This may be an indication of an already weakened business model.*



Dyre had initially emerged as one of the most dangerous financial fraud operations, configured to defraud the customers of more than 1,000 banks and other companies worldwide.

However, the cybercrime group controlling the Dyre financial fraud Trojan suffered a major blow following a Russian law enforcement operation in November. As outlined in a Security Response blog, Symantec telemetry has confirmed a virtual cessation of the group's activities. Dyre (detected by Symantec as Infostealer.Dyre) was spread through email campaigns and no Dyre-related email campaigns have been observed since November 18, 2015. Detections of the Dyre Trojan and associated malware dropped dramatically soon after. Previously, the number of infections was estimated to be above 9,000 per month in early 2015. In November it fell to below 600 per month.

Law enforcement has become more effective at catching cybercriminals like these, and high-profile successes at disrupting them shows how coordinated, international efforts can pay dividends. Rarely is an attack group confined to one country, and with major groups spanning multiple jurisdictions, cross-border cooperation with law enforcement is an important factor to ensure that these successes continue to strike a blow against cybercriminals. We expect to see still more successful law enforcement operations against cybercriminals in the next year.

As the risks for the cybercriminals intensify, the potential rewards will diminish, raising the barrier to entry for any would-be cybercriminals. Other notable successes in 2015 included:

- **Dridex takedown.** The Dridex botnet specialized in stealing bank credentials. In October, an international law enforcement operation coordinated efforts to sinkhole thousands of compromised computers, cutting them off from the botnet's control, and saw one man charged. However, this may have been a partial success as Dridex continues to propagate, indicating that many key elements of the operation are still functioning. As such, we expect the group to continue to pose a serious threat during 2016.
- **Simda takedown.** In April, infrastructure owned by the Simda botnet's controllers, including a number of command-and-control servers, was seized by law enforcement. According to Interpol, "Simda was used by cyber criminals to gain remote access to computers enabling the theft of personal details, including banking passwords, as well as to install and spread other malware."
- **Ramnit seizure.** In February, a law enforcement operation led by Europol and assisted by, among others, Symantec and Microsoft, seized servers and other infrastructure owned by the cybercrime group behind the Ramnit botnet.
- **Multi-national banking and financial services fraud-related indictments.** Federal authorities indicted at least four men in connection with hacking incidents that resulted in the theft of over 100 million customer records. They were charged with hacking into multiple financial institutions and for operating a stock pump-and-dump scheme. One of the attacks occurred in 2014, and netted more than 80 million customer records, a breach that the US Justice Department dubbed the "largest theft of customer data from a US financial institution in history."

Cybercrime and Keeping out of Harm's Way

Organizations and individuals need to realise that even if they don't think they're an obvious target for cybercriminals, it doesn't mean they're not one.

The key is to remain vigilant both on a personal level by:

- Not opening emails from unknown senders.
- Looking for the padlock and checking the SSL certificate on any sites where you enter sensitive data.
- Not using unsecured networks when accessing sensitive data.

Remain vigilant at an organizational level by:

- Deploying intrusion prevention and detection software.
- Knowing what valuable data you have and harnessing data loss prevention technology.
- Monitoring where data is, and who has access to it.
- Ensuring you have a good incident response plan for when an attack is detected. It's not a question of what to do if an attack occurs, but when. ■

CLOUD & INFRASTRUCTURE

COMPUTERS, CLOUD COMPUTING AND IT INFRASTRUCTURE

IT systems continue to come under attack from rapidly evolving malware. No operating system is automatically immune, and malware threats against Linux and Mac OS X are increasing. Even cloud-hosted and virtualized systems are vulnerable. Malware is able to seek-out virtualized environments and infect them.

Protecting the System

The days of an operating system avoiding attacks simply by not being Windows is long behind us. Attacks against Mac OS X and Linux have both increased considerably in 2015 and cybersecurity is a necessity across the board for all operating systems—not just for Windows—to avoid the consequences of attack.

Cybersecurity affects everyone. Businesses need to protect their computers and IT infrastructure to stop data theft, fraud, and malware attacks. Likewise, businesses and consumers should be concerned about ransomware holding their data hostage, identity theft, and attackers using their computers as a springboard to attack others.

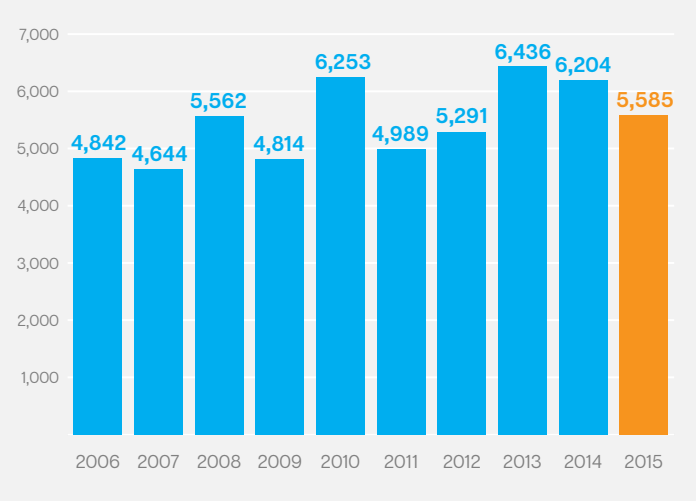
At a fundamental level, cybersecurity is about protecting the sinews of IT everywhere: computers, servers, and networks. The problem is that malware is ubiquitous. In 2015, we have seen many more systems come under attack, including Linux, Macs, virtualized computers, and cloud systems. Each year, the cloud handles more of our data, whether it is for customer relationship management, invoicing services, social networking, mobile email, and a whole gamut of other applications

One route for attacks is through exploiting vulnerabilities, and most systems have vulnerabilities. These exist in the operating systems and applications used on them, and are an important aspect of cybersecurity. If left unpatched, a vulnerability may

leave the path clear for would-be attackers to exploit them and use them for malicious purposes. Each year, researchers uncover new vulnerabilities, and the most coveted of these are zero-days, a special type of vulnerability for which a patch is not yet available.

Total Number of Vulnerabilities

- *The chart suggests an inflection towards a downward trend since 2013, markedly accentuated in 2015.*



Germophobes may not like it, but bacteria and viruses cover every surface. They live on our skin and in the air, and they are not going away. Likewise, vulnerabilities are a part of the computing environment. They are not going away either, and a slipshod approach to patching—whether through carelessness, misconfiguration, human error, or negligence—is a major cause of malware infections. Well-managed, well-patched systems are much less likely to become infected.

Nothing Is Automatically Immune

In the last year, Symantec has seen threats to almost every kind of computer, operating system, and other essential IT services, including:

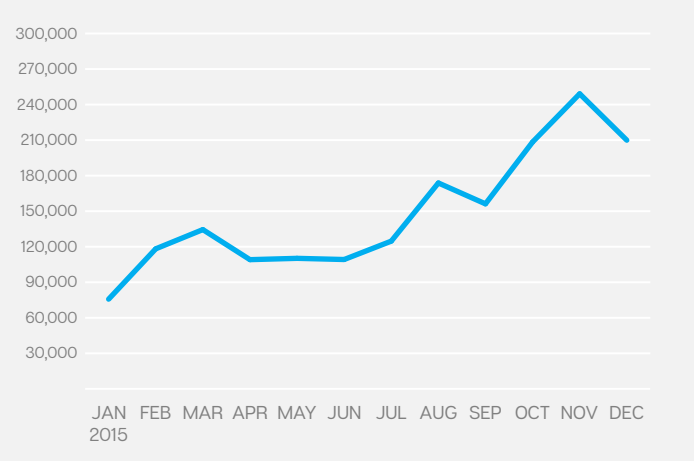
- **Mac OS X.** In addition to more vulnerabilities being uncovered in 2015, proof-of-concept ransomware and several methods for Trojans to gain unauthorised access to affected computers were also discovered.
- **MySQL.** Symantec researchers discovered malware that attacks MySQL—a very popular database system—and uses it to launch denial-of-service attacks on other systems.
- **Linux.** There was a rapid growth in Linux malware in 2015, including attack kits that hackers can use to infect unpatched Linux web servers.
- **Virtualised systems.** Even virtualised systems are not immune. Sixteen percent of malware is routinely able to recognize and exploit a virtual machine environment, and vulnerabilities such as VENOM could allow an attacker to escape an infected virtual machine and attack others on the same system, or even attack the host hypervisor.

Mac OS X

Apple's Mac OS X operating system was targeted for a variety of attacks in 2015, including a proof-of-concept ransomware threat called Mabouia (detected as OSX.Ransomcrypt), the first effective file-based ransomware threat against OS X. Previously, browser-based threats against Macs have been found, including ransomware targeting Safari through a malicious website.

Moreover, the volume of OS X malware has doubled (100% growth) since the start of 2015. In Q1, Symantec blocked approximately 3,650 attacks each day, rising to 7,255 by the end of Q4.

Mac OS X Malware Volume



Top Ten Mac OS X Malware Blocked on OS X Endpoints

▶ *Many OS X malware variants were additionally blocked using generic detection for which specific definitions are not created. Generic detection protects against many Trojans that share similar characteristics.*

Rank	Malware Name	Percent of Mac Threats 2015	Malware Name	Percent of Mac Threats 2014
1	OSX.Sudoprint	42.0%	OSX.RSPlug.A	21.2%
2	OSX.RSPlug.A	16.8%	OSX.Okaz	12.1%
3	OSX.Klog.A	6.6%	OSX. Flashback.K	8.6%
4	OSX.Keylogger	5.6%	OSX.Keylogger	7.7%
5	OSX. Wirelurker	5.0%	OSX.Stealbit.B	6.0%
6	OSX.Luaddit	3.2%	OSX.Klog.A	4.4%
7	OSX. Flashback.K	3.1%	OSX.Crisis	4.3%
8	OSX.Crisis	2.1%	OSX.Sabpab	3.2%
9	OSX.Okaz	1.7%	OSX.Netweird	3.1%
10	OSX.Stealbit.B	1.6%	OSX.Flashback	3.0%

Linux in the Firing Line

Although the overall volume is lower by comparison, the number of malware attacks against Linux has risen has risen almost fourfold (286 percent increase) since the start of the year. In Q1, Symantec blocked approximately 1.3 attacks each day, rising to 5.2 by the end of Q4.

Linux Malware Volume

▶ *In 2015, Symantec saw a surge in malware targeting Linux–the most common operating system on website servers, among other essential Internet services.*

Top Ten Linux Malware Blocked on Linux Endpoints

▶ *Fifty-five percent of Linux malware in 2015 related to variants of Linux.Xorddos, a Trojan horse that opens a back door on the compromised computer and includes a rootkit device that can hide network traffic and other files. It may also download other potentially malicious files.*

Rank	Malware Name	Percent of Linux Threats 2015
1	Linux.Xorddos	54.9%
2	Linux.Dofloo	13.9%
3	Linux.Wifatch	12.7%
4	Linux.Shelock	4.2%
5	Linux.Spalooki	3.9%
6	Linux.Kaiten.B	3.8%
7	Linux.Mumblehard	2.4%
8	Linux.Moose	1.6%
9	Linux.Raubdo	1.0%
10	Linux.Xnote	0.5%

Linux is ubiquitous, and one server may accommodate thousands of websites within the datacenter of any hosting provider. Linux has become an attractive target for hackers because with access

to one server, an attacker can potentially infect all of the websites hosted on it, and in turn all of their visitors and customers.

Attackers will often contaminate compromised web servers with code that links to exploit toolkits, or they to send spam emails and steal usernames and passwords. Additionally, compromised web servers are often a springboard from which an attacker will conduct a wide variety of other attacks, including very powerful DDoS attacks, where the bandwidth of a hosting provider is considerably greater than that of a home-user with a broadband connection.

A proliferation of specialized, automated attack toolkits have emerged, making it easier for cyber criminals to carry attacks against Linux systems. These toolkits help attackers to sniff-out potentially vulnerable servers, scanning for insecure content management systems and other exposed web applications.

Ransomware targeting Linux was also uncovered in 2015, targeted in particular files with extensions associated with web applications. The program also encrypted archives and directories that contained the word 'backup,' making it particularly difficult for anyone without offsite backups.

Cloud and Virtualized Systems

The term "cloud computing" covers a wide variety of technical solutions and environments, including software-as-a-service (SaaS), platform-as-a-service (PaaS), or infrastructure-as-a-service (IaaS) models. IaaS is growing in popularity among businesses, and as more data and services move to the cloud, it is attracting more attention from security researchers and cybercriminals. As with any system, each time a new layer is introduced to a service stack, the attack surface increases. While cloud environments may suffer from common vulnerabilities, such as SQL injection flaws, they may also be impacted by other issues. For example, in 2015, Symantec found that misconfiguration and poor management (by users, not cloud service providers) left cloud-hosted systems vulnerable to unauthorized access. Additionally, 11,000 publicly accessible files—some containing sensitive personal information—were also unearthed. Stolen credentials for cloud-based systems are regularly traded on underground markets, typically for less than US$10.

Cloud Vulnerabilities

It is not necessarily the case that cloud systems are inherently less-secure than traditional IT services. Nevertheless, administrators need to ensure that the cloud services they use are properly configured and all data is adequately protected. They should take care to control access to their cloud systems, preferably with two-factor authentication.

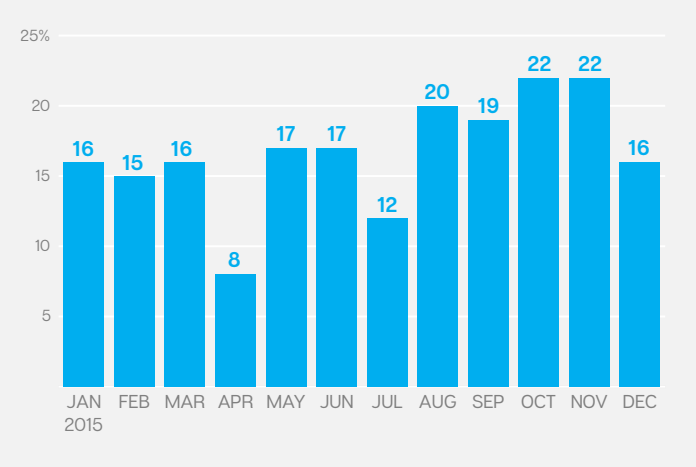
Vulnerabilities, like VENOM, could allow an attacker to escape from a guest virtual machine (VM) and access the native host operating system, along with other VMs running on the same platform. Attackers exploiting the VENOM bug could potentially steal sensitive data on any of the virtual machines on the affected system, and gain elevated access to the host's local network and its systems. The VENOM bug (CVE-2015-3456) existed since 2004 in the open-source hypervisor QEMU, which is often installed by default in a number of virtualized infrastructures using Xen, QEMU, and KVM. However, it is important to note that VENOM does not affect VMware, Microsoft Hyper-V, and Bochs hypervisors.

To date, the VENOM bug has not known to have been exploited in the wild, and QEMU's developers and other affected vendors have since created and distributed patches for VENOM.

One in six (16 percent) malware variants is able to detect the presence of a virtualized environment, compared with one in five (20 percent) in 2014. This ability can help the malware to better evade detection, particularly on security sandboxing systems using virtualization. More concerning is that an attack may detect when it is able to exploit and infect other virtual machines on the same system.

Proportion of Malware Samples That Are Virtual Machine Aware

Approximately 16 percent of malware is routinely able to detect and identify the presence of a virtual machine environment, peaking at around 22 percent in Q4.



Having a robust security profile for virtual systems is now more important than ever. Virtual machines and cloud services need securing in the same way as other services and devices. Policies should cover the virtual infrastructure as well as the physical one, and the use of integrated security tools across all platforms will help to mitigate such problems in the future.

Protecting the IT infrastructure

In the face of these threats, and many others like them, the old advice holds good for any infrastructure services, including file servers, web servers, and other Internet-connected devices:

- Stay informed about emerging threats.
- Keep systems up to date with patches and updates.
- Use integrated security software, including anti-malware technology.
- Use a strong firewall that only permits known traffic, and review access logs regularly to detect potentially suspicious activity.
- Employ multi-layer protection, so if one layer is compromised, there are other layers to protect different areas the system.
- Apply good policies and train staff well.
- Control access on a least-privilege basis.
- Deploy network intrusion prevention and detection and monitor email services running on the server.
- Always keep backups offsite.

Be concerned about cloud systems too. Here are some additional considerations:

- Safeguard all credentials used to access the cloud-based administration functions and ensure access is controlled on a need-to-know basis.
- Ensure that you understand the settings of your cloud resources and configure them accordingly.
- Enable event logging to keep track of who is accessing data in the cloud.
- Read the cloud providers' service-level agreements to learn how data in the cloud is secured.
- Include cloud IP addresses in vulnerability management processes and perform audits on any services that are provided through the cloud.

Protect Information Wherever It Is

As companies move their IT systems to virtual and cloud-hosted environments, they face new security challenges. In addition, as ever, human nature itself is a threat, with poorly-managed security leading to shadow IT systems. Shadow IT refers to solutions used inside organizations without explicit organizational approval, and solutions used by departments other than the IT department. It can sometimes be all too easy for a group of employees to turn to external products to fulfil an immediate need. IT decision makers should understand what is influencing their employees to turn to these solutions, and when the IT department should be involved to help shape those decisions.

It is important for the CIO to understand what the organization is doing, and whether certain teams are looking for services or applications that are not provided for, then determine how to address that need and offer that service in a secure fashion. Having the right processes is key to protecting information and data, even when it is not housed inside the enterprise.

DDOS ATTACKS AND BOTNETS

Distributed denial-of-service (DDoS) attacks are growing in number and intensity, but most last for 30 minutes or less. The availability of botnets-for-hire has fueled this increase and we are likely to see the Internet of Things provide more fodder for these botnet armies.

DDoS at Large

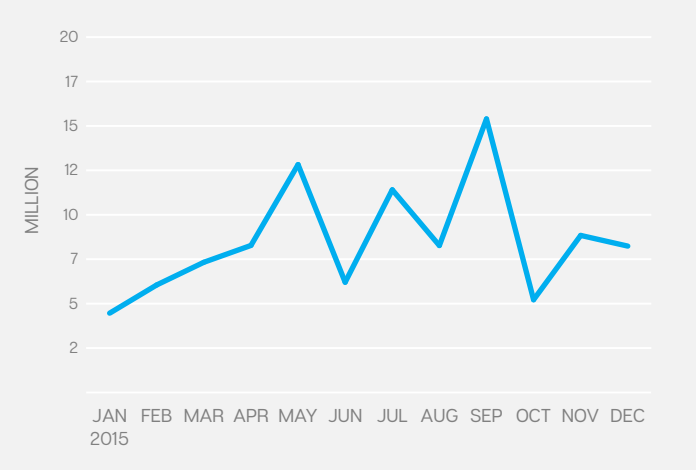
Some DDoS attacks can still afford criminals many opportunities for financial reward through extortion and blackmail by disrupting an organization's website. Following the money trail made this more difficult and DDoS mitigation technologies meant the attackers needed greater and greater bandwidth in order to make an impact. More recently, however, it is hacktivist groups and sometimes state actors that are complicit in some of the biggest attacks.

The recent attack on the BBC, which saw its website and associated services including iPlayer (the BBC's Internet catch-up TV and radio service in the UK) taken down for several hours on New Year's Eve, is a prime example. It is thought to be the biggest ever DDoS attack, according to New World Hacking, the anti-Islamic State organisation that claimed responsibility. The attackers claimed that the BBC's scale offered a chance for them to test their capabilities and claim the attack reached a peak of 602 Gbps.

There are rewards to be gained through a DDoS attack, the most obvious being blackmail. Victims are threated to pay or have their sites remain under attack. DDoS has also been used as a "distraction" tool in conjunction with some high-profile targeted attacks in 2015, where attackers flooded the website of the targeted organisation, leaving the IT team believing it was the prelude to a ransom demand. In reality, another, stealthier attack was quietly taking place at the same time.

DDoS Attack Volume Seen by Symantec's Global Intelligence Network

The chart shows the number of DDoS attacks per month, and this number has grown in the second half of 2015, before tailing-off at the end of the year. There were more notable spikes of activity, as attack durations become shorter and more discreet.



Top Five DDoS Attack Traffic Seen by Symantec's Global Intelligence Network

The majority of DDoS attacks were ICMP flood attacks, where a large volume of (typically) 'ping' requests eventually overload the target until it can no longer handle legitimate traffic.

	2015 Attacks	2015 Attack Rate	2014 Attacks	2014 Attack Rate
1	Generic ICMP Flood Attack	85.7%	DNS Amplification Attack	29.4%
2	Generic TCP Syn Flood Denial of Service Attack	6.4%	Generic ICMP Flood Attack	17.2%
3	Generic Ping Broadcast (Smurf) Denial of Service Attack	2.1%	Generic Ping Broadcast (Smurf) Denial of Service Attack	16.8%
4	Generic Teardrop/ Land Denial of Service Attack	2.0%	Generic Teardrop/Land Denial of Service Attack	7.2%
5	RFProwl Denial of Service Attack	0.6%	Generic ICMP Unreachable Denial of Service Attack	5.7%

Different attack groups have different preferences for their DDoS campaigns, and ICMP flood attacks were one of the main methods used by the Darkness/Optima botnet. Some methods, particularly amplification attacks, may no longer work that well over time. For example, when the media extensively covers a high-profile attack, more people will patch their servers. In addition, botnets that were used to perform previous attacks may be taken down or upgraded to newer versions that provide new functionality.

Simple but Effective

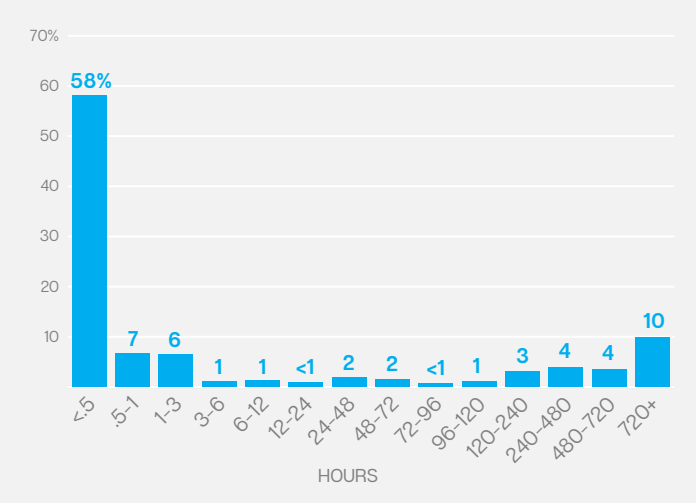
So why are DDoS attacks so popular? The answer is the same now as it was when we first wrote about them in December 2002: they are simple to set up, difficult to stop, and very effective. This is truer than ever with the rise of botnets-for-hire.

Botnets-for-hire were implicated in roughly 40 percent of all DDoS network layer attacks in the second quarter of 2015, according to Incapsula, a Symantec partner. While criminals can go to the effort of infecting multiple vulnerable devices and creating their own botnet to carry out DDoS attacks, it's often much easier to hire pre-made botnets for a set amount of time.

Prices remained fairly steady in the black market in 2015, where DDoS attacks can be ordered from just US$10 to US$1,000 per day. The cost to a business will be significantly higher, perhaps as much as a thousand times greater, depending on the nature of the business and the importance of the company's website. In 2015, Incapsula reported a DDoS attack can cost an organization as much as US$40,000 per hour. Consequently the potential rewards for an attacker successfully holding a company to ransom in this way will more than compensate for their costs. For example, one Australian email provider was attacked and attackers demanded a payment of 20 Bitcoins, worth about US$6,600. Another company that paid the demand was soon subjected to another assault shortly afterwards.

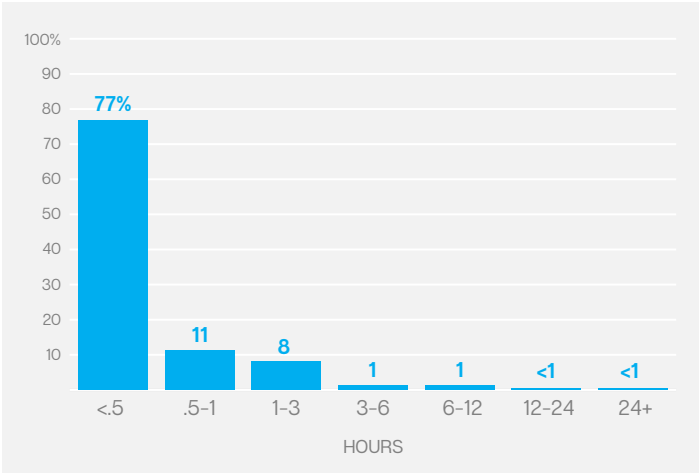
Distribution of Network Layer DDoS Attacks by Duration (Q3)

The chart shows how by the end of Q2 2015, there were still a significant proportion of DDoS attacks that could last for several hours, days, weeks, or months even. Chart courtesy of Incapsula.



Distribution of Network Layer DDoS Attacks by Duration (Q2)

The chart shows that by the end of Q3, the number of DDoS attacks that lasted for more than a day had almost disappeared completely, accounting for less than half of one percent of all DDoS attacks. Chart courtesy of Incapsula.



These shorter hit-and-run style attacks are indicative of a shift towards the greater use of DDoS being offered as a service, where subscribers are allotted limited access to the overall botnet resources, which are shared with other subscribers. This will usually be sufficient for them to conduct a few shorter-duration, mid-sized attacks. This can also help the attackers determine how effective the target infrastructure is at mitigating such attacks, and whether they need to increase the volume. Incapsula also reported that 100+ Gbps attacks became commonplace and a 100+ Gbps attack was mitigated once every other day.

The rise in popularity of DDoS-as-a-service corresponds with the significant drop in network layer attack duration in the third quarter of 2015 compared with the second quarter. Some of these DDoS-for-hire services refer to themselves as "stressers," because conducting a DDoS attack is illegal, they hide behind a veil, inferring they can be used for "stress testing" server resilience.

What's in a Botnet?

Botnets are key to DDoS attacks, whether they're hired or created by the criminals carrying out the attack. The bigger the botnet, the more simultaneous requests it can send and the more disruptive the attack will be.

But it's not just infected PCs that are providing criminals with their robot army. In October, we saw malware target MySQL servers, which often offer a much larger bandwidth capacity for an attack than traditional consumer PCs. This method isn't new, but it shows criminals are continuing to create bigger and better botnets.

In 2015, we also saw criminals making increasing use of the Internet of Things (IoT) to strengthen their botnet ranks. CCTV cameras proved particularly popular, likely because they are one of the most common IoT devices, with 245 million professionally installed video surveillance cameras active and operational globally in 2014.

Looking ahead, it's likely that criminals will make increasing use of vulnerable IoT devices to execute large-scale DDoS attacks. While solutions exist to mitigate against DDoS attack, organizations will also face new challenges in implementing appropriate security on non-traditional devices to ensure they don't become part of the problem. Perhaps more concerning, without the right security in place, it will be even more difficult to know when your printer, or refrigerator, thermostat, or toaster is actually part of a toxic global botnet. ■

CONCLUSIONS

Why is Cybersecurity so Important?

This is the 21st edition of the Symantec Internet Security Threat Report and much has changed since the first one. Each year we take a fresh look at the structure and contents of the report. As well as focusing on the threats and reporting the findings from our research, Symantec also tracks industry trends, and in the report, we try to highlight the important developments and look to future trends. This goes beyond just looking at computer systems, smartphones, and other products, and extends into broad concepts like national security, the economy, data protection, and privacy.

Cybersecurity Matters

This report takes a high-level view of cybersecurity and Internet threats, underlining the notable changes and developments. However, we must not forget that cybercrime is not victimless. For example, ransomware locks people out of their computers, holding treasured family photos to ransom, hijacking unfinished manuscripts for novels, and blocking access to tax returns, banking records, and other valuable documents. Moreover, there are no guarantees that paying the ransom will release those padlocks. Businesses, as well as home users, have become victims, and relying on backups is often the last line of defense when cybersecurity should really be the first.

Targeted attacks steal invaluable intellectual property from businesses, and a data breach can shred an organization's reputation—even threatening its survival. Cyber insurance claims are growing in number and cost, pushing premiums even higher. In the broadest sense, cybersecurity problems threaten national security and economic growth, which ultimately affects us all.

Web Security and the Industry's Responsibility

Updates to protect against such vulnerabilities are released regularly, including for SSL/TLS protocol libraries, such as OpenSSL, but website owners still have to install them. We have seen in this report and over the past few years that this is still not happening quickly enough. The number of vulnerable websites continues to persist year after year, with very little improvement to show. While the move from SHA-1 certificates to the much stronger SHA-2 is gaining momentum, organizations must deploy the new certificates properly in order for the changes to be effective.

Criminals continued to find vulnerabilities in the underlying infrastructure of website security in 2015, exploiting weaknesses in the underlying encryption systems, allowing attackers to intercept and control secure connections. The wider debate around security, privacy, and strong encryption will ultimately affect all of us.

Nothing Is Automatically Immune

No system is automatically immune from cyber threats, and in this report, the consequences of ignoring the risks from complacency, negligence, and incompetence are clear. In 2015, an unprecedented number of vulnerabilities were identified as zero-day exploits that have been weaponized, and web attack exploit kits are adapting and evolving them more quickly than ever. As more devices are connected, vulnerabilities will be exploited. Safeguarding Internet-connected devices will become critically important to ensuring the safety of industrial control systems (ICS) and medical devices in the community.

Alongside the rising number of software vulnerabilities, and the parade of attacks on different systems, the future will bring with it a greater range of diversity as threats against Windows systems will extend to other operating systems, mobile, and other IoT devices.

Digital Hygiene and a Cleaner Future

In cybersecurity, we often talk about infections and viruses. But the state of ubiquitous attacks, epic data breaches, and advanced threats we have seen this year suggest that there are better medical analogies. Instead of infection, we might think of disease both chronic and acute, serious, and benign.

Instead of thinking in binary terms of infection-free and compromised, we should move to a wellness model that considers susceptibility, resilience, wellness, vulnerability to infection, and recoverability. As IT security professionals, we should emphasize prevention, detection, and mitigation, as well as a complete cure. Concepts borrowed from epidemiology, incident response planning, and tools such as security simulation are becoming more important and useful.

For individuals and companies, Internet security is going to be much more like 'wellness' and 'hygiene' than 'medicine,' and focused on the routine of prevention rather than looking for a panacea or cure. We all need to stay digitally healthy and digitally clean, and habits of security will need to be relearned, over and over again.

Similarly, IT departments need to be proactive in reducing the risk from persistent intrusions and malware, and identify breaches quickly. Unfortunately, discovering attacks quickly requires constant, active vigilance. Information security can't wait for support tickets to open or for a favored security tool to identify an issue conclusively. Security needs to start digging through the data proactively during non-breach response time.

As an industry, we need to start moving into a more investigative, clinical-study mindset where we are constantly researching the habits or artifacts that cause the "digital diseases." Taking risks with cybersecurity will be seen as unacceptable, perhaps anathema akin to driving a car while under the influence of alcohol.

Cybersecurity is not just about employing the right kind of technology, it also requires good digital hygiene on the part of everyone; both at home, and in the office. Education and greater awareness of cybersecurity issues will help everyone to become more digitally healthy. By being aware of just how many risks you face, you can reduce them, and learn how to recognize symptoms, and diagnose "digital diseases" before they put your data, and your customers' data at risk. We should reject the misconception that privacy no longer exists. Privacy is precious, and should be protected carefully. ■

For the latest updated figures, please visit:
Symantec's Monthly Threat Report

BEST PRACTICE GUIDELINES FOR BUSINESSES

Employ Defense-in-Depth Strategies

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

Monitor for Network Incursion Attempts, Vulnerabilities, and Brand Abuse

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

Antivirus on Endpoints Is Not Enough

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection, including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints.
- Browser protection for avoiding obfuscated web-based attacks.
- File and web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware.
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware.
- Application control settings that can prevent applications and browser plugins from downloading unauthorized malicious content.
- Device control settings that prevent and limit the types of USB devices to be used.

Secure Websites Against Attacks and Malware Infection

Avoid compromising your trusted relationship with customers by regularly assessing your website for vulnerabilities and malware. Additionally, consider:

- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users.
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

Protect Private Keys

Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures.
- Secure keys in secure, tamper-proof, cryptographic hardware devices.
- Implement physical security to protect your assets from theft.

Use Encryption and DLP to Protect Sensitive Data

Implement and enforce a security policy whereby any sensitive data is encrypted. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution that can help prevent data breaches and minimize their impact.

- Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss.
- Monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.
- DLP should be configured to identify and block suspicious copying or downloading of sensitive data.
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.

BEST PRACTICE GUIDELINES FOR BUSINESSES

Ensure All Devices Allowed on Company Networks Have Adequate Security Protections

If a bring-your-own-device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

Implement a Removable Media Policy

Where practical, restrict unauthorized devices, such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Be Aggressive in Updating and Patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plugins. This also applies to operating systems, not just across computers, but mobile, ICS, and IoT devices as well. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic updates.

Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

Enforce an Effective Password Policy

Ensure passwords are strong. Passwords should be at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

Ensure Regular Backups Are Available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

Restrict Email Attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

Ensure Infection and Incident Response Procedures Are in Place

- Keep your security vendor contact information handy; know who you will call, and what steps you will take if you have one or more infected systems.
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems.
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media.
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

Educate Employees

As ever, basic common sense and the introduction of good security habits can go a long way to keeping sites and servers safe this year.

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless from a trusted source or the download has been scanned for malware.
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends.
- Deploy web browser URL reputation plugin solutions that display the reputation of websites from searches.
- Restrict software to corporate-approved applications, if possible, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites.

BEST PRACTICE GUIDELINES FOR BUSINESSES

- Educate users on safe social media conduct. Offers that look too good usually are, and hot topics are prime bait for scams. Not all links lead to real login pages.
- Encourage them to adopt two-step authentication on any website or app that offers it.
- Ensure they have different passwords for every email account, applications and login—especially for work-related sites and services.
- Remind then to use common sense. Having antivirus and security software doesn't mean it is ok to visit malicious or questionable websites.
- Encourage employees to raise the alarm if they see anything suspicious. For example, if Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (indicative of fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or to use the task manager, and then notify the helpdesk.

Protect Mobile Devices

We recommend that people and employers treat mobile devices like the small, powerful computers that they are and protect them accordingly using:

- Access control, including biometrics where possible.
- Data loss prevention, such as on-device encryption.
- Automated device backup.
- Remote find and wipe.
- Regular updating. For example, the latest version of Android, codenamed 'Honeycomb', includes a number of features designed specifically to thwart attackers.
- Common sense. Don't jailbreak devices and only use trusted app markets.
- Training, particularly around paying attention to permissions requested by an app.
- Security solutions such as Symantec Mobility or Norton Mobile Security

We have seen the number of mobile vulnerabilities increase every year over the past three years—although this is perhaps an indicator of progress rather than a cause for despair. It is an indication that security researchers, operating system developers and app writers are, in fact, paying more attention to mobile security by identifying and fixing more problems.

Although we expect mobile devices to come under growing attack over the next year, there is also hope that with the right preventative measures and continuing investment in security, users can achieve a high level of protection against them.

Building Security into Devices

The diverse nature of ICS and IoT platforms make host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), with customizable rulesets and policies that are unique to a platform and application, suitable solutions.

However, manufacturers of ICS and IoT devices are largely responsible for ensuring that security is built into the devices before shipping.

Building security directly into the software and applications that run on the ICS and IoT devices should prevent many attacks that manage to side-step defenses at the upper layers. Manufacturers should adopt and integrate such principles into their software development processes.

Business users and consumers need to be assured that suppliers are fundamentally building security into the IoT devices that they are buying, rather than it being considered as a bolt-on option.

It's a Team Effort

Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. But it only takes one bad experience of stolen data or a drive-by download to tarnish the reputation of every website in the consumer's mind.

As we said at the start of the report, there is a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks websites potentially pose to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt Complete Website Security in 2016, and together with Symantec, make it a good year for cybersecurity and a very bad one for cybercriminals. ■

BEST PRACTICE GUIDELINES FOR WEBSITE OWNERS

For website security to be effective, it has to be implemented with care and attention and it has to be monitored and maintained continually.

While there are tools to help you keep your website ecosystem secure, it all starts with education. You've read about the risks—now find out what you can do about them.

Get in line with industry standards

- **Implement always-on SSL.** Implement SSL/TLS on every page of your website so that every interaction a visitor has with your site is encrypted. Switching to 'HTTPS everywhere', as it's also called, with OV or EV SSL/TLS certificates demonstrates your credibility and can also improve your search rankings and paves the way for an upgrade to HTTP/2, delivering better performance.
- **Migrate to SHA-2.** As discussed in the report, certificate authorities should have stopped issuing SHA-1 certificates as of 1 January 2016, but you need to ensure any legacy certificates are also upgraded and that any devices and applications that may not currently recognize SHA-2 are upgraded too.
- **Consider adopting ECC.** Symantec also offers the use of the ECC encryption algorithm. All major browsers, even mobile, support ECC certificates on all the latest platforms, and compared to an industry-standard 2048-bit RSA key, 256-bit ECC keys are 64,000 times harder to crack.

Use SSL/TLS Correctly

SSL/TLS is only as good as its implementation and maintenance. So be sure to:

- **Keep protocol libraries up to date.** SSL/TLS implementation is an on-going task and it's vital that any patches or updates to the software you use are implemented as soon as possible.
- **Don't let your certificates expire.** Keep track of what certificates you have, from which certificate authority, and when they are due to expire. Symantec offers a range of automation tools to help you do this, giving you more time for proactive security tasks.
- **Display recognized trust marks.** Display trust marks (such as the Norton Secured Seal) in highly visible locations on your website to show customers your commitment to their security.

Manage your SSL/TLS keys properly. Limit the number of people with access to them; have separate administrators for managing the passwords for the server where they're kept and for managing the systems they're actually stored in; and use automated certificate and key management systems to reduce human involvement.

Any breach affecting SSL keys should be notified to the CA quickly, so that corresponding certificates can be revoked.

Adopt Comprehensive Website Security

- **Scan regularly.** Keep an eye on your web servers and watch for vulnerabilities or malware. Automation tools can help with this.
- **Use antivirus.** Antivirus software isn't just for PCs and smartphones—it's for servers too and could help prevent a serious malware attack against your entire website infrastructure.
- **Be picky about your plugins.** The software you use to manage your website comes with vulnerabilities too. The more third-party software you use, the greater your attack surface; so only deploy what's absolutely necessary.
- **Consider the whole ecosystem.** Have you deployed a Web Application Firewall to defend against injection attacks? Is your code signing secure for your web apps? Do you have automated tools to detect and defend against the increasingly common problem of DDoS attacks?

Symantec offers a range of tools that makes maintaining complete website security a straightforward and efficient task.

Avoid Compromising Trusted Relationships with Customers by:

- Regularly assessing your website for any vulnerabilities.
- Scanning your website daily for malware.
- Setting the secure flag for all session cookies.
- Securing your websites against man-in-the-middle (MITM) attacks and malware infection.
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users.
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

There Is No 'I' in Team

Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. It only takes one bad experience to tarnish the reputation of every single one in the consumer's mind.

As we said in the report, there exists a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks your website potentially poses to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt comprehensive website security in 2016 and, together with Symantec, make it a good year for cyber security and a very bad one for cybercriminals.

20 CRITICAL SECURITY CONTROLS

Overview

The Council on Cybersecurity 20 Critical Security Controls is a prioritized list designed to provide maximum benefits toward improving risk posture against real-world threats. This list of 20 control areas grew out of an international consortium of U.S. and international agencies and experts, sharing from actual incidents and helping to keep it current against evolving global cybersecurity threats. Led by the Center for Internet Security (CIS), the CIS Critical Security Controls ("the Controls") have been matured by an international community of individuals and institutions, and were updated in 2015 to version six. For more information please refer to the documentation found at http://www.cisecurity.org/critical-controls.

Many organizations face the challenges and increasing threats to their cybersecurity by strategically choosing a security controls framework as a reference for initiating, implementing, measuring and evaluating their security posture, and managing risk. Over the years, many security control frameworks have been developed (for example, NIST), with the common goal of offering combined knowledge and proven guidance for protecting critical assets, infrastructure, and information. Based on the information we have today about attacks and threats, what are the most important steps that enterprises should take now to secure systems and data?

The Critical Security Controls are designed to provide organizations the information necessary to increase their security posture in a consistent and ongoing fashion. The Controls are a relatively small number of prioritized, well-vetted, and supported set of security actions that organizations can take to assess and improve their current security state.

To implement the Controls you must understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversary actions that could impact your ability to be successful in the business or operations.

TOP 5 PRIORITIES

We emphasize the use of the first five Controls for every organization. This helps establish a foundation of security and has the most immediate impact on preventing attacks. From this foundation organizations can apply other Controls as they meet the business need of the organization.

In the following pages you will see a table that outlines the areas identified in the ISTR and ties them to Critical Security Controls:

01

Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

02

Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

03

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

04

Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

05

Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CRITICAL CONTROLS

06

Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

07

Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

08

Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

09

Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

10

Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

11

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

12

Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

13

Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

14

Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

15

Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

16

Account Monitoring and Control

Keep attackers from impersonating lActively manage the life cycle of system and application accounts – their creation, use, dormancy, and deletion - in order to minimize opportunities for attackers to leverage them.

17

Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission – critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

18

Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

19

Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

20

Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

CRITICAL CONTROL PROTECTION PRIORITIES

	HARDEN DEFENSES	ENHANCE DETECTION	REDUCE IMPACT
MOBILE DEVICES	03 04 07 11 18	01 02 06 08 15	05 10 13 17
INTERNET OF THINGS	03 04 11 14 18	01 02 06 08 15	05 09 12 17
WEB-BASED THREATS	03 04 07 18	01 02 06 08 16	05 09 10 12 17
SOCIAL MEDIA & EMAIL THREATS	03 04 07	01 02 08 20	05 10 12 17
TARGETED ATTACKS & SPEAR PHISHING	03 04 07 11 14 18	01 02 06 08 16 20	05 09 10 12 13 17 19
DATA BREACHES	03 04 07 11 14 18	01 02 06 15 16 20	05 09 10 12 13 17 19
E-CRIME & MALWARE	03 04 07 11 14 18	01 02 06 08 16 20	05 09 10 12 13 17 19
CLOUD & INFRASTRUCTURE	03 04 11 14 18	01 02 06 08 15 16 20	05 09 10 12 13 17 19
WEB SERVERS	03 04 11 14 18	01 02 06 08 16 20	05 09 10 12 13 17 19
DDOS & BOTNETS	03 04 11 18	01 02 06 08 20	05 09 12 17 19

BEST PRACTICE GUIDELINES FOR CONSUMERS

Protect Yourself

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file- and heuristic-based) and behavioral malware prevention can prevent unknown malicious threats from executing.
- Bi-directional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer.
- Browser protection will protect against obfuscated web-based attacks.
- Use reputation-based tools that check the reputation and trust of a file and website before downloading, and that check URL reputations and provide safety ratings for websites found through search engines.
- Consider options for implementing cross-platform parental controls, such as Norton Online Family.

Update Regularly

Keep your system, program, and virus definitions up-to-date; always accept updates requested by the vendor.

Running out-of-date versions can put you at risk from being exploited by web-based attacks. Only download updates from vendor sites directly. Select automatic updates wherever possible.

Be Wary of Scareware Tactics

Versions of software that claim to be free, cracked, or pirated can expose you to malware or social engineering attacks that attempt to trick you into thinking your computer is infected and getting you to pay money to have it removed.

Use an Effective Password Policy

Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or websites.

Use complex passwords (upper/lowercase and punctuation). Passphrases and password management apps can help too.

Think Before You Click

Never view, open, or copy email attachments to your desktop or execute any email attachment unless you expect it and trust the sender. Even when receiving email attachments from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails or social media communications, even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using a preview tool or plugin.
- Use a web browser plugin or URL reputation site that shows the reputation and safety rating of websites before visiting.
- Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop up asking you to install media players, document viewers, and security updates. Only download software directly from the vendor's website.
- Be aware of files you make available for sharing on public sites, including gaming, BitTorrent, and any other peer-to-peer (P2P) exchanges. Keep Dropbox, Evernote, and other usages to a minimum for pertinent information only, and only use when approved for corporate use.

Safeguard Your Personal Data

Limit the amount of personal information you make publicly available on the Internet (in particular via social networks). This includes personal and financial information, such as bank logins or birth dates. Additionally:

- Regularly review your bank, credit card, and credit information frequently for irregular activity.
- Avoid banking or shopping online from public computers (such as libraries, Internet cafes, and similar establishments) or from unencrypted.

Wi-Fi Connections

When using public wireless hotspots consider the following:

- Use HTTPS when connecting via Wi-Fi networks to your email, social media, and sharing websites. Check the settings and preferences of the applications and websites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

CONTRIBUTORS

Paul Wood, Executive Editor
Ben Nahorney, Cybersecurity Threat Analyst
Kavitha Chandrasekar, Cybersecurity Threat Analyst
Scott Wallace, Graphics & Design
Steven Rankin, Infographics
Kevin Haley, Technical Advisor

Contributors

Axel Wirth
Bartlomiej Uscilowski
Brian Witten
Candid Wueest
Dermot Harnett
Dick O'Brien
Dipesh Shah
Dylan Morss
Efrain Ortiz
Gaurang Bhatt
Gavin O'Gorman
Himanshu Mehta
Kent McMullen
Laura O'Brien
Mario Ballano Barcena
Michael Klieman
Nicholas Johnston
Peter Coogan
Pierre-Antoine Vervier
Preeti Agarwal
Rauf Ridzuan
Roberto Sponchioni
Roger Park
Sara Groves
Satnam Narang
Shankar Somasundaram
Stephen Doherty
Vaughn Eisler
William Wright

Special Thanks To

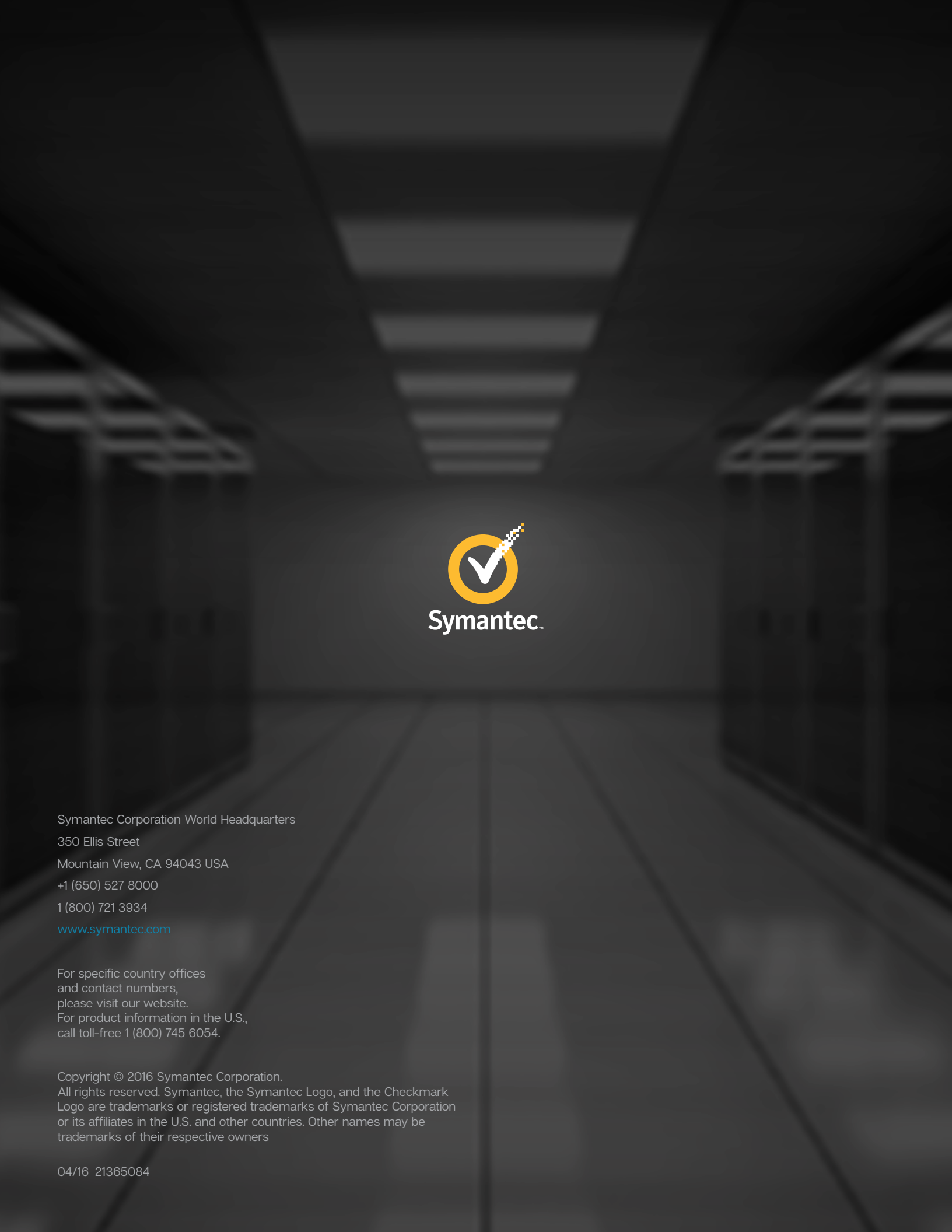
Alejandro Borgia
Anna Sampson
Cheryl Elliman
Jennifer Duffourg
Linda Smith Munyan
Mara Mort
Marianne Davis

ABOUT SYMANTEC

Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

MORE INFORMATION

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/



Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

04/16 21365084