



WSTR

WEBSITE SECURITY THREAT REPORT | 2015

PART 1

CONTENTS

Introduction	3
Executive summary	4
Web threats	5
eCrime	21
Recommendations	36
About Symantec	40



INTRODUCTION

Symantec has the most comprehensive source of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 41.5 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™ products
- Symantec Website Security Solutions
- and other 3rd party data sources.

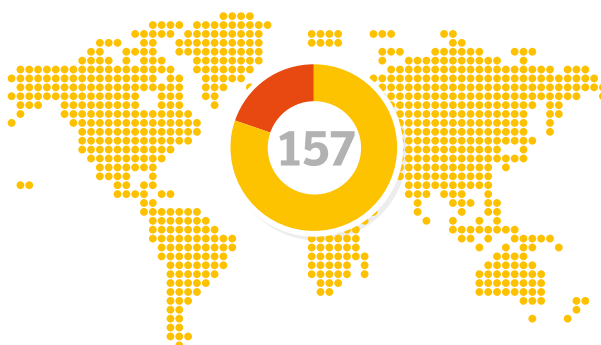
Symantec also maintains one of the world's most comprehensive vulnerability databases, made of over 60,000 recorded vulnerabilities from over 19,000 vendors representing over 54,000 products.

Spam, phishing, and malware data is captured through sources including:

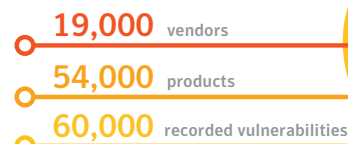
- The Symantec Probe Network, a system of more than 5 million decoy accounts
- Symantec.cloud
- Symantec Website Security Solutions Malware and Vulnerability products
- and a number of other Symantec security technologies.

Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before they reach customers' networks. Over 8.4 billion email messages are processed each month, and more than 1.7 billion web requests filtered each day across 14 data centers. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 50 million consumers.

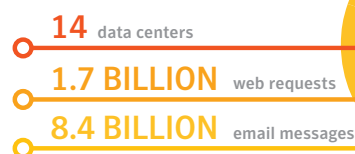
The result is the Symantec Website Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.



Symantec maintains one of the world's most comprehensive vulnerability databases



Skeptic™, the Symantec.cloud proprietary heuristic technology



Symantec Website Security Solutions provides 100 percent availability, and processes over 6 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. 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.

EXECUTIVE SUMMARY

The biggest story in 2014 was, of course, the Heartbleed bug, which shook the foundations of Internet security. This wasn't about criminals being clever; it was about the inherent vulnerabilities of human-built software, and it reminded everyone of the need for vigilance, better implementation, and more diligent website security.

Of course, while Heartbleed hit the headlines, criminals were still hard at work making their own opportunities for exploitation, theft and disruption. 2014 saw criminals grow more professional, sophisticated, and aggressive in their tactics to the detriment of businesses and individuals alike.

Vulnerabilities Leave Us All Exposed

Heartbleed wasn't the only vulnerability to hit this year. Poodle and Shellshock also provided ways for criminals to use websites to access servers, steal data, and install malware.

Interestingly, the number of websites found with malware in 2014 fell dramatically, halving to 1 in 1,126. This is despite the fact that three-quarters of scanned websites had vulnerabilities—the same as last year. In part this may be down to website security, but it may also be that criminals are focusing on alternative methods of malware delivery, such as social media and malvertising.

Unfortunately, more generally, many people failed to install patches for vulnerabilities in the software running on their devices and servers, which made exploitation by criminals all too easy. Attackers often use a specialist 'dropper', perhaps delivered via a drive-by attack or social media scam, which scans for a range of known vulnerabilities and exploits any unpatched security weakness.

Cybercriminals Take Their Business to the Next Level

2014 saw criminal operations grow evermore sophisticated, with specializations, service providers, and fluctuating markets mirroring the legitimate technology industry.

A drive-by download web toolkit, for example, which includes updates and 24/7 support, can be rented for between \$100 and \$700 per week. Distributed denial-of-service (DDoS) attacks can be ordered from \$10 to \$1,000 per day¹, and in terms of the buyer's market, credit card details can be bought for between \$0.50 and \$20 per card, and 1,000 followers on a social network can cost as little as \$2 to \$12.

Attack Tactics Are Amoral and Aggressive

Criminals have never much cared about their victims, but 2014 saw their malicious behavior reach new heights.

Between May and September alone Symantec saw a 14-fold increase in cryptoware². This variant of ransomware encrypts a victim's files—everything from photos to vital contracts and invoices—and holds the private keys needed for their decryption to ransom. People are often instructed to pay up in Bitcoins, using a Tor web page, making the criminals behind the scam virtually impossible to trace and shut down.

Social media and phishing scams also looked to take advantage of people's fears around hacking and health scare stories to entice them into clicking; the profit being in affiliate programs that pay for clicks and sign ups, malware downloads that further exploit the victim, or data gathered when victims fall for filling in their information on a linked phishing site.

¹ <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

² <http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware>

WEB THREATS



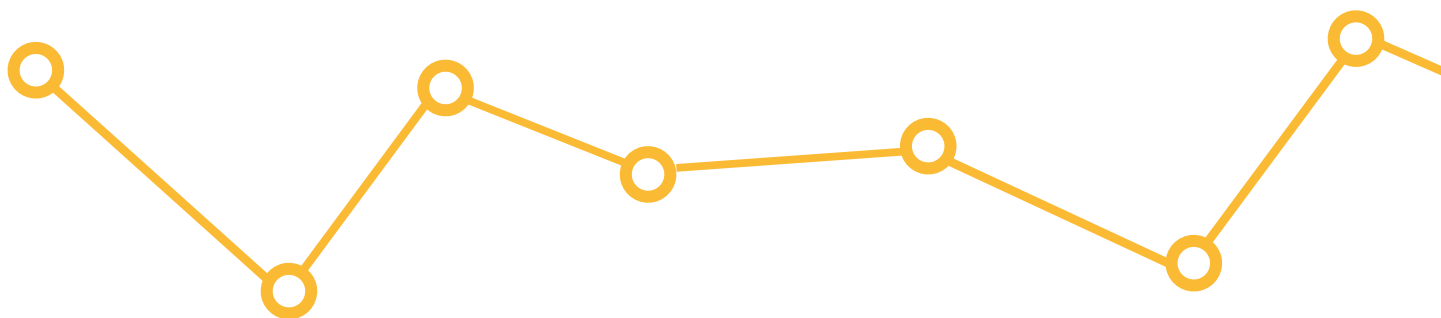
WSTR

The logo for WSTR is centered within a dark gray rectangular box with a thin orange border. The letters 'W', 'S', and 'T' are white with a thin orange outline, while the 'R' is solid orange. To the left and right of the box, orange lines with circular nodes extend outwards, resembling a network or data flow diagram.

AT A GLANCE

1	The Heartbleed vulnerability left approximately half a million trusted websites at risk of significant data breaches in April ³ .
2	The Heartbleed scare caused many more people to take note and improve standards in SSL and TLS implementation.
3	Criminals are taking advantage of the technology and infrastructure that legitimate ad networks have created to distribute malicious attacks and scams.
4	A big jump to 5 percent of total infected websites has bumped anonymizer sites into the top 10 types of infected sites for 2014.
5	The total number of sites found with malware has virtually halved since 2013.

³ <http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html>

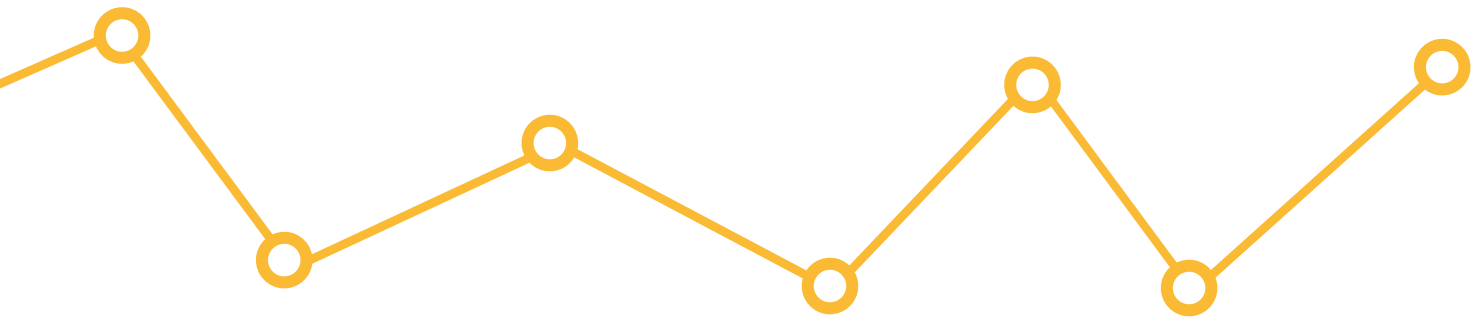


INTRODUCTION

Web threats got bigger and much more aggressive in 2014 as holes in commonly used tools and encryption protocols were exposed, and criminals made it harder to escape their malicious clutches.

The web presented an incredibly threatening landscape in 2014, a trend set to continue in 2015. Vulnerabilities and new variants of malware underlined that website security deserves full-time, business-critical attention.

At the time of writing, a new SSL/TLS vulnerability dubbed “FREAK” was identified in 2015 by several security researchers⁴. FREAK allows man-in-the-middle attacks on encrypted communications between a website visitor and website, which ultimately could allow attackers to intercept and decrypt communications between affected clients and servers. Once the encryption is broken by the attackers, they could steal passwords and other personal information, and potentially launch further attacks against the affected website.



⁴ <http://www.symantec.com/connect/blogs/freak-vulnerability-can-leave-encrypted-communications-open-attack>

HIGH PROFILE VULNERABILITIES

Heartbleed

Heartbleed hit the headlines in April, when it emerged that a vulnerability in the OpenSSL cryptographic software library meant attackers could access the data stored in a web server's memory during an encrypted session. This session data could include credit card details, passwords, or even private keys that could unlock an entire encrypted exchange⁵.

At the time, it was estimated that Heartbleed affected 17 percent of SSL web servers, which use SSL and TLS certificates issued by trusted certificate authorities⁶. This had a massive impact on businesses and individuals.

Not only was a great deal of sensitive data at risk, but the public also had to be educated about the vulnerability, so they knew when to update their passwords. Website owners had to first update their servers to the patched version of OpenSSL, then install new SSL certificates, and finally revoke the old ones. Only then would a password change be effective against the threat, and communicating that to the general public posed a real challenge.

Fortunately, the response was swift and within five days none of the websites included in Alexa's top 1,000 was vulnerable to Heartbleed, and only 1.8 percent of the top 50,000 remained vulnerable⁷.

ShellShock and Poodle

Heartbleed wasn't the only vulnerability to come to light in the online ecosystem in 2014. In September a vulnerability known as 'Bash Bug', or 'ShellShock', which affected most versions of Linux and Unix as well as Mac OS X, was discovered. ShellShock was a particularly good example that highlighted how quickly the security landscape could change for website owners; one day their servers are securely patched and up-to-date, and

then very suddenly the next day they are not, and many of the initial patches were incomplete and had to be patched again.

The easiest route of attack was through web servers as attackers could use Common Gateway Interface (CGI), the widely used system for generating dynamic web content, to add a malicious command to an environmental variable, which Bash, the server component containing the vulnerability would interpret and run⁸.

Numerous threats took advantage of ShellShock, exposing servers, and the networks they were connected to, to malware that could infect and spy on multiple devices.

Attention then turned back to encryption in October, when Google discovered a vulnerability, known as Poodle. Potentially, this vulnerability would allow criminals to exploit servers that still support an older SSL protocol, known as SSL 3.0, by interfering with the 'handshake' process, which verifies which protocol the server can use, and forcing it to use SSL 3.0—even if a newer protocol is supported⁹.

A successful exploit would allow an attacker to carry out a man-in-the-middle attack to decrypt secure HTTP cookies, which then lets them steal information or take control of the victim's online accounts. Fortunately, this was not as serious as Heartbleed. To take advantage of the Poodle vulnerability, the attacker would need to have access to the network between the client and server, for instance through a public Wi-Fi hotspot.

⁵ <http://www.symantec.com/connect/blogs/heartbleed-bug-poses-serious-threat-unpatched-servers>

⁶ <http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html>

⁷ <http://www.symantec.com/connect/blogs/heartbleed-reports-field>

⁸ <http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability>

⁹ <http://www.symantec.com/connect/blogs/poodle-vulnerability-old-version-ssl-represents-new-threat>

HIGH PROFILE VULNERABILITIES

High-profile Vulnerabilities and Time to Patch

The attacks that quickly followed the announcement of these vulnerabilities were big news in and of themselves, albeit in a different manner than attention-grabbing zero-day vulnerabilities. Heartbleed and ShellShock could be seen as a different class of vulnerability altogether, being used to compromise servers more than end points. The key factor with these high-profile vulnerabilities was the prevalence of the software they affected, found in so many systems and devices. Given their wide-spread existence, these vulnerabilities instantly became hot targets for attackers, and were both being exploited within hours of disclosure.

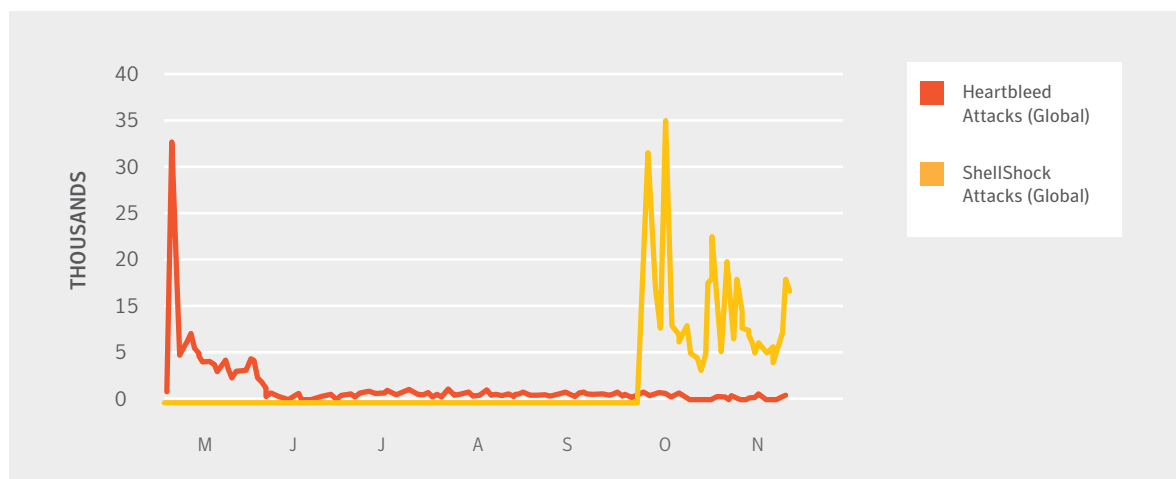
The large spikes seen in these demonstrate that, while Symantec signatures were in place to detect and block attacks, almost immediately after disclosure, there were already a large number of attacks underway. Attackers were able to exploit the Heartbleed vulnerability within 4 hours of it becoming public.

SSL and TLS certificates are still vital to security

It's important to note that while online security was shaken in 2014, SSL certificates and their more modern counterparts, TLS certificates, still work and are still essential. In fact, the Heartbleed incident demonstrated just how quickly the online security community could respond to these types of threats.

Industry standards are also constantly improving thanks to the hard work and vigilance of organizations like the CA/ Browser Forum, of which Symantec is a member. In other words, the foundations of Internet security, which keep your site and its visitors safe, are still strong and are only getting stronger.

GLOBAL HEARTBLEED AND SHELLSHOCK ATTACKS APRIL - NOVEMBER 2014



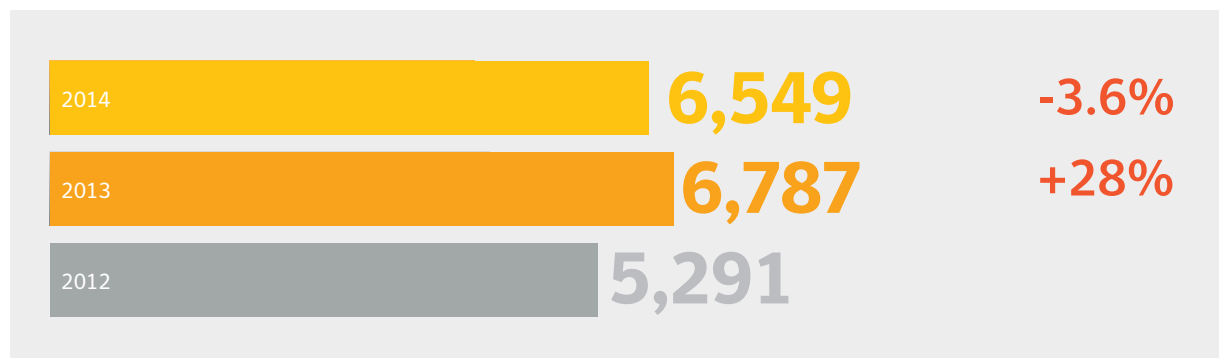
Source: Symantec

VULNERABILITIES AS A WHOLE

With minor fluctuations from year to year, the trend in the number of vulnerabilities continues upwards. Remedies, workarounds, or patches are available for the majority of reported vulnerabilities. However, malware authors know that many people do not apply these updates, and so they are able to exploit well-documented vulnerabilities in their attacks. In many cases, a specialist ‘dropper’ scans for a number of known vulnerabilities and uses any unpatched security weakness as a backdoor to install malware. This, of course, underlines the crucial importance of applying updates.

This is how web exploit toolkits, such as Sakura and Blackhole, have made it easier for attackers to exploit an unpatched vulnerability published months, or even years previously. Several exploits may be created for each vulnerability, and a web attack toolkit will first perform a vulnerability scan on the browser to identify any potentially vulnerable plugins and the best attack that can be applied. Many toolkits won’t utilize the latest exploits for new vulnerabilities if an old one will suffice; exploits against zero-day vulnerabilities are uncommon and highly sought after by the attackers, especially for use in watering-hole-style targeted attacks.

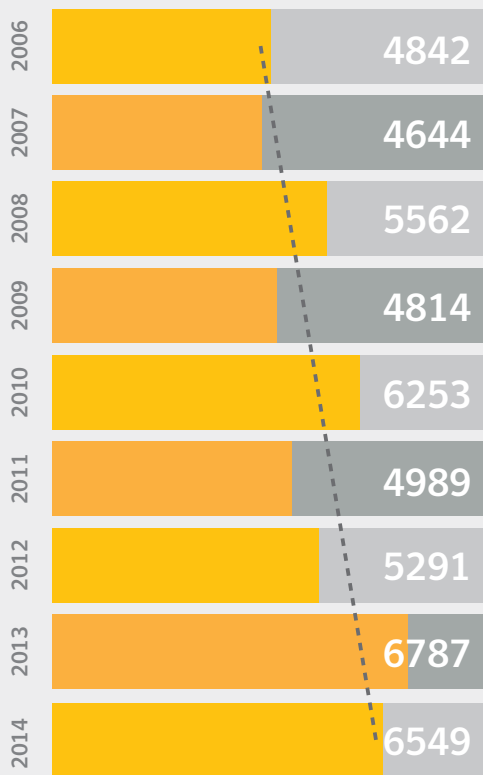
NEW VULNERABILITIES



Source: Symantec | Deepsight

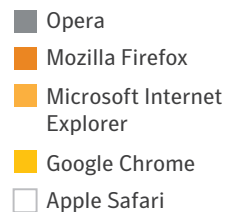
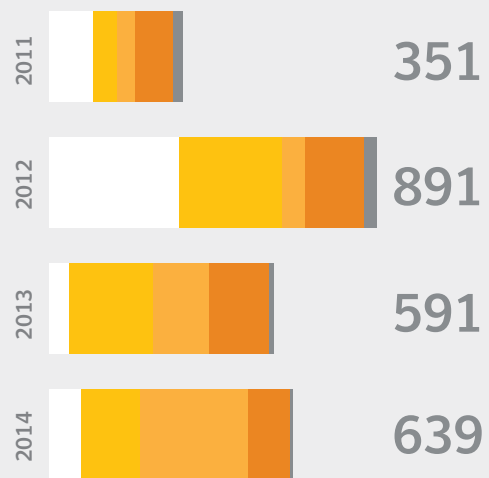


TOTAL NUMBER OF VULNERABILITIES, 2006 – 2014



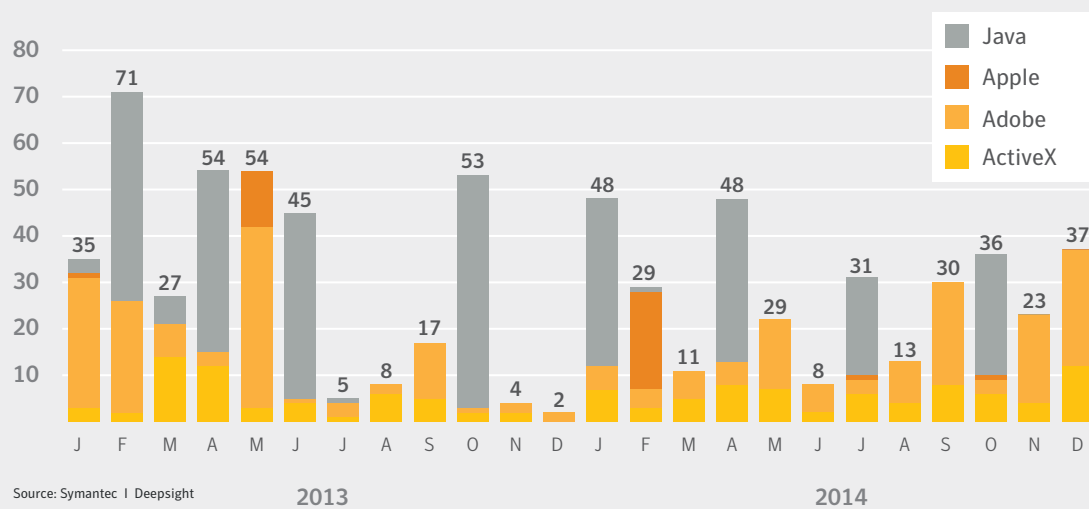
Source: Symantec | Deepsight

BROWSER VULNERABILITIES, 2011 – 2014



Source: Symantec | Deepsight

PLUG-IN VULNERABILITIES BY MONTH 2013 – 2014



Source: Symantec | Deepsight

2013

2014

While reported vulnerabilities represent a general risk, zero-day vulnerabilities are potentially much more serious. These are vulnerabilities that are only discovered after they are exploited by attackers.

COMPROMISED SITES

Of all the websites Symantec scanned for vulnerabilities in 2014, around three quarters were found to have vulnerabilities—about the same as last year. The percentage of those vulnerabilities classed as critical, however, increased from 16 to 20 percent.

In contrast, the number of websites actually found with malware was much lower than last year, having reduced from 1 in 566 to 1 in 1,126. This seems to have had a knock-on effect on the number of web attacks blocked per day, which has also decreased—though only by 12.7 percent. This suggests that infected websites were, (on average), responsible for more attacks each in 2014. One reason for this is the way that some web-attack toolkits are designed to be used in the cloud, as Software-as-a-Service (SaaS). For example, a compromised website may use a HTML iframe tag or some obfuscated JavaScript in order to inject malicious code from the SaaS-based exploit toolkit, rather than launch the malicious attack directly from exploit code hosted on the compromised website itself. This growth in SaaS-based exploit toolkits is also evidenced in the decline in the number of new malicious domains used to host malware, which fell by 47 percent, from 56,158 in 2013 to 29,927 in 2014.

Web-attack toolkits perform scans on the victims' computers, looking for vulnerable plugins in order to launch the most effective attack. Moreover, these SaaS toolkits are often located on bullet-proof hosting services, with IP addresses that can change quickly and domain names that may be dynamically generated, making it more difficult to locate the malicious SaaS infrastructure and shut it down. Attackers are also able to control how the exploits are administered, for example, by only enabling the attacks if a cookie has been set by the initial compromised website, preserving the malicious code from the prying eyes of search engines and security researchers. Web attack toolkits are discussed in more detail later in this chapter.

In terms of the type of websites most frequently exploited, it's interesting to note the inclusion of anonymizer websites in the top 10 this year. This is perhaps another case of criminals following the crowds as more people look to evade tracking by ISPs and others, and increase their browsing privacy.

TOP-TEN VULNERABILITIES FOUND UNPATCHED ON SCANNED WEB SERVERS

RANK	NAME
1	SSL/TLS POODLE vulnerability
2	Cross Site Scripting
3	SSL v2 support detected
4	SSL Weak Cipher Suites Supported
5	Invalid SSL certificate chain
6	Missing Secure Attribute in an Encrypted Session (SSL) cookie
7	SSL and TLS protocols renegotiation vulnerability
8	PHP 'strchr()' Function Information Disclosure vulnerability
9	http TRACE XSS attack
10	OpenSSL 'bn_wexpnd()' Error Handling Unspecified vulnerability

Source: Symantec | Trust Services

SCANNED WEBSITES WITH VULNERABILITIES

76%

2014

-1%

77%

2013

+25%

55%

2012

Source: Symantec | Trust Services

... % OF WHICH WERE CRITICAL

20%

2014

+4%

16%

2013

+8%

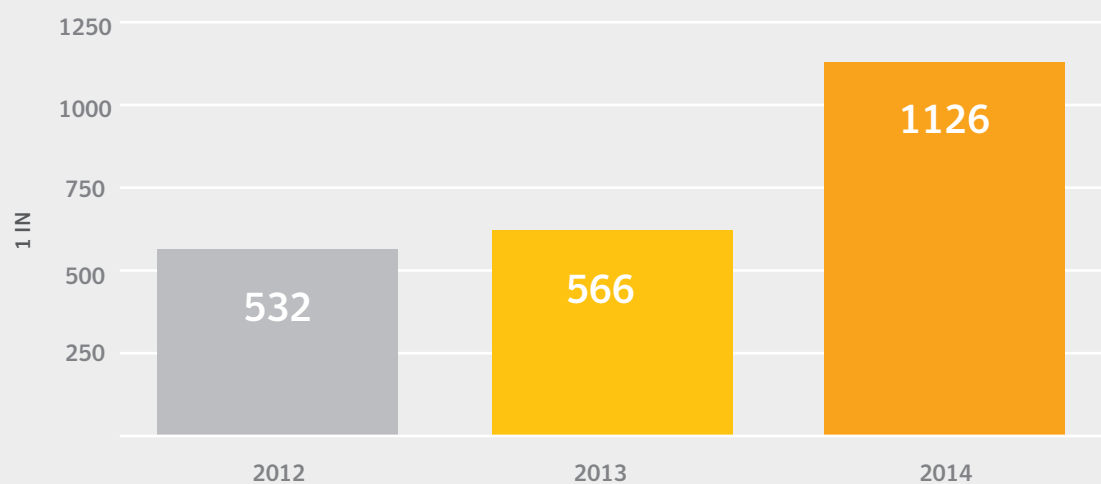
24%

2012

Source: Symantec | Trust Services

In 2014, 20 percent (1 in 5) of all vulnerabilities discovered on legitimate websites were considered critical, that could allow attackers access to sensitive data, alter the website's content, or compromise visitors' computers.

WEBSITES FOUND WITH MALWARE



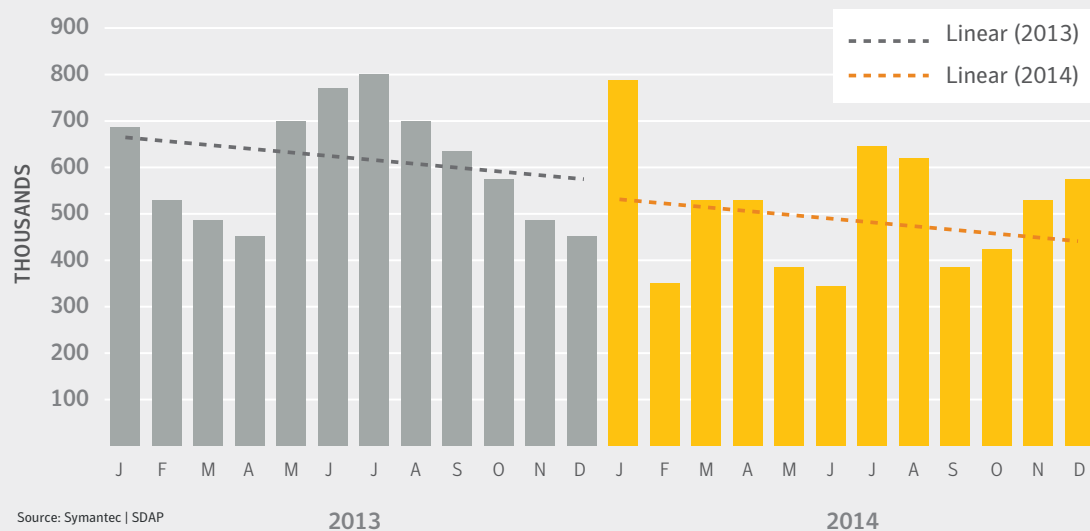
Source: Symantec | Trust Services

CLASSIFICATION OF MOST FREQUENTLY EXPLOITED WEBSITES, 2013 – 2014

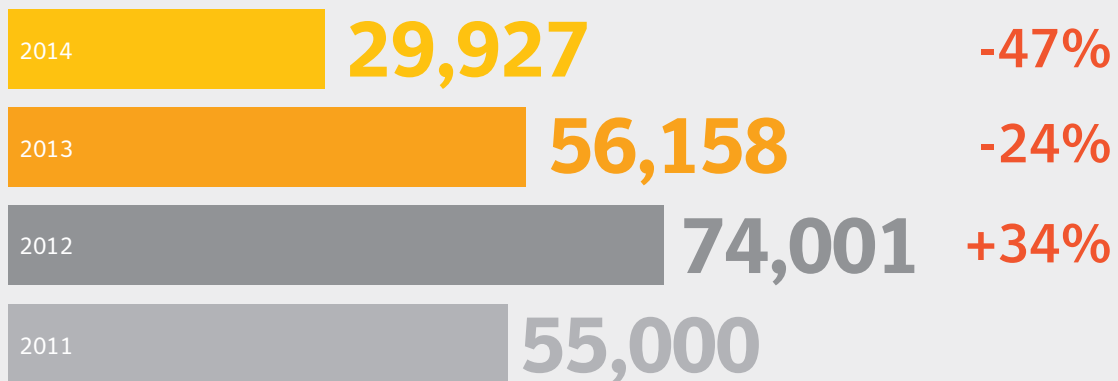
RANK	2014 Top-10 Most Frequently Exploited Categories of Websites	2014 Percent of Total Number of infected Websites	2013 Top 10	2013 Percentage
1	Technology	21.5%	Technology	9.9%
2	Hosting	7.3%	Business	6.7%
3	Blogging	7.1%	Hosting	5.3%
4	Business	6.0%	Blogging	5.0%
5	Anonymizer	5.0%	Illegal	3.8%
6	Entertainment	2.6%	Shopping	3.3%
7	Shopping	2.5%	Entertainment	2.9%
8	Illegal	2.4%	Automotive	1.8%
9	Placeholder	2.2%	Educational	1.7%
10	Virtual Community	1.8%	Virtual Community	1.7%

Source: Symantec | SDAP, Safe Web, Rulespace

WEB ATTACKS BLOCKED PER MONTH, 2013 – 2014



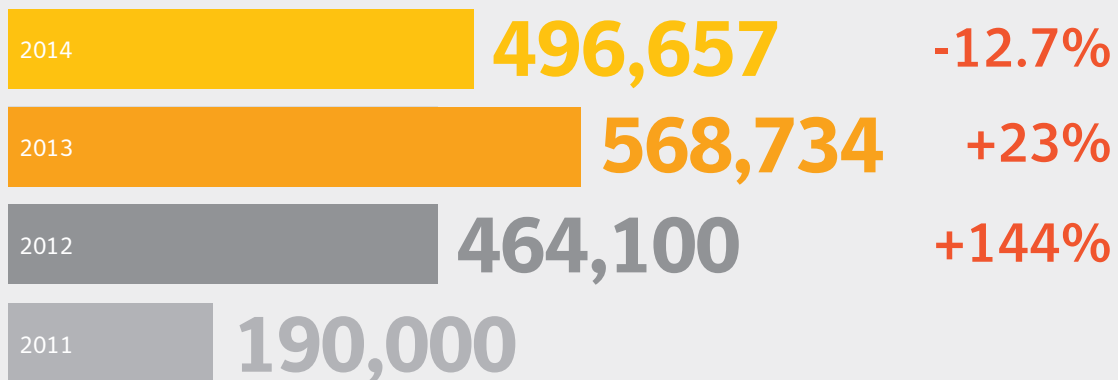
NEW UNIQUE MALICIOUS WEB DOMAINS



Source: Symantec | .cloud

In 2014, a 47% drop in unique malicious web domains indicates an increase in the use of cloud-based Software-as-a-Service (SaaS) type toolkits.

WEB ATTACKS BLOCKED PER DAY



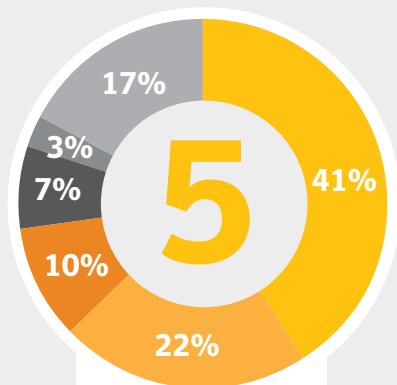
Source: Symantec | SDAP

For the most part, the bulk of the -12.7% drop in the average number of daily attacks blocked occurred in the latter half of 2013, since the decline throughout 2014 has been much more shallow.

With the majority of websites still accommodating vulnerabilities, it is apparent that many website owners are not keeping on top of vulnerability scans. They may be paying more attention to malware scans that could potentially reveal malicious software, yet malware is often planted following the earlier exploitation of vulnerabilities. Prevention is always better than cure.

With so many potentially vulnerable websites, criminals were already achieving considerable success exploiting them, and many were also quick to take advantage of some of those SSL and TLS vulnerabilities that were also exposed in 2014. Moreover, the greater prevalence of social media scams and malvertising in 2014 suggests criminals are already turning to them as alternative methods of malware distribution.

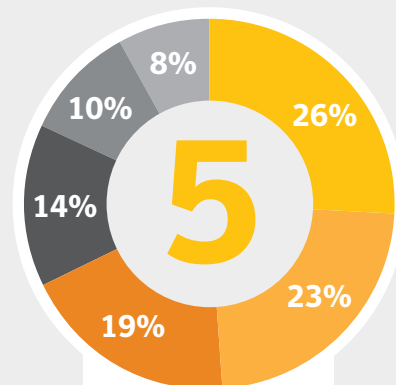
TOP 5 WEB ATTACK TOOLKITS, 2012



- Blackhole
- Sakura
- Phoenix
- Redkit
- Nuclear
- Others

Source: Symantec | SDAP, Wiki

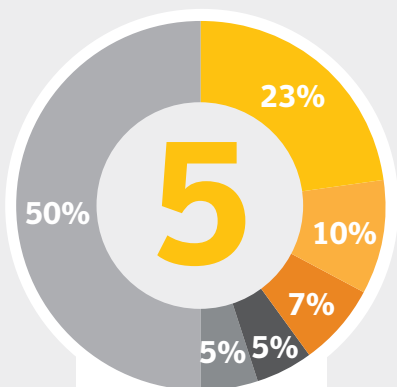
TOP 5 WEB ATTACK TOOLKITS, 2013



- Others
- G01 Pack
- Blackhole
- Sakura
- Styx
- Coolkit

Source: Symantec | SDAP, Wiki

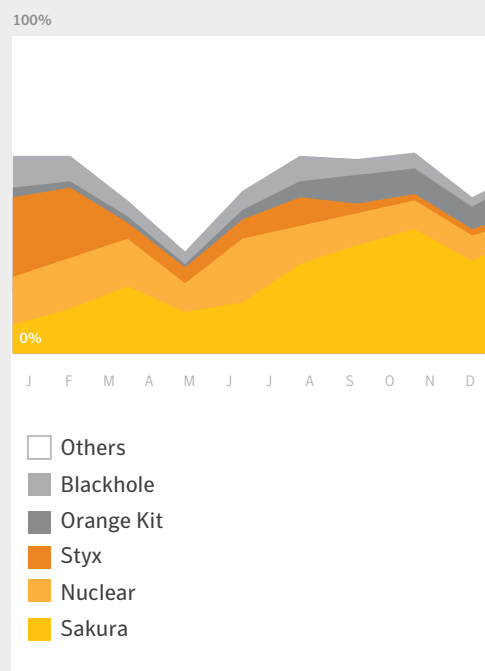
TOP 5 WEB ATTACK TOOLKITS, 2014



- Sakura
- Nuclear
- Styx
- Orange Kit
- Blackhole
- Others

Source: Symantec | SDAP, Wiki

TOP 5 TIMELINE OF WEB ATTACK TOOLKIT USE 2014



Source: Symantec | SDAP, Wiki

MALVERTISING

As we moved into 2014, we saw ransomware and malvertising cross paths, as the number of victims getting redirected to the Browlock website hit new heights.

Browlock itself is one of the less aggressive variants of ransomware. Rather than malicious code that runs on the victim's computer, it's simply a web page that uses JavaScript tricks to prevent the victim from closing the browser tab. The site determines where the victim is and presents a location-specific web page, which claims the victim has broken the law by accessing pornography websites, and demands that they pay a fine to the local police.

The Browlock attackers appear to be purchasing advertising from legitimate networks to drive traffic to their site. The advertisement is directed to an adult web page, which then redirects to the Browlock website. The traffic that the Browlock attackers purchased comes from several sources, but primarily from adult advertising networks¹⁰.

All victims have to do to escape is close their browser, but the investment criminals are making to get traffic suggests people are just paying up. Perhaps this is because the victim has clicked on an advert for a porn site before ending up on the Browlock web page: guilt can be a powerful motivator.

Malvertising at Large

It's not just ransomware that malvertising helps to spread: malicious adverts also redirect to sites that install Trojans. Some malicious adverts are able to infect a victim's device even without the user clicking on the advert, using a drive-by attack.

The appeal for criminals is that malvertising can hit major, legitimate websites, drawing in high volumes of traffic. Ad networks also tend to be highly localized in their targeting, meaning criminals can tailor their scams to specific victims, for example people searching for financial services. Legitimate ad networks sometimes inadvertently do all the work for the criminals.

Criminals also switch tactics to avoid detection. For example, they'll run a legitimate ad for a few weeks, to appear above board, and then convert it to a malicious ad. In response, ad networks need to run regular scans, rather than just when a new ad is uploaded.

For website owners, it's hard to prevent malvertising, as they have no direct control over the ad networks and their customers. However, site managers can reduce risk by choosing networks that restrict ad functionality, so advertisers can't embed malicious code in their promotions. And of course, when selecting an ad network, due diligence goes a long way.



Example of a Browlock web page, demanding a fine for surfing pornography illegally¹¹

¹⁰ <http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware>

¹¹ Ibid

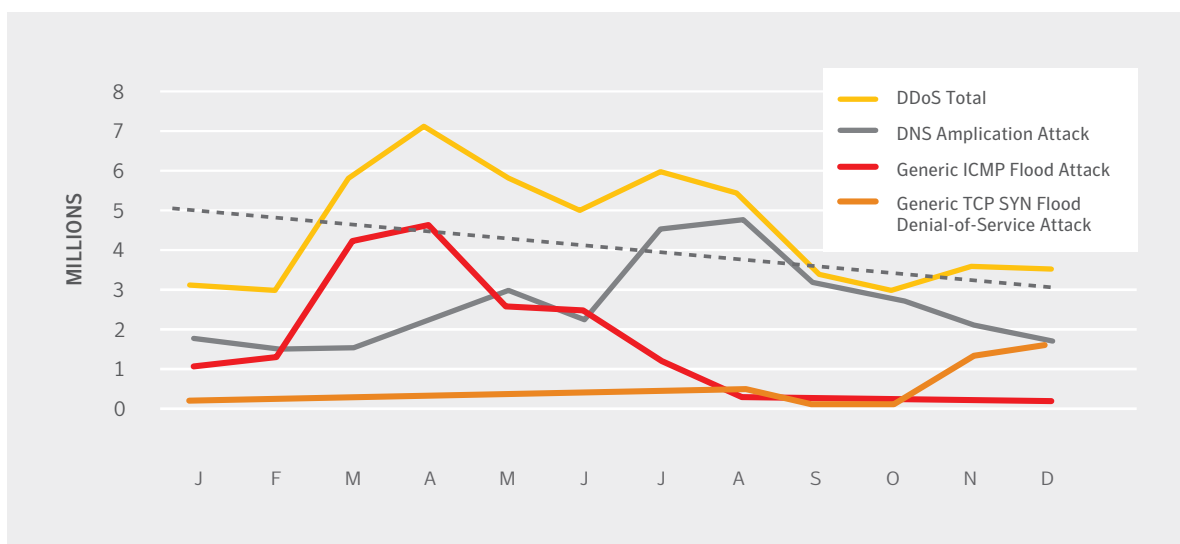
DENIAL-OF-SERVICE (DDOS)

Denial-of-service attacks give attackers another way to target individual organizations. By blocking access to critical systems, such as websites or email, through overloading them with internet traffic, denial-of-service attacks can wreak financial havoc and disrupt normal operations.

Distributed denial-of-service attacks (DDoS) are not new, but they are growing in intensity and frequency¹². For example, Symantec saw a 183 percent increase in DNS amplification attacks between January and August 2014¹³. According to a survey by Neustar, 60 percent of companies were impacted by a DDoS attack in 2013,

and 87 percent were hit more than once¹⁴. Motives include extortion for money, diversion of attention away from other forms of attack, hacktivism, and revenge. Increasingly, would-be deniers of service can rent attacks of a specified duration and intensity for as little as \$10-20 in the black market online.

DDOS ATTACK TRAFFIC SEEN BY SYMANTEC'S GLOBAL INTELLIGENCE NETWORK



Source: Symantec | DeepSight Symantec Global Intelligence Network

¹² <http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong>

¹³ <http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong>

¹⁴ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

THE VULNERABILITY RISES

by Tim Gallo

Over the past few years the idea of vulnerability management has been something that was frequently talked about, but often seen as an annoyance or a process that, while interesting, isn't as important as breach response or adversary tracking. However, 2014 gave vivid examples of the importance of vulnerabilities. Three major vulnerabilities were in the news, and not just security industry news, receiving coverage by major media news outlets as well. They were colloquially known as Poodle, ShellShock, and Heartbleed.

Each of these vulnerabilities was discovered in areas traditionally not covered by most vulnerability management processes at the time. These processes have, as of late, been focused on laptops and servers, thanks to the regularity of publicized vulnerabilities by Adobe and Microsoft, and these companies' speed in releasing patches. While we have seen, and will continue to see, new vulnerabilities in these applications, solid processes have been established here in patch deployment, vulnerability disclosure, and the overall patch management processes.

It is this automation of patch deployment by operating system and application vendors that has forced attackers to shift their tactics somewhat. Attackers have moved to new methods of exploitation, or perhaps more accurately, they have moved back into the vulnerability research game. This shift back to combing through applications more thoroughly on the attacker's part has resulted in vulnerabilities being discovered in areas previously thought to be secure.

Let's take one of these vulnerabilities, ShellShock, as an example of what we will likely see in the coming years. ShellShock was at best a flawed feature, and at worst a design flaw, in the Bourne Again Shell (BASH)¹⁵ that went overlooked for over 25 years before it was discovered to be exploitable, and subsequently disclosed publicly. ShellShock has been a part of the fabric of the Internet



The Heartbleed vulnerability even got its own logo

for most of the Internet's existence. In fact, the targets of ShellShock weren't just routers or Linux web servers, but also email servers and even DDoS bots that utilize the shell—anything Unix-based that makes use of BASH.

¹⁵ For those unfamiliar with UNIX terminology a shell is a command line user interface for interacting with the operating system. In this case BASH is one of the most widely used shells in all of the UNIX and LINUX worlds

We will likely continue to see vulnerabilities like this as the new normal for the coming years, for a few reasons. For starters, it is now apparent that the attackers are not going to rely on reusing the same old methods and the same old exploits, instead investing in researching new vulnerabilities in frequently used, older infrastructure that provides a broad attack surface.

These three high-profile vulnerabilities were also interesting because, not only did they expose flaws in major components of Internet infrastructure, they also highlighted one of the dirty secrets of application development: code reuse. Code reuse is when a developer copies sections of code from existing applications for use in development of new applications. It is this practice, which has been around for as long as coding has existed, that can lead to vulnerabilities being present in systems that may be completely unrelated.

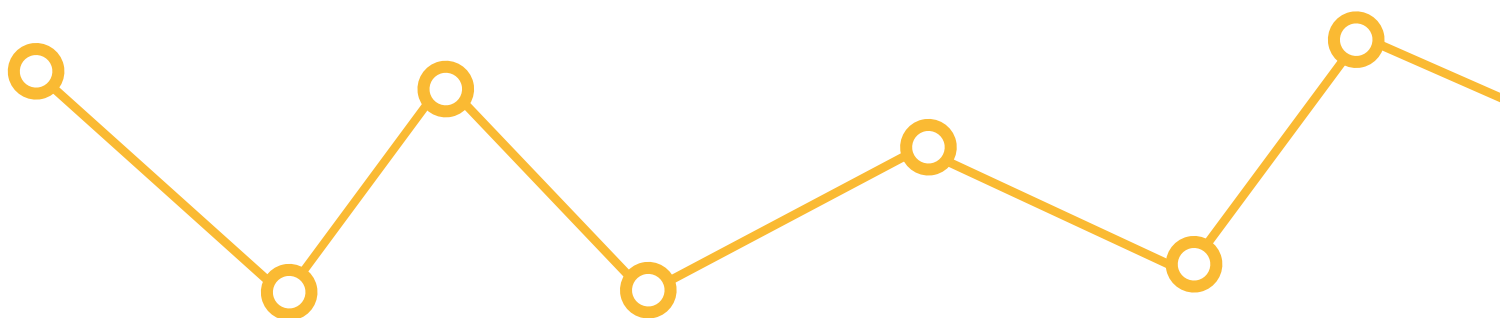
When looking at the situation that led up to the Heartbleed discovery, legitimate uses of the OpenSSL library were a perfect example of code reuse. This code had long been seen as reliable and often went untested, as it was considered “a solved problem.” However, new vulnerabilities in the library were discovered, and developers around the globe had to scramble to determine if their code reuse implementations were vulnerable.

Additionally, we have seen a rise in bug bounty programs and we no longer see governments threatening vulnerability researchers with jail time as in years past¹⁶. Therefore the incentive to research vulnerabilities has increased and the repercussions of irresponsible disclosure, or even outright mercenary behavior, is no longer something researchers fear.

However what we will also hopefully see is that remediation and better security practices become more prevalent. It only takes the average IT professional a few weeks of all-nighters to decide that planning ahead is far more advantageous. Better enforcement of configuration, policy, and patching across entire infrastructures will help. The moving of infrastructure to the cloud also helps an overworked IT professional manage these issues as well.

As we look at the “detect and remediate” cycle of security, the return of vulnerabilities is a key point in understanding the threat landscape. For us to be more effective security professionals, we need to additionally think about how we “protect and respond”, and “inform and assess” as well. That means we need to become better planners, testers, look to intelligence to help keep us informed, and know our environment well enough to understand if that intelligence is actionable.

We need to better understand that the fabric of the Internet is likely still riddled with holes, and it is our responsibility to maintain vigilance in order to be prepared to deal with new vulnerabilities as they are disclosed in a process-oriented and programmatic manner. To not do so would be detrimental to our future.



¹⁶ <http://www.wired.com/2013/03/att-hacker-gets-3-years>

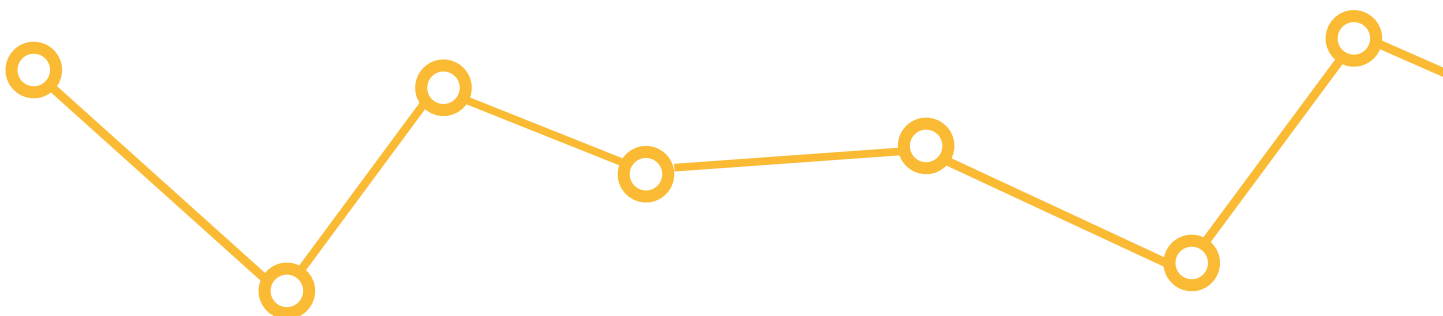
E-CRIME & MALWARE



WSTR

AT A GLANCE

1	Prices holding steady in the underground economy, suggesting continuing high levels of demand for stolen identities, malware and e-crime services.
2	Number of vulnerabilities down relative to 2013, but the general trend is still upwards.
3	The number of new malware variants grew by 317,256,956 in 2014—a 26 percent increase compared with the growth in 2013.
4	Ransomware is getting nastier, as well as increasing in volume. The amount of crypto-ransomware has also grown over 45 times larger than in 2013.
5	The number of bots declined by 18 percent in 2014.



INTRODUCTION

Every day, personal banking details are phished by fake emails and websites. Computers infected with malware are used to send out spam, or contribute to distributed denial-of-service attacks. Perhaps the most unlucky see all their files encrypted and their computer made unusable by ransomware.

Email continues to be an effective delivery vehicle for spam, phishing, and malware, and overall, the proportion of emails that include malware is rising. Cybercriminals rely on an underground online economy to buy and sell services, malware, and fence stolen credit cards and botnets.

Working with security firms including Symantec, law enforcement has continued to disrupt botnets and make arrests. This has produced noticeable, if temporary, improvements on the overall levels of cybercrime.

The Underground Economy

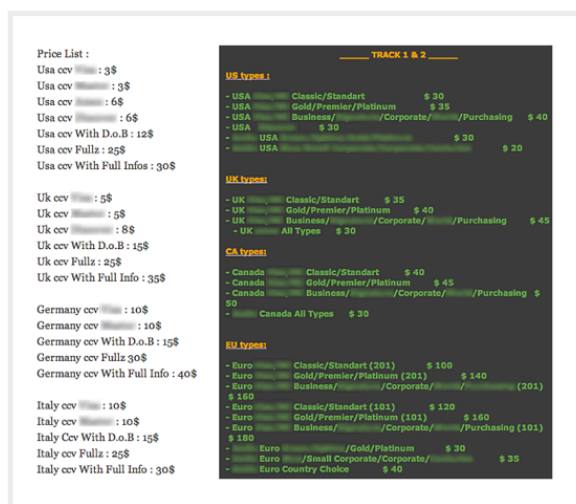
The underground black market is thriving. In the darker corners of the internet, there's a huge trade in stolen data, malware, and attack services¹⁷. Criminals are moving their illegal marketplaces further from public gaze, for example by using the anonymous Tor network, and limiting access to an invitation-only basis¹⁸. Price changes give some indication of supply and demand. Overall, email prices have dropped considerably, credit card information a little, and online bank account details have remained stable.

Cybercriminals can also buy malware, attack kits, and vulnerability information off the shelf. They can even buy 'crimeware-as-a-service' which comes with the entire infrastructure to run online scams.

These markets allow a division of labor. Some people specialize in writing trojans and viruses, others in malware distribution, botnets, or monetizing stolen

credit card details. Some of these markets have existed for at least ten years, but Symantec sees increasing professionalization of all the elements. Any product or service directly linked to monetary profit for the buyer retains a solid market price¹⁹.

A drive-by download web toolkit, which includes updates and 24/7 support, can be rented for between \$100 and \$700 per week. The online banking malware SpyEye (detected as Trojan.Spyeye) is offered from \$150 to \$1,250 on a six-month lease, and distributed denial-of-service (DDoS) attacks can be ordered from \$10 to \$1,000 per day²⁰.



Price List :	
Usa ccv	: 3\$
Usa ccv	: 3\$
Usa ccv	: 6\$
Usa ccv	: 6\$
Usa ccv With D.o.B	: 12\$
Usa ccv Fullz	: 25\$
Usa ccv With Full Info	: 30\$
Uk ccv	: 5\$
Uk ccv	: 5\$
Uk ccv	: 8\$
Uk ccv With D.o.B	: 15\$
Uk ccv Fullz	: 25\$
Uk ccv With Full Info	: 35\$
Germany ccv	: 10\$
Germany ccv	: 10\$
Germany ccv With D.o.B	: 15\$
Germany ccv Fullz	: 30\$
Germany ccv With Full Info	: 40\$
Italy ccv	: 10\$
Italy ccv	: 10\$
Italy ccv With D.o.B	: 15\$
Italy ccv Fullz	: 25\$
Italy ccv With Full Info	: 30\$
TRACK 1 & 2	
US Types :	
- USA Classic/Standard	\$ 30
- USA Gold/Premier/Platinum	\$ 35
- USA Business/Corporate/Purchasing	\$ 40
- USA All Types	\$ 30
UK Types :	
- UK Classic/Standard	\$ 35
- UK Gold/Premier/Platinum	\$ 40
- UK Business/Corporate/Purchasing	\$ 45
- UK All Types	\$ 30
CA Types :	
- Canada Classic/Standard	\$ 40
- Canada Gold/Premier/Platinum	\$ 45
- Canada Business/Corporate/Purchasing	\$ 50
- Canada All Types	\$ 30
EU Types :	
- Euro Classic/Standard (201)	\$ 100
- Euro Gold/Premier/Platinum (201)	\$ 140
- Euro Business/Corporate/Purchasing (201)	\$ 140
- Euro Classic/Standard (101)	\$ 120
- Euro Gold/Premier/Platinum (101)	\$ 160
- Euro Business/Corporate/Purchasing (101)	\$ 160
- Euro Small Corporate/Corporate	\$ 30
- Euro Country Choice	\$ 40

Underground economy prices for credit cards in various countries.

¹⁷ <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

¹⁸ <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

¹⁹ <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

²⁰ <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

VALUE OF INFORMATION SOLD ON BLACK MARKET

<i>1,000 Stolen Email Addresses</i>	\$0.50 to \$10	Spam, Phishing
<i>Credit Card Details</i>	\$0.50 to \$20	Fraudulent Purchases
<i>Scans of Real Passports</i>	\$1 to \$2	Identity Theft
<i>Stolen Gaming Accounts</i>	\$10 to \$15	Attaining Valuable Virtual Items
<i>Custom Malware</i>	\$12 to \$3,500	Payment Diversions, Bitcoin Stealing
<i>1,000 Social Network Followers</i>	\$2 to \$12	Generating Viewer Interest
<i>Stolen Cloud Accounts</i>	\$7 to \$8	Hosting a Command-and-Control (C&C) Server
<i>1 Million Verified Email Spam Mail-outs</i>	\$70 to \$150	Spam, Phishing
<i>Registered and Activated Russian Mobile Phone SIM Card</i>	\$100	Fraud

Source: Symantec

MALWARE

At the end of 2013, Russian authorities arrested 'Paunch', the alleged author of the Blackhole exploit kit which was responsible for a very large number of infections worldwide^{21,22}. It was a small victory in a long war against malware in all its forms.

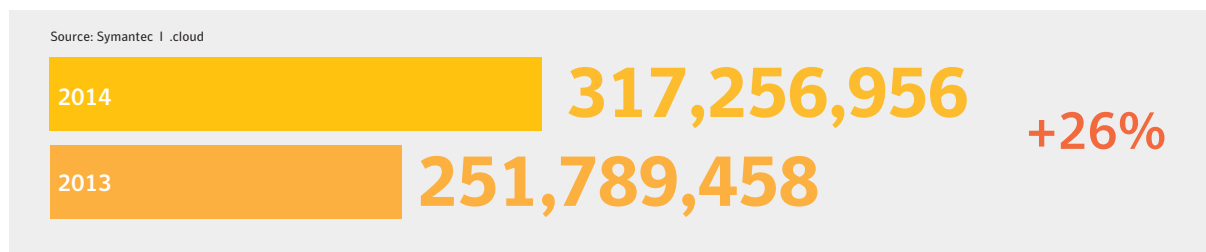
Inevitably, other attack kits have come up to fill the void. Malware designed to steal bank details continues to be prevalent and 2014 also saw malware target new 'markets' as the Snifula banking trojan attacking Japanese financial institutions²³ and an indigenous group of attacks emerged in the Middle East using malware called njRAT²⁴.

In October, only seven percent of malicious spam emails contained URL links. That number jumped to 41 percent in November, and continued to climb in early December thanks to a surge in social engineering-themed messages, including malicious fax and voicemail notification emails.

The links in these emails use hijacked domains, and have a URL path that leads to a PHP landing page. If the user clicks on the links, they are led to a malicious file. In particular, we have seen Downloader.Ponik and Downloader.Upatre being used in these emails. These are well-known Trojans that are used for downloading additional malware onto compromised computers, including information stealers like Trojan.Zbot (also known as Zeus)²⁵.

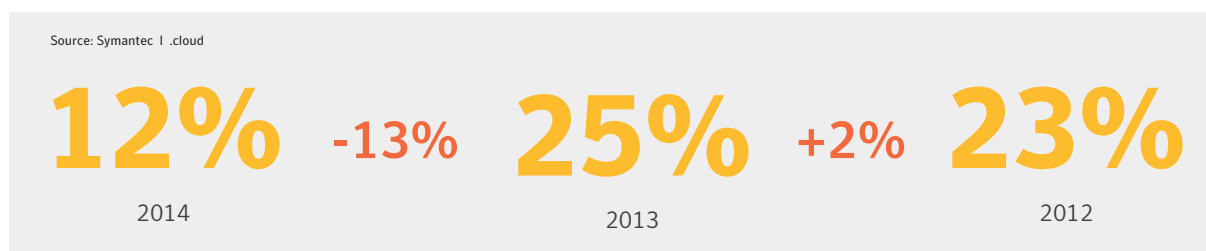
Overall, emails that distribute malware have declined in 2014, after appearing to have peaked in 2013.

NEW MALWARE VARIANTS (ADDED IN EACH YEAR)



With more than 317 million (317M) new pieces of malware created in 2014, or close to 1 million new pieces of unique malware each day; the overall total number of malware is now approaching 2 billion (1.7B).

EMAIL MALWARE AS URL VS ATTACHMENT



²¹ http://en.wikipedia.org/wiki/Blackhole_exploit_kit

²² <http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/>

²³ <http://www.symantec.com/connect/blogs/snifula-banking-trojan-back-target-japanese-regional-financial-institutions>

²⁴ <http://www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene>

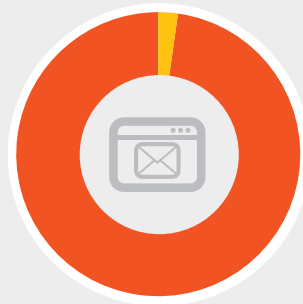
²⁵ <http://www.symantec.com/connect/blogs/malicious-links-spammers-change-malware-delivery-tactics>

EMAIL MALWARE RATE (OVERALL)



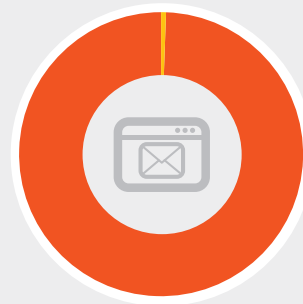
1 IN 244

2014



1 IN 196

2013

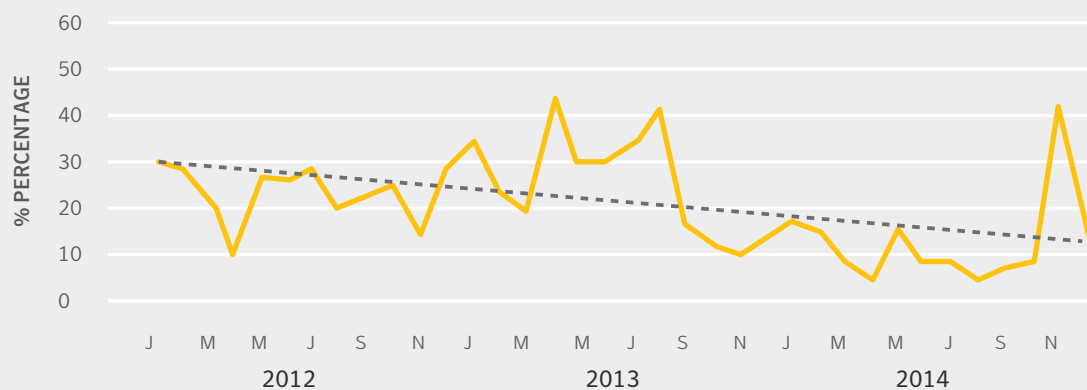


1 IN 291

2012

Source: Symantec | .cloud

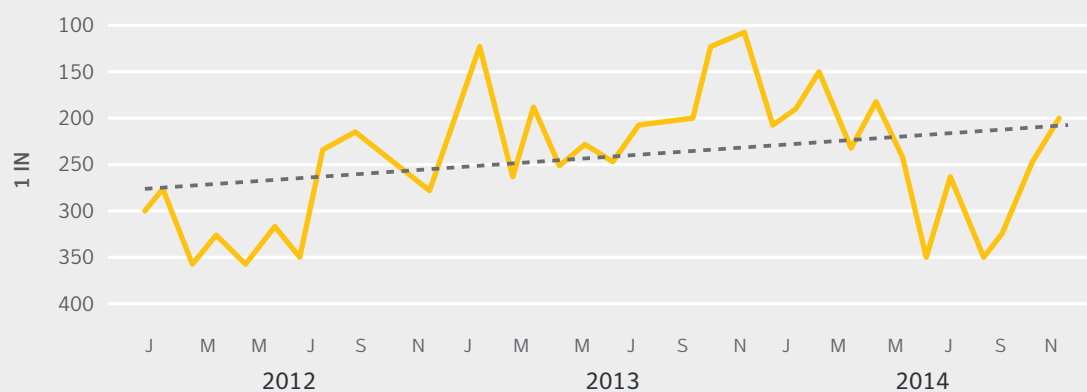
PERCENTAGE OF MAIL MALWARE AS URL VS ATTACHMENT BY MONTH



Source: Symantec | .cloud

12 percent of email-borne malware in 2014 comprised a malicious link, rather than attached to the email, compared with 25 percent in 2013.

PROPORTION OF EMAIL TRAFFIC IN WHICH VIRUS WAS DETECTED, 2012-2014



Source: Symantec | .cloud

RANSOMWARE

Ransomware attacks more than doubled in 2014, from 4.1 million in 2013, up to 8.8 million. More concerning is the growth of file-encrypting ransomware (what Symantec refers to as “crypto-ransomware”), which expanded from 8,274 in 2013 to 373,342 in 2014.

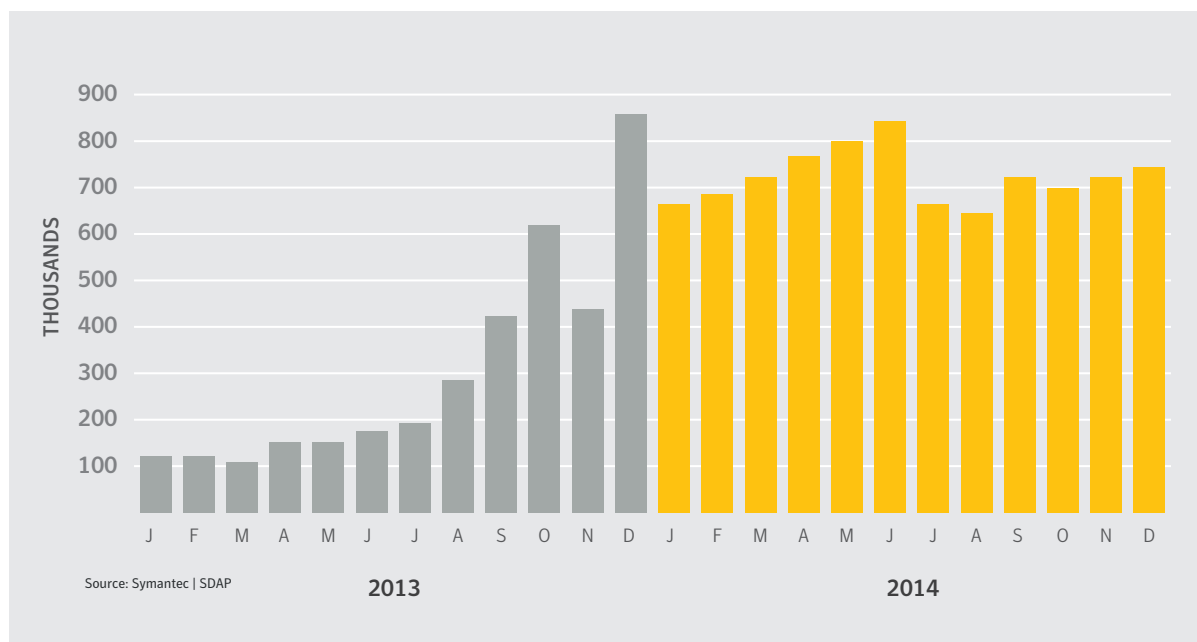
This is 45 times more crypto-ransomware in the threat landscape within a one-year span. In 2013, crypto-ransomware accounted for 0.2 percent (1 in 500) of ransomware, and was fairly uncommon; however, by the end of 2014 it accounted for 4 percent (1 in 25) of all ransomware.

On a human level, ransomware is one of the nastiest forms of attack for victims. Criminals use malware to encrypt the data on victims’ hard drives—family pictures, homework, music, that unfinished novel—and

demand payment to unlock the files. The best, and pretty much only, defense is to keep a separate backup of your files, preferably offline, to restore from.

There are many ransomware variants, and no operating system guarantees immunity²⁶. And while the advice remains the same—do not pay the criminals—many businesses and individuals simply want or need their files back. So they pay, and thus the scam remains profitable.

RANSOMWARE OVER TIME, 2013 – 2014



Source: Symantec | Response

²⁶ <http://www.symantec.com/connect/blogs/windows-8-not-immune-ransomware-0>

CRYPTO-RANSOMWARE

The bad news is that, while ransomware has doubled, between 2013 and 2014 Symantec saw the amount of crypto-ransomware in the threat landscape grow over 45 times larger²⁷.

There are several different crypto-ransomware families such as Cryptolocker²⁸, Cryptodefense²⁹, and Cryptowall³⁰, but their method of exploitation is the same. Rather than locking your desktop behind a ransom wall, crypto-ransomware encrypts your personal files, and holds the private keys to their decryption for ransom at a remote site. This is a much more vicious attack than traditional ransomware.

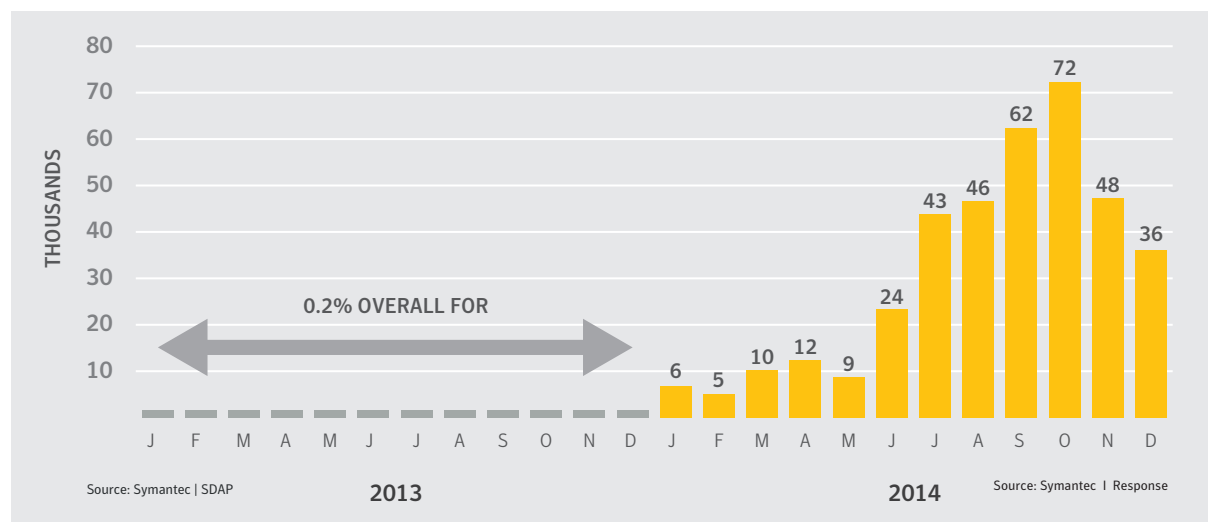
Methods of infection vary, but commonly it's via a malicious email attachment, purporting to be an invoice, energy bill, or image. The delivery often forms part of a service actually provided by different criminals from those executing the crypto-ransomware. This is just one of the darker sides of the underground economy, where criminals offer services such as 'I can infect x computers for a fixed price of y'.

CryptoDefense, brought to light back in March, is a perfect example of just how serious crypto-ransomware is, and how hard the criminals behind it are to track. Such malware is delivered via malicious email attachments, and encrypts a victim's files with public-key cryptography using strong RSA 2048-bit encryption.

In order to pay the ransom, the victim has to visit a web page on the Tor network³¹. The payment itself is then requested in Bitcoins. These are typical moves of a crypto-ransomware criminal, making it incredibly difficult to track and shut down such scams.

And then we get to the crux of the entire scam: the profit. Symantec estimated that the cybercriminals behind CryptoDefense earned over \$34,000 in just one month³². It's no wonder crypto-ransomware is considered to be the most effective cybercrime operation out there at the moment.

CRYPTO-RANSOMWARE, 2013 – 2014



In 2013, crypto-ransomware accounted for approximately 0.2 percent of all ransomware attacks. By the end of 2014, this figure grew to 4 percent.

²⁷ <http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware>

²⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

²⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99

³⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99

³¹ Tor is a combination of software and an open network that protects users against traffic analysis and helps to preserve their anonymity and privacy online. While not inherently criminal, it also helps to protect the anonymity of criminals in this case.

³² <http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month>

BOTS AND BOTNETS

The number of bots declined by 18 percent in 2014 compared to the previous year. In large measure, this is because the FBI, the European Cybercrime Centre (EC3) at Europol, and other international law enforcement agencies, working with Symantec and other tech firms, have been active in disrupting and shutting them down. Most notably, the Gameover Zeus botnet was shut down

in 2014. It was responsible for millions of infections worldwide since its arrival in 2011^{33,34}. This is one in a series of botnet takedowns over the past couple of years^{35,36} that have seen IT firms and law enforcement working together effectively.

MALICIOUS ACTIVITY BY SOURCE: BOTS, 2013–2014

Country/Region	2014 Bots Rank	2014 Bots percent	2013 Bots Rank	2013 Bots percent
China	1	16.5 percent	2	9.1 percent
United States	2	16.1 percent	1	20.0 percent
Taiwan	3	8.5 percent	4	6.0 percent
Italy	4	5.5 percent	3	6.0 percent
Hungary	5	4.9 percent	7	4.2 percent
Brazil	6	4.3 percent	5	5.7 percent
Japan	7	3.4 percent	6	4.3 percent
Germany	8	3.1 percent	8	4.2 percent
Canada	9	3.0 percent	10	3.5 percent
Poland	10	2.8 percent	12	3.0 percent

Source: Symantec | GIN

The U.S. and China, two of the most populated countries with the greatest concentration of internet-connected users, swapped the number one and two places in 2014. This switch can likely be attributed to the takedown of the Gameover Zeus botnet.

³³ <http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network>

³⁴ <http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/>

³⁵ <http://www.computerweekly.com/news/2240185424/Microsoft-partnership-takes-down-1000-cybercrime-botnets>

³⁶ <http://www.computerweekly.com/news/2240215443/RSA-2014-Microsoft-and-partners-defend-botnet-disruption>

NUMBER OF BOTS



Source: Symantec | GIN

The decline in bots in 2014 was in part fuelled by the disruption of the GameOver Zeus botnet, with “Operation Tovar.” This botnet had largely been used for banking fraud and distribution of the CryptoLocker ransomware³⁷.

TOP-TEN SPAM SENDING BOTNETS, 2014

Country/Region	% of Botnet Spam	Estimated Spam Per Day	Top Sources of Spam From Botnet		
			Rank #1	Rank #2	Rank #3
KELIHOS	51.6%	884,044	Spain 10.5%	United States 7.6%	Argentina 7.3%
UNKNOWN/OTHER	25.3%	432,594	United States 13.5%	Brazil 7.8%	Spain 6.4%
GAMUT	7.8%	133,573	Russia 30.1%	Vietnam 10.1%	Ukraine 8.8%
CUTWAIL	3.7%	63,015	Russia 18.0%	India 8.0%	Vietnam 6.2%
DARKMAILER5	1.7%	28,705	Russia 25.0%	Ukraine 10.3%	Kazakhstan 5.0%
DARKMAILER	0.6%	9,596	Russia 17.6%	Ukraine 15.0%	China 8.7%
SNOWSHOE	0.6%	9,432	Canada 99.9%	United States 0.02%	Japan 0.01%
ASPROX	0.2%	3,581	United States 76.0%	Canada 3.4%	UK 3.3%
DARKMAILER3	0.1%	1,349	United States 12.7%	Poland 9.6%	Korea, South 9.1%
GRUM	0.03%	464	Canada 45.7%	Turkey 11.5%	Germany 8.5%

Source: Symantec | .cloud

³⁷ <http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network>

OSX AS A TARGET

Over the last few years Apple has sat up and taken notice of the threats that have been targeting OSX, rolling out a couple of much-needed security features to the operating system. XProtect scans downloaded files for signs of malware, warning users if they download a malicious file known to Apple. GateKeeper limits what apps can be run within an OSX computer using code signing. There are varying degrees of protection with GateKeeper, ranging from limiting installation to the official Mac App Store, developers identified as trustworthy by Apple, or any developer that signs their apps.

However, while these security features have made it more difficult for threats to gain a foothold in OSX, threats have nevertheless succeeded in getting past them. As with any signature-based security solution, apps have managed to compromise computers before signatures could be put in place to block them. Malicious apps have also appeared with legitimate developer signatures, either through stealing legitimate credentials or creating false ones.

The most common threats seen in 2014 had similar behaviors to those found on other operating systems. There were Trojans that arrived via browser exploits. Notorious threats such as Flashback, which infected over 600,000 Macs in 2012, are still fairly prevalent, with variants taking up the number three and ten spots in 2014. Threats that modify settings, such as DNS, browser, or search settings on the OSX computer also rank highly.

Two notable threats highlighted a significant issue in the OSX threat landscape: pirated OSX apps that contain malware.

OSX.Wirelurker is a dual-threat Trojan horse, impacting both Macs running OSX and any iOS devices connected to a compromised computer. This threat gained major attention when it was discovered within 467 OSX applications hosted on a third-party OSX app store in China. These malicious apps were downloaded more than 356,000 times before Apple stepped in and blocked them to prevent them from running.

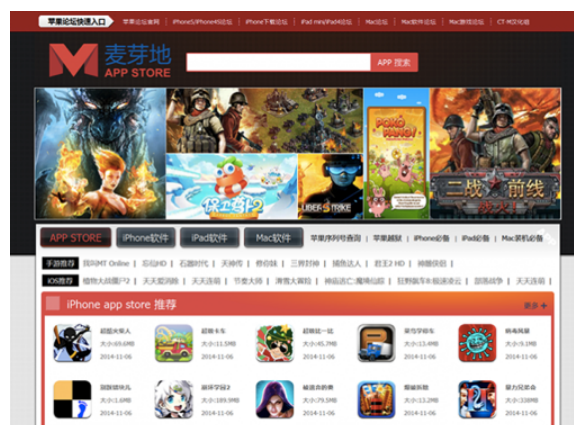
OSX.Luaddit (a.k.a. iWorm) is a threat that added compromised computers to an OSX botnet. This threat was found bundled with pirated copies of commercial products like Adobe Photoshop, Microsoft Office, and Parallels³⁸. These apps were posted to torrent sites, and were downloaded thousands of times.

In terms of other notable OSX threats, **OSX.Stealbit.A** and **OSX.Stealbit.B** are bitcoin stealing threats that monitor browsing traffic, looking for login credentials to major bitcoin websites. The latter was one of the top five OSX threats seen in 2014.

OSX.Slordu is a back door Trojan horse that appears to be used for gathering information about the compromised computer. What is interesting about this threat is that it appears to be an OSX port of a popular Windows back door.

OSX.Ventir is a modular threat, equipped with option components that can open a back door, log keystrokes, or contain spyware capabilities. Depending on what the attacker wished to gain from the compromised computer, different modules would be downloaded and installed in OSX.

OSX.Stealbit.A is a bitcoin-stealing threat that monitors browsing traffic, looking for login credentials to major bitcoin websites.



³⁸ <http://www.thesafemac.com/iworm-method-of-infection-found/>

TOP-TEN MAC OSX MALWARE BLOCKED ON OSX ENDPOINTS, 2013-2014

Rank	Malware Name	Percent of Mac Threats 2014	Malware Name	Percent of Mac Threats 2013
1	OSX.RSPlug.A	21.2%	OSX.RSPlug.A	35.2%
2	OSX.Okaz	12.1%	OSX.Flashback.K	10.1%
3	OSX.Flashback.K	8.6%	OSX.Flashback	9.0%
4	OSX.Keylogger	7.7%	OSX.HellRTS	5.9%
5	OSX.Stealbit.B	6.0%	OSX.Crisis	3.3%
6	OSX.Klog.A	4.4%	OSX.Keylogger	3.0%
7	OSX.Crisis	4.3%	OSX.MacControl	2.9%
8	OSX.Sabpab	3.2%	OSX.FakeCodec	2.3%
9	OSX.Netweird	3.1%	OSX.Iservice.B	2.2%
10	OSX.Flashback	3.0%	OSX.Inqtana.A	2.1%

Source: Symantec | SDAP

MALWARE ON VIRTUALIZED SYSTEMS

Virtualization is no protection against malware. Increasingly, malware can detect whether it is running on a virtual machine and, instead of quitting, it can change its behavior to reduce the risk of detection³⁹. Historically, the proportion of malware that detected whether or not it was running on VMware hovered around 18 percent, but spiked at the beginning of 2014 to 28 percent⁴⁰.

But this type of functionality is not just being used to avoid security researchers. Once installed on a virtual machine, malware could hop to other virtual machines on the same hardware, or infect the hypervisor, massively increasing the risk and the difficulty of removal⁴¹. This behavior has already been seen in the wild: the W32.Crisis malware which tries to infect virtual machine images stored on a host computer⁴².

For IT managers, this kind of attack poses special risks. It is unlikely to be detected by perimeter security like intrusion detection systems or firewalls that use virtual machines for detecting threats in virtual “sandboxes”, and virtual machines may not have the same level of protection as traditional clients or servers because of the (false) assumption that malware doesn’t attack virtual machines. Organizations need to consider technology like network hardware, hypervisors, and software-defined networks in their security plans and patch cycles.

³⁹ <http://www.symantec.com/connect/blogs/does-malware-still-detect-virtual-machines>

⁴⁰ Ibid

⁴¹ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/threats_to_virtual_environments.pdf

⁴² Ibid

DIGITAL EXTORTION: A SHORT HISTORY OF RANSOMWARE

by Peter Coogan

In 2014, crypto-ransomware was rarely out of the news. The latest and deadliest trend in the on-going ransomware saga, crypto-ransomware differs from its standard ransomware siblings, which simply lock the device, in that it encrypts data files on the compromised device and, in most cases, leaves the victim with no way to rescue their data. Both, however, are in the business of extorting a ransom from victims for the removal of the infection.

This type of malware has been around for over a decade, but has grown in prevalence over the last few years. This growth is the result of cyber criminals shifting from the creation of fake antivirus software to the more lucrative ransomware. While we can trace an evolution from fake antivirus, to ransomware, and on to crypto-ransomware, malware authors rarely rest on their laurels. We can clearly see the new areas of the threat landscape that these digital extortionists are heading towards.

Fake AV, or rogue security software, is a misleading application that fraudulently deceives or misleads a user into paying for the removal of malware. While this software has been around for quite some time now, its prevalence peaked around 2009, with a Symantec report at that time observing 43 million rogue security software installation attempts from over 250 distinct programs, at a cost of \$30 to \$100 for anyone who purchased the software⁴³.

Ransomware is malicious software that locks and restricts access to infected computers. The ransomware software then displays an extortion message using a social engineering theme that demands a ransom payment to remove the restriction. In 2012, Symantec reported on the growing menace of ransomware, with fraudsters charging in the range of €50 to €100 in Europe, or up to \$200 USD in America for the removal of restrictions⁴⁴.

Now, after the emergence and perceived success of the now infamous Trojan.Cryptolocker⁴⁵ in 2013, malware

authors have been turning their attention to writing new Crypto-ransomware style threats. This has led to a surge in new Crypto-ransomware families being seen in 2014 that incorporate new innovations, platforms and evasion tactics alongside both old and new tricks in an attempt to extort money from victims.

One of the more prolific new Crypto-ransomware in 2014 was Trojan.Cryptodefense⁴⁶ (a.k.a. Cryptowall). This threat appeared in late February 2014 and was initially marketed as Cryptodefense. It employed techniques such as the use of Tor and Bitcoins for anonymity, strong RSA 2048-bit encryption of data, and the use of pressure tactics to scare victims into payment. With an initial ransom demand of 500 USD/EUR, it soon increased to 1000 USD/EUR if payment was not forthcoming. However, following analysis, it was found that the malware author's poor implementation of the cryptographic functionality had left their hostages with the key to their own escape, in the form of the private encryption key being left on the system. After this information was made public, the issue was fixed by the malware authors, and it was rebranded as Cryptowall. Since this time, Cryptowall has continued to evolve by weaponizing itself further, with an elevation of privilege exploit, anti-analysis checks, and the use of Invisible Internet Project (I2P) for communication anonymization. The known earnings of Cryptowall were at least \$34,000 in its first month⁴⁷, with researchers determining that it made in excess of 1 million dollars over a six-month period⁴⁸.

The Windows PC landscape has been a lucrative area for ransomware authors, and this will likely continue to be the case. However, in 2014, the attackers behind these digital extortion tools began to tackle new platforms. We saw the Reveton gang release Android ransomware known as Android.Lockdroid.G⁴⁹ (a.k.a. Koler). Through their use of a Traffic Distribution System (TDS), this now allowed the Reventon gang to perform a three-pronged ransomware attack. Depending on certain conditions,

⁴³ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_exec_summary_20326021.en-us.pdf

⁴⁴ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

⁴⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

⁴⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99

⁴⁷ <http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month>

⁴⁸ <http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/>

⁴⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2014-050610-2450-99

such as the browser being used to view a website controlled by the gang, traffic would be redirected to a fitting ransomware.

Ransomware had suddenly become platform independent. Android users would be redirected to download Android.Lockdroid.G, Internet Explorer users to the Angler Exploit kit delivering a payload of Trojan.Ransomlock.G⁵⁰, and other browsers used on Windows, Linux or Mac would be redirected to Browlock⁵¹, another form of ransomware that attempts to lock the computer and extort money from the user by simply using tools in their web browser.

In June 2014, the first file-encrypting ransomware for Android, known as Android.Simplocker⁵², was discovered. With a demand initially in Russian, by July 2014 an updated English version (Android.Simplocker.B⁵³) was being seen that employed an FBI social engineering theme. October 2014 saw the emergence of Android.Lockdroid.E⁵⁴ (a.k.a. Porndroid) that once again used a fake FBI social engineering theme. This threat, however, also used the device's camera to take a picture which was then displayed alongside the ransom demand. Android.Lockdroid further spawned new variants that included worm capabilities, allowing self-replication via SMS messages sent to contacts in the address book on an infected device, along with a social engineering catch.

Ransomware authors even began looking past mobile devices to see where else they could possibly extort money, and realized that network-attached storage (NAS) devices, where large quantities of files are stored, could also be targeted. Trojan.Synolocker⁵⁵ (a.k.a. Synolocker), targeted Synology NAS devices by using a previously unknown vulnerability in Synology's DiskStation manager software to gain access to the devices, and then encrypted all the files, holding them for ransom. These devices have since been patched against further attacks, but this case highlights that ransomware attackers are continuing looking for new areas to attack.

So why are we seeing such rapid changes in ransomware? Ransomware is a lucrative business for cyber criminals, with ransom demands ranging anywhere from \$100 to \$500 USD. During 2014, we also saw Bitcoins become the ransom payment method of choice by most new ransomware. Given Bitcoins' strong anonymity, it allows cyber criminals to easily hide and launder their ill-gotten gains.

While we have observed a surge in new ransomware families, Symantec has also seen an increase in the overall growth path. Compared to 2013, there has been a 113 percent rise in the occurrence of ransomware seen. However, given the lucrative nature of these threats, and the number of new ransomware families appearing, it is unlikely that ransomware-type scams will drop off the threat landscape anytime soon, with future growth being more likely.

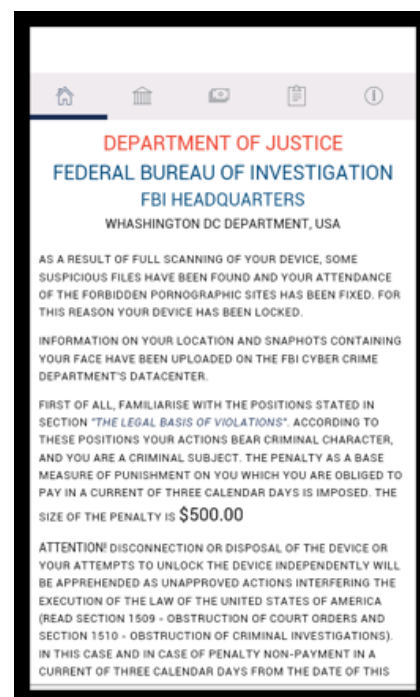
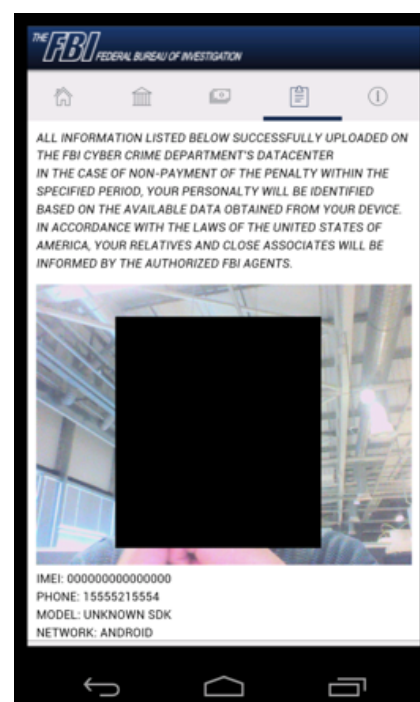


Figure. "Porndroid" Android ransomware threat.



⁵⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2011-051715-1513-99

⁵¹ <http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware>

⁵² http://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99

⁵³ http://www.symantec.com/security_response/writeup.jsp?docid=2014-072317-1950-99

⁵⁴ http://www.symantec.com/security_response/writeup.jsp?docid=2014-103005-2209-99

⁵⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2014-080708-1950-99

RECOMMENDATIONS AND BEST PRACTICE



WSTR

The logo for WSTR is centered within a yellow rectangular border. The letters 'W', 'S', and 'T' are white with a thin yellow outline, while the letter 'R' is solid yellow. A yellow line graph with circular markers at its endpoints extends horizontally from the left and right sides of the yellow box, passing behind it.



Despite this year's vulnerabilities, when it comes to protecting your website visitors and the information they share with you, SSL and TLS remain the gold standard. In fact, due to the publicity that Heartbleed received, more companies than ever have started hiring SSL developers to work on fixes and code. This has made for more eyes on the SSL libraries and common good practices in implementation.



Get Stronger SSL

2014 saw SSL certificate algorithms become stronger than ever. Symantec, along with several other CAs, have moved to SHA-2 as default, and is winding down support for 1024-bit rootsⁱ.

Microsoft and Google announced SHA-1 deprecation plans that may affect websites with SHA-1 certificates expiring as early as January 1, 2016ⁱⁱ. In other words, if you haven't migrated to SHA-2, visitors using Chrome to access your site will likely see a security warning, and as of January 1, 2017, your certificates just won't work for visitors using IE.

Symantec is also advancing the use of the ECC algorithm—a much stronger alternative to RSA. All major browsers, even mobile, support ECC certificates on all the latest platforms, and there are three main benefits to using it:

1. Improved security. Compared to an industry-standard 2048-bit RSA key, ECC-256-bit keys are 10,000 times harder to crackⁱⁱⁱ. In other words, it would take a lot more computing power and a lot longer for a brute force attack to crack this algorithm.

2. Better performance. Website owners used to worry that implementing SSL certificates would slow their site down. This led to many sites having only partial-on SSL, which creates serious vulnerabilities. ECC requires much less processing power on the website than RSA, and can handle more users and more connections simultaneously. This makes the implementation of Always-on SSL not only sensible, but viable too.

3. Perfect Forward Secrecy (PFS). Although PFS is an option with RSA-based and ECC-based certificates, performance is much better with ECC-based certificates. Why does that matter? Well, without PFS, if a hacker got hold of your private keys, they could retrospectively decrypt any and all data they had captured. Considering the Heartbleed vulnerability made this a very real possibility for so many websites, this is a problem. With PFS, however, if a hacker cracks or gets hold of your SSL certificate private keys, they can only decrypt information protected with those keys from that point on. They can't decrypt any historical data.



Use SSL Right

As we've seen from 2014, SSL is only as good as its implementation and maintenance. So be sure to:

- **Implement Always-on SSL.** Use SSL certificates to protect every page of your website, so that every interaction a visitor has with your site is authenticated and encrypted.
- **Keep servers up to date.** This applies beyond server SSL libraries: any patch or update should be installed as soon as possible. They're released for a reason: to reduce or eliminate a vulnerability.
- **Display recognized trust marks** (such as the Norton Secured Seal) in highly visible locations on your website to show customers your commitment to their security.
- **Scan regularly.** Keep an eye on your web servers and watch for vulnerabilities or malware.
- **Keep server configuration up to date.** Make sure that old, unsecure versions of the SSL protocol (SSL2 and SSL3) are disabled, and newer versions of the TLS protocol (TLS1.1 and TLS1.2) are enabled and prioritized. Use tools like Symantec's SSL Toolbox to verify proper server configuration^{iv}.

ⁱ <http://www.symantec.com/page.jsp?id=1024-bit-certificate-support>

ⁱⁱ <http://www.symantec.com/en/uk/page.jsp?id=sha2-transition>

ⁱⁱⁱ <http://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa>

^{iv} <https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp>



Educate Employees

Basic common sense and the introduction of some good security habits can go a long way to keeping sites and servers safe this year:

- Ensure employees don't open attachments from senders they don't know
- Educate them on safe social media conduct: offers that look too good, are; 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 them to use common sense—having anti-virus software doesn't mean it's ok to go on malicious or questionable websites



Get Safe or Get Shamed

Attackers have become more aggressive, more sophisticated, and more ruthless than ever in their attempts to exploit the Internet for ill gains. There is, however, plenty individuals and organizations can do to limit their impact.

SSL and website security is now in the public consciousness, and if you're not doing your part, you could find yourself being publicly shamed on HTTP Shaming, a site set up by software engineer, Tony Webster^v.

When it comes to businesses and their websites, good security processes and implementations are all that stand in the way of total ruin: financial and reputational. So get secure in 2015 with Symantec.

^v <http://arstechnica.com/security/2014/08/new-website-aims-to-shame-apps-with-lax-security/>

COMING NEXT

PART 2: TARGETED ATTACKS AND DATA BREACHES

The logo for WSTR is displayed within a dark gray rectangular box with a white border. The letters 'W', 'S', and 'T' are white, while the letter 'R' is yellow. The box is centered on a yellow background that features a white line with circular nodes passing behind it.

WSTR

Get up-to-speed on the latest
devious cyber espionage, plus new
techniques employed in targeted
attacks, spear-phishing,
wateringhole attacks, and more.

ABOUT SYMANTEC

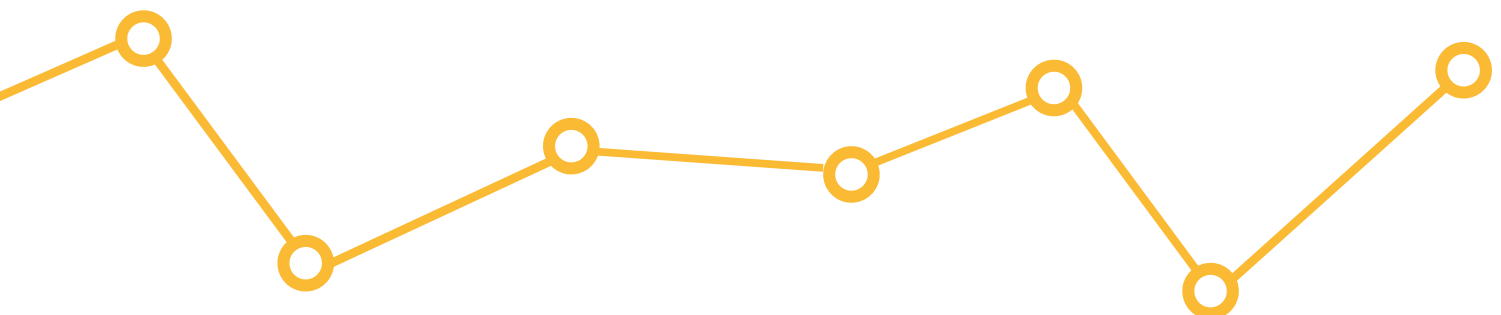
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of \$6.9 billion.

To learn more, go to **www.symantec.com**

or connect with Symantec at: **go.symantec.com/socialmedia**.

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/
- Norton Cybercrime Index: <http://us.norton.com/cybercrimeindex/>



For specific country offices and contact numbers, please visit our website.

For product information in the US,

Call: 1-866-893-6565

The logo features the letters 'WSTR' in a stylized, outlined font. The 'W' and 'S' are white, while the 'T' and 'R' are yellow. The letters are enclosed within a yellow rectangular border. A yellow line graphic, consisting of three connected segments with circular nodes at the joints, extends from the left and right sides of the rectangle.

WSTR

Symantec World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

1-866-893-6565

www.symantec.com/ssl

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Circle Logo, and the Norton Secured Logo are trademarks, or registered trademarks, of Symantec Corporation, or its affiliates, in the U.S. and other countries. Other names may be trademarks of their respective owners.