## Contents

**The Symantec™ Global Intelligence Network**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
</tr>
</tbody>
</table>

### WSTR introduction

- Websites are still vulnerable to attacks leading to malware and data breaches
- Comprehensive website security
- Notable events in 2015
- Key takeaways
- Moving to stronger authentication
- Reasons for hope

### 2015 in numbers

- The state of play
- Slipping through the cracks
- The insider threat
- Money, money, money
- The underground economy and law enforcement
  - Business in the cyber shadows
  - Booming business
  - They can run, but they can’t hide
  - Reducing the risk

### It’s not just about the device or the network – Targeting the individual behind the computer

- Trust no one
- Secrets and lies
- Mistaken identity
- Put your money where your mouse is
- Chipping away at public confidence
  - Stand and deliver
  - But why are criminals favoring ransomware, especially crypto-ransomware?
  - The Dyre consequences, and law enforcement
  - Language and location is no barrier
- Privacy laws
- Averting cybergeddon

### It’s not just about the device or the network – Targeting the organization behind the network

- Persistent attacks
- Diversity in zero days
- Active attack groups in 2015
- Global terror, local attacks
- Insider trading and the butterfly effect
- Cybersecurity, cybersabotage and coping with Black Swan events
- Obscurity is no defense

### Vectors of attack

- Web attacks, toolkits and exploiting vulnerabilities online
- Linux in the firing line
- Problematic plugins
  - The end is nigh for Flash
  - Exploiting plugins for web servers
- Infection by injection
- Web attack exploit toolkits
- Tech support scams go Nuclear, spreading ransomware
- Distributed-Denial-Of-Service
  - DDoS at large

- Simple but effective
- Web connected applications increasingly threatened
- What’s in a botnet?
- Malvertising

### On the client side

- Smartphones and mobile devices
  - One phone per person
  - Cross-over threats
  - Android attacks become more stealthy
  - Android users under fire with phishing and ransomware
  - Apple iOS users now more at risk than ever
- Protecting mobile devices
- Looking ahead
- Email and communications threats
  - Email abuse
  - Spam
  - Phishing
  - Email malware
  - Email encryption
  - Bypassing encryption:
    - communications attacks
  - Email security advice
- Protecting mobile devices
- Looking ahead

### The Industry’s reply

- The evolution of encryption
- Strength in numbers
- Checks and balances
- Accelerating to Always-On SSL
- Reinforced reassurance

### Looking ahead

- On the rise
  - More phishing
  - HTTPS everywhere, for everyone
  - Hybrid threats: mobile attacks
  - The growing need for the right security skills
- Hot topics
  - Spotlights on authentication
  - The Internet of Insecure Things
  - Hacktivism, terrorism, government responsibility and privacy rights
- TLS 1.3 – by Ivan Ristic

### Recommendations and best practice

- Get in line with industry standards
- Use SSL/TLS correctly
- Adopt complete website security
- Educate employees
- Protect mobile devices
- It’s a team effort
The Symantec™ Global Intelligence Network

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 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
- Symantec Website Security
- and other 3rd party data sources.

Symantec also maintains one of the world’s most comprehensive vulnerability databases, made of over 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 sources including:

- The Symantec Probe Network, a system of more than 5 million decoy accounts
- Symantec.cloud
- Symantec Website Security
- 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 9 billion email messages are processed each month and more than 1.8 billion web requests filtered each day across 13 data centres. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 50 million consumers.

Symantec Website Security secures more than one million web servers worldwide with 100 percent availability since 2004. The validation infrastructure 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. 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 Website Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.

www.symantec.com/page.jsp?id=seal-transition
WSTR introduction

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 your server and visitors to your website. Organizations need to start thinking about their websites as part of an entire ecosystem that needs constant care and attention if they want to retain people’s trust and confidence.

There’s a lot at stake as ecommerce becomes increasingly common in our daily lives. From ordering groceries to booking holidays, we are doing more and more online. In fact, Ecommerce Europe reports that global business-to-consumer ecommerce turnover grew by 24 percent to reach $1.943 billion in 2014 and business-to-business ecommerce is expected to be worth $6.7 trillion by 2020. Website security has never been more important or relevant.

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.

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 your company network, they are a way into your data and they are a way to reach your 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 this infrastructure could be prevented with regular maintenance, 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.

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.

Comprehensive website security

Criminals continued to find vulnerabilities in the underlying infrastructure of website security in 2015, including FREAK, which allowed attackers who intercepted the setting up of a secure connection to force the use of easier-to-crack protocols.

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.

Distributed-Denial-of-Service (DDoS) attacks have also continued to prove disruptive to businesses in 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.
The message is clear: 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.

Notable events in 2015

- The price of stolen data, such as email addresses or credit cards, dropped in 2015 suggesting an increasing supply.
- China was the origin of 46 percent of malicious bot activity in 2015 (up from 16 percent in 2014), compared with the US, which fell from 16 percent to 8 percent in the same period.
- Cyberinsurance claims became more common this year, pushing-up the premiums, and the overall cost of data breaches. The annual NetDiligence Cyber Claims study saw claims ranging up to $15 million, while typical claims ranged from $30,000 to $263,000.
- The median number of identities exposed in each breach decreased by around a third to 4,885 identities per breach. However, the number of breaches reported that did not include a figure for identities exposed increased by 85 percent.
- One notable victim of a security breach was Hacking Team, an Italian firm that provides covert surveillance and espionage software to various government customers. A number of the weaponized exploits the firm specialized in creating were leaked online, finding their way into web attack exploit toolkits.
- Malvertising continues to plague websites along with attacks on Linux servers that host them. The number of infected websites grew again this year.
- Attacks against the healthcare and insurance sectors rose, including the loss of nearly 80 million patient records in a major data breach at Anthem. Healthcare was the top sub-sector for data breaches in 2015.
- We’ve seen sophisticated attacks originating from well-resourced and well-funded organizations before and we’ve long suspected them to be government-backed but 2015 saw the discovery of the Butterfly group, which used similarly advanced techniques for commercial gain.
- The security of the Internet of Things came under the spotlight with cars, smart home devices and medical devices, not to mention industrial control systems, coming under attack.
- Phones came under sustained attack as mobile vulnerabilities increased dramatically and the number of malicious Android apps grew. Attacks became stealthier and more sophisticated, and for the first time Apple iOS devices were also being compromised without the need to be jailbroken, as in previous years.
- Ransomware numbers declined in 2015. Although attacks focused more on crypto-ransomware. Linux servers hosting websites were targeted too. Smartphones, and proof-of-concept attacks against smart TVs and smartwatches were also uncovered.
- Inevitably, in light of the notorious Ashley Madison breach, revealed details of would-be cheaters on the dating site, coupled with the growth of online sextortion in Asia, the value of personal data took on another dimension as victims were further exploited for profit.

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.

Key takeaways

Zero day vulnerabilities have reached unprecedented levels this year. While still going after common targets, like web-based plugins and operating systems, other targets are on the rise, such as open source software. Most concerning of all is that severe zero day vulnerabilities targeting ICSs were discovered in 2015.

Reconnaissance attacks are continuing to play a big part in targeted attacks, allowing attackers quietly to gather information about the systems they wish to target before launching full-scale attacks. Such attacks played no small part in high-profile cybersabotage attacks such as those utilizing Trojan.Laziok and the BlackEnergy Trojan, targeting the energy sector in the Middle East and Ukrainian power plants, respectively.
Data breaches are up across nearly all metrics in 2015, with record-breaking numbers of attacks, identities stolen, and mega breaches. When looking particularly at high-risk breach types, industries such as hotels and other lodging places and insurance carriers stand out where they normally would not. These industries are specifically being targeted for private information, such as credit card details or healthcare information, and are likely being leveraged by attackers more frequently than in other industries.

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 to make issuing SSL/TLS certificates more transparent.

Crucially, nearly 40% 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% of the world’s internet traffic over the coming year.

Unfortunately, as Robert Hoblit, VP of Revenue and Emerging Products at Symantec explains, “in a world where everything is encrypted, consumers have a false sense of security that any time they see HTTPS, they are on a site hosted by an authentic, validated organization.”

In reality, the vast majority of fraud has historically occurred on Domain Validated (DV) sites, which offer no validation of the organization behind the site. “What I think you’ll see,” suggests Hoblit, “is a move by organizations, driven by PCI compliance, to ratchet up the requirements for authentication.”

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 organizations, 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, SHA-1 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. This is the idea, 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 SHA-1 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.

https://googleonlinesecurity.blogspot.co.uk/2014/09/gradually-sunsetting-sha-1.html
Reasons for hope

Despite all the gloom and doom, well-run companies and careful users can protect themselves against all but the most determined threats. There are other reasons for hope too. For example, nearly 40% of downstream internet traffic in the US is now encrypted and that will rise over the coming year. The latest browser and web standards emphasize encryption and security.

Likewise, developers of the Internet of Things, phones and software are upping their game when it comes to security (albeit from a low level in some cases). And, of course, companies like Symantec are deploying their full force to fight back against internet criminals, spies, and mischief-makers.

"IN A WORLD WHERE EVERYTHING IS ENCRYPTED, CONSUMERS HAVE A FALSE SENSE OF SECURITY THAT ANY TIME THEY SEE HTTPS, THEY ARE ON A SITE HOSTED BY AN AUTHENTIC, VALIDATED ORGANIZATION."

Robert Hoblit, VP of Revenue and Emerging Products at Symantec
2015 in numbers

Whether insider attack or criminal scam, focused on websites or point-of-sale devices, data breaches continued apace in 2015, costing victims more than ever.

The state of play
The average total cost of a data breach has risen by 23 percent in the last two years to $3.79 million according to the 2015 Cost of Data Breach Study. Since our figures show the total number of breaches has dropped slightly, and the median number of identities exposed per breach has dropped by around a third to 4,885, this suggests the data stolen in each breach is more valuable or sensitive and the impact to the business greater than in previous years.

<table>
<thead>
<tr>
<th>TOTAL BREACHES</th>
<th>Source: Symantec</th>
<th>CCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Change</td>
<td>2014</td>
</tr>
<tr>
<td>253</td>
<td>+23%</td>
<td>312</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TOTAL IDENTITIES EXPOSED</th>
<th>Source: Symantec</th>
<th>CCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Change</td>
<td>2014</td>
</tr>
<tr>
<td>552 Million</td>
<td>-37%</td>
<td>348 Million</td>
</tr>
</tbody>
</table>

As a result, cyber insurance claims are becoming more common and this year’s NetDiligence Cyber Claims study saw claims ranging up to $15 million, while typical claims ranged from $30,000 to $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.

http://www.symantec.com/cyber-insurance/
http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609A20151012
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.

“We have seen much greater focus in the last year on the code libraries in play related to SSL/TLS implementations,” says Michael Klieman, General Manager and Senior Director, Product Management at Symantec. “As a result we have seen a reasonably 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.

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, eavesdropping on secure communication, or carry out denial-of-service attacks.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSL/TLS POODLE Vulnerability</td>
</tr>
<tr>
<td>2</td>
<td>Missing X-Content-Type-Options Header</td>
</tr>
<tr>
<td>3</td>
<td>Missing X-Frame-Options Header</td>
</tr>
<tr>
<td>4</td>
<td>SSL Certificate Signed Using Weak Hashing Algorithm</td>
</tr>
<tr>
<td>5</td>
<td>Cross Site Scripting Vulnerability</td>
</tr>
<tr>
<td>6</td>
<td>Missing Strict-Transport-Security Header</td>
</tr>
<tr>
<td>7</td>
<td>SSL v2 Support Detected</td>
</tr>
<tr>
<td>8</td>
<td>Missing Secure Attribute in an Encrypted Session (SSL) Cookie</td>
</tr>
<tr>
<td>9</td>
<td>SSL Weak Cipher Suites Supported</td>
</tr>
<tr>
<td>10</td>
<td>SSL and TLS Protocols Renegotiation Vulnerability</td>
</tr>
</tbody>
</table>

The insider threat

While insider theft only accounted for around ten 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.

Insider threats have always been a hot topic in cyber security but in 2015 government bodies not only started to take notice, but took action too.

• 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 Defense Enterprise sponsored several projects in 2015 aimed at monitoring employee digital behavior to predict and identify insider threats in real time as well as learning simulators to help people spot risk.

Money, money, money

The biggest drive for data breaches continues to be money: the more details someone has about an individual, the easier it is to commit identity fraud and criminals are targeting insurance, government, and healthcare organizations to get more complete profiles of individuals.

The types of information that thieves are pursuing 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 30 to 40 percent range, as in 2014, though their order of appearance has changed slightly. Rounding out the top 10, email addresses, phone numbers, insurance information, and user names/passwords again appear in the 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 card owners) and stolen card data has a limited shelf life. However, there is an evergreen market for credit card information.

Top Causes of Data Breach by Incidents, 2013-2015

Source: Symantec | CCI

<table>
<thead>
<tr>
<th>Year</th>
<th>Attackers</th>
<th>Accidentally Made Public</th>
<th>Theft or Loss of Computer or Drive</th>
<th>Insider Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>34%</td>
<td>29%</td>
<td>27%</td>
<td>6%</td>
</tr>
<tr>
<td>2014</td>
<td>49%</td>
<td>22%</td>
<td>21%</td>
<td>8%</td>
</tr>
<tr>
<td>2015</td>
<td>46%</td>
<td>22%</td>
<td>21%</td>
<td>10%</td>
</tr>
</tbody>
</table>

http://uk.businessinsider.com/ashley-madison-ceo-says-hack-was-an-inside-job-2015-7
## TOP 10 SECTORS BREACHED BY NUMBER OF IDENTITIES EXPOSED, 2-DIGIT

Source: Symantec | CCI

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

## TOP 10 TYPES OF INFORMATION EXPOSED

Source: Symantec | CCI

<table>
<thead>
<tr>
<th>Rank</th>
<th>2014 Type</th>
<th>2014 %</th>
<th>2015 Type</th>
<th>2015 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Real Names</td>
<td>68.9%</td>
<td>Real Names</td>
<td>78.3%</td>
</tr>
<tr>
<td>2</td>
<td>Gov. ID Numbers (e.g., SSN)</td>
<td>44.9%</td>
<td>Home Addresses</td>
<td>43.7%</td>
</tr>
<tr>
<td>3</td>
<td>Home Addresses</td>
<td>42.9%</td>
<td>Birth Dates</td>
<td>41.2%</td>
</tr>
<tr>
<td>4</td>
<td>Financial Information</td>
<td>35.5%</td>
<td>Gov. ID numbers (e.g., SSN)</td>
<td>38.4%</td>
</tr>
<tr>
<td>5</td>
<td>Birth Dates</td>
<td>34.9%</td>
<td>Medical Records</td>
<td>36.2%</td>
</tr>
<tr>
<td>6</td>
<td>Medical Records</td>
<td>33.7%</td>
<td>Financial Information</td>
<td>33.3%</td>
</tr>
<tr>
<td>7</td>
<td>Phone Numbers</td>
<td>21.2%</td>
<td>Email Addresses</td>
<td>20.8%</td>
</tr>
<tr>
<td>8</td>
<td>Email Addresses</td>
<td>19.6%</td>
<td>Phone Numbers</td>
<td>18.6%</td>
</tr>
<tr>
<td>9</td>
<td>User Names &amp; Passwords</td>
<td>12.8%</td>
<td>Insurance</td>
<td>13.2%</td>
</tr>
<tr>
<td>10</td>
<td>Insurance</td>
<td>11.2%</td>
<td>User Names &amp; Passwords</td>
<td>11.0%</td>
</tr>
</tbody>
</table>
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 reason in each case differs when looking at the sub-sectors contained within these high-level classifications.

The largest number of recorded 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.)

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 the 1990s and the 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 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 $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, however, cards are much more difficult to clone. 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.

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 was 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 use 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.

http://www.usatoday.com/story/money/personalfinance/2015/09/30/chip-credit-card-deadline/73043464/
Out of the ordinary

The 2015 Hacking Team breach stood out because the criminals weren’t after money or identities: they were after cyber weapons. Of course it also stood out because essentially, the hackers got hacked.

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.

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 specialisms. Just as legitimate businesses have partners, associates, resellers, vendors, etc., so do those enterprises operating in the shadows.

Booming business
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 24/7 support, can be rented for between $100 and $700 per week, while Distributed Denial-Of-Service (DDoS) attacks can be ordered from $10 to $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 changed very little since 2014.

They can run, but they can’t hide
“Law enforcement has got more effective at tackling these groups in the last year,” says Dick O’Brien, Senior Information Developer at Symantec. “It requires a coordinated, international effort because rarely is an attack group confined to one country, but the successes strike a blow against the attackers and raise the risk and potential cost of running illegal operations.”


<table>
<thead>
<tr>
<th>Rank</th>
<th>2014 Country/Region</th>
<th>2014 Bots %</th>
<th>Rank</th>
<th>2015 Country/Region</th>
<th>2015 Bots %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
<td>16.5%</td>
<td>1</td>
<td>China</td>
<td>46.1%</td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>16.1%</td>
<td>2</td>
<td>United States</td>
<td>8.0%</td>
</tr>
<tr>
<td>3</td>
<td>Taiwan</td>
<td>8.5%</td>
<td>3</td>
<td>Taiwan</td>
<td>5.8%</td>
</tr>
<tr>
<td>4</td>
<td>Italy</td>
<td>5.5%</td>
<td>4</td>
<td>Turkey</td>
<td>4.5%</td>
</tr>
<tr>
<td>5</td>
<td>Hungary</td>
<td>4.9%</td>
<td>5</td>
<td>Italy</td>
<td>2.4%</td>
</tr>
<tr>
<td>6</td>
<td>Brazil</td>
<td>4.3%</td>
<td>6</td>
<td>Hungary</td>
<td>2.2%</td>
</tr>
<tr>
<td>7</td>
<td>Japan</td>
<td>3.4%</td>
<td>7</td>
<td>Germany</td>
<td>2.0%</td>
</tr>
<tr>
<td>8</td>
<td>Germany</td>
<td>3.1%</td>
<td>8</td>
<td>Brazil</td>
<td>2.0%</td>
</tr>
<tr>
<td>9</td>
<td>Canada</td>
<td>3.0%</td>
<td>9</td>
<td>France</td>
<td>1.7%</td>
</tr>
<tr>
<td>10</td>
<td>Poland</td>
<td>2.8%</td>
<td>10</td>
<td>Spain</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

They can run, but they can’t hide
“Law enforcement has got more effective at tackling these groups in the last year,” says Dick O’Brien, Senior Information Developer at Symantec. “It requires a coordinated, international effort because rarely is an attack group confined to one country, but the successes strike a blow against the attackers and raise the risk and potential cost of running illegal operations.”

Reducing the risk

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.
• Employ encryption where appropriate to secure confidential data.
• Implement 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 tools 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.

Security should be an essential part of operations and employee behavior, rather than an add-on or something to appease auditor. 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 IT manager and lays in every employee’s hands.

Successes in 2015 included:

• **Dridex takedown.** The Dridex botnet specialized in stealing bank credentials, and in October an international law enforcement operation saw one man charged and a coordinated effort to sinkhole thousands of compromised computers, cutting them off from the botnet’s control.

• **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.

• **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.

[Read more on Symantec's website](http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation)
It’s not just about the device or the network –
Targeting the individual behind the computer

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 in 2015. Whether it’s personal photos, banking logins or medical histories, it’s safe to assume your data is anything but private.

Trust no one

2015 saw plenty of traditional scams and malware attacks intended to gather personal information. Examples included the promise of free bulk followers on Instagram to entice people to reveal their passwords or impersonating the tax office to get people to download malicious email attachments.

In their simplest form, many scams still rely on the poor security habits of the general public in order 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 perhaps are attacks in 2015 that make 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 to exploit the public’s trust in authority figures to gain access to email accounts without raising the victims’ suspicions. (See sidebar for more details.)

How the Google mail scam works

1. An attacker gets hold of a victim’s email address and phone number – both of which are usually publicly available.

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

3. 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.”

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

5. 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.

http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access
**Secrets and lies**

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

**Sextortion**, for example, is particularly prevalent in Asia. Criminal groups target individuals using an attractive alias to encourage the victim to send sexually-explicit videos.

The criminals then tell the victim to download an app to “continue the liaison”, which gathers the victim’s phone details and contacts.

Finally, 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 same vein, the Ashley Madison attack prompted 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?” Even the hack itself was unusual in that its ramifications went well beyond the financial sphere to affect people’s personal relationships and reputations.

---

**SOCIAL MEDIA SCAMS, 2013–2015**

Source: Symantec | Safe Web

<table>
<thead>
<tr>
<th>Year</th>
<th>Manual sharing</th>
<th>Fake offering</th>
<th>Likejacking</th>
<th>Fake apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>2%</td>
<td>70%</td>
<td>23%</td>
<td>2%</td>
</tr>
<tr>
<td>2014</td>
<td>76%</td>
<td>17%</td>
<td>5%</td>
<td>1%</td>
</tr>
<tr>
<td>2015</td>
<td>81%</td>
<td>7%</td>
<td>5%</td>
<td>2%</td>
</tr>
</tbody>
</table>

---

http://www.symantec.com/connect/blogs/online-criminal-group-uses-android-app-sextortion
http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?_r=0
Mistaken identity

Social media scams continued in 2015, as criminals did their best to leverage the trust people have in their own social circles to spread scams, fake links, and phishing.

Using more progressive and ingenious tactics in order to dupe its victims, for these to succeed, the social engineering involved must be convincing.

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 get follows 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.

When choosing who to trust on social media, consider the following advice:

• **Look for the blue verified badge.**

  Twitter users should always check to see if a brand or celebrity has been verified before following. The blue verified badge denotes that Twitter has verified the authenticity of the owner of an account.

• **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.

Put your money where your mouse is

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

Ecommerce is big business, and Ecommerce Europe reported that global business-to-consumer ecommerce turnover grew by 24 percent, reaching $1.943 billion in 2014. However, that may seem small compared to the $6.7 trillion that Frost & Sullivan estimates the business-to-business ecommerce 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.

http://www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00&src=PR
Chipping away at public confidence
Other forms of attack we’ve seen in 2015 also prove just how sophisticated and ruthless criminals are willing to be to make a profit.

Stand and deliver
Ransomware has become increasingly dominant in recent years and in 2015 many expected to see this trend continue. However, whilst 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.

A Symantec researcher even demonstrated that smart TVs were potentially vulnerable to ransomware.

Some ransomware now also threatens to publish your files online unless you pay – an interesting and sinister twist, which is likely to increase since the traditional advice of ‘keep effective backups’ doesn’t 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 for card payments in the US, the potential profit criminals can gain by exploiting stolen credit card details has reduced.

• Credit card fraud involves multiple people to execute and consumer legislation ensures the victim’s financial loss is minimized. In contrast, an attacker can easily get a ransomware toolkit from an underground source and then target their victims, who 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.

The Dyre consequences, and law enforcement

After police shut down several major financial botnets, 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, often adding it to the perpetrator’s network of botnet computers.

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.

Language and location is no barrier

Other forms of attack we’ve 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, for example, a payment system used in Brazil 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 whatever the location and whatever 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 to a non-native speaker may appear convincing enough.

Privacy laws
“People are not only interested in ‘who can hack’ but also ‘who can leak’,” says Shankar Somasundaram, Senior Director, Product Management and Engineering at Symantec.

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 Organization 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.”

http://www.cio.com/article/3008661/google-receives-steady-stream-of-right-to-be-forgotten-requests.html#tk.rss_all
http://www.google.com/transparencyreport/removals/europeprivacyfaq/?hl=en#common_delisting_scenarios

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.
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.

For businesses, it’s time to start approaching security in terms of education and epidemiology. Every employee has to be part of the effort to stay digitally healthy and 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 they put customer data and customer confidence at risk.

Symantec is a true and fond believer in privacy, and a staunch privacy advocate around the world. We should not accept the misconception that privacy no longer exists, rather that it is something precious to be protected carefully.

Averting cybergeddon
Cybercrime costs the global economy up to $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’s everyone’s responsibility to do all they can to prevent that from happening.

For consumers, it’s time to kick their bad habits. Many people know the basics of good cyber security, yet 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.

CYBERCRIME COSTS THE GLOBAL ECONOMY UP TO $575 BILLION ANNUALLY

It’s not just about the device or the network – Targeting the organization behind the network

At a glance: 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 was revealed. Spear-phishing campaigns became stealthier, targeting fewer individuals within a smaller number of select organizations.

**Persistent attacks**

78 million patient records were exposed in a major data breach at Anthem, the second largest healthcare provider in the US. The attack came to light in February 2015. 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.

Persistent attacks in 2015 also 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, business intellectual property such as designs, patents and plans and, as evidenced by recent data breaches, personal information.

Zero-day vulnerabilities are particularly valuable to attackers. For example, attackmtt will design malware that only activates at a certain time or in certain locales so that it remains hidden from security researchers who run the software at a different time or in a different place.

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 exploit 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 publicly by the relevant vendor, these watering-hole sites will often switch over to using another unpublished exploit for a different zero-day vulnerability, in order to remain hidden.

Symantec’s continuing investigation into the Regin trojan gives us a glimpse into the technical capabilities of state-sponsored attackers. It revealed 49 new modules, each of which adds new capabilities such as keylogging, email and file access, and an extensive command-and-control infrastructure. Our analysts say 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.

http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541
http://ca.reuters.com/article/technologyNews/idCAKBN0OQ2GA20150610
http://www.wired.com/2015/06/breached-security-privacy-debate/
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.

Diversity in zero days

There were 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 advance attackers, and there is no sign of this trend changing.

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 reported zero-day vulnerabilities underestimates the total number.

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.

Active attack groups in 2015

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

- **Black Vine** – China-based attacks on primarily aerospace and healthcare, including Anthem and the Office of Personnel Management (both in the US), in search of intellectual property and identities
- **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, international policy and private research organizations and is believed to have been around since 2010
- **Emissary Panda** – China-based 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
Global terror, local attacks

“Cybercriminals are getting more professional and becoming braver in the targets they go after and the amount of money they transfer,” says Stephen Doherty, Senior Threat Intelligence Analyst at Symantec.

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.

A recent spam campaign impersonated local law enforcement officials in the Middle East and Canada, tricking people into downloading malware by telling them they were security tips that would keep the victim safe. All officials used in the cybercriminals’ scheme were currently in office and the subject in most cases 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 localization, which potentially requires hundreds of people to execute, 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 organizations you would expect in a legitimate business sector. And as with many other industries, up-and-coming economies, such as China, come to dominate.

Insider trading 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, either by selling market-sensitive data or using it themselves for ‘insider’ trading. We first saw these attacks in 2013 when they compromised some well-known companies including Apple, Microsoft, and Facebook. However, they use sophisticated counter-measures to cover their tracks, including encrypted virtual command and control servers. Their use of zero-day vulnerabilities in attacks reveals a level of sophistication that we have not seen before in commercially-motivated attacks.

### TOP 10 INDUSTRIES TARGETED IN SPEAR-PHISHING ATTACKS 2014-2015

Source: Symantec | cloud

#### 2014
- Manufacturing
- Services - Non-Traditional
- Finance, Insurance & Real Estate
- Services - Professional
- Wholesale
- Transportation & Public Utilities
- Public Administration (Gov.)
- Retail
- Mining
- Construction

#### 2015
- Finance, Insurance & Real Estate
- Services
- Manufacturing
- Transportation & Public Utilities
- Wholesale Trade
- Retail Trade
- Public Administration
- Non-Classifiable Establishments
- Mining
- Construction

### SPEAR PHISHING ATTACKS BY SIZE OF TARGETED ORGANIZATION 2011-2015

Source: Symantec | cloud

<table>
<thead>
<tr>
<th>Year</th>
<th>Large Enterprises (2,500+ Employees)</th>
<th>Medium-Size Businesses (251 to 2,500 Employees)</th>
<th>Small Businesses (SMBs) (1 to 250 Employees)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>50%</td>
<td>32%</td>
<td>18%</td>
</tr>
<tr>
<td>2012</td>
<td>50%</td>
<td>19%</td>
<td>31%</td>
</tr>
<tr>
<td>2013</td>
<td>39%</td>
<td>31%</td>
<td>30%</td>
</tr>
<tr>
<td>2014</td>
<td>41%</td>
<td>25%</td>
<td>34%</td>
</tr>
<tr>
<td>2015</td>
<td>35%</td>
<td>22%</td>
<td>43%</td>
</tr>
</tbody>
</table>
Cybersecurity, cybersabotage and coping with Black Swan events

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 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. But 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.

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: reviewing their security and incident response plans, getting advice and help if required, updating their technical defenses, putting good personnel policies and training in place, and staying up-to-date with the latest information.
Vectors of attack

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.

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.

As ever, the numbers suggest that website owners aren't patching and updating their sites and servers as often as they should.

Linux in the firing line
2015 has seen a surge in malware targeting Linux – the most common operating system on website servers, among other essential internet services.

Attackers will often contaminate compromised web servers with code that links to exploit toolkits, or 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 out 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.

How to keep your server safe

- Keep your server patched and up-to-date.
- Employ multi-layer protection, so if one layer gets breached there are other layers to protect different areas of the system.
- Deploy network intrusion prevention and detection and monitor email services running on the server.
- Use a good firewall and review access logs regularly to detect potentially suspicious activity.
- Use anti-virus software – if it detects the malware it can block it.
- Backup offsite.

Ransomware targeting Linux was also uncovered in 2015; it 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 back-ups.

**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.

**The end is nigh for Flash**

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 of the Adobe vulnerabilities related to the Adobe Flash Player (also known as Shockwave 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 5 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 both Google and Mozilla recently announced that Flash will no longer be supported natively in Chrome and Firefox.

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

**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 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.

**Infection by injection**

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

“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.

Following the 2015 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.


TOP-FIVE WEB ATTACK TOOLKITS, 2014

Source: Symantec

- Sukura 23%
- Nuclear 10%
- Styx 7%
- Orange Kit 5%
- Blackhole 5%
- Others 50%

TOP-FIVE WEB ATTACK TOOLKITS, 2015

Source: SDAP, Wiki

- Angler 23%
- Nuclear 6%
- Magnitude 2%
- Rig 4%
- Neutrino 1%
- Others 64%
One notable exploit toolkit called Angler, was the most active 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.

Tech support scams have been distributing Cryptowall ransomware through the Nuclear exploit kit.

Three countries most affected:

- USA
- Canada
- UK
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.

In total, Symantec blocked more than 100 million tech support scams last year. The countries targeted the most by tech support scams were the US, UK, France, Australia, and Germany.

**Distributed-Denial-Of-Service**

Distributed-Denial-Of-Service (DDoS) attacks are getting bigger and more prolonged as botnets-for-hire increase in popularity and the Internet of Things provide more fodder for 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, it was sometimes the last resort in paying the ransom. 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 taken down for several hours on New Year’s eve, is a prime example. It’s thought to be the biggest ever DDoS attack, at least according to New World Hacking. The anti-Islamic State organization claimed responsibility because the BBC’s scale offered a chance for them to test their abilities. The group claims the attack reached a peak of 602Gbps.

That said, there are rewards to be gained through a DDoS attack, the most obvious being blackmail: pay us or your site remains under attack. DDoS has also been used as a “distraction” tool in conjunction with some targeted attacks in 2015, where attackers flood the website of the targeted organization, leaving the IT team believing it to be the prelude to a ransom demand; however, in reality another, stealthier attack is quietly taking place at the same time.
The chart shows how the number of DDoS attacks has grown in the latter part of the year, before tailing-off dramatically in November and December. There were more spikes of activity in 2015, as attack durations become shorter and more discreet.

<table>
<thead>
<tr>
<th>Rank</th>
<th>2015 Attacks</th>
<th>2015 Attack Rate</th>
<th>2014 Attacks</th>
<th>2014 Attack Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generic ICMP Flood Attack</td>
<td>85.7%</td>
<td>DNS Amplification Attack</td>
<td>29.44%</td>
</tr>
<tr>
<td>2</td>
<td>Generic TCP Syn Flood Denial of Service Attack</td>
<td>6.4%</td>
<td>Generic ICMP Flood Attack</td>
<td>17.20%</td>
</tr>
<tr>
<td>3</td>
<td>Generic Ping Broadcast (Smurf) Denial of Service Attack</td>
<td>2.1%</td>
<td>Generic Ping Broadcast (Smurf) Denial of Service Attack</td>
<td>16.78%</td>
</tr>
<tr>
<td>4</td>
<td>Generic Teardrop/Land Denial of Service Attack</td>
<td>2.0%</td>
<td>Generic Teardrop/Land Denial of Service Attack</td>
<td>7.17%</td>
</tr>
<tr>
<td>5</td>
<td>RFProwl Denial of Service Attack</td>
<td>0.6%</td>
<td>Generic ICMP Unreachable Denial of Service Attack</td>
<td>5.71%</td>
</tr>
</tbody>
</table>

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.

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 2002: they are simple to set up, difficult to stop, and highly disruptive in nature. This is truer than ever with the rise of botnets-for-hire.

Botnet-for-hire fingerprints were on roughly 40 percent of all DDoS network layer attacks in the second quarter of 2015, according to Imperva 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 $10 to $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. Consequently the potential rewards for an attacker will more than compensate for their costs.

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 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.

http://www.symantec.com/connect/articles/barbarians-gate-introduction-distributed-denial-service-attacks
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, as shown in the chart below. 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.

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.
While the attack duration is decreasing due to attackers’ preference for short bursts of attacks, it has also meant that the actual number of attacks is on the rise as observed by Imperva Incapsula, who have reported a staggering 133.8 percent increase in the frequency of network layer attacks in the second half of 2015.

**Web connected applications increasingly threatened**
Similar to network layer attacks, application layer incidents also continued to shorten in duration, while losing nothing in tenacity. The largest application layer attack mitigated in Q4 2015 was a very short and very intense burst that peaked at 161,300 Requests per Second.

On the one hand, this serves as a reminder that DDoS is a communal problem that affects the entire internet ecosystem. On the other, it represents just how easy it is to sustain a sizable application layer attack, with only a few compromised devices needed to generate enough traffic to take down a mid-sized website, and keep it down for a very long period of time.

As a result, Q4 2015 continued to see a high frequency of repeated application layer attacks, with 44.7 percent of targets attacked more than once and 18 percent attacked more than five times.

https://www.incapsula.com/blog/ddos-report-q4-2015.html
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 offer a much larger bandwidth capacity for an attack than traditional consumer targets, to make them conduct DDoS attacks against other websites. This method isn’t new, but it shows criminals are continuing to create bigger and better botnets.

2015 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 attacks, 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.
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 nuances 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.

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 analyse, 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.

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

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

http://www.symantec.com/connect/blogs/malvertising-campaign-targets-brazilian-users
On the client side

Smartphones and mobile devices

At a glance: Smartphones are an increasingly attractive target for online criminals. As a result, they are investing in more sophisticated attacks that are more effective at stealing valuable personal data or extorting money from victims. Although Android users are 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 (27 January 2016). Five out of six new phones were running Android, with one in seven running Apple’s iOS operating system (IDC, 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. 2015 saw the launch of Apple Pay and other mobile payment systems will follow. All this makes them 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 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.

APP ANALYSIS BY SYMANTEC’S NORTON MOBILE INSIGHT

Source: Symantec | SDAP

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Apps Analyzed</td>
<td>6.1 Million</td>
<td>6.3 Million</td>
<td>10.8 Million</td>
</tr>
<tr>
<td>Total Apps Classified As Malware</td>
<td>0.7 Million</td>
<td>1 Million</td>
<td>3.3 Million</td>
</tr>
<tr>
<td>Total Apps Classified As Grayware</td>
<td>2.2 Million</td>
<td>2.3 Million</td>
<td>3 Million</td>
</tr>
<tr>
<td>Total Grayware Further Classified As Malware</td>
<td>1.2 Million</td>
<td>1.3 Million</td>
<td>2.3 Million</td>
</tr>
</tbody>
</table>

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, hack 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.

http://www.idc.com/getdoc.jsp?containerId=prUS40980416
http://www.idc.com/prodserv/smartphone-os-market-share.jsp
http://www.ericsson.com/mobility-report
https://www.census.gov/population/international/data/idb/worldpopgraph.php
The number of Android malware families added in 2015 grew by 6 percent, compared with the 20 percent growth in 2014.

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 authorised 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 App 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 jailbroken, in order to compromise an iOS device.

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 unauthorised 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 before they start their attacks and some malware now checks to see if it is running on real phones or the kind of emulators that security researchers use.

Android users under fire with phishing and ransomware

Besides familiar tricks such as selling fake apps that aren’t as advertised, 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.

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, where possible, biometrics
• 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, and don’t jailbreak devices
• 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 and when 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, perhaps commercialised 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 and improvements in application delivery. Phone users should become used 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.

Email and communications threats
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. Malicious emails grew in number since 2014, and remain an effective medium for cybercriminals, even if spam does not.

Email abuse
Email continues to dominate digital communications, in the face 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 favoured way to do it.

No wonder it is still widely used by internet criminals for spam, phishing, and email malware. However, 2015 saw email threats in decline. Email-based attacks from phishing and malware are spam, and accounted for approximately 1 percent of all spam. Symantec provides further analysis of malware and phishing attacks, as these threats have potentially significant, harmful consequences, and for this reason, it is useful to know more about them.

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.

https://support.google.com/accounts/answer/41078?hl=en
Spam
More than half of inbound business email traffic was spam in 2015, despite a gradual decline over recent years, 2015 saw spam reach its lowest level since 2003. However, the spam problem is still 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.

Phishing
Over the years, phishing campaigns have become much easier to operate, thanks to the evolving cybercriminal marketplace. Attackers will cooperate, with some specialising in phishing kits, and others selling them on to other scammers who want to conduct phishing campaigns. These kits often trade for between $2 and $10, and their users do not require much in the way of technical skills to operate them or customise 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.

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

Threats like Dridex exclusively use spam email campaigns, and use 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 every single type of spam attack and malware propagation vector; from simple malware attachments, links in the message body that point to an exploit kit landing page, to 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.

No wonder it is still widely used by internet criminals for spam, phishing, and malware. However, 2015 saw all three forms of abuse decline again as these graphs reveal.

http://www.symantec.com/connect/blogs/dridex-and-how-overcome-it
PHISHING RATE, 2013–2015
Source: Symantec | .cloud

PROPORTION OF EMAIL TRAFFIC IN WHICH A VIRUS WAS DETECTED, 2013–2015
Source: Symantec | .cloud
Email encryption

Email encryption is valuable because it protects the privacy of the messages and can help to authenticate senders. It is under threat because of vulnerabilities in the underlying technology (see previous page) 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. For example, Google reports that around 40 percent of incoming messages over the last year were not encrypted.

Good desktop and gateway email encryption tools 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.

Bypassing encryption: 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 security advice

Organizations and individuals need to realize 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/TLS certificate on any sites where you enter sensitive data
• Not using unsecured networks when accessing sensitive data

And to 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 your data is and who has access to it
• Ensuring you have a good incident response plan for when an attack is detected

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, with many attacks already shifted towards using 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 in developing countries, we may even expect to see a growth in phishing attacks in these areas. For example, paying utility bills, booking doctor’s appointments, applying for university, managing frequent flyer accounts, taking out insurance and so on. All these, and more, will provide fruitful inspiration for phishing attacks.

http://www.google.com/transparencyreport/saferemail/
https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp
Computers, cloud computing and IT infrastructure

IT systems – computers and networks – 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.

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 cyberattacks that may encrypt their data and hold it to ransom, identity theft and attackers using their computers as a springboard from which 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 to 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.

The chart shows a downward trend since 2013, markedly accentuated in 2015.
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 unauthorised 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 $10.

Cloud vulnerabilities

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 virtual machine 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 virtualisation. More concerning is that it can also afford the attacker the ability to recognize when it is able to exploit and infect other virtual machines on the same system.

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 is where IT systems and solutions are used inside organizations without explicit organizational approval, and solutions are 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 not involving the IT department 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 to 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.

http://www.symantec.com/connect/blogs/monitoring-shadow-it
The Industry’s reply

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

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 card numbers, sales information or private electronic mail messages, on the network.”

Twenty years later, people’s concerns remain the same; although behavior perhaps suggest they are willing to take the risk, relying on their bank to bail them out 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 moves forward at a pace.

As computing power has increased so has a hacker’s ability to break hashing algorithms through sheer brute force, and 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.

“We agree with the positions of Microsoft and Google that SHA-1 certificates should not be issued after January 1, 2016, or trusted after January 1, 2017,” 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) and meant that 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.

9.6%
Checks and balances

In order to strengthen the SSL/TLS ecosystem, Symantec has also been pushing 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 issued on its Certificate Transparency log and since 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/TLS certificates in nearly real time.”

Accelerating to Always-On SSL

Nearly 40% 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% 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, 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.
- **Internet 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 be secured by an SSL/TLS certificate. Symantec is even working with web hosting providers to help them provide encryption as part of their service to website owners.

### Certificate Details

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Domain validated?</th>
<th>https encrypted?</th>
<th>Identity validation?</th>
<th>Address validation?</th>
<th>Padlock displayed in browser user interface</th>
<th>Green address bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>DV</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>OV</td>
<td>Yes</td>
<td>Yes</td>
<td>Good</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EV</td>
<td>Yes</td>
<td>Yes</td>
<td>Strong</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

https://casecurity.org/2013/09/25/what-is-certification-authority-authorization/
https://knowledge.symantec.com/support/certificates-support/index?page=content&id=AR2177
https://www.certificate-transparency.org
http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/
http://googlewebmastercentral.blogspot.co.uk/2014/08/https-as-ranking-signal.html
https://www.mnot.net/blog/2015/06/15/http2_implementation_status
Reinforced reassurance

Several major browsers are also improving their security indicators – the colors 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 offer a secure connection, 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.

---

MOZILLA’S NEW SECURITY INDICATORS

Source: Taken from Mozilla’s Security Blog

<table>
<thead>
<tr>
<th>PREVIOUS VERSION</th>
<th>NEW VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites with DV certificates</td>
<td></td>
</tr>
<tr>
<td>Sites with EV certificates</td>
<td></td>
</tr>
<tr>
<td>Sites with mixed active content blocked</td>
<td></td>
</tr>
<tr>
<td>Sites with mixed active content allowed</td>
<td></td>
</tr>
<tr>
<td>Sites with mixed passive content loaded</td>
<td></td>
</tr>
</tbody>
</table>
Looking ahead

Discover in this section what 2016 and the coming years hold: from emerging trends to new and ongoing discussions, we’ve gathered Website Security topics you will hear about and may want to keep at the back of your mind throughout the year. For regular updates on the latest security news, you can also check our dedicated blog on Symantec Connect.

On the rise: More phishing
We anticipate that phishing will increase, despite a general trend downwards over the past few years, firstly because people are consuming more and more online media, and secondly because internet access and online transactions is becoming more and more common in developing countries.

Add to this the development of internet services for everyday tasks - paying utility bills, booking doctor’s appointments, applying for university, managing frequent flyer accounts, taking out insurance and so on – and you get fruitful inspiration for phishing attacks.

On the rise: HTTPS everywhere, for everyone
We’re observing a large increase in the promotion and adoption of SSL/TLS certificates – at both individual and organization levels - with new initiatives to make encryption accessible to everyone, by offering SSL/TLS certificates as an extra feature, for example with hosting services or cloud services. This trend is very likely to grow, especially on the DV (Domain Validation) market.

The complexity of management of SSL/TLS certificates resulting from the never-ending stream of hosts to authenticate, secure and monitor is also a new area of focus, and we’re expecting the number of management tools and services to grow even further, at the same time as the growing awareness of security needs. We could notably hold the increasing media coverage of breaches and web security threats accountable for this trend.

On the rise: Hybrid threats: mobile attacks
Unsurprisingly, we predict that mobile threats will continue to proliferate in 2016. We may soon see PC-like exploit kits for phones, perhaps commercialized on the black market. We have seen the number of mobile vulnerabilities increase every year over the past three years. This is perhaps an indicator of progress, rather than a cause for despair. It suggests that security researchers, operating systems, 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.

On the rise: The growing need for the right security skills
Online threats are evolving much, much faster than we are increasing our capacity to understand them and provide pro-active counter-measures. And it’s not just hackers becoming more creative, it is also because a tremendous amount of new services on the Internet are developed every day; most of the time, these services are conceived by people whose priority is to offer something new, exclusive, useful, or innovative. Security is never on top of the list.

Another sad explanation is that the skills we require to build a bulletproof network are currently held by the bad guys in the industry. IT security employees are still essentially trained on creating and maintaining a good network infrastructure before anything else, and are often unprepared for all the threats and vulnerabilities to deal with on a company network. More importantly, IT security employees can rarely tell the profile of a potential hacker and do not necessarily understand what could motivate them to attack a company. Unpatched servers and poorly configured networks are not just the result of laziness; it’s more often the result of a lack of information. In this context, it obviously becomes very hard for anyone to initiate pro-active measures against network attacks. The only ones who could do this…are the hackers themselves.

This is the reason why we expect the market of freelance “white hat hacking” and IT security consultancy to grow even more in the coming years. Companies will start hiring more penetration testers, more freelance hackers and use more IT security consultancy services as they have the knowledge and skills requested. The need for compliance – notably on some specific sectors dealing with sensitive data such as banking and health - will also drive this demand.

Hot topics: Spotlights on authentication
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 and build trust. Two-factor authentication is becoming an imperative to ensure confidence. New solutions to get rid of password authentication are even starting to appear, aiming at reducing the risk of phishing fraud and the inevitable costs associated.

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 and improvements in application delivery. Phone users should get used to frequent, perhaps on-by-default, application and operating system updates and the need for security software on their mobile devices.

Hot topics: The Internet of Insecure Things
Although the concept of IoT (Internet of Things) is not new – it was first used in 1999 – it’s been a trending topic for the past two years, and the expression mainly used to describe the major impact of connected devices on our daily lives: the Internet is now everywhere.

The topic is without hesitation going to remain a major trend in the years ahead; however the excitement of living in a connected world is now giving way to growing concerns about the security of connected devices and the potential threats it would represent. Car hacking was one of the most widely discussed IoT security issues in 2015, and we expect more similar topics to be raised during the years to come. Once again, the increasing media coverage of such events plays an important role in raising awareness about security in the IoT.

Hot topics: Hacktivism, terrorism, government responsibility and privacy rights
Hacktivism and terrorism have never been so present in the news; the Web is not only becoming the #1 vector for propaganda and communication within extremist groups, but it is also becoming a privileged place for such groups to demonstrate their presence and capacities. Anonymous networks such as TOR are no longer reserved for black markets, and there is no doubt that in the years to come we will see more and more spectacular hacks with political or ideological purposes take place - we can very certainly expect collateral damage on companies and organizations when this happens.

This increased presence of online hacktivism has shifted governments’ focus on online encrypted communication over the past years. The revelations of Edward Snowden in 2013 about the involvement of some governments in surveillance programs exposed what many were suspecting already; yet it still had the effect of a bombshell on public opinion. Since then we’ve seen more and more discussions around what motivates the right for a government to actively spy on anyone. The recent rejection of Safe Harbor by the European court of Justice has revived the debate, and should remain a very important topic for 2016.

Did you know
Symantec has created root certificates specifically for IoT users. To deploy these, or any other root certificates, in your IoT devices just get in touch.
The history of Transport Layer Security (TLS) began in 1994, with the release of SSL 2.0—a poorly designed, but good-enough protocol to support a boom of ecommerce and the commercial Web. Over the next 22 years we continued to improve the security as our knowledge of cryptography improved; the latest stable release today is TLS 1.2, from 2008. This version, which achieved wider adoption only in 2013, provides reasonable security for commercial applications.

Despite wide criticism of TLS in recent years, this protocol has served us well, as evidenced by the phenomenal growth of the Internet, with few security incidents related to encryption. If anything, you could argue that most of our security troubles in this space come from our stubborn resistance to actually deploy encryption or to adopt newer and more secure protocols. On the Web, we are seeing some good progress, with most important sites improving their security at a good pace. Overall, however, it’s likely that the percentage of encrypted websites is still in the single digits. When it comes to email, we’re also struggling. For example, in January 2016, Gmail delivered 82 percent of its emails securely, but only 58 percent of the inbound email was encrypted. Compared to the Web, getting email encryption right is easy because a small number of email providers handle a large percentage of the world’s email. On the other hand, most organizations still prefer insecure transport of their emails over delivery failures.

But the tide has turned; it’s evident that we’re moving toward a robustly encrypted internet.

The work on the next version of TLS, version 1.3, began in late 2012 and is nearing completion. The developers recently invited a wider security audience of cryptographers to take a good look at the protocol drafts. If we want to develop a good protocol that will serve us for the next 20 years, we want to poke holes in it now, before it is being deployed. Despite the modest change in the version number, TLS 1.3 is a substantially different protocol. It will not only be more secure, but—crucially—it will also be faster (measured primarily in network latency, which is the only remaining bottleneck today).

In practical terms, the biggest immediate impact of TLS 1.3 will be the removal of cruft accumulated since the first SSL version, which remained in 1.2 and earlier versions. As a matter of fact, the biggest practical obstacle to security today is education: TLS 1.2 can be configured to be very secure, but to do so you need to know how to avoid the many pitfalls lurking. There are books that explain how to do this, but they run into many hundreds of pages. In most cases, website operators don’t possess the skills or are simply not motivated enough to deal with this problem. The short-term answer of the community was to tie security to performance improvements. For example, HTTP/2 can be deployed only with TLS 1.2 and using a subset of features that are properly secure. Long term, TLS 1.3 will be secure by default, no matter what configuration.

How can we prepare for the imminent arrival of TLS 1.3? The key is to start thinking about where you need security and how you are obtaining it. If your critical sites depend on third parties—for example if you’re outsourcing website hosting, or using hardware appliances—talking to your vendors now is critical. Let them know that you care, and get them to pledge timely support of new security features. After all, it isn’t only your security that’s at stake, it’s the performance of your websites too.
Recommendations and best practice

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 and TLS are only as good as their 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** (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.

Adopt complete 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 simple and efficient task.

http://www.symantec.com/page.jsp?id=seal-transition
Educate employees
As ever, 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, application 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.
• Apply effective access controls to protect servers and private keys working on a least-privilege basis.

Protect 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.
• Regular updating. For example, the latest version of Android, codenamed ‘Marshmallow’, includes a number of features designed specifically to thwart attackers.
• Don’t jailbreak devices and only use trusted app markets.
• User training, particularly around paying attention to permissions requested by an app.
• Security solutions such as Symantec Mobility or Norton Mobile Security.

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 your website potentially poses to consumers, but it will take commitment and action from website owners for it to become a reality.

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