Symantec.

PART 1

WSTR

WEBSITE SECURITY
THREAT REPORT 2016

Contents

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
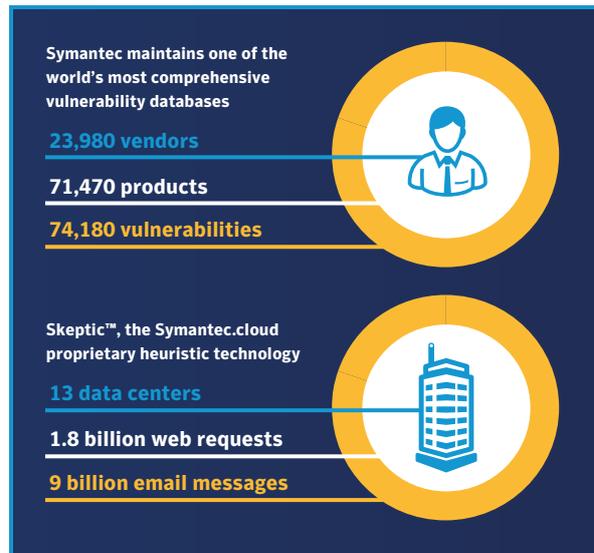- and other 3rd party data sources.

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 centers. 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.

157 countries

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

23,980 vendors

71,470 products

74,180 vulnerabilities

Skeptic™, the Symantec.cloud proprietary heuristic technology

13 data centers

1.8 billion web requests

9 billion email messages

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.

www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014
www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00
www.bbc.co.uk/news/technology-35204915

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.

http://netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf
http://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it

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://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html
http://www.symantec.com/connect/blogs/dangers-domain-validated-ssl-certificates
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.

TOTAL BREACHES
Source: Symantec | CCI

2013	Change	2014	Change	2015
253	+23%	312	+2%	318

TOTAL IDENTITIES EXPOSED
Source: Symantec | CCI

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

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-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF
http://www.symantec.com/cyber-insurance/
http://netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf
http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012

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.

TOP 10 VULNERABILITIES FOUND UNPATCHED ON SCANNED WEBSERVERS
Source: Symantec | Trusted Services

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

http://www.symantec.com/connect/blogs/critical-openssl-vulnerability-could-allow-attackers-intercept-secure-communications
http://www.symantec.com/connect/blogs/new-openssl-vulnerability-could-facilitate-dos-attacks

TOP CAUSES OF DATA BREACH BY INCIDENTS, 2013-2015
Source: Symantec | CCI

Legend:
- 2013
- 2014
- 2015

Category	2013	2014	2015
Attackers	34%	49%	46%
Accidentally made public	29%	22%	22%
Theft or loss of computer or drive	27%	21%	21%
Insider theft	6%	8%	10%

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.

http://netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf
http://uk.businessinsider.com/ashley-madison-ceo-says-hack-was-an-inside-job-2015-7
http://cdn2.hubspot.net/hubfs/407136/PDFs/Symantec/MeriTalk_-_Symantec_-_Inside_Job_Report_-_FINAL.pdf?t=1445970735623
https://www.gov.uk/government/news/protecting-information-from-an-insider-threat
https://www.gov.uk/government/news/identifying-cyber-insider-threats-in-real-time
https://www.gov.uk/government/news/securing-against-the-insider-threat

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 10 SECTORS BREACHED BY NUMBER OF IDENTITIES EXPOSED, 2-DIGIT
Source: Symantec | CCI

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

TOP 10 TYPES OF INFORMATION EXPOSED
Source: Symantec | CCI

Rank	2014 Type	2014 %	2015 Type	2015 %
1	Real Names	68.9%	Real Names	78.3%
2	Gov. ID Numbers (e.g., SSN)	44.9%	Home Addresses	43.7%
3	Home Addresses	42.9%	Birth Dates	41.2%
4	Financial Information	35.5%	Gov. ID numbers (e.g., SSN)	38.4%
5	Birth Dates	34.9%	Medical Records	36.2%
6	Medical Records	33.7%	Financial Information	33.3%
7	Phone Numbers	21.2%	Email Addresses	20.8%
8	Email Addresses	19.6%	Phone Numbers	18.6%
9	User Names & Passwords	12.8%	Insurance	13.2%
10	Insurance	11.2%	User Names & Passwords	11.0%

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.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks
http://www.usatoday.com/story/money/personalfinance/2015/09/30/chip-credit-card-deadline/73043464/
http://arstechnica.com/business/2015/10/today-all-stores-in-the-us-should-accept-chip-and-pin-cards-yeah-right/

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.

http://www.symantec.com/connect/blogs/hacking-team-woes-adds-dangers-faced-internet-using-public

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.

TOP 10 MALICIOUS ACTIVITY BY SOURCE: BOTS, 2014–2015
Source: Symantec | GIN

Rank	2014 Country/Region	2014 Bots %	Rank	2015 Country/Region	2015 Bots %
1	China	16.5%	1	China	46.1%
2	United States	16.1%	2	United States	8.0%
3	Taiwan	8.5%	3	Taiwan	5.8%
4	Italy	5.5%	4	Turkey	4.5%
5	Hungary	4.9%	5	Italy	2.4%
6	Brazil	4.3%	6	Hungary	2.2%
7	Japan	3.4%	7	Germany	2.0%
8	Germany	3.1%	8	Brazil	2.0%
9	Canada	3.0%	9	France	1.7%
10	Poland	2.8%	10	Spain	1.7%
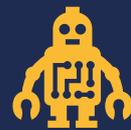
They can run, but they can't hide

"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."

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

Successes in 2015 included:

- **Dridex takedown.** The Dridex botnet specialized in stealing bank credentials, and in October an <u>international law enforcement operation</u> 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 <u>assisted by, among others, Symantec and Microsoft,</u> 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.

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 auditors. Data breaches are unlikely to stop any time soon, but the scale and impact of them could certainly be reduced if organizations recognized that security goes well beyond the bounds of the CIO or IT manager and lays in every employee's hands.

http://www.symantec.com/connect/blogs/dridex-takedown-sinks-botnet-infections
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/free-instagram-followers-compromised-accounts-phishing-sites-and-survey-scams
http://www.Symantec.com/connect/blogs/australians-beware-scammers-are-impersonating-australian-taxation-office
http://www.Symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access
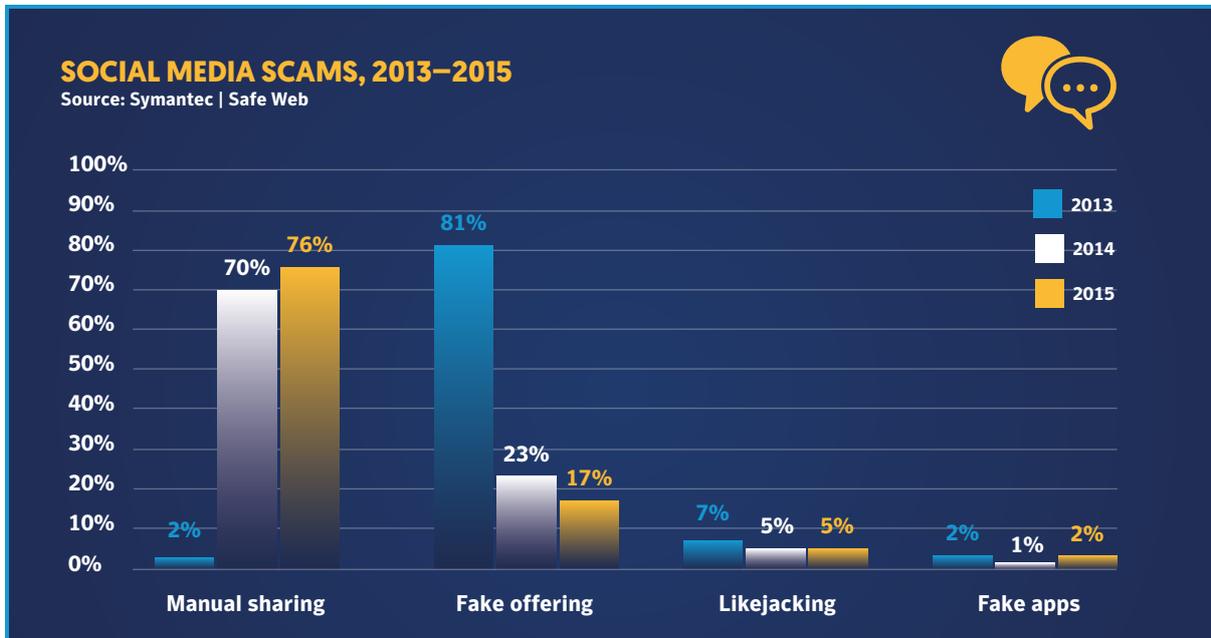
Secrets and lies

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

Category	2013	2014	2015
Manual sharing	2%	70%	76%
Fake offering	81%	23%	17%
Likejacking	7%	5%	5%
Fake apps	2%	1%	2%

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
http://www.symantec.com/connect/blogs/scammers-quick-capitalize-ashley-madison-breach

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.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/uncovering-a-persistent-diet-spam-operation-on-twitter.pdf
https://nrf.com/media/press-releases/thanksgiving-weekend-shopping-brings-big-store-and-online-crowds-according-nrf
http://www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014
http://www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00&src=PR
https://gds.blog.gov.uk/2015/10/23/how-digital-and-technology-transformation-saved-1-7bn-last-year/

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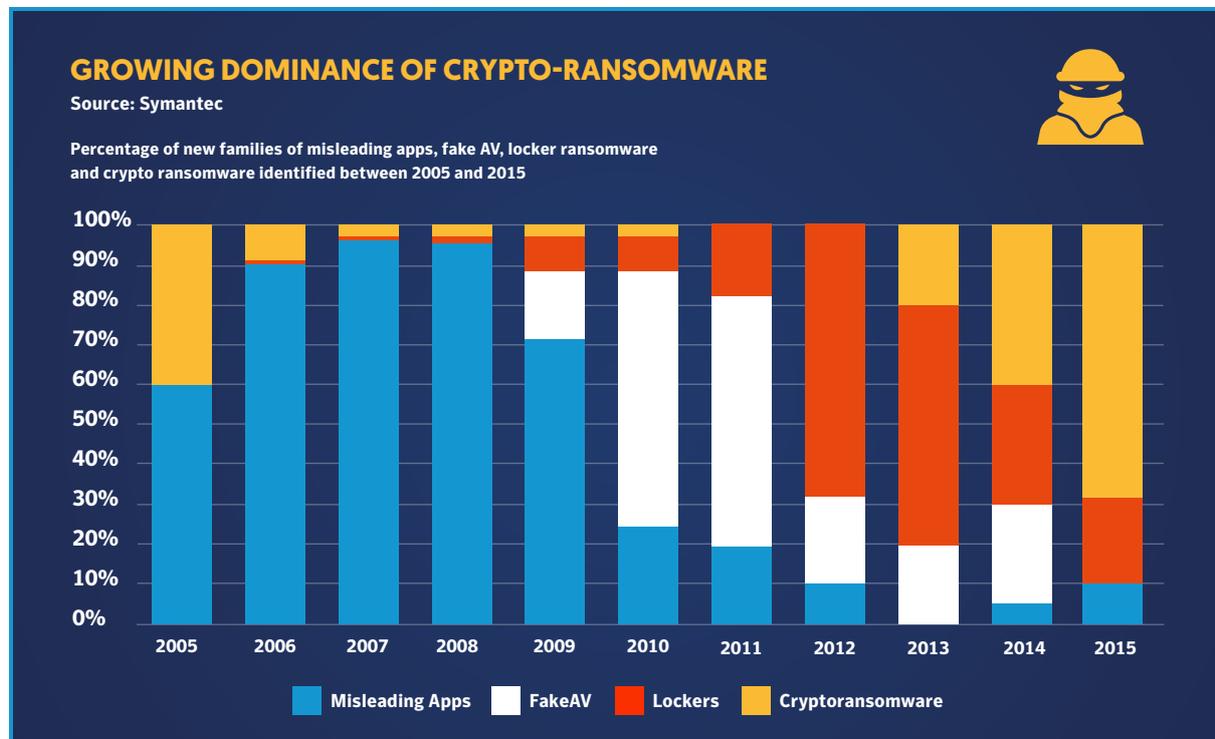
A Symantec researcher even demonstrated that smart TVs were potentially vulnerable to ransomware.

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.

GROWING DOMINANCE OF CRYPTO-RANSOMWARE

Source: Symantec

Percentage of new families of misleading apps, fake AV, locker ransomware and crypto ransomware identified between 2005 and 2015

Legend: Misleading Apps, FakeAV, Lockers, Cryptoransomware

http://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it
http://www.computerworld.com/article/3002120/security/new-ransomware-program-threatens-to-publish-user-files.html
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

The Dyre consequences, and law enforcement

After police shut down several major financial botnets, Dyre stepped up to take their place.

DYRE DETECTIONS OVER TIME, 2014–2015
Source: Symantec
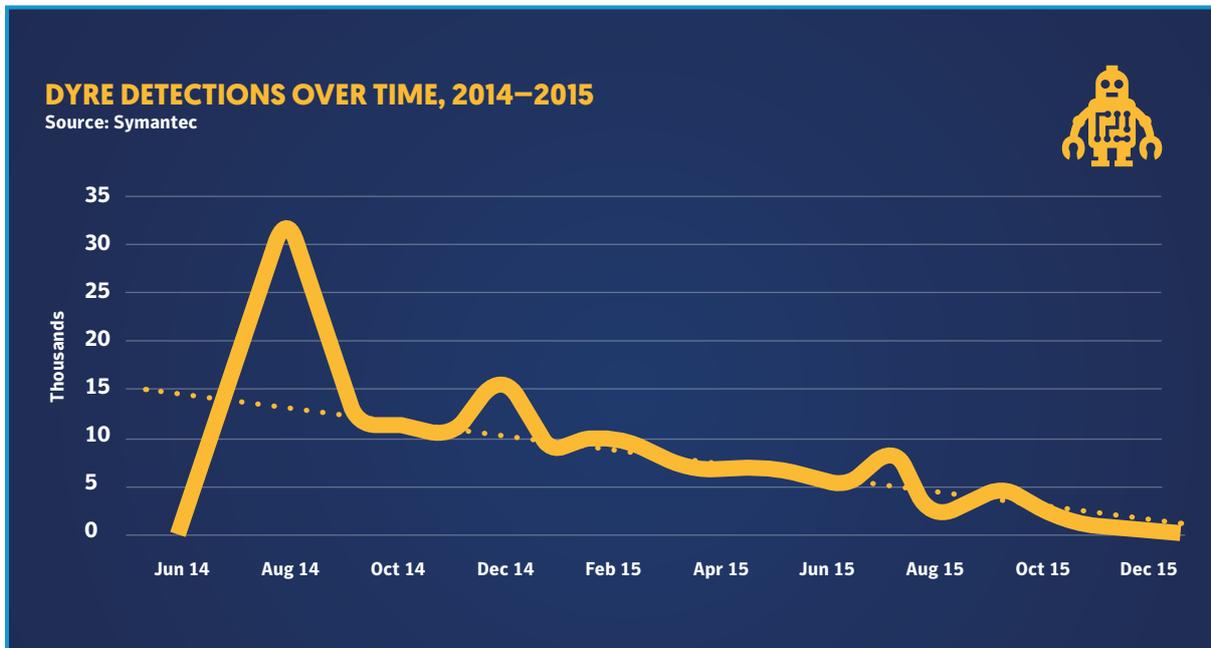
Not only could Dyre hijack common web browsers and intercept internet banking sessions to steal information, it could also download additional malware to the victim's computer, often adding it to the perpetrator's network of botnet computers.

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.

http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat
http://www.symantec.com/connect/blogs/dyre-operations-bank-fraud-group-grind-halt-following-takedown
http://www.symantec.com/security_response/writeup.jsp?docid=2014-061713-0826-99
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/boleto-malware.pdf

NUMBER OF PHISHING URLS ON SOCIAL MEDIA, 2009–2015
Source: Safe Web
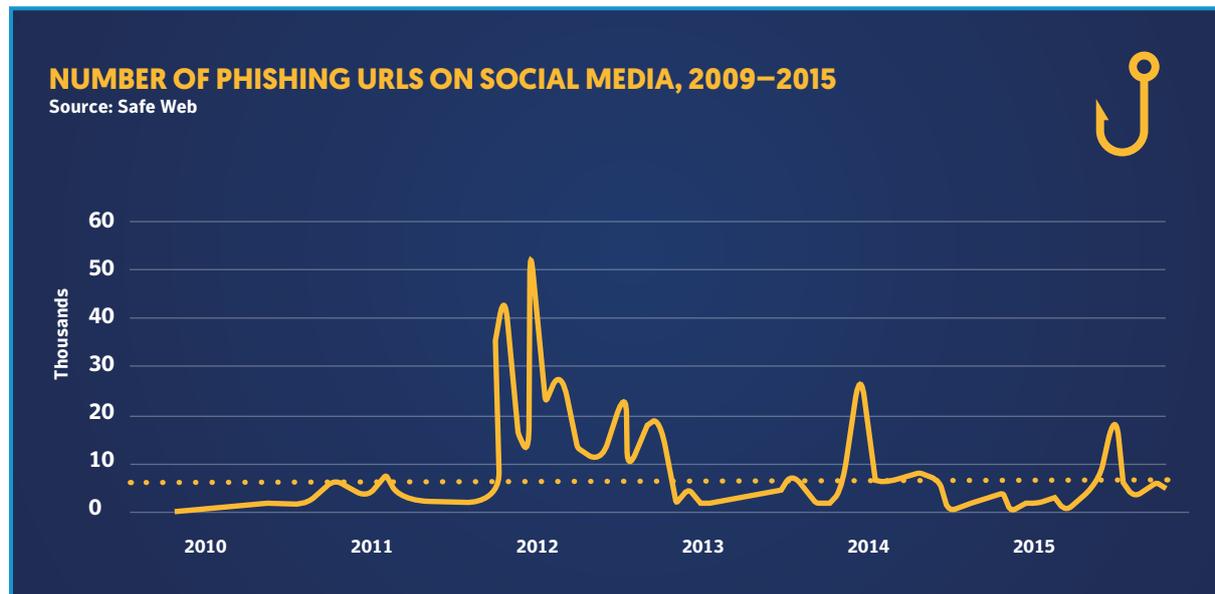
The chart shows how social media has played a crucial role in the social engineering of attacks in the past. In recent years, these sites have clamped-down on such abuses, and made it much harder for the attackers to exploit them.

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/europeprivacy/faq/?hl=en#common_delisting_scenarios
http://www.beuc.eu/publications/beuc-pr-2015-020_historic_victory_for_europeans_personal_data_rights.pdf
http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection

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

$575 BILLION

http://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt

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.

Targets of cyberespionage 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, we saw a previously-unknown vulnerability used to attack a government agency using an infected Word document sent by email. Indeed, such vulnerabilities are so valuable that attackers work hard to limit their exposure, maintaining their advantage. For example, attackers 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.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf
http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/
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/opm-breach-security-privacy-debacle/
http://www.symantec.com/connect/blogs/regin-further-unravelling-mysteries-cyberespionage-threat
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

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

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

ZERO-DAY VULNERABILITIES
Source: Symantec I SDAP, Wiki

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

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

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf
http://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets
http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
http://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks
http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats

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.
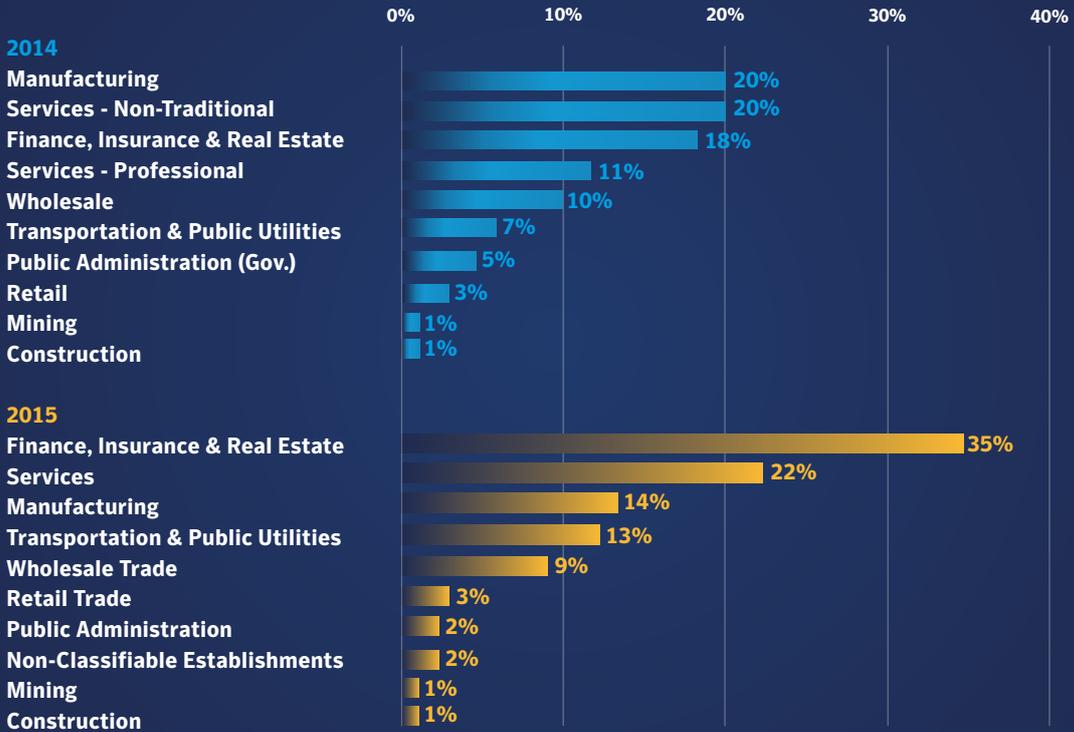
This level of research and localization, which potentially requires hundreds of people to execute, is becoming increasingly common in botnet scams. The underground economy isn't just about selling stolen goods: it's an entire industry with the talented professionals and organizations you would expect 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.
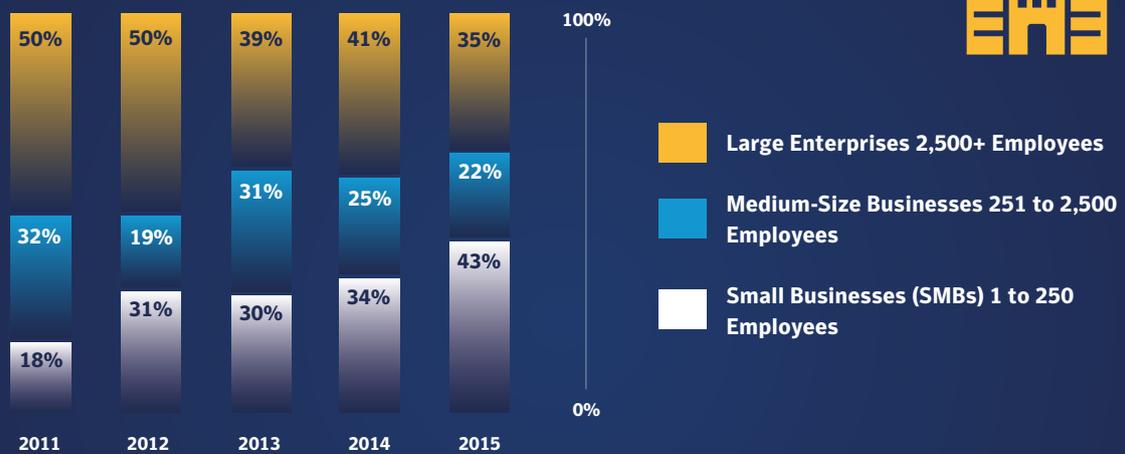
http://www.symantec.com/connect/blogs/terror-alert-spam-targets-middle-east-canada-spread-malware

TOP 10 INDUSTRIES TARGETED IN SPEAR-PHISHING ATTACKS 2014-2015
Source: Symantec I cloud

2014

Industry	Percentage
Manufacturing	20%
Services - Non-Traditional	20%
Finance, Insurance & Real Estate	18%
Services - Professional	11%
Wholesale	10%
Transportation & Public Utilities	7%
Public Administration (Gov.)	5%
Retail	3%
Mining	1%
Construction	1%

2015

Industry	Percentage
Finance, Insurance & Real Estate	35%
Services	22%
Manufacturing	14%
Transportation & Public Utilities	13%
Wholesale Trade	9%
Retail Trade	3%
Public Administration	2%
Non-Classifiable Establishments	2%
Mining	1%
Construction	1%

SPEAR PHISHING ATTACKS BY SIZE OF TARGETED ORGANIZATION 2011-2015
Source: Symantec I cloud

Size	2011	2012	2013	2014	2015
Large Enterprises 2,500+ Employees	50%	50%	39%	41%	35%
Medium-Size Businesses 251 to 2,500 Employees	32%	19%	31%	25%	22%
Small Businesses (SMBs) 1 to 250 Employees	18%	31%	30%	34%	43%

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.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
http://www.bbc.co.uk/news/technology-30575104
https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf
https://www.symantec.com/content/en/us/enterprise/images/mktg/Symantec/Email/13927/WSTR_SYM_Spear_Phishing.pdf

Symantec

COMING SOON: WSTR 2016 PART 2

PART 2

WSTR

WEBSITE SECURITY
THREAT REPORT 2016

In the second part of our comprehensive Website Security Threat Report, we examine how cybercriminals are using new and sinister ways to attack. We also take a detailed look at the rapidly increasing proliferation of DDoS attacks, how they are growing in scale and the way the Internet of Things provides new opportunities for attack.

The industry's response to these new threats has been encouraging, but there is more that can be done. Read about the industry's reply, alongside our recommendations and best practice tips to maintain a secure website.

LOOK OUT FOR WSTR 2016 PART 2 IN YOUR INBOX IN THE NEXT COUPLE OF WEEKS.

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

For product information in the UK, call:
0800 032 2101 or +44 (0) 208 6000 740

For product information in the US, call:
1-866-893-6565

Symantec (UK) Limited.
350 Brook Drive,
Green Park, Reading,
Berkshire, RG2 6UH, UK.
www.symantec.co.uk/ssl

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Switzerland Limited
Andreasstrasse 15,
8050 Zurich,
Switzerland
www.symantec.co.uk/ssl

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne,
3004, ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates