February 2016

IBM X-Force Threat Intelligence Report 2016

IBM

Contents

Executive overview

In the modern era of mega breaches, there seems to be an ever-upward trend of more attacks, more leaked records and more varied threats. Yet, by the numbers, 2015 was not a complete disaster. While significant interruptions, shifts in perspective and challenges to the security industry continue to evolve, there are some areas of slowed growth and even improvement.

By the end of 2014, some estimates indicated there were more than one billion leaked emails, credit card numbers, passwords and other types of personally identifiable information (PII) being reported stolen. And today, small shifts to the landscape have been experienced—with cybercriminals focusing more readily on targets of higher-value records such as health-related PII and other highly sensitive data, and with less emphasis on the emails, passwords and even credit card data that were the targets of years past.

The sophistication of attack techniques increased in the year with advances such as overlay malware on mobile platforms, tricking end users into providing personal data as desktop browser web injections had done in years past. Popular attack methods such as distributed-denial-of-service (DDoS) attacks continued to be an attractive means to an end, particularly as a distraction to cover a more targeted attack technique or as a way to demand ransom.

With notable incidents and targeted malware affecting geographies including Canada, Australia, the United Kingdom, France, Turkey and Japan, we look at how attacks adapt to extend beyond borders.

The complexities of doing business at scale, both strategic and technical, create barriers to overcome in preventing these attacks from occurring. A focus on user education and systematic protocols for operating a strong risk assessment program can provide value in that effort.

Let's take a look at some of the notable highlights of this disquieted year and what we might glean for the future.

State of security in 2015: "We take it very seriously!"

Cybercriminals' targets are now bigger, and their rewards greater.

by Jason Kravitz

By January 2015, the connected world was already inundated with a litany of constant data breaches, making it almost too easy to tune out the near daily reports of new incidents. Tuning out, however, was not the appropriate strategy, as existing avenues of attack were adapted and applied vigorously while novel threat techniques and attacks on prominent targets dominated headlines for weeks on end.

The phrase "We take your security very seriously" was an oft-used mantra throughout the year, though it was unfortunately often followed with "but regret to inform you," as hundreds of millions[1] of individuals discovered their private information had been stolen.

A look across the year reveals that the underground demand for leaked data seems to be trending toward higher-value records such as health-related PII and other highly sensitive data, rather than the emails, passwords and even credit card data that were the targets of years past. One of the more disconcerting examples was the US Office of Personnel Management data breach, which resulted in the theft of security clearance information, fingerprints, background check data and comprehensive personal details of millions of federal workers past and present.[2]

Still, lower value records remained in significant demand. For example, the easy availability of millions of email addresses and passwords from previous breaches has led to a number of wide-scale account takeover schemes targeting frequent traveler programs and other services.[3,4] People who reuse passwords across multiple sites face the greatest risk for this kind of attack.

There were, additionally, a number of significant trends in data breaches in 2015. From an industry perspective, healthcare was in the spotlight with a number of high-profile US incidents resulting in the theft of more than 100 million PII records.[5] Malicious advertising (also known as "malvertising") increased throughout 2015.[6] In these cases, infected ads, primarily targeting Adobe Flash vulnerabilities, were served to millions of viewers on popular websites and resulted in the installation of ransomware and other types of malware. Toward the end of the year, a security researcher uncovered a number of misconfigured NoSQL databases that exposed more than 200 million combined records,[7] reinforcing that, more than ever, basic security practices are critical to protecting end-user data.

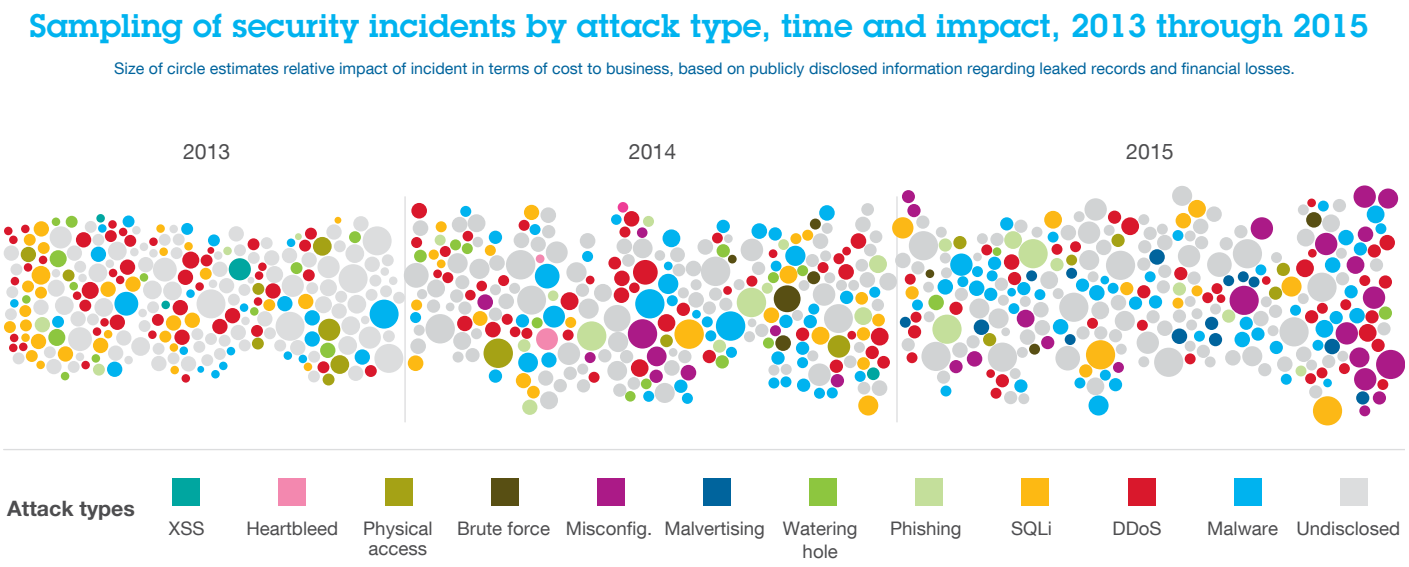

Figure 1. Sampling of security incidents by attack type, time and impact, 2013 through 2015

Figure 1 illustrates a sample of security incidents that occurred between 2013 and 2015. By January 2016, IBM® X-Force® had tracked 272 security incidents for 2015, on par with the 279 incidents tracked in 2014. In terms of total disclosed records, 2014 was notable for more than one billion records being leaked, while 2015 was down to a still staggering 600 million leaked records in incidents tracked by X-Force using public breach disclosures.

As new data breach laws take effect, such as the recent updated mandate in the Netherlands to notify a central authority regarding security breaches, we expect to see the number of reported incidents increase worldwide.[8,9]

Further adventures of POS malware

In 2013 we saw the beginning of a new era of retail breaches with a number of large brands impacted by the theft of data from hundreds of millions of credit card accounts.[10] Since then, attackers have been refining their techniques used to exfiltrate point-of-sale (POS) credit card data using specialized malware. In the United States in 2015, the emphasis seemed to be less on attacking larger retail chains. Instead, a greater number of smaller businesses,[11] POS service providers[12] and niche payment systems were targeted.

Reports surfaced in 2014 about breaches at several large hotel chains and other travel and transportation targets such as airport parking lots. This trend continued into 2015, impacting global hospitality brands including Trump, Starwood and Hyatt hotels, as well as a number of regional resorts, hotels and casinos.[13] Interestingly, in some cases, front desk reservation payment systems were not affected; rather, attackers breached POS terminals in hotel gift shops and restaurants.[14] Other smaller but frequent targets included zoos[15] and other tourist sites.[16] By targeting POS service companies who provide turnkey payment systems to local businesses and restaurants, attackers were positioned to steal credit card data from thousands of retail customers.[17]

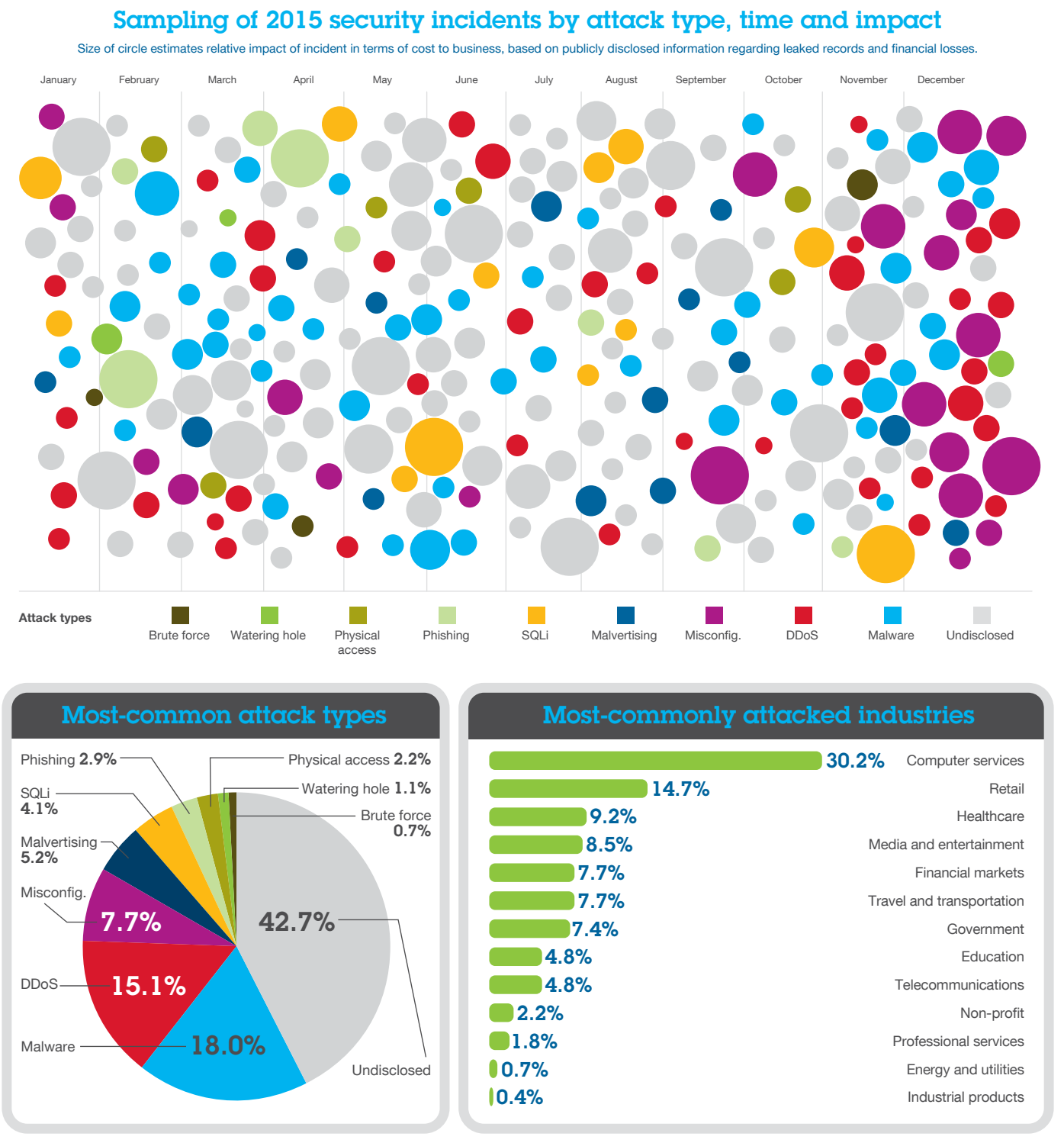

Figure 2. Sampling of 2015 security incidents by attack type, time and impact

In addition to vulnerable point of sale systems, e-commerce retail websites were also at risk due to a vulnerability in the Magento shopping cart platform. It is estimated that months after a patch was released, nearly 100,000 websites using Magento software were still at risk for remote takeover and data loss.[18] This is further evidence that security fundamentals, such as timely application of patches, are essential.

The value of information

February saw the first of five 2015 healthcare mega-breach disclosures, which together exposed nearly 100 million records of patient data.[19] While stolen credit card data and user account information can be valuable, these records have a short lifespan and are replaceable. In contrast, Social Security numbers and health history data stolen in these incidents are both much more sensitive and personal to the victims, as well as much harder to replace. As reported by the recent IBM/Ponemon data breach study, healthcare data breaches cost organizations significantly more than any other industry, as much as USD363 per record compromised, compared to the average for all types of data of USD154.[20]

In addition to the theft of healthcare data, 2015 saw an increase in the trading of another type of highly sensitive information. Breaches at adult websites including Adult Friend Finder[21] and Ashley Madison[22] exposed people's sexual preferences and infidelities to the general public. The intimate nature of this data opened opportunities for extortion and increased social engineering intelligence. It also was linked to a number of suicides of affected victims.[23] More than ever, these incidents bring attention to the complex intersection between our digital and physical identities.

Incidents from digital to physical

The physical effects of online attacks were marked in 2015 by a number of prominent incidents. Security researchers demonstrated how they could remotely take over a vehicle,[24] and attackers successfully disrupted electricity for several days in a region of Ukraine, leaving thousands without power and spotlighting the need to assess critical infrastructure security.[25] Online fraud impacted real-world markets when it came to light that attackers who infiltrated public relations news sites over a five-year period had made more than USD100 million using insider information gleaned from soon-to-be-published corporate press releases.[26] In addition to suffering breached payment systems, the travel industry felt physical impacts of cyber attacks, as seen in the case of a Polish airline. In June, flights were grounded in Warsaw by what was believed to be a DDoS attack that disrupted flight plan computer systems and prevented access to data necessary for departures.[27]

DDoS attacks have been widespread in recent years, and have successfully used increasing amounts of bandwidth to flood targets. Just a few years ago, a 65Gbps DDoS attack was crippling and rare;[28] but in 2015, there were a number of 100+ Gbps attacks,[29] and one reported to be higher than 600Gbps.[30] This sheer amount of traffic affects not only the targeted domain, but can potentially spill over to affect other sites and services managed by overwhelmed Internet service providers.

The success of ransomware schemes targeting end users[31] has laid the groundwork for other types of cyber-extortion. This year saw a rise in DDoS extortion attempts in which attackers threatened website disruptions and demanded a Bitcoin ransom ranging anywhere from the equivalent of a few hundred to tens of thousands of US dollars. Several crime groups such as DD4BC[32] and the Armada Collective[33] targeted a variety of businesses with campaigns that included an attack on several private secure email providers. In most cases, the targeted companies opted not to pay and sustained outages while they tuned their defenses to eventually protect themselves.

Breaches without borders – 2015 overview of global incidents

In addition to the United States, there were a number of high-profile incidents around the world with notable breaches in Canada, Australia, the United Kingdom, France, Turkey and Japan.

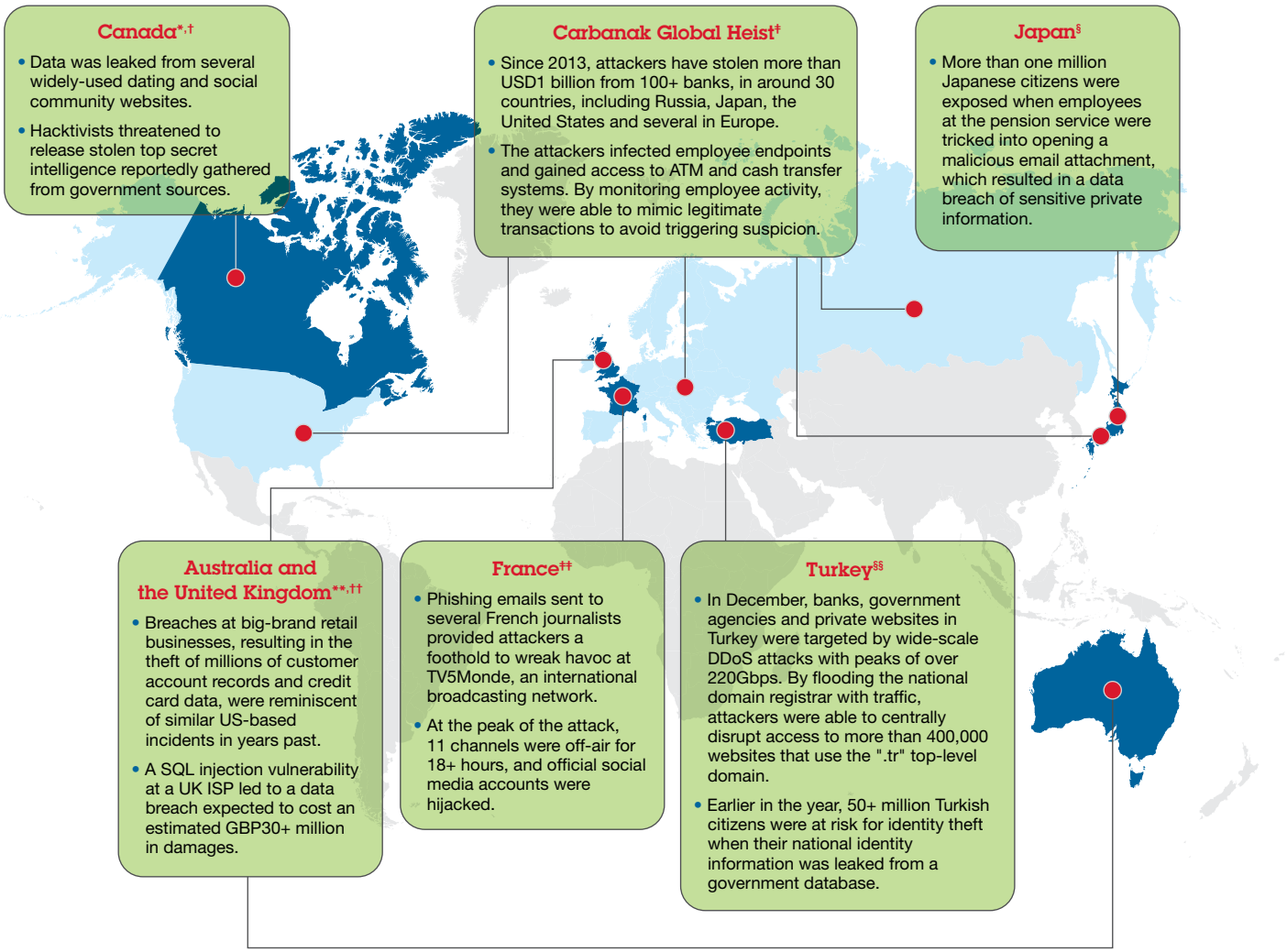

Figure 3: Breaches without borders – 2015 overview of global incidents

* Howard Solomon, "Canadian data breaches in 2105: Big firms weren't the only targets," *IT World Canada*, 21 December 2015.
† Justin Ling, "Anonymous Vows to Keep Leaking Canadian Spy Secrets Over Police Shooting," *Vice News*, 28 July 2015.
‡ "The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide," *Kaspersky Lab*, 16 February 2015.
§ Tomoko Otake, "Japan Pension Service hack used classic attack method," *The Japanese Times*, 02 June 2015.
** Richard Chirgwin, "David Jones follows Kmart into 'we've been attacked' hell," *The Register*, 02 October 2015.
†† John Leyden, "Further confusion at TalkTalk claims it was hit by 'sequential attack,'" *The Register*, 26 October 2015.
‡‡ "'Phishing email' the key to hacking of TV5Monde," *The Local*, 14 April 2015.
§§ Hasan Bozkurt, "Weak state servers breach causes mass identity theft in Turkey; over 50 million citizens' identity info stolen," *DataBreaches.net*, 12 January 2015.

Exploiting the masses

While sophisticated targeted attacks against top organizations generate headlines, attacks of opportunity, which are effective because they cast a wide net, still proliferate. Throughout 2015, millions of visitors to popular sites such as dating communities[34] and mainstream media[35] were exposed to malicious advertising capable of installing ransomware and other malicious software on the end users' systems. These malvertising campaigns are successful due to the inability of advertising networks to adequately review source code before publishing the ads. Malicious ads can be designed to appear legitimate, clear initial analysis and then, once published, redirect visitors to infected or malicious servers that expose users to exploit kits such as the ever-popular off-the-shelf Nuclear[36] or Angler.[37] These attack tools are capable of exploiting of a variety of browser and browser plug-in vulnerabilities to deliver their payload.

Users who don't patch their systems or who run outdated software were most at risk for these types of attacks, though poor security practices affected vendors as well. As developer tools and frameworks become easier to implement, the barriers end users face when creating scalable applications and websites drop. With reduced barriers to entry, more less-experienced developers enter the fray, and the risks of unsafe development increase. For consumers, it is worth remembering that the fact that an application is popular or has millions of users does not mean it is safe. The dangers of rapid development without proper controls or expertise were evident this year. For example, using the Shodan search engine, a security researcher uncovered and disclosed a number of multi-million record databases that were completely open to public browsing with no authentication required.[38]

These vulnerable services used NoSQL databases, which are an excellent solution for creating highly scalable applications and websites, but—when set up without proper permissions—can be a major source of data loss. Some of the affected services stored sensitive healthcare information; another was a forum for a popular children's brand, which contained personal data on more than 200,000 children.[39] One of the most significant

discoveries was an open database that had no discernible affiliation to any organization and contained 191 million US voter records with information such as names, birthdates, political affiliations and logs of whether individuals voted in primary or general elections potentially exposed.[40]

Final thoughts

A televised report filmed inside the offices of a French broadcasting network following a major breach showed sticky notes with account login information taped to an employee's monitor.[41] This lapse in basic security hygiene is indicative of the challenges facing the security industry today. We live in an increasingly connected world where users must understand the importance of a culture of security in the enterprise and at home.

While millions of leaked data records make interesting graphics and statistics, the human impact from all of this stolen data is not always apparent. Breaches and data theft are a powerful warning, however, about the need for proper online behavior—and the effects of improper behavior—as everyday life becomes inseparable from connected devices and stores of personal information. As the dusty corners of our online identities are opened to the physical world, we must hold those we trust to protect our data—ourselves foremost—more accountable.

Cybercrime's epic year

Criminals are chasing opportunities everywhere—and affecting everyone.

by Limor Kessem

Looking back at cybercrime in 2015 leaves little doubt that the year was nothing short of epic. The IBM/Ponemon Institute report *2015 Cost of Data Breach Study* put the average total cost of a data breach at USD3.79 million, an increase from the 2014 figure of USD3.52 million.[20] Another 2015 study projects that cybercrime will become a USD2.1 trillion problem by 2019.[42] That's only three years away, and judging by the way trends and events are going, we might get there sooner than we imagine.

In 2014, IBM Security forecast some trends we anticipated for 2015.[43] They included:

- Cybercrime breaking borders[44]
- Rising card-not-present (CNP) fraud
- An escalation in the sophistication of mobile threats
- Wide use of anonymity networks and stronger encryption
- Burgeoning fraud methods for new payment schemes
- Biometrics becoming a target

These predictions not only materialized, but actually exceeded the forecast. We expect the situation to become very intense in 2016 as more organized crime groups step up their presence in the digital realms.

The mob, digital edition

It is safe to say that we have never before seen the magnitude and sophistication of online crime as we did in 2015—a trend that's already proving to persist into 2016. This prompts us to ask: What is the one most significant factor contributing to cybercrime's escalation in scale and sophistication?

The answer lies in the increasing involvement and investment of full-blown criminal organizations in digital crime, and the resulting increase in numbers of well-orchestrated operations such as Carbanak.[45]

These gangs operate much like businesses, leveraging connections, employing collaboration and deploying teams for different tasks.

Organized cybercrime is no longer made up primarily of small factions, and the days of lone hackers are all but gone. Instead, nowadays we fight against motivated organizations that—like legitimate businesses—are divided into teams, employ highly experienced developers with deep knowledge, leverage connections and encourage collaboration. Also like businesses, these gangs are highly organized, managed by crime lords who fund the operation and deploy various types of troops to achieve their eventual success.

Given this highly organized structure, perhaps the level of sophistication shown in malicious code such as Shifu,[46] for example, should be no surprise. After all, the security and risk management site CSO reports that the average age of a cybercriminal is an experienced 35 years, and 80 percent of blackhat hackers are affiliated with organized crime and work as part of groups.[47] In fact, the same article notes, according to some experts "disorganized cybercrime" no longer exists.

The inner workings of gang-controlled malware exposes the organization and order behind the scenes, with professional programming techniques built into the malware, as well as professional development processes such as change tracking, versioning and application security.

Information security headlines throughout 2015 also often remarked upon the unprecedented modularity of malware that had been less complex before—for example, point-of-sale (POS) malware such as ModPOS,[48] or the JavaScript-based ransomware known as Ransom32 that can be deployed across different platforms.[49] It is no coincidence that malicious code is seeing such a hike in sophistication, however. The promise of a hefty return on investment (ROI) draws organized crime to fund them and lures brilliant minds into the dark world of digital crime.

A scan of the cybercrime events related to financial malware that marked 2015 immediately recalls names such as Dyre,[50] Shifu,[44] Dridex,[51,52] CoreBot[53] and URLZone2,[54] to name only a few, all of which are malicious codes operated by closed groups that develop and exclusively use these Trojans.

The top 10 list of malware code listed in figure 4 below reveals, in fact, that cybercrime is no longer the domain of amateurs. While lone hackers and small factions continue to use the Zeus code for their fraud attempts, the more impactful cybercrime is beyond doubt the domain of organized gangs.

This is a shift from the situation in 2014, when the Zeus Trojan topped the chart as most rampant, being a code that was publicly leaked and used by many different fraudsters across the globe, most of whom have no way to fix bugs in the malware and no way to further develop the code.

Top financial malware gangs – global 2015 vs. 2014

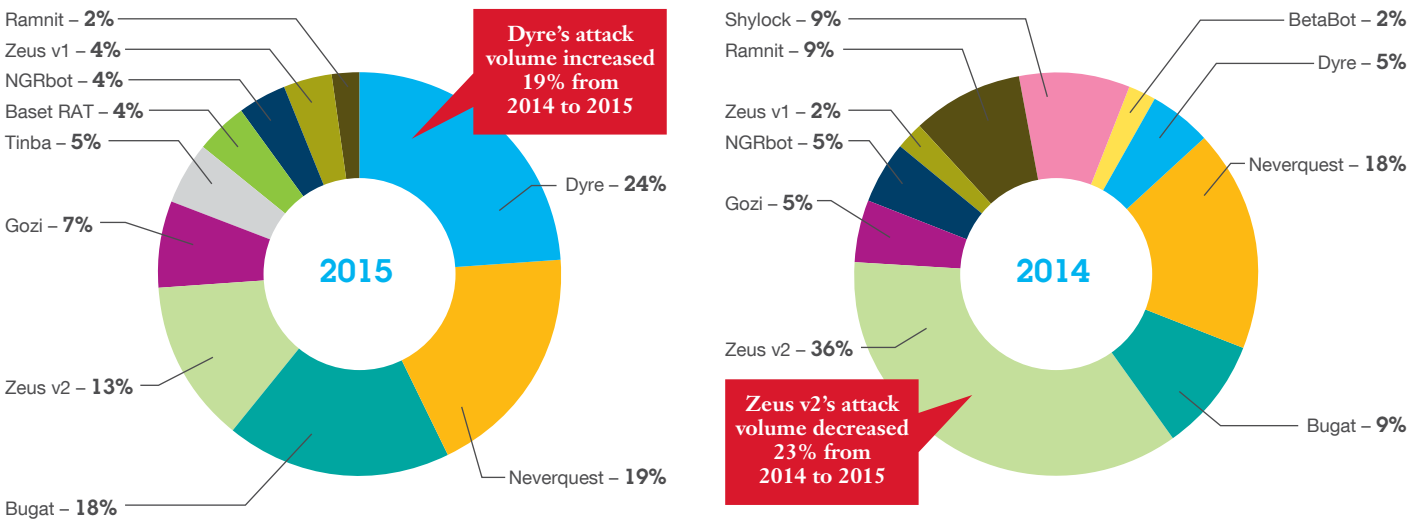

Figure 4. Top financial malware gangs – global 2015 vs. 2014

Beware! Malware crossing

Tracking the evolution of malware and the groups that operate banking Trojans shows that organized cybercrime gangs acquire and move resources to different parts of the globe when they believe they will see success in new regions.

While malware configurations are easy to change, and target lists can be quite dynamic, Figure 5 illustrates the geography crossings that were the most significant cases we took note of in 2015.

The reason these geographical leaps are indicative of increasing sophistication and organization is that they required more than simple changes to configuration files. In each one, malware operators had to go through a preparatory stage to adapt their attack components to the new target geography. They also had to develop or buy email addresses for social engineering in the target geography, rent or pay for spam spreading, study local banks' authentication requirements, develop web injections to correspond with the transaction flow for each target and have local money mules ready to use.

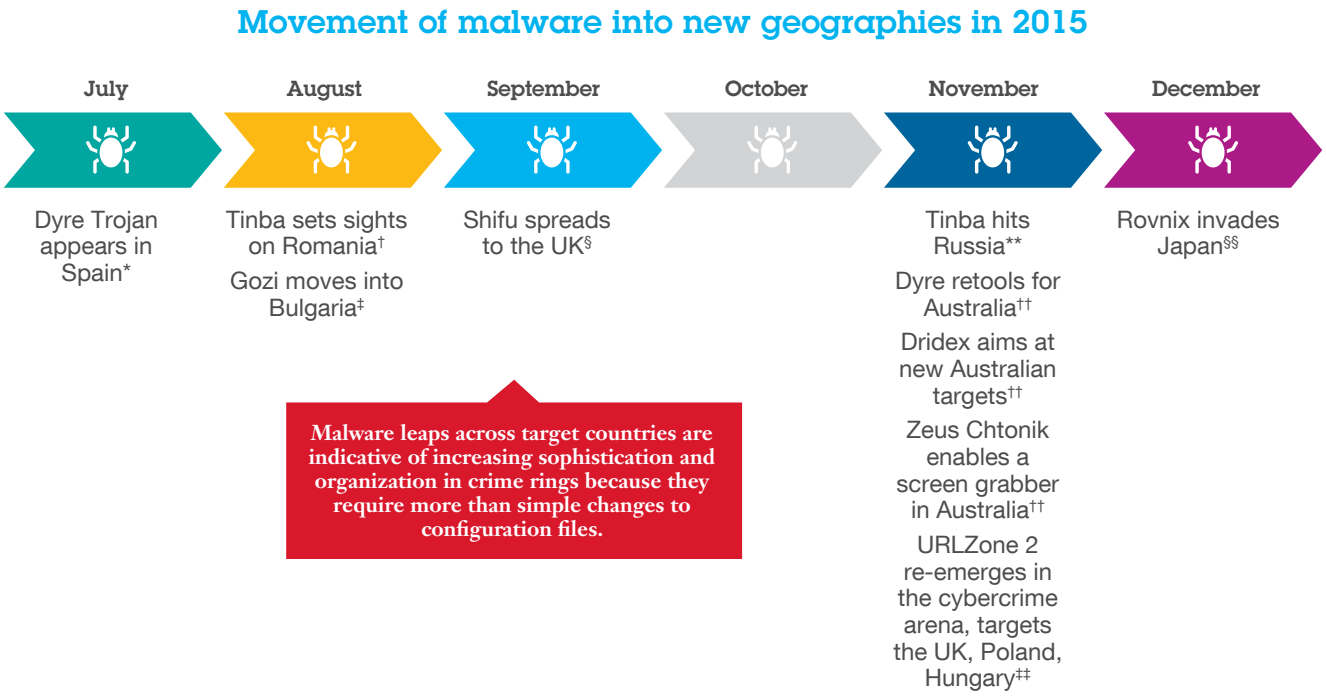

Figure 5. Movement of malware into new geographies in 2015

* Limor Kessem, "Dyre Malware Takes Summer Holiday in Spain," *Security Intelligence*, 14 July 2015.
† Limor Kessem, "Tinba Trojan Sets Its Sights on Romania," *Security Intelligence*, 12 August 2015.
‡ Limor Kessem, "Gozi Goes to Bulgaria — Is Cybercrime Heading to Less Charted Territory?" *Security Intelligence*, 18 August 2015.
§ Limor Kessem, "Shifu Officially Spreads to the UK: Banks and Wealth Management Firms Beware," *Security Intelligence*, 28 September 2015.
** Eduard Kovacs, "Tinba Banking Trojan Targets Russia," *SecurityWeek*, 04 November 2015.
†† IBM X-Force Malware Research team.
‡‡ Limor Kessem, "Organized Cybercrime Big in Japan: URLZone Now on the Scene," *Security Intelligence*, 01 February 2016.
§§ Limor Kessem, "Konnichiwa, Rovnix! Aggressive Malware Hits Japanese Banks," *Security Intelligence*, 07 January 2016.

For example, the most resource-intensive adaptations include Shifu's schemes when it launched its attacks in Japan and then adapted for the UK. In its new, UK-dedicated samples, Shifu no longer injects into the explorer.exe process. Rather, it has modified its action path to launch a new svchost instance and performs all actions from that process instead.[55] Another case that demanded a lot of planning was Rovnix's move from attacking banks in Europe for the past few years, to targeting banks in Japan.[56]

Before the Dyre Trojan began attacking online banking users in Australia and New Zealand, the Dyre operators most probably sent or hired a small group of people to set up an operation locally in those regions. Dyre's configuration files were very telling because:

- The bank URLs that Dyre targeted led to portals for business banking, corporate banking, treasury management and high-value accounts.
- Dyre harvested credentials for local hardware vendors.
- Dyre harvested credentials for local hosting vendors.
- Dyre targeted the advertisers' section of job recruitment sites.

It is no surprise that all these activities can facilitate setting up a local malware server to allow the Dyre team, which is known to be mostly located in Eastern Europe, to operate in Australia and New Zealand.

These Trojan migration feats are typically undertaken primarily by large, closed cybercrime groups. The planning and resources they require suggest that smaller groups would have trouble affording them or creating the necessary local connections with cybercriminals in countries where they never operated before.

Gangs scale up attack magnitude across the board

If there was one trend that stretched across all cybercrime domains in 2015, it was the scaling up of the magnitude and breadth of each malware-related transaction and operation. Every type of malware cyber attack last year—from ransomware to banking Trojans, and from cyber-extortion to targeted attacks—scaled up its per-hit quota. Cybercriminals accomplished this goal by shifting some of their focus from attacking individual consumers, to targeting businesses.

As they shifted to focus on larger rewards, malware groups such as Dyre updated their malicious code with new modules such as "pn32," which is designed to harvest administrative user credentials for enterprise email servers. We suspect that this sort of development was not only part of the process of fraudulent transactions from the corporate account, but also was further designed to enable the gang behind Dyre to target victims with Business Email Compromised (BEC) fraud.[57]

BEC fraud occurs when blackhat hackers compromise business email or enterprise email servers, then use social engineering to send a credible-looking email to the company's accountant or treasurer with instructions to promptly make a large wire transfer. The emails typically purport to come from the CEO or CFO, and sums involved can typically reach USD1 million at a time.

In the context of scaling up the magnitude of attacks by targeting businesses, two striking cases demonstrate just how brazen and well-organized cybercrime has become—first the Dyre Wolf attacks, which use the Dyre Trojan against corporate banking accounts,[58] and second the Evil Corp. attack on Penneco Oil, which used the Trojan known as Dridex.[59]

In each of these cases, malware operators combined the characteristics of a targeted attack with the abilities of Trojan-enabled online banking fraud. Subsequent conversations IBM researchers had with affected victim organizations made it clear that the cybercrime groups that launched these attacks prepared an elaborate social engineering scheme before the actual attempt.[60]

Preparations included moving money from other, smaller accounts the company held to the account owned by the same company the cybercriminals planned to rob; establishing special toll-free numbers for the victims to call; assigning an eloquent, professional sounding "banker" with prior information about the account to speak to the victims; and setting up the type of mule accounts that could receive a large amount of money in one transaction without raising suspicion.

The structured nature of the attacks, combined with having these resources and persons in place to smooth the way for each step of the operation, were the top factors that enabled cybercriminals to successfully rob corporate accounts of millions of US dollars in each case. These attacks marked record highs for cybercrime transactions with a magnitude that far exceeded what we have seen in previous years.

The Dyre Wolf and Evil Corp. attacks were both considered more complex and calculated than the illicit transactions that typically use Dyre or Dridex for online banking fraud, but they were not the only ones where we saw with an increased magnitude.

On the advanced persistent threat front, the Anunak gang managed to amass a reported USD1 billion in illicit profits in the "Carbanak" case[45]—the name given to the malware used in the operation to indicate a cross between Anunak and Carberp code. No digital heist before Carbanak grossed such an amount, and never in such a short time. This stealthy advanced persistent threat attack had gone unnoticed since the end of 2013. It was highly active yet remained undetected. Initial infiltration was facilitated by spear-phishing emails and exploit-laden attachments that compromised employee endpoints with malware, eventually stealing credentials, taking over their endpoints and abusing their user privileges.

Ransomware groups, such as the perpetrators of CryptoLocker (which, in fact, is believed to be wholly controlled and operated by a single crew[61]) reportedly managed to gross an estimated USD300,000 to 30 million in only 100 days.[62]

The most significant cyber-extortion case of 2015, though, may be the case of "TalkTalk." This UK-based telecom group fell victim to a group of blackhat hackers who penetrate organizations with the goal of taking their data hostage and demanding a ransom for its return.

The attackers gained access to the personal and financial details of more than 150,000 TalkTalk customers,[63] then contacted the company with a demand for GBP80,000. Although the ransom alone was relatively easy to pay in order to regain access to TalkTalk's data, the total damage to TalkTalk could be up to GBP35 million in "one-off costs," including lost revenue, costs to respond to the incident and additional IT costs, the chief executive of the business has said.[64] Never before has a cyber-extortion case reached such magnitude and collateral effect, and never has there been this level of public awareness regarding the harm that can come to companies whose digital assets are held for ransom.[65]

A collaborative bunch

Also in 2015, yet another interesting trend emerged that was specific to the attack campaigns by organized cybercrime groups and became progressively more evident in attack campaigns researched by IBM X-Force during the year. The cybercriminal elite, especially those located in or operating out of Eastern Europe, often work with stealthy service providers who supply them with infrastructure, services and crime-specific commodities—a development that has become known as "crimeware as a service" (CaaS).

The use of CaaS became more evident when malware such as Shifu, Neverquest, Dyre and Dridex began to fetch web injections in real time from the same rogue servers. Analysis of actual attacks with these Trojans revealed that exactly the same internal schemes (techniques, tactics and procedures) were being used, in exactly the same geographies.[60]

The identical web injections were not the only commonality, either. In some cases, malware spam and communications came from the same servers used by both Dyre and Dridex, hinting to a possible collaboration or commercial relationship between the gangs, or perhaps to infrastructure they rent or otherwise use with the cooperation of another group.

If those commonalities were not evidence enough, the Dridex Trojan has been operating in the past year in ways that closely imitate Dyre. Beyond mimicking Dyre's attacks on corporate accounts, Dridex launched new attacks in early January 2016 that emulate Dyre's redirection schemes. Redirection attacks rely on bank site replicas prepared in advance for each targeted brand. This represents a considerable investment made by the Dridex crew, bought from those who operate Dyre, or perhaps purchased by Dridex and Dyre operators together from the same crimeware supplier. Curiously enough, in both cases the entire list of targets is for potential victims located in the UK.

Collaboration in the underworld of cybercrime can come in other shapes as well. Take Shifu, for example. This malware, which is believed to have been created by Russian-speaking authors, includes large chunks of code and features copied from other malware such as Zeus and imitating other malware such as Corcow.[66] Copying features from Zeus is an everyday occurrence, since the Zeus v2 code was long ago publicly leaked. But Shifu also used code-specific data theft techniques that were part of the Corcow malware,[67] for example, which is believed to be a privately owned Trojan.

What does organized crime get from this sort of collaboration? As is the case for any exclusive marketplace, it provides criminals with services that are specialized, available, high-quality, trusted and that evolve with their needs. These services in turn accelerate the ability of cybercrime groups to attack in new geographies without each group having to invest a large amount of time creating the tools and locale-specific language collateral. It also gives the groups access to tools that are tested and true.

According to X-Force research findings from actual attacks, groups like Dyre and Dridex have their own internal development teams. That blackhat team programs the more complex components of the Trojan's activity, including the downloaders, the actual malware, the configuration file and the communication encryption schemes.

For example, as soon as Microsoft Windows offered free consumer upgrades of Windows 10 in late 2015, the Dyre and Gozi Trojans promptly updated their codes to deploy properly on Win10 machines, and to successfully inject into the new Microsoft Edge browser. When it comes to the user interface with the victim, X-Force researchers believe the same gangs outsource the code writing to a shortlist of trusted blackhat vendors. Those supplier factions specialize in web injections and sell a software-as-a-service (SaaS) model to cybercrime gangs, adapting off-the-shelf fraud schemes to the targeted online banking platform and country the gang dictates. This information comes from malware configuration files where the Trojan dynamically fetches injections from a remote server. X-Force researchers noted the cases of different malware families communicating with the same remote server to get and deploy the same web injections and display them to the victim.

Mobile malware's quantum leap

Cybercriminals looking to monetize malicious code by targeting mobile devices have long attempted to devise malware that will enable the same fraud scenarios on mobile devices that Trojans enact on PCs.

Although blackhat developers came into the mobile platform with experience and concepts learned from existing PC malware, the crossover to mobile has not matured all that rapidly. The quest for malware that can attack the mobile platform has been ongoing for the past decade, as malicious mobile applications progressed slowly from plain short message service (SMS) hijackers to spyware, remote access Trojans (RATs) and eventually their first true breakthrough in 2015: overlay malware.

From sneaky screen switches to pop-up animation tricks, overlay malware on the mobile operating system is what web injections are to the PC. Though lacking the same sophistication and actual "'injection" effect (as in its PC counterpart), overlay Trojans nonetheless implement a convincing social engineering effect that can fool users into divulging e-payment login details, online banking credentials and payment card details right from their compromised device.[68]

The strength of this type of mobile malware, which emerged in underground boards in the first quarter of 2015, is that it turns the device into a "one-stop shop" for fraudsters. With one overlay malware application, cybercriminals can harvest victim credentials in real time, listen for two-factor authentication codes sent via SMS, or even forward authorization calls to their own numbers in order to complete fraudulent transactions.[69] Attacking users on the mobile device can facilitate account takeover and card fraud at a much lower cost to the criminals, and at a lesser risk of being exposed compared to the costs of amassing and running a PC-based botnet.

Cybercriminals targeting mobile devices typically use malware that was sold to many different actors, making attribution more difficult to ascertain.[60] What's more, when mobile botnets are set up, they use Voice over IP (VoIP) lines and mobile numbers to receive the stolen data from compromised devices. The cybercriminals register these resources with fake names, under bogus addresses. Just as Trojan communication domains can be registered in a different part of the world, mobile botnet resources do not readily lead to the actual actor behind them, especially if they are located in Eastern Europe.

Overlay malware is considered to be the next quantum leap in mobile threats, and this emerging technique is rapidly gaining popularity and prevalence in the wild.

Today, overlay malware is created and sold by blackhat mobile developers in underground communities. They are commoditized into service offerings that include the rental or purchase of the malware, a botnet administration panel, application customization, the necessary operational resources (including hosting, servers and IP-based phone numbers) and 24-hour technical support services.

This CaaS business model for mobile malware is very reminiscent of how commercial Trojans for PCs used to be peddled in the underground until a few years back. By design CaaS enables newcomers to take on the operation of mobile botnets designed for online financial fraud easily for a few Bitcoins, and then watch their operation in real time on a web-based dashboard.

Mob in the mobile

Ever since they began to realize exorbitant profits from online fraud, organized cybercrime has not missed a beat—and it continues to closely follow trends and exploit them as much as possible before security catches up.[70]

The mobile arena is one such trend that organized cybercrime finds lucrative enough to pursue. Take for example the SlemBunk malware—a multiple-stage Google Android Trojan designed to display overlay screens on bank application windows.[71] SlemBunk's code and deployment methodology are quite professional, involving drive-by-downloads and legitimate Android application packages (APKs) for camouflage—all of which suggest a well-organized, evolving threat. Unlike other malware of this sort, which may be operated by opportunistic customers of a CaaS operation, SlemBunk is more likely to be owned by a closed crime group.

On to 2016…

While every year in the past two decades showed an escalation in cybercrime, 2015 was particularly eventful. Attacks such as Carbanak, Dyre Wolf and Dridex on corporate bank accounts made 2015 stand out as some of the grandest digital crimes we have ever seen.

As we kick off 2016, we expect the intensity of threats and increasing sophistication of malware to continue trending upward.[72] IBM Security research teams can help you keep up to date on the trends that matter to your organization—as soon as they emerge.

Vulnerabilities disclosed in 2015

With vulnerabilities commonplace, every organization must better handle the risk.

by Scott Moore, Leslie Wiggins and Vikalp Paliwal

Since 1997, IBM X-Force research and development has been tracking public disclosures of vulnerabilities in software products, a 20-year span of software development. X-Force researchers collect software advisories directly from vendors, subscribe to security-related mailing lists, and analyze hundreds of sources where vulnerabilities and known exploits are disclosed, and where remedial actions are presented.

Our mid-year study, *IBM X-Force Threat Intelligence Quarterly, 3Q 2015*, reported just over 4,000 new security vulnerabilities, with projected estimate of 8,000 total vulnerabilities for the year. In the second half of 2015 we saw an increase in disclosed vulnerabilities for a total of just under 9,000. This represents the highest number of vulnerabilities the X-Force team has seen and recorded in our database. That number doesn't include the roughly 1,400 secure socket layer (SSL) vulnerabilities in Android applications that were discovered using an automated tool by US-CERT in 2014 (seen highlighted in the 2014 first quarter report) and that received a Common Vulnerabilities and Exposures (CVE) identifier.

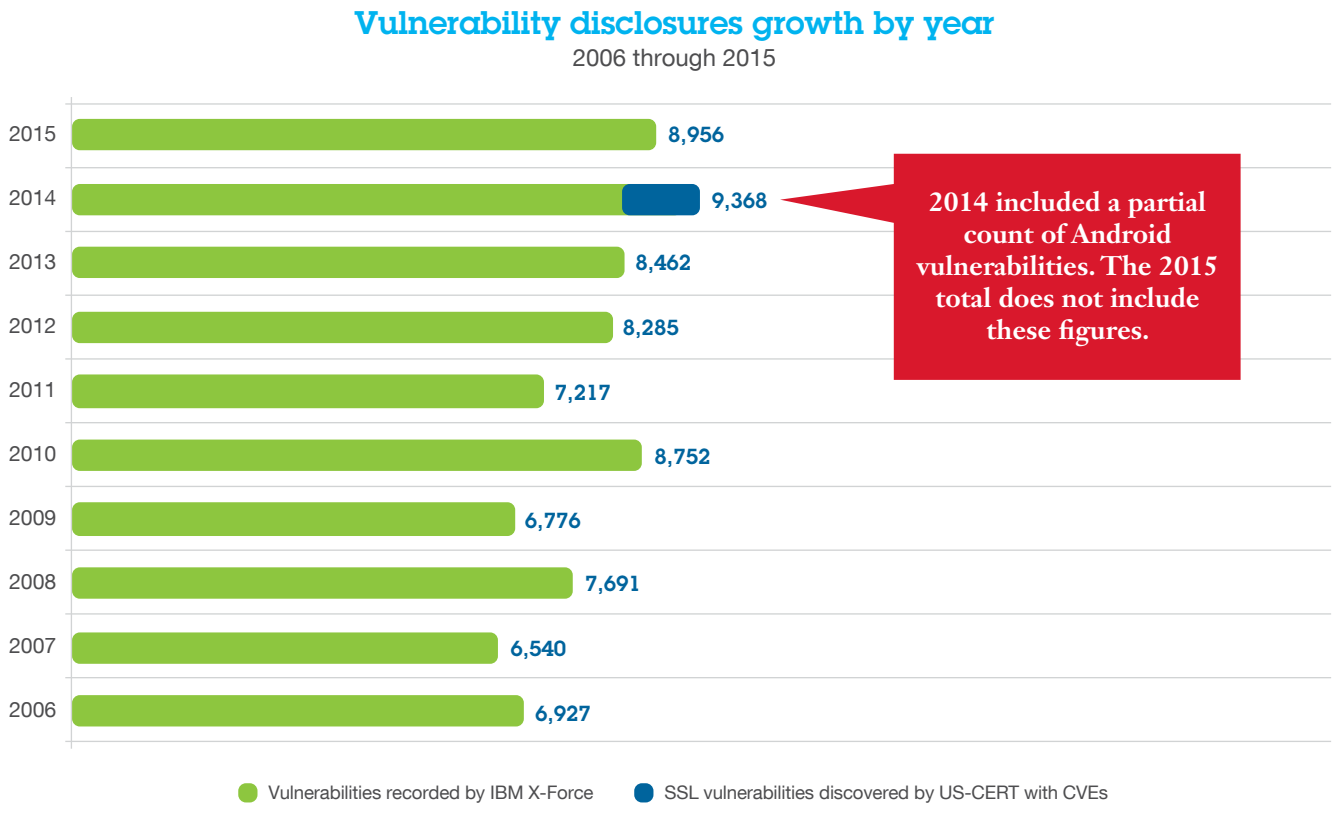

Figure 6. Vulnerability disclosures growth by year, 2006 through 2015

Assessing risk with threat intelligence

These days, data security breaches are more common than ever—and more costly to the victim. The latest research shows that the average total cost of a corporate data breach is now USD3.79 million.[20] With an increase during 2015 in the number of company records stolen, organizations suffered loss of sensitive data, compromised brand reputation and huge costs.

In response to persistent and increasing data breaches, governing bodies around the world have enacted regulations such as the US Health Insurance Portability and Accountability Act (HIPAA), the industry-mandated Payment Card Industry Data Security Standard (PCI DSS), the European Union's Data Protection Directive, the Australian Privacy Act and Japan's Personal Information Protection Act (PIPA). Although the specifics of the regulations may differ, they generally strive to protect sensitive data (such as information about consumers or patients), and failure to comply can result in significant financial penalties, criminal prosecution, or damage to a company's brand, loss of customer loyalty and decreased revenue.

Addressing the security vulnerabilities of data repositories, therefore, should be part of every organization's basic security best practices. However, each year X-Force encounters numerous instances of system vulnerabilities left unpatched or unaddressed during investigations. With several security incidents and announcements related to vulnerable software or services, 2015 was no exception.

X-Force regularly identifies security incidents that are a result of conditions such as weak password policies, excessive privileges, missing patches, denial-of-service attacks, data server misconfigurations, lack of encryption and more. Unpatched vulnerabilities that are known to the world can be easily exploited, resulting in substantial costs. Identified vulnerabilities should be assessed, prioritized and remediated promptly to mitigate potential risks of data breaches, failed audits, loss of compliance, and erosion of customer trust. In spite of these risks, some organizations do not have processes in place to effectively assess and remediate vulnerabilities or to minimize damages to their organizations and their customers.

In our experiences working with clients and prospects, X-Force has seen that many organizations do not sufficiently monitor published vulnerabilities that may affect the technology protecting their data—and as a result, they may be ignorant of the risk and impacts of a data breach. There are common reasons, however, why organizations are in the dark about these exposures and risks, including:

- They don't know all the sources of their data because they lack an asset inventory.
- They don't understand how critical their vulnerabilities are or the danger they pose to effectively supporting and growing the business.
- They intend to do a vulnerability scan to identify risks and remediate vulnerabilities, but, because they don't understand the depth of the risks they face, they never get around to taking action.

Vulnerabilities in major databases, 2011 through 2015

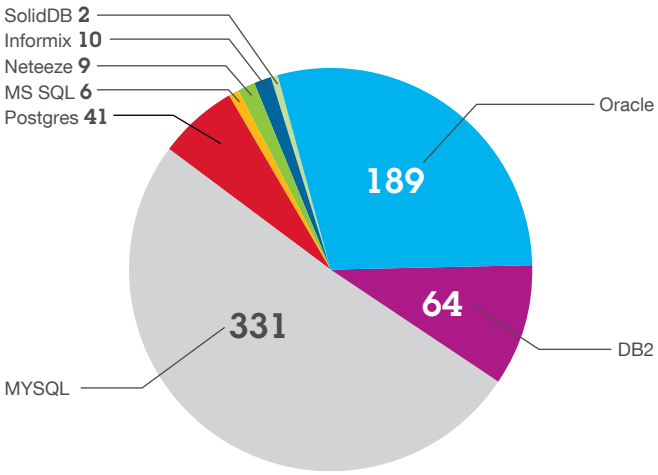

Figure 7. Vulnerabilities in major databases, 2011 through 2015

Covering more than 18 years of vulnerability data, the X-Force database is expected to surpass

100,000 entries

in Q1 2016.

X-Force provides a simple yet effective way to help organizations mitigate the problem of risk identification by researching and analyzing advisories, vulnerabilities and exploits and cataloging the findings in a database. This resource now contains more than 97,000 publicly disclosed unique vulnerabilities and provides the foundation for the IBM Security Network Protection platform. Comprising more than 18 years of vulnerability data, the X-Force database is expected to surpass 100,000 entries in the first quarter of 2016. Organizations can quickly and easily subscribe to IBM X-Force Exchange to get information about the latest published vulnerabilities. X-Force Exchange is a single platform for all publicly disclosed vulnerabilities including data repositories such as IBM DB2®, Oracle Database, Microsoft SQL Server and others.

Security administrators must address open vulnerabilities to minimize the risk of data breaches. From 2011 until year-end 2015, X-Force researched and published information on more than 652 vulnerabilities for data repositories including DB2, Oracle, SQL Server and more. Each published vulnerability comes with a Common Vulnerability Scoring System (CVSS) score, to help security teams assess the severity of the vulnerability. Taking into consideration the CVSS score, together with the data platforms affected and the type of data at risk, the security team can plan their response and prioritize fixes for the most serious vulnerabilities. This helps businesses protect themselves from becoming a target for exploitation. Identifying vulnerabilities in X-Force Exchange is a good first step to kick off this process.

The dangers of building databases for scale, not security

As big-data analytics becomes increasingly popular and increasingly adopted, one of the trends prominent in 2015 was that NoSQL and Hadoop data sources, which are the two main platforms that support big-data analytics, are now appearing more and more frequently in organizations' IT landscape.

The world is becoming smaller and more connected with the prominence of mobile applications. As mobility takes over from traditional platforms, mobile applications contribute massive amounts and types of data into the big-data environment at extremely high rates. Mobile banking, payment and ordering services for on-the-run end users, for example, create huge volumes and varieties of data in real time. Not only is this data "big," it is frequently sensitive—and because it arrives so quickly, in such large volumes and variety of formats, it creates new, more intense challenges for managing data privacy and securing sensitive information. Making matters worse, applications are regularly being deployed via continuous delivery on tight schedules, and developers who may lack a security focus may not have the expertise or the time to identify and address vulnerabilities. This is good news for attackers, who can easily exploit those vulnerabilities. Without proper defense of data sources, businesses offering these services can be increasingly exposed to the risk and threat of a data breach.

Organizations should run vulnerability assessment scans on their data sources to understand the vulnerabilities that exist in the data environment, as well as to understand their overall risk posture. Based on the evidence they develop, security teams should prioritize their vulnerability types and address the most critical data sources first, taking steps to completely remediate and secure (or harden) the data source. These measures also help manage and support compliance requirements for regulations such as PCI DSS, HIPAA and Sarbanes-Oxley, as well as help protect PII.

Companies that have taken advantage of the ability of NoSQL databases to create highly scalable applications and websites also must be aware of vulnerability—because when NoSQL databases are configured with default settings or don't have the proper permissions, harmful effects can occur. For example, several of the known vulnerabilities in NoSQL MongoDB are related to factors that include lack of data encryption, lack of proper authentication and authorization processes; excessive privileges provided to users, and lack of mitigation for denial-of-service concerns.

Specifically, one of these known vulnerabilities for NoSQL database MongoDB (CVE-2015-1609), publicly released in 2015, exposes unpatched databases to a denial-of-service attack via a specially crafted UTF-8 string in a BSON request.

Notable areas of concern for database security

While all vulnerabilities can be harmful to the organization that's facing exposure and risk, here is a quick look at a few specific types of vulnerabilities that came to light in 2015.

Example of a vulnerability with excess privileges

In 2015, multiple vulnerabilities for SQL Server were announced. One in particular, CVE-2015-1761 was related to a SQL Server elevation of privilege. An elevation of privilege vulnerability exists in SQL Server when it improperly casts pointers to an incorrect class. An attacker could exploit the vulnerability if he or she possesses credentials that allow access to an affected SQL Server database. An attacker who successfully exploits this vulnerability could then gain elevated privileges that could be used to view, change or delete data, or to create new accounts. The elevation of privileges such as DB_securityadmin and DB_owner allows database ownership roles to be granted to users.

Since the vulnerability is exploitable only within the context of very specific database schema, data and queries, exploitation can be prevented by strictly controlling who has permissions to create databases and schemata on the server. Note that the vulnerability is exposed in very specific cases. The security update from Microsoft addresses the vulnerability by correcting how SQL Server handles pointer casting.

Example of a remote exploit vulnerability

Another notable vulnerability in 2015 was identified for Oracle Database Server (CVE-2015-4863). The CVSS score of 10 for this vulnerability carries a very high risk if not corrected because it concerns an unspecified vulnerability in the Portable Clusterware component in Oracle Database Server v11.2.0.4, v12.1.0.1, and v12.1.0.2 that could allow remote attackers to affect confidentiality, integrity and availability of the database and its contents. This easily exploitable vulnerability could allow unauthenticated network attacks via Oracle Net. Successful exploitation of this vulnerability could result in unauthorized operating system takeover including arbitrary code execution. Oracle provided a security patch organizations can apply to remedy the vulnerability and protect themselves from these risks.

Final recommendations

Attackers continuously change, evolve, and improve their techniques and their technology—and it can be extremely challenging to keep up with the new and sophisticated threats. To help you keep up to date, X-Force researches the vulnerabilities publicly disclosed every day, and enters that information into the X-Force database. By researching threats and vulnerabilities included in this database, you can better understand the technical details of the vulnerabilities and determine appropriate remediation to help protect your company's assets. Vulnerability assessment and remediation are good first steps that can help organizations take control of the security of their sensitive data. Don't sit idly by and let your open vulnerabilities be exploited. Review the latest published list of vulnerabilities via the IBM X-Force Exchange platform and consider using a data security product such as IBM Security Guardium® to help you automate the vulnerability identification, prioritization and remediation process.

About X-Force

Advanced threats are everywhere. Help minimize your risk with insights from the experts at IBM.

The IBM X-Force research team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats.

IBM Security Services: Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data, and safeguard cloud and mobile. Should you experience an IT security breach, IBM Emergency Response Services can provide real-time on-site support, including intelligence gathering, containment, eradication, recovery and compliance management. IBM Active Threat Assessment consulting services can help you identify hidden but active cyber threats before serious damage occurs to your infrastructure or even your brand. IBM Incident Response Planning can help you structure a cyber-security incident response plan (CSIRP) that incorporates the right processes, tools and resources you need to respond to and help reduce the impact of a cyber attack. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

A number of groups and products within IBM, such as the IBM Security Trusteer® portfolio of solutions, use this rich data to develop protection techniques for our customers. With this report, X-Force now adds IBM Security Guardium, formerly known as IBM InfoSphere Guardium, a solution designed to safeguard critical data, wherever it resides. This comprehensive data security platform—which includes capabilities such as sensitive data discovery, classification, vulnerability assessment, entitlement reporting, encryption, masking, redaction, outlier detection, and more—empowers security teams to automatically analyze what is happening across the data environment to help minimize risk, protect sensitive data from internal and external threats, and seamlessly adapt to changes that affect data security.

Contributors

Producing the IBM X-Force Threat Intelligence Report is a dedicated collaboration across all of IBM Security. We would like to thank the following individuals for their attention and contribution to the publication of this report.

For more information

To learn more about IBM X-Force, please visit:
ibm.com/security/xforce/

Author

Jason Kravitz	**IBM Security, X-Force Research and Techline Pre-Sales** Jason has been researching and reporting on data breaches since 2011 and is the creator of the IBM X-Force Interactive Security Incidents data visualization website.
Limor Kessem	**Senior Cybersecurity Evangelist** As a member of the IBM X-Force team, Limor is one of the top cyber-intelligence experts in the IBM Trusteer organization. She is a seasoned speaker and a regular blogger on SecurityIntelligence.com, and participated as a highly appreciated speaker on live InfraGard New York webcasts. She has spoken at security events worldwide, conducts live webinars on all things fraud and cybercrime, and writes a large variety of threat intelligence publications. Limor is considered an authority on emerging cybercrime threats, covering the full spectrum of trends affecting consumers, corporations and the industry as a whole.
Scott Moore	**Software Developer, Team Lead, IBM X-Force Threat Intelligence Database** With 19 years in IBM X-Force, Scott is the founding member of the research team, and creator of the X-Force vulnerability database. He is a member of the CVSS Special Interest Group.
Leslie Wiggins	**Portfolio Marketing Manager - IBM Security Guardium** Leslie Wiggins joined IBM in 2002 and has held product management and product marketing roles within the IBM WebSphere®, Information Management and Analytics business unit. Until her current position with IBM Security Guardium, Leslie focused on marketing for the IBM InfoSphere® Information Integration portfolio with a focus on big-data integration.
Vikalp Paliwal	**Offering Manager, IBM Security Guardium** Vikalp is Offering Manager for IBM Security Guardium. In prior roles, he held a variety of positions in software product management and business strategy supporting data management, information governance and big-data solutions at IBM.

Additional Contributors

Brad Sherrill	**Engineering Manager, X-Force Exchange and X-Force Database**
Doug Franklin	**Technologist, X-Force Advanced Research**
Leslie Horacek	**X-Force Offering Management, Security Content and Research**
Pamela Cobb	**Portfolio Marketing Manager, IBM X-Force**

1 Violet Blue, "'We take your security seriously,'" *Engadget*, 12 November 2015. http://www.engadget.com/2015/11/12/we-take-your-security-seriously/
2 Patricia Zengerle and Megan Cassella, "Millions more Americans hit by government personnel data hack," *Reuters*, 09 July 2015. http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709
3 Fran Howarth, "POS Malware and Loyalty Card Fraud Growing in Popularity," *Security Intelligence*, 10 December 2015. https://securityintelligence.com/pos-malware-and-loyalty-card-fraud-growing-in-popularity/
4 Avivah Litan, "Where have all our Passwords Gone?" *Gartner Blog Network*, 22 January 2015. http://blogs.gartner.com/avivah-litan/2015/01/22/where-have-all-our-passwords-gone/
5 Lorenzo Franceschi-Bicchierai, "55 Healthcare Data Breaches Have Hit More Than 100 Million People in 2015," *Motherboard*, 11 December 2015. http://motherboard.vice.com/read/55-healthcare-data-breaches-have-hit-more-than-100-million-people-in-2015
6 "Cyphort Labs Issues Special Report on the Rise in Malvertising Cyber Attacks," *Cyphort*, 25 August 2015. http://www.cyphort.com/about/news-and-events/press-releases/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks/
7 Dissent, "Despite warnings earlier this year, tens of thousands of databases continue to leak (update1)," *DataBreaches.net*, 14 December 2015. http://www.databreaches.net/despite-warnings-earlier-this-year-tens-of-thousands-of-databases-continue-to-leak/
8 "New Dutch Law Introduces General Data Breach Notification Obligation and Higher Sanctions," *Hunton & Williams*, 02 June 2015. https://www.huntonprivacyblog.com/2015/06/02/new-dutch-law-introduces-general-data-breach-notification-obligation-higher-sanctions/
9 "Dutch Law Includes General Data Breach Notification Obligation and Larger Fines for Violations of the Data Protection Act," *Hunton & Williams*, 08 January 2016. https://www.huntonprivacyblog.com/2016/01/08/dutch-law-includes-general-data-breach-notification-obligation-and-larger-fines-for-violations-of-the-data-protection-act/
10 Pierluigi Paganini, "2013 Data Breaches: All You Need to Know," *InfoSec*, 09 May 2014. http://resources.infosecinstitute.com/2013-data-breaches-need-know/
11 Jeff Multz, "Small Businesses Suffer Many Breaches," *SecureWorks*, 25 June 2015. http://www.secureworks.com/resources/blog/small-businesses-suffer-many-breaches/
12 Brian Krebs, "Point-of-Sale Vendor NEXTEP Probes Breach," *KrebsOnSecurity*, 09 March 2015. http://krebsonsecurity.com/2015/03/point-of-sale-vendor-nextep-probes-breach/
13 Brian Krebs, "Starwood Hotels Warns of Credit Card Breach," *KrebsOnSecurity*, 20 November 2015. http://krebsonsecurity.com/2015/11/starwood-hotels-warns-of-credit-card-breach/
14 Brian Krebs, "Banks: Card Breach at Hilton Hotel Properties," *KrebsOnSecurity*, 25 September 2015. http://krebsonsecurity.com/2015/09/banks-card-breach-at-hilton-hotel-properties/
15 Jeff Goldman, "Nine Zoos Nationwide Suffer Point-of-Sale Breaches," *eSecurity Planet*, 09 July 2015. http://www.esecurityplanet.com/network-security/nine-zoos-nationwide-suffer-point-of-sale-breaches.html
16 Adam Greenberg, "POS malware threatens payment cards used at Gateway Arch shops," *SC Magazine*, 09 February 2015. http://www.scmagazine.com/pos-malware-threatens-payment-cards-used-at-gateway-arch-shops/article/397201/
17 Jaikumar Vijayan, "Security Breach at Point of Sale Vendor NEXTEP Highlights Third-Party Security Risks," *Security Intelligence*, 13 March 2015. https://securityintelligence.com/news/security-breach-point-sale-vendor-nextep-highlights-third-party-security-risks/
18 Dan Goodin, "Potent, in-the-wild exploits imperil customers of 100,000 e-commerce sites," *Ars Technica*, 23 April 2015. http://arstechnica.com/security/2015/04/23/potent-in-the-wild-exploits-imperil-customers-of-100000-e-commerce-sites/
19 Michelle Alvarez, "The Year of the Health Care Industry Security Breach," *Security Intelligence*, 01 December 2015. https://securityintelligence.com/the-year-of-the-health-care-industry-security-breach/
20 Ponemon Institute Research Report, "2015 Cost of Data Breach Study: Global Analysis," Sponsored by IBM, May 2015. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF
21 Mohit Kumar, "Adult Friend Finder... Hacked & 3.5 Million Users' Database Leaked Online," *The Hacker News*, 21 May 2015. http://thehackernews.com/2015/05/adult-friend-finder.html
22 Brian Krebs, "Online Cheating Site AshleyMadison Hacked," *KrebsOnSecurity*, 19 July 2015. https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/
23 Abby Phillip, "Why the wife of a pastor exposed in Ashley Madison hack spoke out after his suicide," *The Washington Post*, 09 September 2015. https://www.washingtonpost.com/news/acts-of-faith/wp/2015/09/09/why-the-wife-of-a-pastor-exposed-in-ashley-madison-leak-spoke-out-after-his-suicide/
24 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, 22 July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
25 "Hackers caused power cut in western Ukraine," *BBC News*, 12 January 2016. http://www.bbc.com/news/technology-35297464
26 Noeleen Walder, Jonathan Stempel and Joseph Ax, "Hackers stole secrets for up to $100 million insider-trading profit," *Reuters*, 11 August 2015. http://www.reuters.com/article/us-cybercybersecurity-hacking-stocks-arr-idUSKCN0QG1EY20150811
27 Wiktor Szary and Eric Auchard, "Polish airline, hit by cyber attack, says all carriers are at risk," *Reuters*, 22 June 2015. http://www.reuters.com/article/us-poland-lot-cybercrime-idUSKBN0P21DC20150622
28 Matthew Prince, "How to Launch a 65Gbps DDoS, and How to Stop One," *CloudFlare*, 17 September 2012. https://blog.cloudflare.com/65gbps-ddos-no-problem/
29 Ms. Smith, "DDoS attacks almost doubled in year: Akamai State of the Internet Security Report," *Network World*, 01 February 2015. http://www.networkworld.com/article/2878418/microsoft-subnet/ddos-attacks-almost-doubled-in-year-akamai-state-of-the-internet-security-report.html
30 Swati Khandelwal, "602 Gbps! This May Have Been the Largest DDoS Attack in History," *The Hacker News*, 08 January 2015. http://thehackernews.com/2016/01/biggest-ddos-attack.html
31 Lucian Constantin, "CryptoWall ransomware held over 600K computers hostage, encrypted 5 billion files," *IDG News Service*, 29 August 2014. http://www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html
32 Martin McKeay, "DDoS Extortion: Easy and Lucrative," *Security Intelligence*, 15 July 2015. https://securityintelligence.com/ddos-extortion-easy-and-lucrative/
33 Graham Cluley, "More websites hit by Armada Collective DDoS blackmail attacks, but won't pay up," *Cluley Associates Limited*, 10 November 2015. https://www.grahamcluley.com/2015/11/armada-collective-ddos/
34 Mathew J. Schwartz, "Match.com Suspends UK Ads After Malware Attacks," *DataBreachToday*, 04 September 2015. http://www.databreachtoday.com/matchcom-suspends-uk-ads-after-malware-attacks-a-8524

[35] J. Gomez and Genwei Jiang, "Malware With Your News? Forbes Website Victim of Malvertising Attack," *FireEye*, 22 September 2015. https://www.fireeye.com/blog/threat-research/2015/09/malvertising_attack.html

[36] Jeremy Kirk, "Hacked advertising platform sent users to the Nuclear exploit kit," *PCWorld*, 07 May 2015. http://www.pcworld.com/article/2920452/hacked-advertising-platform-sent-users-to-the-nuclear-exploit-kit.html

[37] Jérôme Segura, "Angler Exploit Kit Blasts Daily Mail Visitors Via Malvertising," *Malwarebytes UnPacked*, 13 October 2015. https://blog.malwarebytes.org/malvertising-2/2015/10/angler-exploit-kit-blasts-daily-mail-visitors-via-malvertising/

[38] Dissent, "Misconfigured database may have exposed 1.5 million individuals' PHI: researcher (update1)," *DataBreaches.net*, 22 December 2015. http://www.databreaches.net/misconfigured-database-may-have-exposed-1-5-million-individuals-phi-researcher-2/

[39] Brian Mastroianni, "'Hello Kitty' hack exposes 3.3. million user accounts," *CBS News*, 21 December 2015. http://www.cbsnews.com/news/hello-kitty-hack-exposes-3-3-million-user-accounts/

[40] Dissent, "191 million voters' personal info exposed by misconfigured database (update2)," *DataBreaches.net*, 28 December 2015. http://www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/

[41] Sam Machkovech, "Hacked French network exposed its own passwords during TV interview," *Ars Technica*, 09 April 2015. http://arstechnica.com/security/2015/04/hacked-french-network-exposed-its-own-passwords-during-tv-interview/

[42] James Moar, "The Future of Cybercrime & Security: Financial & Corporate Threats & Mitigation 2015-2020," *Juniper Research*, 05 December 2015. http://www.juniperresearch.com/researchstore/strategy-competition/cybercrime-security/financial-corporate-threats-mitigation

[43] IBM Security, "2015 Cybercrime Trends – Things are Going to Get Interesting," *SlideShare*, 15 January 2015. http://www.slideshare.net/ibmsecurity/2015-cybercrime-trends

[44] Limor Kessem, "Shifu Officially Spreads to the UK: Banks and Wealth Management Firms Beware," *Security Intelligence*, 28 September 2015. https://securityintelligence.com/shifu-officially-spreads-to-the-uk-banks-and-wealth-management-firms-beware/

[45] Limor Kessem, "Carbanak: How Would You Have Stopped a $1 Billion APT Attack?" *Security Intelligence*, 23 February 2015. https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/

[46] Limor Kessem, "Shifu: 'Masterful' New Banking Trojan Is Attacking 14 Japanese Banks," *Security Intelligence*, 31 August 2015. https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/

[47] Taylor Armerding, "Cybercrime: Much more organized," *CSO Online*, 23 June 2015. http://www.csoonline.com/article/2938529/cyber-attacks-espionage/cybercrime-much-more-organized.html

[48] Sara Peters, "Stealthy ModPOS Is 'Most Sophisticated PoS Malware' Ever," *Dark Reading*, 24 November 2015. http://www.darkreading.com/attacks-breaches/stealthy-modpos-is-most-sophisticated-pos-malware-ever-/d/d-id/1323294

[49] Darlene Storm, "Ransom32: First-of-its-kind JavaScript-based ransomware spotted in the wild," *ComputerWorld*, 04 January 2016. http://www.computerworld.com/article/3018972/security/ransom32-first-of-its-kind-javascript-based-ransomware-spotted-in-the-wild.html

[50] John Kuhn, "The Dyre Wolf Campaign: Stealing Millions and Hungry for More," *Security Intelligence*, 02 April 2015. https://securityintelligence.com/dyre-wolf/

[51] Shane Schick, "Dridex Trojan Remains a Risk Even Following Takedown Operation and FBI Arrest," *Security Intelligence*, 19 October 2015. https://securityintelligence.com/news/dridex-trojan-remains-a-risk-even-following-takedown-operation-and-fbi-arrest/

[52] Limor Kessem, "Dridex Launches Dyre-Like Attacks in UK, Intensifies Focus on Business Accounts," *Security Intelligence*, 19 January 2016. https://securityintelligence.com/dridex-launches-dyre-like-attacks-in-uk-intensifies-focus-on-business-accounts/

[53] Limor Kessem, "An Overnight Sensation — CoreBot Returns as a Full-Fledged Financial Malware," *Security Intelligence*, 10 September 2015. https://securityintelligence.com/an-overnight-sensation-corebot-returns-as-a-full-fledged-financial-malware/

[54] Limor Kessem, "Organized Cybercrime Big in Japan: URLZone Now on the Scene," *Security Ingtelligence*, 01 February 2016. https://securityintelligence.com/organized-cybercrime-big-in-japan-urlzone-now-on-the-scene/

[55] Doug Olenick, "Shifu Trojan now striking 14 Japanese banks: IBM," *SC Magazine*, 01 September 2015. http://www.scmagazine.com/shifu-trojan-now-striking-14-japanese-banks-ibm/article/435918/

[56] Jaikumar Vijayan, "Japanese Banks Targeted With New Rovnix Trojan," *Dark Reading*, 08 January 2016. http://www.darkreading.com/vulnerabilities---threats/japanese-banks-targeted-with-new-rovnix-trojan/d/d-id/1323818

[57] "Business E-Mail Compromise: An Emerging Global Threat," *Federal Bureau of Investigation*, 28 August 2015. https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

[58] John Kuhn, Lance Mueller and Limor Kessem, "The Dyre Wolf: Attacks on Corporate Banking Accounts," *IBM MSS Research and Intelligence Report*, April 2015. https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Dyre_Wolf_MSS_Threat_Report.pdf

[59] Thomas Fox-Brewster, "This American Oil Company Lost $3.5 Million To 'Evil Corp' Hackers But Came Out On Top," *Forbes*, 16 October 2015. http://www.forbes.com/sites/thomasbrewster/2015/10/16/evil-corp-dridex-hackers-lose-to-penneco/#82ca431b4e5b

[60] IBM X-Force Malware Research team.

[61] David Gilbert, "CryptoLocker Gang Earns Millions in Just 100 Days," *International Business Times*, 19 December 2013. http://www.ibtimes.co.uk/cryptolocker-criminals-earn-30-million-100-days-1429607

[62] Dave Jeffers, "Crime pays very well: Cryptolocker grosses up to $30 million in ransom," *PCWorld*, 2013. http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html

[63] "Website attack affecting our customers," *Talktalk*, Accessed 04 February 2016. http://help2.talktalk.co.uk/oct22incident

[64] "TalkTalk data breach to cost company up to £35m in one-off costs, CEO says," *Out-Law*, 11 November 2015. http://www.out-law.com/en/articles/2015/november/talktalk-data-breach-to-cost-company-up-to-35m-in-one-off-costs-ceo-says/

[65] "TalkTalk hack to cost £35m – but won't dent profits," *The Week*, 11 November 2015. http://www.theweek.co.uk/66178/talktalk-hack-to-cost-35m-but-wont-dent-profits

[66] Jaikumar Vijayan, "New Shifu Banking Trojan An 'Uber Patchwork' Of Malware Tools," *Dark Reading*, 02 September 2015. http://www.darkreading.com/vulnerabilities---threats/new-shifu-banking-trojan-an-uber-patchwork-of-malware-tools/d/d-id/1322039

[67] Robert Lipovsky, "Corkow: Analysis of a Business-oriented Banking Trojan," *Eset UK*, February 2014. http://www.cio.co.uk/cmsdata/whitepapers/3522992/ESET_-_Corkow_analysis_of_a_business_oriented_banking_trojan.pdf

[68] "GMBot: Android poor man's 'webinjects,'" *CERT Polska*, 02 October 2015. http://www.cert.pl/news/10648/langswitch_lang/en

[69] Jeremy Kirk, "Android malware steals one-time passcodes to hijack accounts protected by two-factor authentication," *PCWorld*, 13 January 2016. http://www.pcworld.com/article/3021930/security/android-malware-steals-one-time-passcodes.html

[70] Douglas Bonderud, "Double Dose of Android Trojan Malware Hits Online Banking Users," *Security Intelligence*, 14 January 2016. https://securityintelligence.com/news/double-dose-of-android-trojan-malware-hits-online-banking-users/

[71] Lucian Constantin, "Android banking malware SlemBunk is part of well-organized campaign," *ComputerWorld*, 14 January 2016. http://www.computerworld.com/article/3023035/security/android-banking-malware-slembunk-is-part-of-well-organized-campaign.html

[72] Limor Kessem, "2016 Cybercrime Reloaded: Our Predictions for the Year Ahead," *Security Intelligence*, 15 January 2016. https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/

Please Recycle

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016

WGL03114-USEN-01