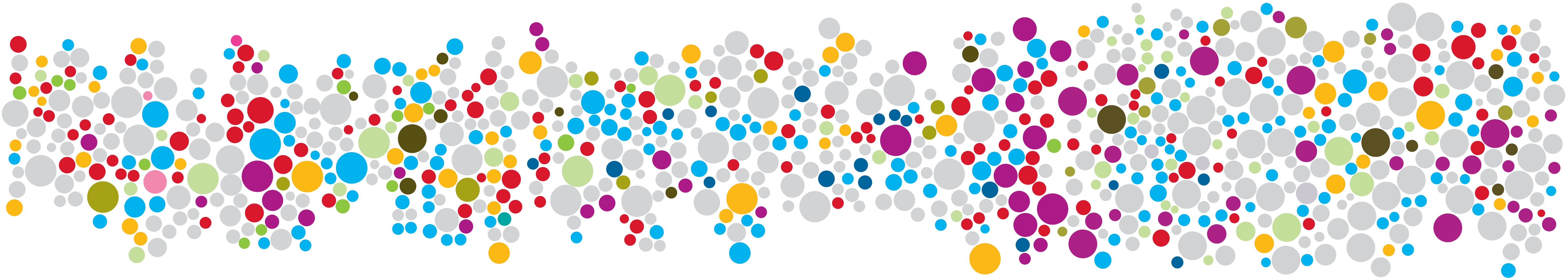
IBM X-Force Threat Intelligence Index 2017

The year of the mega breach



IBM Security
March 2017

TABLE OF CONTENTS

Executive overview 3
Methodology 4
The shifting world of breaches 5
World-changing leaks 5
A history of incidents 6
High-volume hijacks 8
When things go rogue 9
Notable attack vectors 10
Distributing malware through spam 10
Record numbers of vulnerability disclosures 11
Prevalent methods of attack in monitored clients 11
Inject unexpected items 12
Manipulate data structures 12
Collect and analyze information 13
Indicator 13
Employ probabilistic techniques 13
Manipulate system resources 13
Subvert access control 14
Abuse existing functionality 14
Engage in deceptive interaction 14
Top-targeted industries 15
Financial services 16
Information and communications 16
Manufacturing 17
Retail 17
Healthcare 18
Where are the “bad guys”? 19
Insiders versus outsiders 19
External attackers: Focus on organized cybercrime 20
Slow and steady wins the race 21
Cyber gangs sharpen the focus on business accounts 23
Commercial malware making the rounds 24
Venturing into additional cybercrime realms 25
2017 and beyond 26
Contributors 26
About X-Force 26
Footnotes 27
Glossary 29

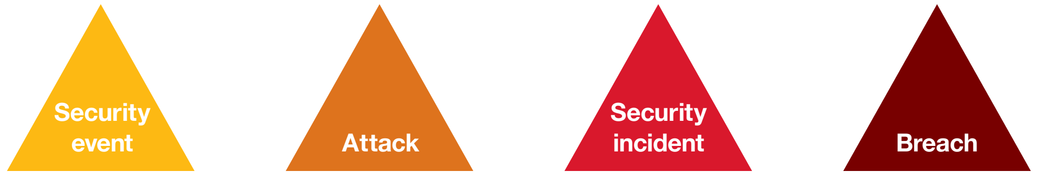
TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

EXECUTIVE OVERVIEW

With Internet-shattering distributed-denial-of-service (DDoS) attacks, troves of records leaked through data breaches, and a renewed focus by organized cybercrime on business targets, 2016 was a defining year for security. Indeed, in 2016 more than 4 billion records were leaked, more than the combined total from the two previous years, redefining the meaning of the term "mega breach." In one case, a single source leaked more than 1.5 billion records.[1]

Definitions of terms



Security event: Activity on a system or network detected by a security device or application.

Attack: A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security incident: An attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation.

Breach: An incident that results in the exfiltration of data. In this report, "breach data" is a sampling of notable publicly disclosed incidents, not monitored security client incidents.

Figure 1: Definitions of terms.

In our monitored client environments, IBM® X-Force® saw that the average client organization experienced more than 54 million security events in 2016—only three percent more events than 2015. At the same time, client organizations monitored by X-Force experienced an average 12 percent decrease in attacks in 2016 compared to 2015 (1,019 attacks in 2016 compared to 1,157 attacks in 2015).

Most notably, the average monitored client was found to have experienced 93 security incidents in 2016, down 48 percent from the 178 discovered in 2015.

Does this reduction in attacks and incidents reflect a safer security environment in 2016? Perhaps. That would be wonderful news to report. However, the reduction in attacks could mean attackers are relying more and more on proven attacks, thus requiring fewer attempts. Additionally, the combination of massive record leaks and a record year of vulnerability disclosures also paints a different picture. Regardless of the total number of attempted attacks or incidents, it takes only one successful compromise for an organization to end up as front page news and facing millions of dollars in data breach costs.[2]

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

METHODOLOGY

To better understand the security threat landscape, X-Force uses both data from monitored security clients and data derived from non-customer assets such as spam sensors and honeynets. X-Force runs spam traps around the world and monitors more than eight million spam and phishing attacks daily. It has analyzed more than 37 billion web pages and images.

IBM Security Services monitors billions of events per year from more than 8,000 client devices in more than 100 countries. This report includes data IBM collected between 1 January 2016 and 31 December 2016. In this year's report, IBM X-Force Threat Research adopted the MITRE Corporation's Common Attack Pattern Enumeration and Classification (CAPEC) standard for attack categorization.

The top five attacked industries were determined based on data from a representative set of sensors from each industry. The sensors chosen for the index had to have event data collected throughout the entire year of 2016.

The insider/outsider identification utilized in this report includes all source and destination IP addresses identified in the attacks and security incidents targeting the representative set of sensors. A single attack may involve one or many attackers.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
World-changing leaks
A history of incidents
High-volume hijacks
When things go rogue
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

THE SHIFTING WORLD OF BREACHES

The year 2016 was notable for the way in which cyber attacks had a discernible impact on real-world events and infrastructure. Beginning in December 2015, for example, reports appeared of a malware-caused power outage in Ukraine,[3] leaving hundreds of thousands of people without electricity for several hours in the middle of winter. Nearly a year later, a smaller but similar Ukrainian power outage surfaced, also attributed to a cyber attack.[4] These two events bookended the year and served as heralds of the widespread impact of security incidents on the physical world, even to those who don’t regularly monitor the security landscape.

World-changing leaks

This impact was most prominently registered through a number of high-profile data leaks that had a direct influence on global politics. In April 2016, 11.5 million leaked documents from the Panamanian law firm Mossack Fonseca[5] exposed offshore accounting of thousands of prominent people from around the world. The “Panama Papers,” as they were dubbed, showed insider financials of several current and former heads of state, their friends and family, as well as businesspeople and celebrities. While offshore accounts are not illegal per se, they often raise suspicion because they can be used for tax evasion and money laundering. In addition to criminal investigations in 79 countries,[6] the disclosure led to anti-government protests in several countries including Pakistan[7] and the UK.[8] In April 2016, the Prime Minister of Iceland stepped down[9] in the aftermath of the leak.

In the US, data leaks were a central topic of the presidential election. Several leaks from the Democratic National Committee (DNC) provided an inside look into private email conversations and strategies, and could have potentially swayed the opinion of some voters for one candidate over another. In both the Panama Papers and DNC leaks, it is reported that attackers used simple techniques such as SQL injection (SQLi)[10] and **phishing** to exploit these influential targets. The fact that vulnerability to fundamental security flaws could have such far-reaching impact is notable.

In past years, data breaches were often in the form of a fixed set of structured information such as credit card data, passwords, national ID numbers, personal health information (PHI) data or key documents. In recent years, X-Force has observed the release of much larger caches of unstructured data, such as the contents of emails, as well. In 2016, there were many notable examples of leaks involving hundreds of gigabytes of email archives, documents, intellectual property and source code, exposing companies’ complete digital footprints to the public.

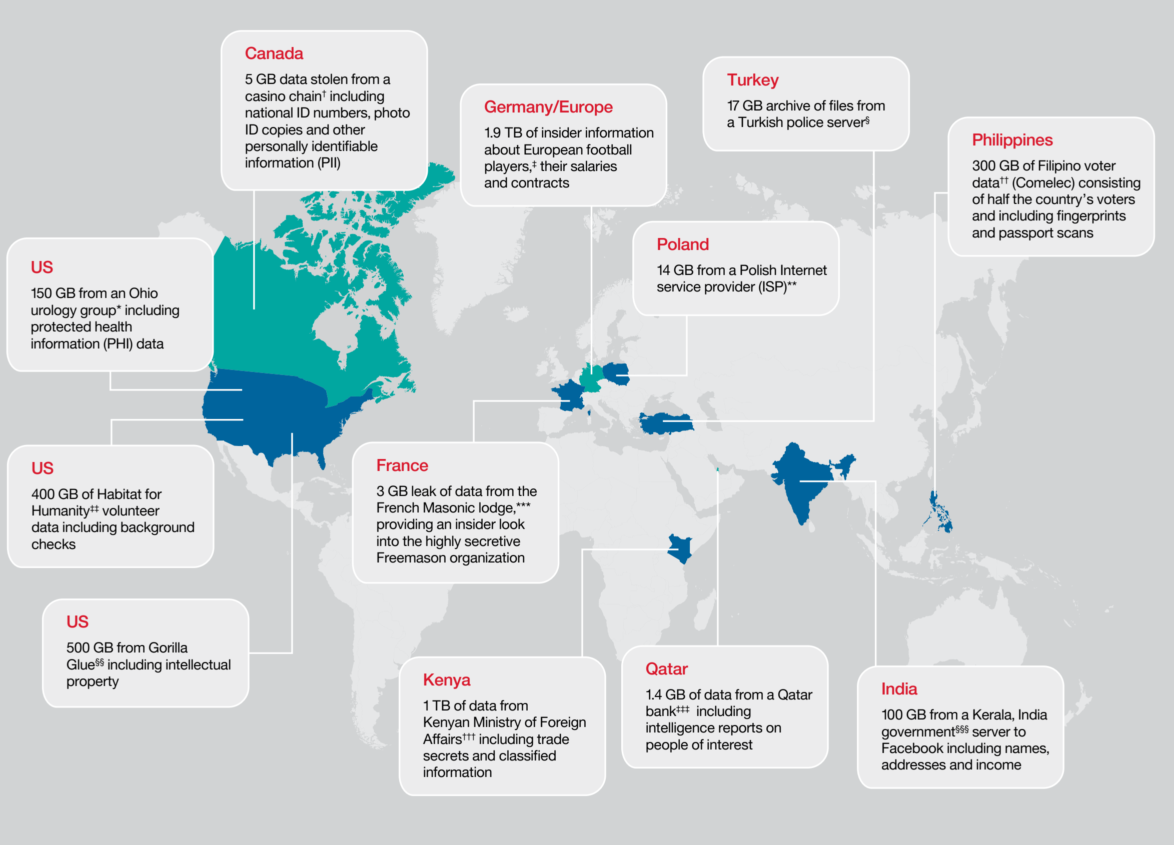
Phishing: The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
World-changing leaks
A history of incidents
High-volume hijacks
When things go rogue
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Click image to enlarge map. Click again for original size.

Notable 2016 global leaks of unstructured data



Canada
5 GB data stolen from a casino chain[†] including national ID numbers, photo ID copies and other personally identifiable information (PII)

Germany/Europe
1.9 TB of insider information about European football players,[‡] their salaries and contracts

Turkey
17 GB archive of files from a Turkish police server[§]

Philippines
300 GB of Filipino voter data[††] (Comelec) consisting of half the country’s voters and including fingerprints and passport scans

US
150 GB from an Ohio urology group[*] including protected health information (PHI) data

Poland
14 GB from a Polish Internet service provider (ISP)[**]

US
400 GB of Habitat for Humanity[‡‡] volunteer data including background checks

France
3 GB leak of data from the French Masonic lodge,[***] providing an insider look into the highly secretive Freemason organization

US
500 GB from Gorilla Glue[§§] including intellectual property

Kenya
1 TB of data from Kenyan Ministry of Foreign Affairs[†††] including trade secrets and classified information

Qatar
1.4 GB of data from a Qatar bank[‡‡‡] including intelligence reports on people of interest

India
100 GB from a Kerala, India government[§§§] server to Facebook including names, addresses and income

[*] Joseph Cox, “Hacker Dumps Sensitive Patient Data From Ohio Urology Clinics,” *Motherboard,* 02 August 2016.

[†] “Hacker dumps stolen Casino Rama information online,” *CTV News Barrie,* 21 November 2016.

[‡] “Football Leaks,” *Wikipedia*, Accessed 05 February 2017.

[§] Waqas, “Anonymous Hacks Turkish National Police Server, Leaks A Trove of Data,” *HackRead,* 16 February 2016.

[**] Waqas, “Ukranian Hacker Hacks Polish Telecom Giant Netia; Leaks Massive Data,” *HackRead,* 09 July 2016.

[††] John Leydon, “Megabreach: 55 MILLION voters’ details leaked in Philippines,” *The Register,* 07 April 2016.

[‡‡] Dell Cameron, “More than 5,000 people exposed in Habitat for Humanity data breach,” *The Daily Dot,* 28 October 2016.

[§§] Joseph Cox, “Hackers Claim Theft of Data from Gorilla Glue,” *Motherboard,* 17 November 2016.

[***] Dominique Filippone, “Le cloud de la Grande Loge de France piraté,” *Lemonde Informatique,* 15 April 2016.

[†††] Waqas, “Anonymous Leaks 1 TB of Data from Kenya’ Ministry of Foreign Affairs,” *HackRead,* 28 April 2016.

[‡‡‡] Varun Haran, “Qatar National Bank Suffers Massive Breach,” *Data Breach,* 26 April 2016.

[§§§] Mazhar Farooqui, “Data of 34 million Keralites leaked in massive breach,” *Gulf News,* 16 November 2016.

Figure 2: Notable 2016 global leaks of unstructured data.

A history of incidents

X-Force has been tracking and reporting on publicly disclosed security incidents and data breaches since 2011. Figure 3 (next page) illustrates a sampling of security incidents and attack techniques during 2014, 2015 and 2016. In 2016, X-Force observed several record-breaking metrics such as the number of previously leaked records that surfaced during the year and an increase in the size and scope of DDoS attacks.

While the number of leaked records is not the only indicator of the impact of a breach, it is still a useful metric to track year to year. In 2015, X-Force tracked just over 600 million leaked records, down from more than one billion leaked in 2014. At over 4 billion, the number of records leaked in 2016 was more than double that of both previous years combined.

The year 2016 was somewhat unusual, however, as several “historical hacks” from breaches occurring in earlier years surfaced publicly, with revelations that billions of previously unreleased records were being sold on the Dark Web. These leaked records are associated with the year in which the organization disclosed the breach and not the year the breach occurred. In some cases, it’s not known or disclosed when the actual breach occurred.

In one significant example of a historical hack, Yahoo alerted customers[11] in December 2016 that the company had discovered two breaches resulting in leaks of 500 million records in 2014, and one billion records in 2013. And Yahoo’s

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
World-changing leaks
A history of incidents
High-volume hijacks
When things go rogue
Notable attack vectors
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Sampling of security incidents by attack type, time and impact, 2014 through 2016

Size of circle estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.

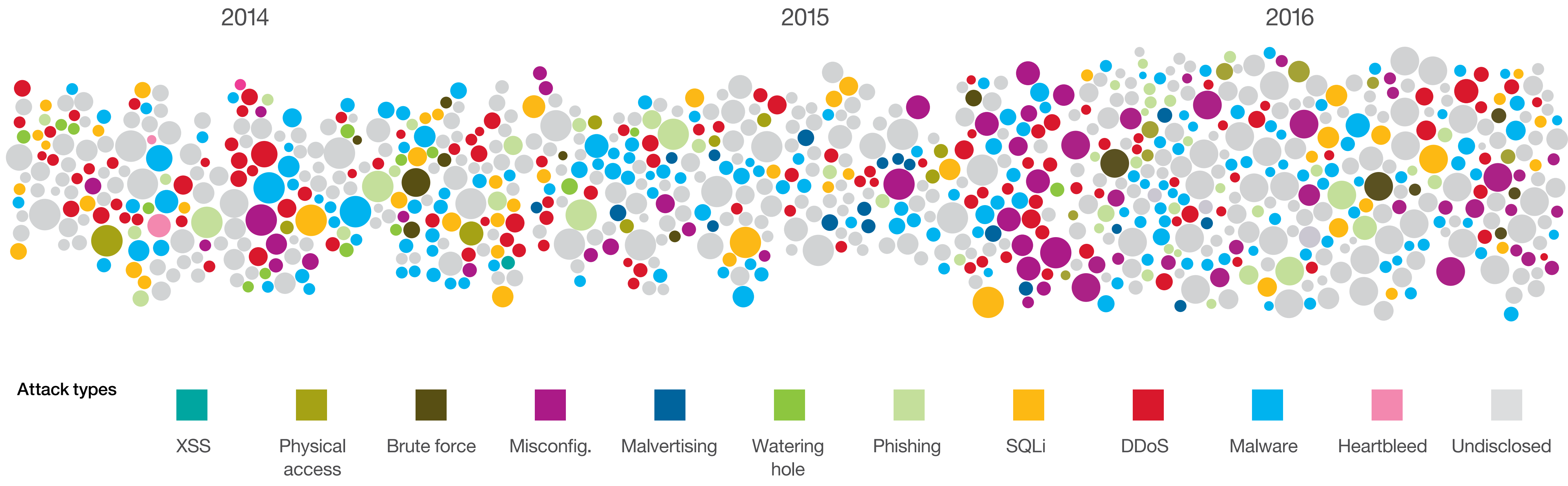


Figure 3: Sampling of security incidents by attack type, time and impact, 2014 through 2016.

disclosure was not the only one of its kind. Reports of significant, older breaches occurred throughout 2016, with data from a number of historical hacks posted for sale on the Dark Web, most often by the same seller.[12]

Several of these breaches, such as those occurring at LinkedIn, Dropbox,[13] and Last.fm,[14] were already disclosed in prior years, though the impact was under-reported at the time. For example, in 2012, LinkedIn disclosed a breach impacting 6.5 million users, but in 2016, after a verifiable **dump** was posted for sale on the Dark Web, it was revealed[15] that 117 million emails and passwords were actually stolen in that breach.

Dump: Data copied in a readable format from main or auxiliary storage to an external medium.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
World-changing leaks
A history of incidents
High-volume hijacks
When things go rogue
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

One of the dangers of these older leaks is that passwords often were stored less securely than they are today, or in some cases, millions of passwords were not encrypted at all. Many Internet giants previously used easy-to-crack hashing algorithms such as MD5.[16] The result is that there are billions of email and plain-text password combinations available for those interested in purchasing them—and many of these parties have successfully used these credentials to hijack accounts on other sites and services.

High-volume hijacks

During 2016, there were several high-profile account takeover campaigns in which the targeted service was not breached, but rather a large number of the targeted service's customers lost control of their accounts because they had reused the same email and password from another Internet account. For example, attackers captured more than 20 million accounts[17] at the Chinese auction site Taobao in a **brute force attack** that leveraged more than 100 million combinations of harvested credentials from other breaches. They used these hacked accounts primarily for sending spam, as well as bolstering the reputation of select accounts, and manipulating supply and demand of auction items.

Companies allowing virtual assets to be converted to currency, including frequent buyer programs, loyalty cards and travel points programs, were also targeted by account takeover.

Another novel use of comprised credentials was a campaign to log in to Internet-facing PCs running remote administration software. In June 2016, remote access service TeamViewer reported an uptick[18] in compromised accounts that was believed to be linked to a flood of leaked credentials. People who reused their LinkedIn password for their TeamViewer PC login, for example, would be susceptible to this type of account takeover.

One positive development during 2016 is that many companies now are using more secure hashing functions such as bycrypt to store passwords. The result is that even after a breach, such as the theft of 43 million Weebly[19] accounts and 87 million Daily Motion[20] accounts in October, it may be more difficult to crack the passwords, devaluing the data and the scope of the attack. Still, given the frequently reported top 10 password lists that have been circulating for several years, it might be useful for web services to reject some of the most common passwords and require users to set something more secure.

Brute force attack: Use of trial and error to obtain a user name and password for a valid account on a web application to access sensitive data such as credit card numbers.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
World-changing leaks
A history of incidents
High-volume hijacks
When things go rogue
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

When things go rogue

Whether motivated by political protest, crippling a competitor or just for laughs, large-scale DDoS attacks have been a mainstay for many years. Not long ago, 100Gbps attacks were unprecedented—but by 2016, they were more of the norm.[21] An attack on a French-based hosting provider,[22] for example, reportedly topped a gargantuan 1 Tbps. Tools for DDoS attacks have become more accessible as well. In October, the open-source Mirai botnet was used to cause a large Internet-wide disruption of major sites such as Etsy[23] and Twitter by targeting their DNS provider, Dyn.

Mirai[24] is the latest evolution of DDoS attack malware, weaponizing home routers and other connected devices, including Internet-accessible camera systems and digital video recording devices. Large botnets of Internet “things” can be amassed due to the sheer number of these systems and their ease of exploitation, due to basic security holes.

Another Internet of Things (IoT) DDoS botnet, dubbed Leet[25] by security firm Incapsula, launched a 650Gbps attack in December. One interesting feature of this attack was that it used two different SYN payloads for maximum impact. Sending a high packet rate of regular sized SYN packets (40 to 60 bytes) and interspersing very large packets (799 to 936 bytes) makes the attack difficult to mitigate because it ties up end systems handling the requests with high volume number of packets and floods switches with demands for huge bandwidth.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Distributing malware through spam
Record numbers of vulnerability disclosures
Prevalent methods of attack in monitored clients
Inject unexpected items
Manipulate data structures
Collect and analyze information
Indicator
Employ probabilistic techniques
Manipulate system resources
Subvert access control
Abuse existing functionality
Engage in deceptive interaction
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

NOTABLE ATTACK VECTORS

Distributing malware through spam

Spam email remains a primary tool in the attacker’s toolkit, reinforcing the pervasiveness of malware and the potential for inadvertent insider attacks. Figure 4 shows the overall spam volume observed by X-Force in its network of sensors in 2015 and 2016. The average monthly spam volume of the first quarter of 2015 is shown as 100 percent, and the red in the bars indicates the amount of spam with malicious attachments.

By the end of 2016, in fact, X-Force had noted a fourfold increase in the volume of spam over the previous year, as well as a marked increase in malicious attachments to that spam.

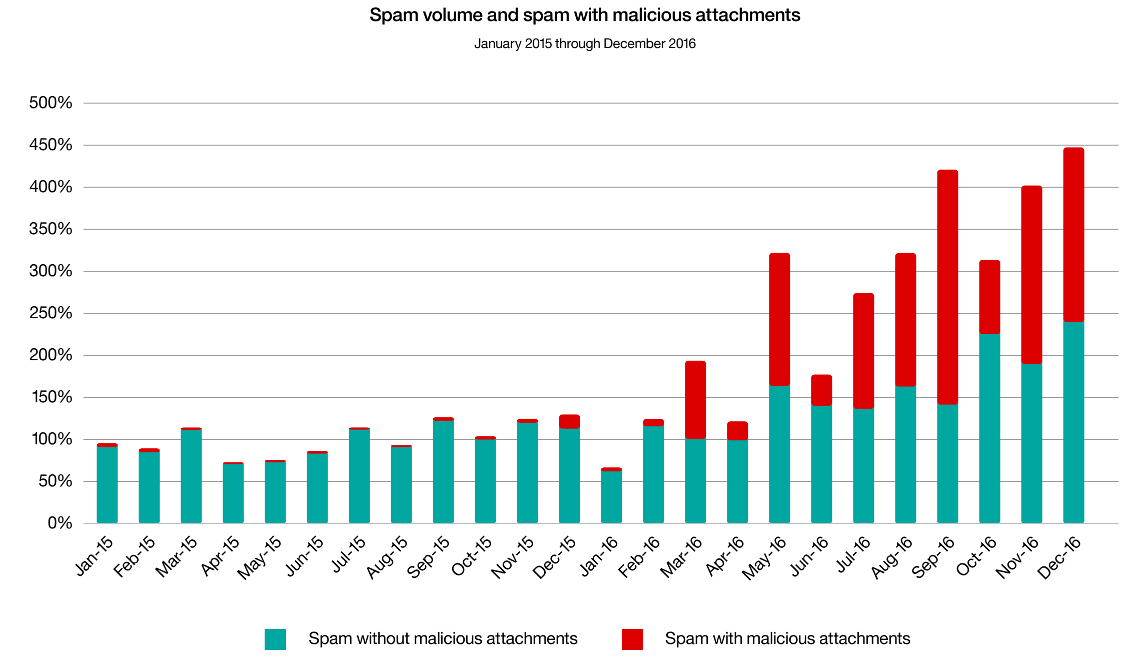


Figure 4: Spam volume and spam with malicious attachments – January 2015 through December 2016.

Click image to enlarge graph. Click again for original size.

Among malicious attachments to spam, ransomware accounted for the vast majority—85 percent. Ransomware continues to be one of the most profitable forms of malware in terms of effort versus earnings. While these attacks were already established and profitable, the February 2016 case of a California hospital[26] that paid a ransom of 40 Bitcoins (approximately USD17,000 at the time) to unlock encrypted files foreshadowed a renewed campaign of similar attacks against the healthcare industry in several countries. Given that disruptions of hospital operations can be both financially damaging and literally matters of life and death—exacerbated by outdated security processes and infrastructure—the healthcare sector became a lucrative worldwide target[27] throughout the year.

To learn more about how to prepare for and respond to ransomware, read the IBM Security Ransomware Client Engagement Guide.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Distributing malware through spam
Record numbers of vulnerability disclosures
Prevalent methods of attack in monitored clients
Inject unexpected items
Manipulate data structures
Collect and analyze information
Indicator
Employ probabilistic techniques
Manipulate system resources
Subvert access control
Abuse existing functionality
Engage in deceptive interaction
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Record numbers of vulnerability disclosures

The X-Force vulnerability database has been tracking public disclosures of software vulnerabilities since 1997. In 2016, the 20th year of documenting these threats, X-Force recorded the highest single-year number in its history: 10,197 vulnerabilities.

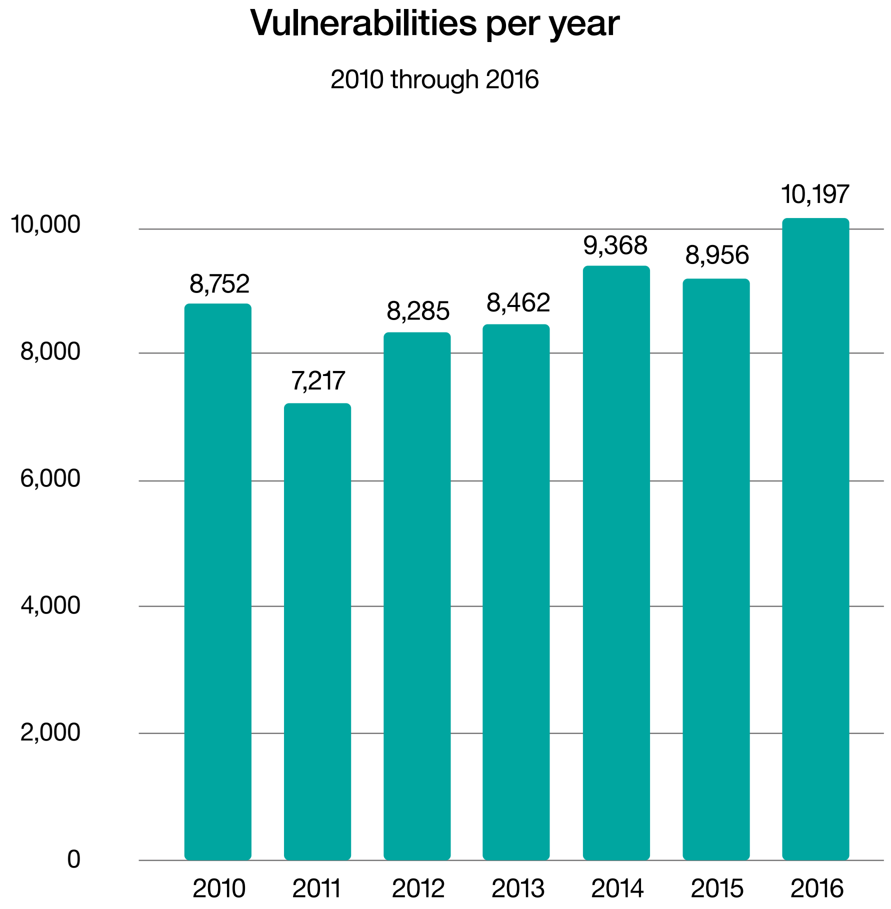


Figure 5: Vulnerabilities per year – 2010 through 2016.

Web application vulnerability disclosures made up 22 percent of the total vulnerability disclosures in 2016. A large majority of those were cross-site scripting and SQLi vulnerabilities, which could be leveraged by attackers to target vulnerable systems.

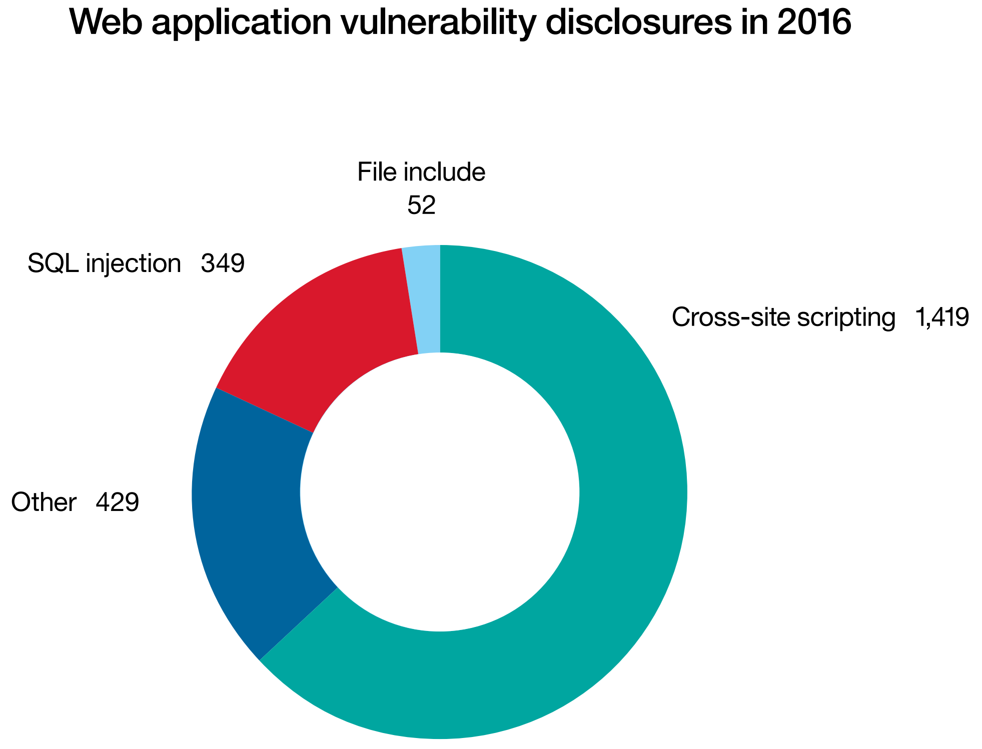


Figure 6: Web application vulnerability disclosures in 2016.

Prevalent methods of attack in monitored clients

To assist in analyzing and describing threats to its monitored security clients, X-Force has grouped 2016 observed attack types according to the standard set by the MITRE Corporation's CAPEC effort. This system, as described by MITRE, "organizes

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Distributing malware through spam
Record numbers of vulnerability disclosures
Prevalent methods of attack in monitored clients
Inject unexpected items
Manipulate data structures
Collect and analyze information
Indicator
Employ probabilistic techniques
Manipulate system resources
Subvert access control
Abuse existing functionality
Engage in deceptive interaction
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

attack patterns hierarchically based on mechanisms that are frequently employed in exploiting a vulnerability."[28] The only exception is the "Indicator" category, which describes conditions and context of threats and attack patterns.

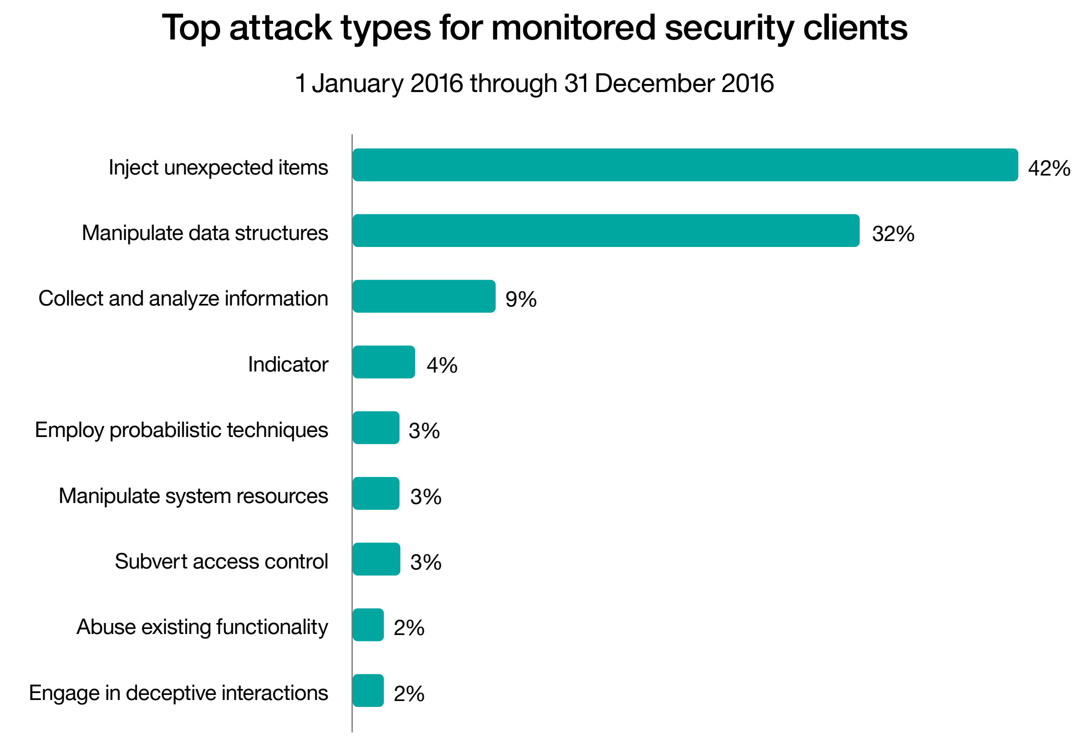


Figure 7: Top attack types for monitored security clients – 1 January 2016 through 31 December 2016.

Inject unexpected items

According to the X-Force analysis of 2016 data, the number one attack vector targeting X-Force-monitored clients—at 42 percent—involves using malicious input data to attempt to control or disrupt the target system. Command injection, which includes operating system command injection (OS CMDi) and SQLi, belongs in this category. OS CMDi is also known as "shell command injection," for which the now infamous and widely prevalent **Shellshock** vulnerability is named. Shellshock activity surged across all industries before its two-year anniversary in September 2016 and made up just over one-third of all attacks targeting healthcare in 2016.

In a publicly reported breach during the summer of 2016, a SQLi attack using the software vBulletin[29] was used to steal millions of user records[30] from gamting forums and other sites with large user bases. Even though a patch had been issued earlier, there were still many sites running older or unpatched versions, and it is often easy for attackers to scan the web for potential targets running this software.

Manipulate data structures

The number two attack vector, accounting for 32 percent of attacks, was the attempt to gain unauthorized access through the manipulation of system data structures. As CAPEC states, "Often, vulnerabilities [such as buffer overflow vulnerabilities], and therefore exploitability of these data structures, exist due to ambiguity and assumption in their design and prescribed handling."[31]

Shellshock: A family of security bugs (aka "Bashdoor") that uses vulnerable versions of Bash command language to execute arbitrary commands and gain unauthorized access to a computer system.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Distributing malware through spam
Record numbers of vulnerability disclosures
Prevalent methods of attack in monitored clients
Inject unexpected items
Manipulate data structures
Collect and analyze information
Indicator
Employ probabilistic techniques
Manipulate system resources
Subvert access control
Abuse existing functionality
Engage in deceptive interaction
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Collect and analyze information

Attacks focused on the collection and theft of information made up nine percent of attacks targeting client devices. Most of these involved fingerprinting, often viewed as a kind of pre-attack that gathers information on potential targets to discover their existing weaknesses. Essentially, an attacker compares output from a target system to known "fingerprints" that uniquely identify specific details about the target, such as the type or version of its operating system or an application. Attackers can use the information to identify known vulnerabilities in the target organization's IT infrastructure.

Indicator

Note that "Indicator" is not a CAPEC mechanism of attack. A cyber-threat indicator consists of certain observable conditions as well as contextual information about the condition or pattern. These events, which accounted for four percent of all attacks, could indicate either an attempted or a successful attack on the target system. A large percentage of the attacks involved targeted systems experiencing 100 or more external destinations in a short time, which might indicate a compromised internal host. If compromised, a host could be attacking other targets or communicating with other compromised hosts.

Employ probabilistic techniques

The fifth most prevalent attack type, at three percent, involved an attacker using what CAPEC describes as "probabilistic techniques to explore and overcome security properties of the target."[32] Most of the activity involved brute-force password attacks, a tactic in which an intruder tries to guess a username and password combination to gain unauthorized access to a system or data. Most of the attacks observed by X-Force targeted the Secure Shell (SSH) service. Users favor SSH because it can provide secure remote access. On the downside, however, it can provide attackers with shell account access across the network.

Manipulate system resources

Attacks attempting to manipulate some aspect of a system's resource state or availability accounted for three percent of all attacks. Resources include files, applications, libraries and infrastructure, and configuration information. Successful attacks in this category could allow the attacker to cause a denial of service, infect a machine to become a botnet command-and-control (C&C) server or execute arbitrary code on the target.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Distributing malware through spam
Record numbers of vulnerability disclosures
Prevalent methods of attack in monitored clients
Inject unexpected items
Manipulate data structures
Collect and analyze information
Indicator
Employ probabilistic techniques
Manipulate system resources
Subvert access control
Abuse existing functionality
Engage in deceptive interaction
Top-targeted industries
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Subvert access control

Attacks attempting to subvert access control through the "exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication"[33] accounted for three percent of attacks. Most of the attacks observed in this category involved the exploitation of vulnerabilities in the target's client-server communication channel for authentication and data integrity by leveraging the implicit trust a server places in what it believes to be a valid client.

Abuse existing functionality

Two percent of attacks involved attempts to abuse or manipulate "one or more functions of an application in order to achieve a malicious objective not originally intended by the application, or to deplete a resource to the point that the target's functionality is affected."[34] Successful attacks in this category could allow the attacker to obtain sensitive information or cause a denial of service, as well as execute arbitrary code on the target.

The Mirai IoT botnet conducted **flooding** attacks, which fall under this category of attack. The Mirai botnet also played a large role in several large telecom breaches during a "global" Internet attack in mid- to late 2016.

Flooding attack: A technique in which an attacker rapidly engages in a large number of interactions with a target, consuming the target's resources in order to crash the target.

Engage in deceptive interaction

Two percent of attacks made attempts to fool victims into opening malicious documents or clicking on links to malicious sites. Particularly in the healthcare sector, these attacks are proving very successful. Attack documents and links are often delivered via phishing campaigns.

In terms of simple yet highly profitable attacks, reports of many successful business email compromise (BEC) scams emerged in the first half of the year, resulting in the theft of hundreds of millions of US dollars. BEC is primarily a social engineering attack in which attackers send an email pretending to be a company official. They may send an email from a domain similar to the victim's domain, or actually take over the account of the impersonated executive and mimic the person's writing style. In either case, an email is sent to an employee responsible for company funds or employee tax records. With feigned urgency, the employee is immediately requested to wire money, send employee W-2 tax forms or leak other critical data. The US Federal Bureau of Investigation (FBI) published an advisory[35] about this threat that estimated more than USD3.1 billion had been stolen by June 2016.

These attacks seemed to be more widely reported in the first half of the year than the latter, perhaps indicating that companies were more alert to these types of scams as the year progressed. However, by early 2017, these attacks had renewed, as tax season brought a renewed opportunity for attackers to trick people into sending out W-2 forms.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Financial services
Information and communications
Manufacturing
Retail
Healthcare
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

TOP-TARGETED INDUSTRIES

Breaking out publicly disclosed security events in 2016, X-Force sees that the industries experiencing the highest number of incidents and reported records breached were information and communications and government. It is worth noting that the healthcare industry, which fell just outside the top five in terms of records breached, continued to be beleaguered by a high number of incidents. However, attackers focused on smaller targets, resulting in a lower number of leaked records in that industry.

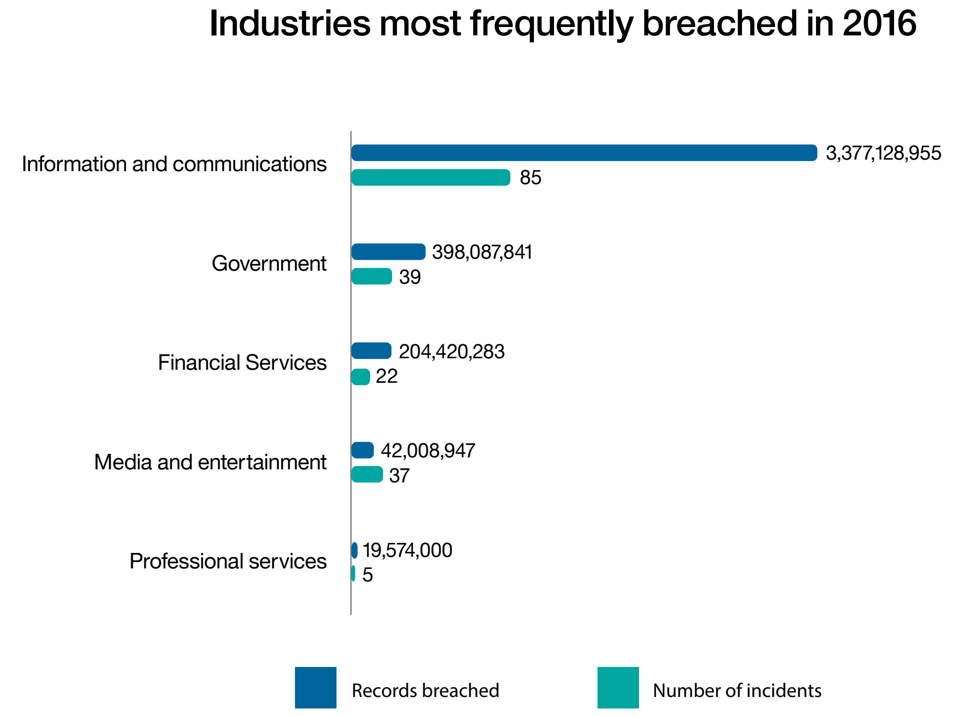


Figure 8: Industries most frequently breached in 2016.

Click image to enlarge graph. Click again for original size.

While X-Force analyzes publicly disclosed breaches, IBM also has the advantage of visibility into X-Force-monitored security client environments. This visibility allows X-Force to drill further into why certain industries may be more susceptible to successful attacks. By comparing publicly disclosed breaches with actual attack metrics from X-Force-monitored security client environments, it's possible to observe trends in the security practices of different industries that may be a result of regulatory or other governance practices.

During 2016, IBM Managed Security Services identified five key sectors that provide critical insights into trends and practices:

- Financial services
- Information and communications
- Manufacturing
- Retail
- Healthcare

Two common attack types stand out from the rest across these five attacked industries: SQLi and OS CMDi—and that should be no surprise. Cybercriminals often consider SQLi and OS CMDi vulnerabilities to be "low-hanging fruit" or relatively easy to exploit. And despite a downward trend in the number of

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Financial services
Information and communications
Manufacturing
Retail
Healthcare
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

publicly disclosed SQLi and CMDi vulnerabilities, according to data from the X-Force vulnerability database, attackers continue to exploit the existing unpatched vulnerabilities in web servers and applications.

Learn how researchers categorize patterns of attacks according to CAPEC in an IBM blog.

Financial services

According to figures compiled by IBM Managed Security Services, the financial services sector moved from the third most-attacked industry in 2015 (behind healthcare and manufacturing) to the first most-attacked in 2016, due primarily to a large rise in SQLi and OS CMDi attacks. In this year, these attacks alone were responsible for almost half of all attacks among the financial sector of IBM Managed Security Services customers. SQLi and OS CMDi are perhaps the most popular attack vectors within this sector because successful exploitation of these vulnerabilities provides attackers with the ability to read, modify and destroy sensitive data. And there's a large amount of PII contained within the databases of financial institutions.

Hackers value PII because it can be sold at a handsome profit, and also can be held hostage, requiring the financial institution to pay a ransom for its return or to prevent its public disclosure.

In 2016, there was a notable rise in publicly reported Society for Worldwide Interbank Financial Telecommunication (SWIFT) attacks against the messaging system used by thousands of banks and companies to move money around the world.[36] The result was that millions of US dollars were stolen and illegally transferred from various global banks using custom malware and SQLi attacks.[37] In 2017, SQLi and OS CMDi are positioned to continue to be the primary methods of attacking data stores.

Access and authentication controls play a major role in financial services security, and in 2016 subversion of these controls was the second most prevalent type of attack on this sector. The method of attack classified as "Subvert Access Control" is an attack type commonly carried out by insiders to gain control of end systems.

To learn more, check out the "Security Trends in Financial Services" white paper from X-Force.

Information and communications

The information and communications technology sector moved up into the top five attacked sectors, taking second place among monitored industries in 2016. IBM-monitored security client data shows the number one mechanism of attack in this industry was "Manipulate Data Structures." **Buffer overflow** conditions, which fall under this attack category, were exploited

Buffer overflow: An exploitation method that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Financial services
Information and communications
Manufacturing
Retail
Healthcare
Where are the "bad guys"?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

in many of these attacks, which accounted for 51 percent of all attacks seen in this sector. SQLi and OS CMDi were the second most frequent attack types detected in this sector during 2016, accounting for 30 percent of the total attacks, confirming X-Force predictions[38] that these attacks would not wane anytime in the near future.

Ranking as the third most prevalent attack type targeting the information and communications technology sector was the "Indicator" category, which was due largely to attempted connections from Tor software exit nodes. Tor (an abbreviation of the original project name, "The Onion Router") is designed to allow full anonymity to the end user. Although not all traffic coming from the Tor network is indicative of an attack, by using a Tor client, a cybercriminal can disguise the attack's originating network location and its path to the target, making identification virtually impossible.

Manufacturing

In 2016, SQLi accounted for the majority of all attacks—more than 71 percent—in manufacturing. This industry is a tempting target, as many systems within the sector are perceived to be weak by design as a result of a failure to be held to compliance standards.

The second most popular attack mechanism in manufacturing was "Abuse Existing Functionality," which accounted for about 7 percent of all attacks detected. Many of these attacks involved flooding a target system with a large number of requests, to create a state of denial of service. "Collect and Analyze Information" was in position number three at 6 percent.

To learn more, check out the "Security Trends in Manufacturing" white paper from X-Force.

Retail

The retail industry remains at risk from any threat that targets credit card or gift card data. Retailers maintain an extremely large amount of financial records and other personal information such as credit card and Social Security numbers, and SQLi and CMDi attacks are often used to steal this information. These attacks accounted for 50 percent of all attacks against the industry in 2016.

Buffer manipulation and brute force attacks took second and third place during 2016, and collectively represent 28 percent of the total attacks on retailers. One notable publicly disclosed breach against a retailer occurred late in the year, when attackers targeted accounts at a UK food delivery service by using brute force authentication details gleaned from other

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Financial services
Information and communications
Manufacturing
Retail
Healthcare
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

public data breaches. Customers who reused passwords discovered that unauthorized food purchases had been made via their hijacked accounts.[39]

To learn more, check out the “Security Trends in Retail” white paper from X-Force.

Healthcare

SQLi and OS CMDi attacks represented the majority of attacks within healthcare in 2016, at a combined 48 percent. Healthcare records are always a top prize for cybercriminals and, as X-Force has seen in the retail industry, are widely for sale on the Dark Web.[40]

Attack methods categorized as “Manipulate Data Structures” account for the second most popular attack type within the industry and “Manipulate System Resources” is third. These attacks focus on known vulnerabilities within an application, which, when successful, can lead to full system compromise.

The category “Image File Attacks,” in which malicious code is hidden within a variety of image file types, were the third most prevalent type of attempted attacks seen in healthcare, at 28 percent. Brute force attacks, which are part of a CAPEC mechanism of attack named “Employ Probabilistic Techniques,”[41] used against authentication mechanisms, round out the top attacks in position four, at 6 percent.

To learn more, check out the “Security Trends in Healthcare” white paper from X-Force.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

WHERE ARE THE “BAD GUYS”?

Insiders versus outsiders

In prior years, X-Force looked at the totality of data collected from all industries and compared insider versus outsider IP addresses to present a global view of where the threats were originating. For 2016, X-Force looked at each industry to see how they compared.

Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

🟩 Fewer

🟥 More

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

When discussing attackers versus attacks, it helps to understand how X-Force classifies attacks. An attack is a security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself. An attack may be carried out by a single attacker sourced from one IP address, or many hundreds of attackers from multiple IP addresses. A flooding attack is one type of attack where there could be many attackers striking within a short period of time. This is why DDoS attacks are successful; attackers who wish to disrupt access to a service or website can increase their attack traffic by using many compromised hosts.

The industry experiencing the highest number of attacks in 2016 was financial services. The data for this sector reveals a greater percentage (58 percent) of insider attacks versus outsider attacks (42 percent). The insiders are composed of both inadvertent actors (53 percent) and malicious insiders (5 percent).

The fifth ranked sector, healthcare, also has a greater percentage (71 percent) of insiders (inadvertent at 46 percent and malicious at 25 percent) versus outsiders (29 percent). It can be useful to think of inadvertent actors as compromised systems carrying out attacks without the user being aware of it as is the case with the “Subvert Access Control” attack type. This often happens when a desktop client is compromised via malicious email attachments, **clickjacking**, phishing or vulnerable computer services that have been attacked from another internal networked system.

Clickjacking: An attack that tricks victims into initiating a malicious action in one system while thinking they are interacting with a completely different system where they are authenticated.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

The fact that the insider attacks targeting the financial services and healthcare were largely the result of inadvertent actors may be due these industries having a greater susceptibility to phishing attacks. Organizations in these sectors should focus on educating employees about phishing and how to avoid becoming a victim, use a variety of approaches—video, webinars, in-person instruction—and require training at intervals to make the risk clear.

The remaining three of the top five attacked sectors had a greater percentage of outside attackers than insiders. Within information and communications, manufacturing, and retail, 60 percent of the attacks were categorized as “Inject Unexpected Items” (58 percent by outsiders plus 2 percent by insiders). Of the attacks categorized as “Inject Unexpected Items,” a total of 48 percent (46 percent by outsiders plus 2 percent by insiders) of the total attacker count launched SQLi attacks. Another 10 percent (nine percent by outsiders plus one percent by insiders) employed OS CMDi attacks.

The second highest mechanism of attack involving outsiders falls within the category “Manipulate Data Structures.” These attacks accounted for 23 percent of the total attackers, with less than one percent coming from insiders. Most attacks in this category were more specifically classified as “**Buffer Manipulation**” attacks.

Industries such as information and communications, manufacturing, and retail experience more outsider attacks because they may be seen as prime targets for exploitation of SQLi, OS CMDi and buffer overflow vulnerabilities. To help protect themselves organizations in these sectors may want to review their patch management processes.

External attackers: Focus on organized cybercrime

With the investigation into external actors, it’s necessary to consider shifts in organized cybercrime during 2016. This was a year when some countries experienced a marked increase in financial cybercrime specifically. This portion of the report dives deeper into findings from X-Force malware researchers who investigate cybercrime trends and financial malware campaigns.

During 2016, X-Force researchers noticed some shifts in the usual undercurrents of organized cybercrime. By using techniques such as **poisoned macros**, **exploit kits**, fake fax messages or alarming notices from attackers posing as tax authorities, cybercriminals all too often find a way to make victims click on their Pandora’s Box of threats and infect them

Buffer manipulation: A method of manipulating an application’s buffer interaction to read or modify data to which the attacker should not have access. The buffer itself is the attack target.

Poisoned macro: A macro embedded in an office productivity file that features harmful code or an exploit that will execute and cause the endpoint to become infected if not fully patched.

Exploit kit: A programming tool that allows someone who does not have any experience writing software code to create, customize and distribute malware.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

with banking Trojans or **ransomware**. In the first quarter of 2016, almost two-thirds of malware infections were Trojans,[42] the most powerful information stealers available to financially motivated criminals.

Malware statistics gathered during 2013-2015 indicate that during those years 431 million new malware variants joined the existing pool of malware.[43] The crimeware arena is replete with mutations, and new strains become more varied every year.[44]

With this ongoing growth in new **malware families, offspring and hybrids**, it is helpful to look at the big picture. In doing so, X-Force found that 2016 was defined by the following high-level trends:

- Slow and steady wins the race
- Cyber gangs sharpen the focus on business accounts
- Commercial malware making the rounds
- Venturing into additional cybercrime realms

Slow and steady wins the race

Cybercriminals aim to spread their malware as far and wide as possible, since their profit relies on a numbers game. To increase the chances of systems and software becoming infected, the assumption has been that the more spam they send out, the better. But this is no longer true. Today, spreading malware via mass spam blasts can draw unwanted attention and, in many cases, detection by security solutions.

As a result of this close scrutiny of spam, malware can be captured and meticulously analyzed, its communication infrastructure can be identified and blacklisted, and the malware’s lifecycle can be drastically shortened. By the time the criminals are ready to attack after their infection campaigns, banks and other businesses often already have protections in place, considerably lowering the percentage of successful attacks.

On the consumer side, Internet service providers can more easily identify and block mass campaigns that spread malware using email, storage devices, or compromised or malicious websites that redirect visitors to exploits and infection zones. Identifying and blocking campaigns can result in their reaching many fewer people than the criminals intend.

Ransomware: Malware spread by infected email attachments or programs that encrypts data and demands payment for a decryption key.

Malware family: Malware thought to be linked to botnets and other malware operators.

Malware offspring: A new version of malware that is thought to be created by the same developer as another type of malware.

Malware hybrid: New malware incorporating characteristics of two types of malware.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the "bad guys"?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

The balancing act between the desire to mass distribute malware and the risk that mass campaigns will result in easy detection does not affect the lower end, opportunistic malware such as ransomware, **IoT bots**, or **keyloggers**. That's because these threats are often spread by affiliates or amateurs and not by an organized gang, and they continue to be cast in wide nets. This phenomenon has become clear to the more sophisticated cybercrime gangs, and in 2016, X-Force researchers saw them change tactics in an attempt to avoid detection and analysis at all costs.

One of the techniques malware attackers use in their attempt to evade detection is to change the malware's **dropper** and the dropper's anti-security features, the malware's deployment flow, and the malware's persistence mechanisms. Those are the popular "moving parts" where developers can invest relatively small amounts of time and expect to see an improved ability to bypass anti-virus software and some security tools. These sorts of changes happen almost every week, for example, in the type of financial malware that cyber gangs own and operate. With a relatively small investment having the potential for big returns, X-Force predicts criminals will continue to use these tactics.

Another interesting method of evading detection that emerged in 2016 is the use of minimal campaigns, often targeting only one country. These campaigns allow specified IP address ranges to run the malware, and then carefully test the malware's success without allowing it to unveil its secrets.

For example, the operators of the Zeus Sphinx botnet, which surfaced in 2016, have shown extremely careful and precise operating patterns. Not only are the malware configurations targeting one country at a time, but X-Force researchers noticed that the campaigns often used a barely-there attack strategy by deploying the payload on only five machines at a time, evaluating successful exploitation and immediately vanishing. Sphinx emerged in 2016 as commercial malware, so even unsophisticated cyber gangs can use the toolkit. This might very well be the case with recent Sphinx botnets discovered in Canada and in Australia,[45] as criminals are making frequent upgrades to the malware's security evasion mechanisms.

Another example of a tactic to evade detection is the GootKit Trojan.[46] This malware appears to be owned by one cyber gang that targets banks in Europe, specifically favoring the UK, France, Italy and Spain. GootKit typically separates configurations for each country, and many times it will target a relatively small number of banks in each geography. According

IoT bot: Software that hijacks computers, smart appliances and devices connected to the Internet of Things to conduct operations such as stealing data or sending malicious spam.

Keylogger: Software that records a computer user's keystrokes to capture passwords, financial data or other sensitive information for theft or other malicious activities.

Dropper: An installer that secretly carries viruses, back doors and other malware for execution on a compromised machine.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

to X-Force research, GootKit’s developers appear to frequently change the malware’s security evasion mechanisms, and their careful distribution keeps them off the radar as they continue to operate slowly and silently.

Perhaps the most interesting example of 2016 is the Dridex malware—a banking Trojan owned by one of the top cybercrime gangs, active since 2014. Dridex campaigns[47] became smaller overall in 2016, at times vanishing[48] altogether. It appears that Dridex’s operators’ top goals for 2016 were to sharpen its focus on business accounts,[49] where they were hoping to find larger sums of money to steal, route stolen funds through uncommonly targeted countries[50] such as Latvia and Estonia, and diversify their income using ransomware.[51]

In their efforts to continually launch fraud attacks, Dridex’s operators reduced the amount of wide-spread spam, created more specific email ploys to target employees, and preferred the use of Microsoft Office document macros to deliver their Trojan. At times they even password-protected the files[52] to prevent automated detection.

Cyber gangs sharpen the focus on business accounts

Touching on the trend of working slowly and steadily, especially in the use of malware such as Dridex, criminals are increasing their focus on either consumer or business bank accounts, and configuring malware to target only the desired type.

Examining malware configurations fetched by banking Trojans up until 2014, X-Force in 2016 identified a mixed-bag of targets of all types, with a majority of personal banking services emerging as the top target according to URL count.

In mid-2014, however, when the Dyre Trojan entered the cybercrime arena, a more focused approach began to emerge, this time targeting business accounts more than personal banking. Since then, the business focus has grown more pronounced in the number of URLs targeting business banking services, in the specification of targeted URLs, and in specific elements targeted in a bank’s web applications for business customers.

In 2016, X-Force saw a number of organized cyber gangs sharpen focus on businesses in this manner. Some examples of the malware used include:

Dridex: At least 50 percent of its targets are business banking services[53]
GozNym: 52 percent of its targets are business banking services[54]
TrickBot: 42 percent of its targets are business banking services[55]

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the "bad guys"?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Organized gangs lean toward targeting businesses because they can steal more money at a time than they could with consumer accounts. Gangs are also the type of players in the cybercrime arena that have the necessary resources at their disposal to steal larger amounts of money. These resources include:

- Experienced fraudsters who can conduct reconnaissance and plan out the fraud scenario, which often entails the theft of millions of dollars at a time[56]
- Funding to hire professional criminal call centers to support the fraud process and manipulate the victim
- Straw companies and straw men to funnel, then cash out millions in stolen funds and launder them afterward

Commercial malware making the rounds

Commercial banking Trojans, sold as ready-made malware kits that can be purchased and easily deployed, were severely curtailed on most underground boards after law enforcement agencies managed to infiltrate the ranks[57] of the Internet's criminal underbelly in 2010-2012. That precedent had a lasting effect on malware authors who have been much more careful ever since.

While some low-level vendors continued to sell executable files they could generate from their existing malware builders, X-Force saw little evidence of developers selling full kits of banking Trojans with all the necessary modules, a proper "license" and all the bug fixes and technical support fraudsters have been accustomed to buying.

In 2016, it became quite evident that commercial malware was making a comeback in a number of ways:

- Android **overlay malware** replaced banking Trojans as the "banking malware" commodity in open and semi-open forums on the cybercrime underground.
- Ransomware and ransomware-as-a-service offerings are low-cost money makers for gangs that wish to make a minimal up-front investment.
- New malware variants built on the Zeus v2 source code, leaked in 2011, kept Zeus at the top of the list of prolific malware.
- A new developer arose in an attempt to sell brand new banking Trojan NukeBot[58] in the underground.

You can learn more about commercial malware trends in the "Commercial Malware Makes a Comeback in 2016" blog post.

Overlay malware: A type of mobile malware designed to mimic the look and feel of a legitimate target application.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
Insiders versus outsiders
External attackers: Focus on organized cybercrime
Slow and steady wins the race
Cyber gangs sharpen the focus on business accounts
Commercial malware making the rounds
Venturing into additional cybercrime realms
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

Venturing into additional cybercrime realms

Malware actors are often cybercrime factions or gangs whose goal is to steal the largest amounts of money and act as quickly as possible. Eighty percent of cybercrime is conducted by organized crime,[59] which often tends to diversify[60] its illicit income sources. In 2016, cybercriminals acted like traditional organized crime gangs by also diversifying their illicit profit sources.

One example of diversifying illicit profit sources is the Dridex banking Trojan and the Locky[61] ransomware duo. Online banking fraud facilitated by Dridex is one of the most sophisticated malware operations in the cybercrime arena, and not only is ransomware technically inferior, operating ransomware demands much less knowledge and skill, which has attracted lower-level criminals to it in the past decade. But there is a connection now between them, and it appears that Locky adds a new profit source to the Dridex gang.

Dridex botnets began distributing Locky in early 2016. At first the relationship seemed unlikely, but it later became clearer that the two are indeed bound together through common malware campaigns, distribution by the Necurs botnet,[62] and notably, in some campaigns, Dridex samples downloaded Locky into a TEMP folder and executed it.

A similar occurrence came in the shape of a rather unique new Trojan hybrid. In April 2016, X-Force researchers uncovered the case of a ransomware dropper, Nymaim, into which a Gozi banking Trojan module was embedded, creating a new two-headed beast: GozNym.[63]

In virtually no time, the evidently well-funded joint GozNym[64] gang abandoned the ransomware business, for the most part, and began launching financial fraud attacks on banks in the US. GozNym then expanded its attack scope into Europe, launching redirection attacks on Polish,[65] English[66] and German banks.[67] Before long, its aggressive debut garnered GozNym some attention from law enforcement and saw some of its operators arrested[68] and indicted before the end of 2016.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

2017 AND BEYOND

Whether deluged by spam or targeted by cybercrime, organizations of all kinds clearly must continue to practice security fundamentals. To complement a solid information security foundation, organizations can continue to engage in collaboration to learn best practices and share findings and insights with colleagues. The faster they react to cybercrime findings and share their experiences across the security community, the less time each malware variant can live and or see successful fraud attacks. As a result, cybercrime can become much less financially viable for attackers, as exposure can weed out large numbers of fraudsters who abandon their criminal pursuit for lack of profit.

Beyond sharing intelligence, IBM Security has evolved to bring cognitive capabilities into the fight against cybercrime, with the goal of transforming it altogether. IBM Watson® for Cyber Security is already being used by 40 organizations, where it is helping spot cyber attacks. Cognitive computing is not only 30 to 40 percent faster than traditional systems,[69] it also continually learns and doesn’t repeat the same mistake twice, reducing false positives, and keeping up with threats. Before long, cognitive cybersecurity could outsmart human cybercrime and turn the tables on cybercriminals.

CONTRIBUTORS

Michelle Alvarez, *IBM X-Force Threat Research*
Nicholas Bradley, *IBM X-Force Threat Research Practice Lead*
Pamela Cobb, *IBM X-Force Portfolio Marketing*
Scott Craig, *IBM X-Force Threat Research*
Ralf Iffert, *IBM X-Force Content Security Manager*
Limor Kessem, *Executive Security Advisor*
Jason Kravitz, *IBM X-Force Research*
Dave McMillen, *IBM X-Force Threat Research*
Scott Moore, *IBM X-Force Software Developer*

ABOUT X-FORCE

IBM X-Force studies and monitors the latest threat trends, advising customers and the general public about emerging and critical threats, and delivering security content to help protect IBM customers. From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your critical assets. IBM Security protects some of the most sophisticated networks in the world and employs some of the best minds in the business.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

FOOTNOTES

[1] Thomas Fox-Brewster, “Yahoo: Hackers Stole Data on Another Billion Accounts,” *Forbes,* 14 December 2016.

[2] “2016 Cost of Data Breach Study: Global Analysis,” *Ponemon Institute,* June 2016.

[3] “Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure,” *ICS-CERT,* 25 February 2016.

[4] Swati Khandelwal, “Hackers Suspected of Causing Second Power Outage in Ukraine,” *TheHackerNews,* 20 December 2016.

[5] Luke Harding, “What are the Panama Papers? A guide to history's biggest data leak,” *The Guardian,* 05 April 2016.

[6] Patrick Evans, “Panama Papers: What happened next?” *BBC,* 26 December 2016.

[7] Asad Hashim, “Clashes as Pakistani anti-government protesters bear down on capital,” *Reuters,* 31 October 2016.

[8] “Panama Papers: Protesters demand Cameron’s resignation,” *Al Jazeera,* 09 April 2016.

[9] Will Fitzgibbon and Emilia Diaz-Struck, “Panama Papers Have Had Historic Global Effects—and the Impacts Keep Coming,” *ICIJ,* 01 December 2016.

[10] John Leyden, “SQL injection vuln found at Panama Papers firm Mossack Fonseca,” *The Register,* 11 April 2016.

[11] Sam Thielman, “Yahoo hack: 1bn accounts compromised by biggest data breach in history,” *The Guardian,* 15 December 2016.

[12] Andy Greenberg, “An Interview with the Hacker Probably Selling your Password Right Now,” *Wired,* 09 June 2016.

[13] Patrick Heim, “Resetting passwords to keep your files safe,” *Dropbox Blogs,* 25 August 2016.

[14] Dissent, “Last.fm data from 2012 added to LeakedSource,” *Data Breaches,* 01 September 2016.

[15] Robert Hackett, “LinkedIn Lost 167 Million Account Credentials in Data Breach,” *Fortune,* 18 May 2016.

[16] Dan Goodin, “8 million leaked passwords connected to LinkedIn, dating website,” *Ars Technica,* 06 June 2012.

[17] Paul Ducklin, “Data breach in China: 100 million records used to hack 20 million Taobao users,” *Naked Security,* 05 February 2016.

[18] Dan Goodin, “TeamViewer confirms number of abused user accounts is ‘significant’,” *Arstechnica,* 05 June 2016.

[19] Maitza Santillan, “Weebly to Notify 43 Million Customers of Data Breach,” *Tripwire,* 21 October 2016.

[20] Catalin Cimpanu, “DailyMotion Allegedly Hacked, 85 Million User Accounts Stolen,” *Bleeping Computer,* 05 December 2016.

[21] Charlie Osborne, “Thanks, script kiddies: 100Gbps DDoS attacks now commonplace,” *ZDNet,* 19 July 2016.

[22] Swati Khandelwal, “World’s largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices,” *The Hacker News,* 27 September 2016.

[23] Nicole Perlroth, “Hackers Used New Weapons to Disrupt Major Websites Across U.S.,” *The New York Times,* 21 October 2016.

[24] Nicky Woolf, “DDoS attach that disrupted internet was largest of its kind in history, experts say,” *The Guardian,* 26 October 2016.

[25] Avishay Zawozni and Dima Bekerman, “650Gbps DDoS Attack from the Leet Botnet,” *Imperva Incapsula,* 26 December 2016.

[26] Richard Winton, “Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating,” *Los Angeles Times,* 18 February 2016.

[27] JP Buntinx, “UK’s NHS Hospital Postpones Transplants Due to Ransomware Attack,” *PRCoin,* 02 November 2016.

[28] “CAPEC VIEW: Mechanisms of Attack (Version 2.9),” *CAPEC,* 07 December 2015.

[29] Michael Kan, “Hackers tap vBulletin vulnerability to break into 27 million more accounts,” *PCWorld,* 24 August 2016.

[30] Brendan Caldwell, “9.3 Million Accounts Compromised In Epidemic Of Forum Hacks: Funcom, Epic, and More,” *Rock Paper Shotgun,* 27 August 2016.

[31] “CAPEC CATEGORY: Manipulate Data Structures,” *CAPEC,* 07 December 2015.

[32] “CAPEC CATEGORY: Employ Probabilistic Techniques,” *CAPEC,* 06 January 2017.

[33] “CAPEC CATEGORY: Subvert Access Control,” *CAPEC,* 06 January 2017.

[34] “CAPEC CATEGORY: Abuse Existing Functionality,” *CAPEC,* 06 January 2017.

[35] “Losses From Business Email Compromise Scams Top $3.1 Billion: FBI,” *SecurityWeek,* 16 June 2016.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

[36] Charles Riley, “Hackers stole millions in third attack on global banking system,” *CNN Money,* 20 May 2016.

[37] Sergei Shevchenko, “Two bytes to $951m,” *BAE Systems Threat Research Blog,* 25 April 2016.

[38] Dave McMillen, “Command Injection: A Deadly Needle in the Haystack,” *SecurityIntelligence,* 14 July 2016.

[39] “Deliveroo customers have been hit by account breaches and rogue food orders,” *Irish Examiner,* 23 November 2016.

[40] IBM internal data.

[41] “Capec Category: Employ Probabilistic Techniques,” *CAPEC,* 06 January 2017.

[42] “Insights from APWG’s 1st Quarter 2016,” *FraudWatch International,* 22 June 2016.

[43] “Global number of new malware variants added annually from 2013 to 2015 (in millions),” *Statista,* 2016.

[44] Limor Kessem, “Three and a Half Crimeware Trends to Watch in 2017,” *SC Media,* 10 January 2017.

[45] Limor Kessem, “Around the World With Zeus Sphinx: From Canada to Australia and Back,” *SecurityIntelligence,* 26 January 2017.

[46] Limor Kessem, “GootKit: Bobbing and Weaving to Avoid Prying Eyes,” *SecurityIntelligence,* 08 July 2016.

[47] Brad Duncan, “Dridex malspam example from January 2016,” *Internet Storm Center,* 28 January 2016.

[48] Joseph Cox, “One of the World’s Largest Botnets Has Vanished,” *Motherboard,* 08 June 2016.

[49] Limor Kessem, “Dridex Launches Dyre-Like Attacks in UK, Intensifies Focus on Business Accounts,” *SecurityIntelligence,* 19 January 2016.

[50] Limor Kessem, “Hey Dridex, Tu Runā Latviski?,” *SecurityIntelligence,* 15 September 2016.

[51] “Dridex Botnet Spreading Locky Ransomware Via JavaScript Attachments” *SecurityWeek,* 10 March 2016.

[52] Catalin Cimpanu, “Dridex Spam Now Using Password-Protected Office Documents,” *Softpedia,* 27 September 2016.

[53] Configurations sampled in Q4-2016: MD5 eb9100b7119d03b354de4e0bee13bd03 and 0770dc5cf9257455324d226cb9ba6950

[54] Configuration sampled: 53842d56867f63f2670072061b38137a

[55] Configuration sampled: 9875438e51fad8286059405516d7268e

[56] John Kuhn and Lance Mueller, “The Dyre Wolf Campaign: Stealing Millions and Hungry for More,” *SecurityIntelligence,* 02 April 2015.

[57] Nelson D. Schwartz, “F.B.I. Says 24 Are Arrested in Credit Card Theft Plan,” *The New York Times,* 26 June 2012.

[58] Limor Kessem, “Nuclear Bot NukeBot aka Micro Banking Trojan,” *IBM,* 07 February 2017.

[59] Lillian Ablon, Martin C. Libicki and Andrea A. Golay, “Markets for Cybercrime Tools and Stolen Data,” *RAND Corp.,* 2014.

[60] “Transnational organized crime,” *Wikipedia,* 15 February 2017.

[61] Peter Stephenson, “Locky and Dridex - New Wine in Old Bottles,” *SC News,* 2016.

[62] Jean-Michel Picod, “Locky, Dridex, Necurs: the evil triad,” *Botconf,* 2016.

[63] Limor Kessem, “Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim,” *SecurityIntelligence,* 14 April 2016.

[64] Lior Keshet, “Two Heads Are Better Than One: Going Under the Hood to Analyze GozNym,” *SecurityIntelligence,* 12 July 2016.

[65] Limor Kessem, “Time Is Money: GozNym Launches Redirection Attacks in Poland,” *SecurityIntelligence,* 25 April 2016.

[66] Limor Kessem, “GozNym: Living in America,” *SecurityIntelligence,* 22 June 2016.

[67] Limor Kessem, “GozNym’s Euro Trip: Launching Redirection Attacks in Germany,” *SecurityIntelligence,* 23 August 2016.

[68] Robert Abel, “GozNym hacker faces 100 years in prison,” *SC Media,* 19 December 2016.

[69] Brian Barrett, “IBM’s Watson Now Fights Cybercrime in the Real World,” *Wired,* 06 December 2016.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

GLOSSARY

Brute force attack: Use of trial and error to obtain a user name and password for a valid account on a web application to access sensitive data such as credit card numbers.

Buffer manipulation: A method of manipulating an application’s buffer interaction to read or modify data to which the attacker should not have access. The buffer itself is the attack target.

Buffer overflow: An exploitation method that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

Clickjacking: An attack that tricks victims into initiating a malicious action in one system while thinking they are interacting with a completely different system where they are authenticated.

Dropper: An installer that secretly carries viruses, back doors and other malware for execution on a compromised machine.

Dump: Data copied in a readable format from main or auxiliary storage to an external medium.

Exploit kit: A programming tool that allows someone who does not have any experience writing software code to create, customize and distribute malware.

Flooding attack: A technique in which an attacker rapidly engages in a large number of interactions with a target, consuming the target’s resources in order to crash the target.

Injection attack: An attack technique that exploits websites by manipulating input.

IoT bot: Software that hijacks computers, smart appliances and devices connected to the Internet of Things to conduct operations such as stealing data or sending malicious spam.

Keylogger: Software that records a computer user’s keystrokes to capture passwords, financial data or other sensitive information for theft or other malicious activities.

Malware family: Malware thought to be linked to botnets and other malware operators.

Malware hybrid: New malware incorporating characteristics of two types of malware.

Malware offspring: A new version of malware that is thought to be created by the same developer as another type of malware.

Overlay malware: A type of mobile malware designed to mimic the look and feel of a legitimate, target application.

Phishing: The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity.

Poisoned macro: A macro embedded in an office productivity file that features harmful code or an exploit that will execute and cause the endpoint to become infected if not fully patched.

Ransomware: Malware spread by infected email attachments or programs that encrypts data and demands payment for a decryption key.

Shellshock: A family of security bugs (aka “Bashdoor”) that uses vulnerable versions of Bash command language to execute arbitrary commands and gain unauthorized access to a computer system.

TABLE OF CONTENTS

Executive overview
Methodology
The shifting world of breaches
Notable attack vectors
Top-targeted industries
Where are the “bad guys”?
2017 and beyond
Contributors
About X-Force
Footnotes
Glossary

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.