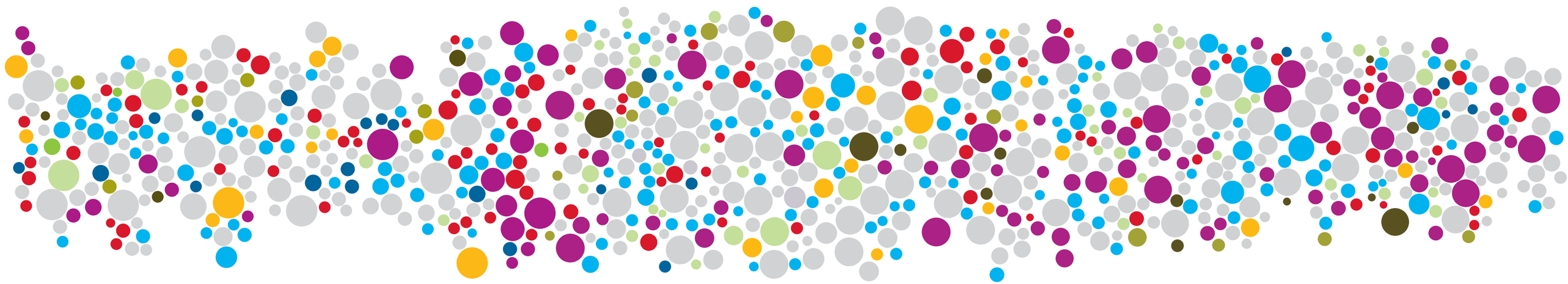
IBM X-Force Threat Intelligence Index 2018

Notable security events of 2017, and a look ahead



IBM Security
March 2018

TABLE OF CONTENTS

TABLE OF CONTENTS

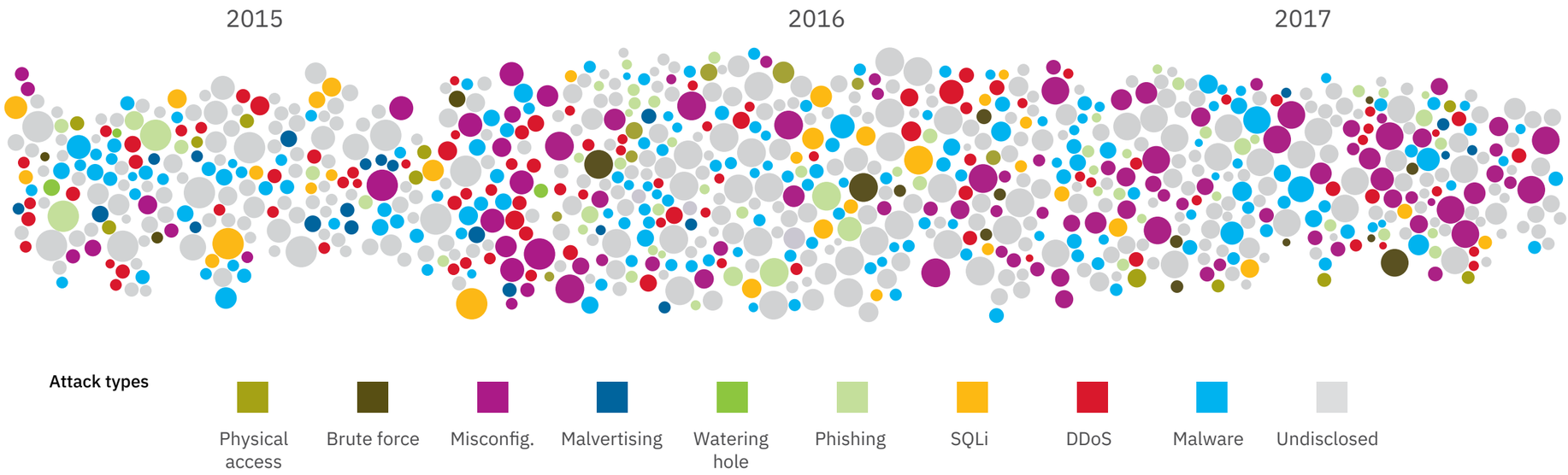
THE IBM SECURITY THREAT INTELLIGENCE POWERHOUSE

IBM® Security analyzes data and insight derived from monitored security clients, incident response services and penetration testing engagements. IBM X-Force® research teams analyze data from hundreds of millions of protected endpoints and servers, along with data derived from non-customer assets such as spam sensors and honeynets. X-Force also runs spam traps around the world and monitors tens of millions of spam and phishing attacks daily. It analyzes billions of web pages and images to detect fraudulent activity and brand abuse.

IBM Security Services monitors billions of security events per year from thousands of client devices in nearly 100 countries. In this report, we've culled the data IBM collected between 01 January 2017 and 31 December 2017, to deliver insightful information about the global threat landscape and apprise security professionals about the threats most relevant to their organizations.

Sampling of security incidents by attack type, time and impact, 2015 through 2017

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.



Cover Image: Sampling of security incidents by attack type, time and impact, 2015 through 2017.

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

Each year, new, old and retro cyber threats with new twists plague consumers and enterprises, mostly in search of hefty-yet-rapid financial gain.

The 2017 cybersecurity threat landscape presents a familiar picture, albeit with its own nuances and emerging trends. Three examples from 2017 include the X-Force research discovery of new banking Trojan IcedID, as well as established injection attacks that continued to plague enterprise networks, and the unexpected and widespread destructiveness of **ransomworms**.

In 2017, more than 2.9 billion records were leaked from publicly disclosed incidents. The number of breached records dropped by nearly 25 percent in 2017 as cybercriminals shifted to a focus on ransomware attacks. Instead of compromising data in large quantities, attackers instead regularly locked down access to data, demanding ransom payments from the data owners. As a result, it's been estimated that ransomware attacks cost companies more than USD8 billion[1] globally last year in downtime and other impacts to business, and in ransomware payments. In fact, a few major ransomware attacks on global logistics and transportation companies in 2017 alone cost hundreds of millions of dollars in lost revenue.

The following are the key findings from X-Force data analysis for 2017.

On the enterprise network attacks front:

- **Top-targeted industries experienced a decline in attacks and security incidents, 18 percent and 22 percent respectively, in 2017 over the previous year.** A significant decrease in **Shellshock** attacks is the major contributor to the decline.
- **Injection attacks, the number-one attack vector, nearly doubled in 2017 over the previous year.** Injection attacks accounted for 79 percent of the malicious activity on enterprise networks. The majority of the attacks involved botnet-based command injection (CMDi) local file inclusion (LFI) attacks and CMDi attacks containing embedded coin-mining tools.[2]
- **Financial services tops the targeted industry charts for the second year in a row.** Financial services experienced the highest volume of security incidents and the third highest volume of cyber attacks.

Ransomworm: Malware that exhibits the behaviors of both ransomware, which encrypts data and demands payment for a decryption key, and a worm, which self-replicates by exploiting security vulnerabilities and can automatically propagate throughout a network without user interaction.

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

Most notable financial malware, botnet and ransomworm activity:

- **The most active financial malware, Gozi (Ursnif), toppled Zeus from its number one position.** Gozi activity made up nearly one-fourth of the activity tracked, proving that organized crime is overtaking all other classes of actors in the financial malware-facilitated fraud scene.
- **Only the fittest survive in the financial malware arena.** Once-notorious financial Trojans Neverquest, GozNym and Shifu saw their demise in 2017.
- **Necurs was one of 2017's most notorious botnets.** Despite a relatively inactive first quarter, the Necurs botnet made up for this lack of activity throughout the rest of the year, sometimes spewing millions of spam messages over the span of just a couple of days to recipients across the globe. Necurs spread banking Trojan Dridex and ransomware Locky, GlobeImposter, Scarab and Jaff in campaigns throughout 2017 and into 2018.
- **Destructive ransomworm attacks highlighted the critical need for incident response and disaster recovery.** The three unprecedented and disruptive ransomworm attacks in 2017—WannaCry, NotPetya and Bad Rabbit—used sophisticated exploits against organizations tasked with serving everyday national needs and local economies alike.

A focus on the **inadvertent insider**:

- **Inadvertent insiders were responsible for more than two-thirds of total records compromised in 2017.** Misconfigured cloud servers and networked backup incidents unintentionally exposed more than 2 billion records—making confidential data ripe for picking.
- **Security incidents as a result of inadvertent insider actions are on the rise.** Inadvertent insiders were responsible for more than 20 percent of the publicly reported security incidents that X-Force tracked in 2017—a marked increase from 2016, when inadvertent insiders made up only around 15 percent of reported incidents.
- **More than one-third of inadvertent activity experienced by X-Force-monitored clients involved attackers attempting to trick users into clicking on a link or opening an attachment.** This statistic emphasizes the need for enterprises to embrace a culture of dynamic cybersecurity awareness that adjusts and grows alongside the changing threat landscape.

X-Force also recognizes that the cybercrime economy is thriving on cryptocurrency, and this trend, which largely shaped the threat landscape in 2017, will continue to have an impact in 2018. Drawn to its anonymity factor and peaking market value, attackers are capitalizing on the rise of crypto coins in a variety of ways, from coin-stealing banking Trojans, to ransomware attacks, to directly targeting the cryptocurrency exchange platforms and causing immense losses in that sector.

Inadvertent insiders: Those who are unknowingly the root cause of a security incident through their unaware or negligent actions

TABLE OF CONTENTS

NOTABLE NETWORK ATTACK TRENDS

Security incidents and attacks

A large majority of monitored **security events** are benign. To assess the threat landscape, X-Force filters out non-malicious activity and focuses on **security incidents** and **attacks**. Security incident and attack volume across the top-targeted industries declined in 2017 from 2016, down 22 percent and 18 percent respectively.

A significant decline in Shellshock attacks in 2017, which for more than two years[3] represented a majority of monitored activity since their outbreak in September 2014, is the major contributor to the decline in attacks and security incidents. These CMDi attacks exploit a vulnerability in the GNU Bash shell, which is widely used on Linux, Solaris and Mac OS systems. There were 71 percent fewer Shellshock attacks in 2017 than 2016.

Shellshock attacks declined as a result of the diminishing available attack surface due to patching. However, because of the ease of exploitation, we will more than likely continue to see Shellshock attack activity for years to come, only at a much lower volume than in previous years.

While a decrease in Shellshock attacks and the overall decline in malicious activity targeting monitored networks is welcome news, organizations were still targeted with injection attacks focused on targeting applications.

Year-over-year comparison of monitored security incidents and attacks in top-targeted industries

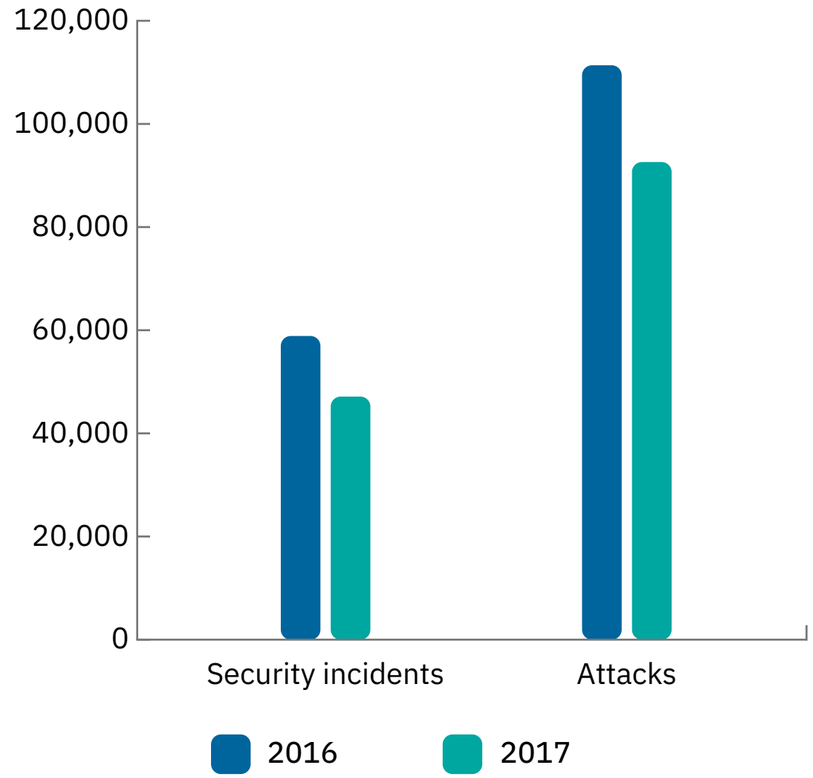


Figure 1: Year-over-year comparison of monitored security incidents and attacks in top-targeted industries.

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's 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.

TABLE OF CONTENTS

Network attack vectors

The mechanisms of attack or attack vectors described in this section are classified according to the MITRE Corporation's Common Attack Pattern Enumeration and Classification (CAPEC) standard. This nomenclature system, as described by MITRE, "organizes attack patterns hierarchically based on mechanisms that are frequently employed in exploiting a vulnerability."[4] The data used in analysis represents attempted attacks against X-Force-monitored security clients.

The most significant finding: The volume of injection-type attacks nearly doubled in 2017 over the previous year as a result of botnet-based CMDi LFI attacks and CMDi attacks utilizing coin-mining tools.

The following sections describe each of the attack types in more detail.

Mechanisms of attack for monitored security clients

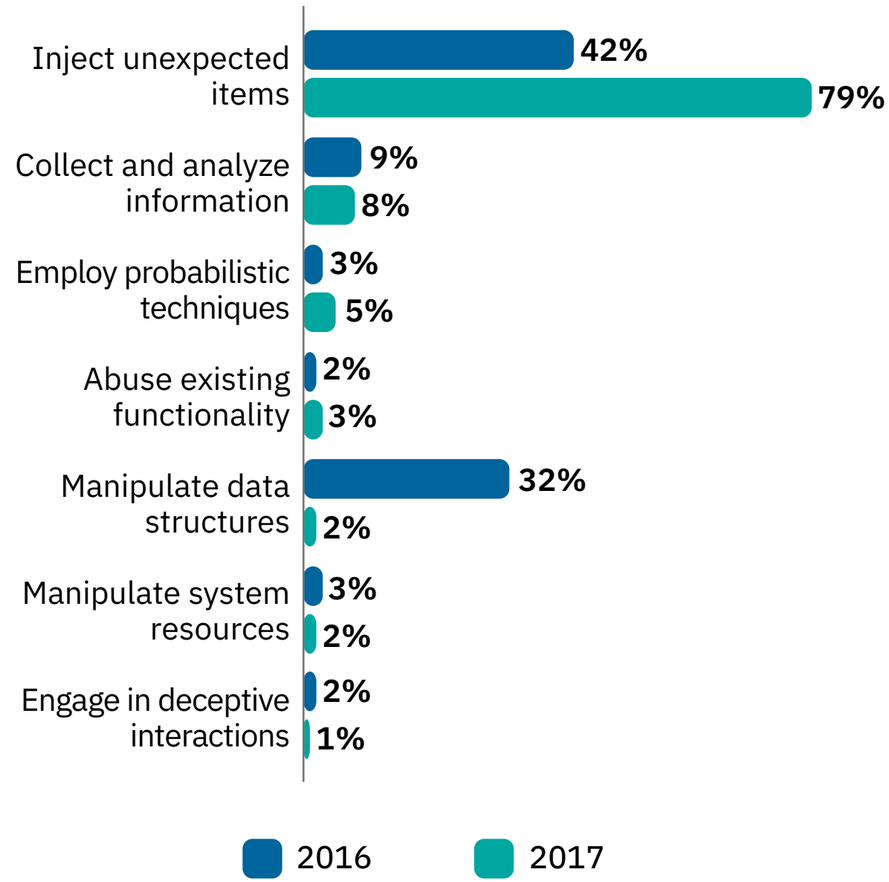


Figure 2: Mechanisms of attack for monitored security clients.

TABLE OF CONTENTS

Inject unexpected items

According to X-Force analysis of 2017 data, the number-one attack vector targeting X-Force-monitored clients—at 79 percent—involved using malicious input data to attempt to control or disrupt the target system. Command injection, which includes operating system CMDi (OS CMDi) and SQL injection (SQLi), belongs in this category.

Injection-type attacks increased significantly—up 37 percent in 2017 from 2016. The majority of the activity can be attributed to two types of attacks: botnet-based CMDi LFI attacks and CMDi attacks utilizing coin-mining tools.

Botnet-based CMDi LFI attacks

More than half of the injection-type attacks can be attributed to botnet-based activity launching CMDi LFI attacks from hundreds of unique source addresses. With a CMDi LFI attack, the attacker attempts to upload malicious files to vulnerable servers using shell commands without requiring user interaction. X-Force observed this activity[5] beginning in late September 2017 and continues to do so into 2018.

Network attacks containing embedded miners

Another third of injection attacks consisted of CMDi attacks involving embedded mining tools with the capability to mine several different crypto coins. In most cases, the attackers attempted to mine CryptoNote-based currencies such as Monero (XMR), which employs the CryptoNight mining algorithm. Monero, reported to offer higher levels of privacy than Bitcoin, is one of several cryptocurrencies growing in popularity among cybercriminals.[6]

These tools were hidden within fake image files, a technique known as steganography, hosted on compromised web servers running Joomla! or WordPress.

This activity, which grew notably[2] over the second and third quarters in 2017, has also continued into 2018 and is most likely driven by the aforementioned rising value of crypto coins and attackers' interest in profiting off of compromised endpoints.

Collect and analyze information

The number-two attack vector, accounting for eight percent of attacks targeting client devices, focused on the collection and theft of information. At one percent lower volume than 2016, most of these attacks involved fingerprinting, often viewed as reconnaissance to gather information on potential targets and 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 an OS or application. Attackers can use the information to identify known vulnerabilities in the target organization's IT infrastructure.

TABLE OF CONTENTS

Employing probabilistic techniques

The third most-prevalent attack type, at five percent, rose two spots from 2016 and involved an attacker using what CAPEC describes as "probabilistic techniques to explore and overcome security properties of the target."[7] 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.

Abuse of existing functionality

Three 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."[8]

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.

Manipulating data structures

In 2016, attacks attempting to gain unauthorized access through the manipulation of system data structures made up 32 percent of observed activity. This percentage dropped significantly in 2017, making up only two percent of the activity, as attackers focused their efforts on using the injection vector. 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."[9]

Manipulating system resources

Attacks attempting to manipulate some aspect of a system's resource state or availability accounted for two 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.

Engaging in deceptive interaction

Only one percent of attacks made attempts to spoof or falsify content, such as a web page or the attacker's identity, in order to appear legitimate to the target victim.

TABLE OF CONTENTS

Most frequently targeted industries

The most frequently targeted industries highlighted in this report were determined based on attack and security incident data from a representative set of X-Force sensors from each industry. The sensors chosen for the index were those that featured event data for the entire year of 2017.

Since security incidents have the highest severity of the monitored event data, they are weighted accordingly when ranking. For this reason, although the information and communications technology industry experienced the highest number of attacks, it ranks second to financial services, which experienced nine percent more security incidents.

The number-one attack vector targeting all top industries in 2017 was injection attacks. Examples and data from notable publicly disclosed security incidents are used in the following sections to provide additional insight regarding the threats targeting the top five targeted industries.

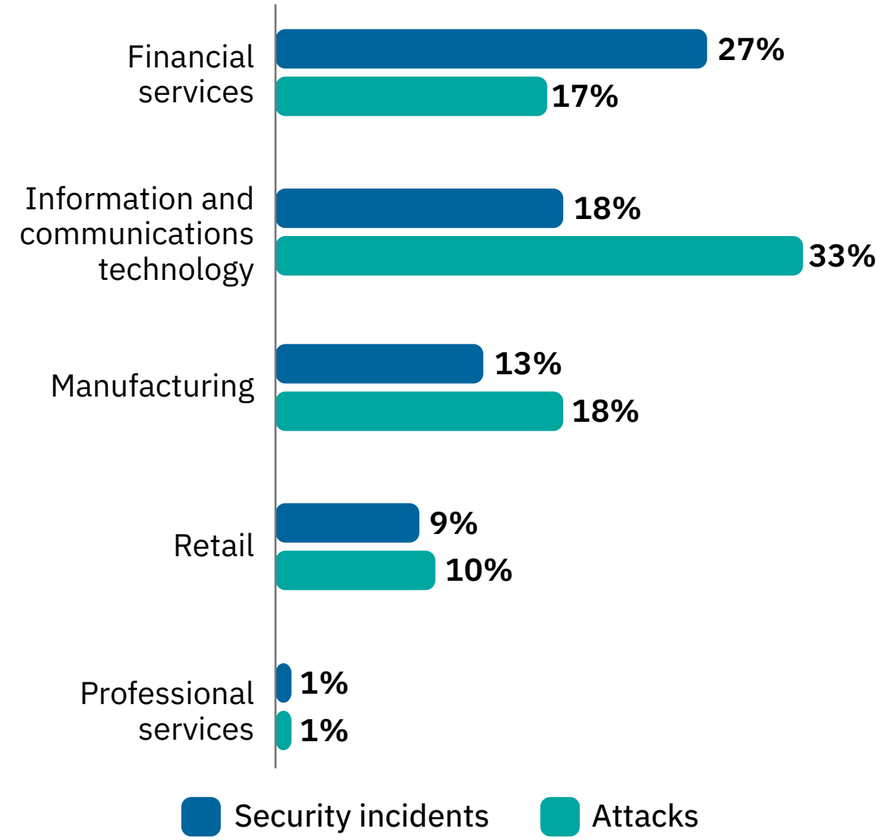


Figure 3: Top five most frequently targeted industries – Percentage of security incidents and attacks in 2017.

TABLE OF CONTENTS

Financial services

According to X-Force data, the financial services sector has been the most-attacked industry two years in a row. Financial services experienced 27 percent of security incidents and 17 percent of attacks. More than 76 percent of the activity involved injection attacks, while nearly 10 percent involved reconnaissance activity.

Losses due to cybercrime are a growing issue for financial organizations across the globe, and seeing this sector top the chart is not a surprise. Attackers are committing direct monetary theft from bank accounts by using phishing and credential-stealing malware, as well as running malicious code to intercept online transactions. Attacks on the financial sector more commonly target bank customers, but organized crime gangs are also after the enterprise networks of those organizations.

For example, in February 2017, reports surfaced[10] indicating that attackers used a **watering-hole attack** by compromising the web servers of a Polish financial regulator, the website of the National Banking and Securities Commission of Mexico, and the website of a state-owned bank in Uruguay. With suspected links to the threat actor known as the Lazarus Group, attackers targeted more than 100 entities and successfully infected at least 30 organizations with malware that was used to exfiltrate data and money from their internal networks over an encrypted tunnel.[11]

Attackers have also been able to hurt financial organizations by preying on unpatched vulnerabilities in their networks. One of the most notable publicly reported financial **breaches** of 2017 affected a major US credit reporting firm and may have impacted more than 145 million people, whose names, birth dates and addresses fell into the hands of attackers.[12] On top of information about nearly half of the US population, the attack involved the theft of 209,000 credit card data sets and documents with personally identifiable information for approximately 182,000 US consumers. This gargantuan data breach was reportedly the result of an unpatched web application vulnerability that led to the unauthorized access of highly sensitive information that could then be used to steal identities and commit fraud.[13]

Another notable breach reported in 2017 affected the US Securities and Exchange Commission (SEC) and also involved the exploitation of a software vulnerability.[14] In the aftermath of the breach, it was determined that information stolen from the SEC may have been used for illegal stock trades, potentially affecting different organizations' bottom lines.[15]

Aside from targeting unpatched vulnerabilities, attackers launched distributed-denial-of-service (DDoS) attacks against financial institutions, impacting business operations and disrupting services.[16] In other cases related to the financial sector, hackers compromised cryptocurrency exchange providers, and in one instance hacked the same platform twice, causing losses so significant that they forced the vendor to shut down its operations altogether.[17]

Breach: An incident that results in the exfiltration of data. In this report, "breaches" refer to notable publicly disclosed incidents, not monitored security client incidents.

Watering-hole attack: A cyber attack in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit.

TABLE OF CONTENTS

Information and communications

The second most-targeted industry, with 18 percent of the security incidents and 33 percent of the attacks, was the information and communications technology sector. The evolution and increasingly interconnected nature of information and communications technology devices and systems, along with modern society's dependence on the technologies and services this sector provides, expose it to more threats than ever and extend the risk of cyber attacks and their potential impact.

Organizations in this sector also suffered a rather elevated rate of network attacks. At more than 89 percent, information and communications technology experienced a notably higher volume of injection attacks as compared to the 79 percent across industries.

There was no shortage of publicly disclosed incidents that plagued this industry in 2017. Malware, malvertising, phishing and SQLi-based incidents[18] were some of the more prominent attack vectors used to compromise information and communications technology networks. In one notable publicly disclosed ransomware incident, a Canadian company in the sector was forced to pay CAD425,000 to restore production and backup databases after attackers successfully infected computers by spear phishing no fewer than six senior company officials.[19]

Three of the top 10 publicly disclosed breaches per records compromised fall under this sector. In terms of cause and effect, two were the result of inadvertent database and server misconfigurations, accounting for more than 1.1 billion records compromised in 2017 alone.[20] At nearly 1.4 billion records, this industry experienced the largest number of records compromised out of all sectors in 2017—for the second year in a row.

Manufacturing

Companies in the manufacturing industry produce new products or goods to include auto, chemical, appliance and equipment manufacturers, to name a few. Manufacturers experienced 13 percent of the security incidents in 2017 and, at 18 percent of attacks, experienced slightly more attacks than the number-one targeted industry, financial services. Nearly 30 percent of all network attacks in this sector involved SQLi tactics, many of which could be avoided today with better security reviews and controls.

Few manufacturing sector incidents were disclosed publicly in 2017. X-Force researchers suspect some underreporting may be the reason. This could be because the manufacturing sector is not subject to the same obligations to report breaches as industries such as financial services, healthcare and retail. Nevertheless, there were some incidents in which customers were affected that did see public reporting. In one such incident, the financing department at the Canadian branch of an international car manufacturer alerted customers that their data may have been stolen in a breach exposing vehicle identification numbers (VINs) and credit information for more than one million people.[21]

The manufacturing sector was also hit by various ransomware attacks in 2017, which notably caused downtime after disruptive cases of WannaCry and NotPetya infections.[22]

TABLE OF CONTENTS

Retail

The fourth most-targeted industry, retail, experienced nine percent of the security incidents and 10 percent of the attacks. The retail industry was not as affected by injection attacks and ranked well below the cross-industry average of 79 percent, with just 57 percent of activity involving injection attacks. Retailers did experience a greater-than-average number of brute-force attacks, at nearly 25 percent of attacks.

While injection and brute-force attacks plagued retailers' networks, point-of-sale (POS) malware remained a constant threat to retailers' POS systems,[23] which are the most decentralized part of retail businesses. This factor makes these systems harder to protect than the organization's core networks since they reside in multiple individual retail locations versus centralized corporate offices.

In the aftermath of many of the publicized cases, POS malware proved to have remained undetected for months, even up to a year, before the attack was identified and remediated. In one reported incident, a US retail chain with more than 800 stores disclosed that, over a seven-month period, payment card data was continually stolen from POS systems at some of its locations.[24] In another reported incident, malware was used to steal credit card data from customers at 223 retail locations of a large clothing store during a nearly one-year period.[25]

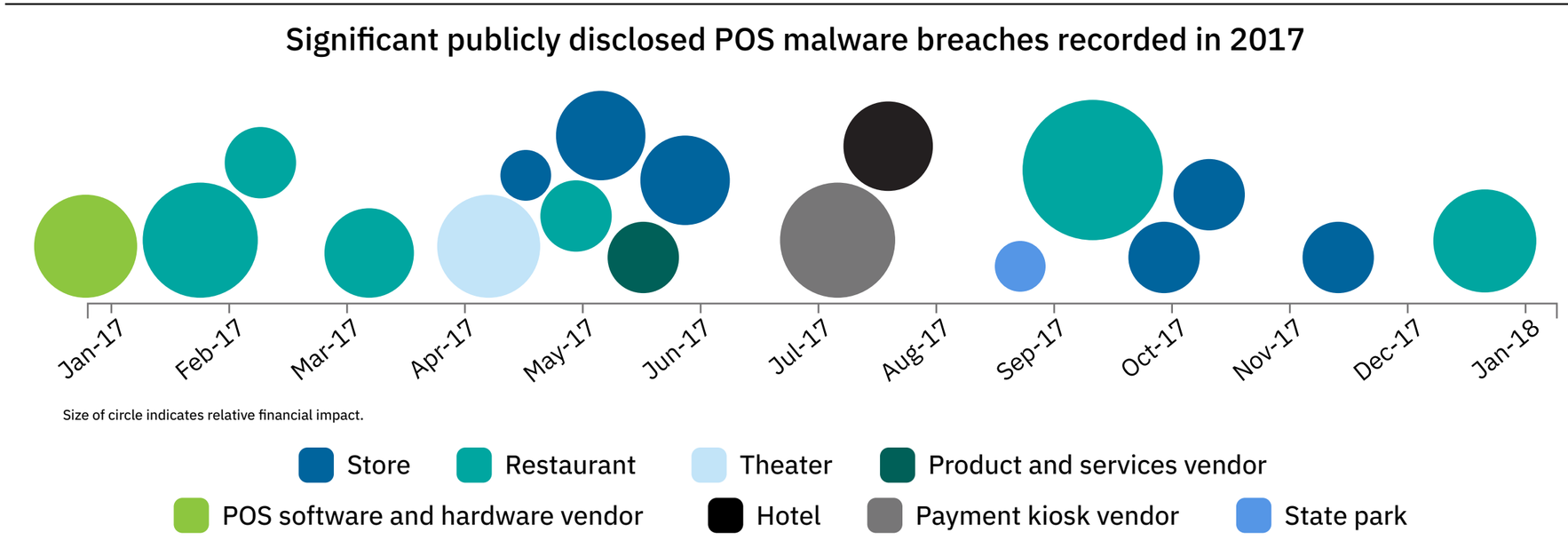


Figure 4: Significant publicly disclosed POS malware breaches recorded in 2017.

TABLE OF CONTENTS

Professional services

The fifth most-targeted industry, professional services, experienced 14 percent of the security incidents and one percent of the attacks. More than 62 percent of the attack activity involved injection attacks, while a little more than 20 percent involved the abuse of existing functionality. Many of the attacks that abused functionality were flooding attacks intended to cause a denial of service.

At nearly 390,000,000 compromised records, the professional services industry ranked third among the sectors for most compromised records in 2017. The largest breach publicly disclosed in this industry involved a misconfigured cloud server. Over a 12-day period, a conservative data firm that tracks voter preferences inadvertently exposed 1.1 terabytes (TBs) of sensitive information, potentially comprising the personal details of 61 percent of the US population.[26] The other two largest publicly disclosed breaches in this sector also involved misconfigured and unsecure databases, underscoring the rising urgency of security controls and audits in complex IT environments.[20]

TABLE OF CONTENTS

MOST NOTABLE MALWARE SHIFTS OF 2017 AND BEYOND

Losses due to cybercrime are a growing issue for banks and service providers across the globe—with one firm forecasting USD2.1 trillion in losses by 2019,[27] and another firm predicting losses up to USD6 trillion by 2021.[28] These attention-grabbing amounts should urge organizations to take heed and plan for protecting their assets and customers.

A large part of overall losses to cybercrime is generated by financial fraud and financially motivated attacks. Within that domain, banking Trojan-driven attacks have gradually become the playing field of organized crime groups—a trend that has become quite pronounced in the past three years.

X-Force research tracks banking Trojan activity and indicates that new financial malware most often will feature sophisticated source codes, high-value targets and grand-larceny capabilities that paint the picture of an organized operation rather than a small team or lone actor.

As an example, groups operating the Dridex or TrickBot Trojans can easily include dozens of people in different roles and need-to-know levels. Other malware groups, such as the operators of Gozi, are considered crime-as-a-service operations and can have links to an even larger number of actors in different geographical hubs.[29]

While it would appear that the financial crimeware arena has reached a somewhat predictable form, shifts that shaped 2017 and that will likely affect 2018 show it is still an evolving landscape.

2017's most active financial malware families

Looking back at the most active financial Trojans in 2017 cybercrime shows that, for the first time, Zeus Trojan variants placed lower than Gozi in terms of activity for the year. This change further demonstrates that cybercrime has moved on from commercial and fly-by-night malware operators, and that organized, business-like gangs are taking the lead in 2018.

Most prevalent financial malware families – 2017

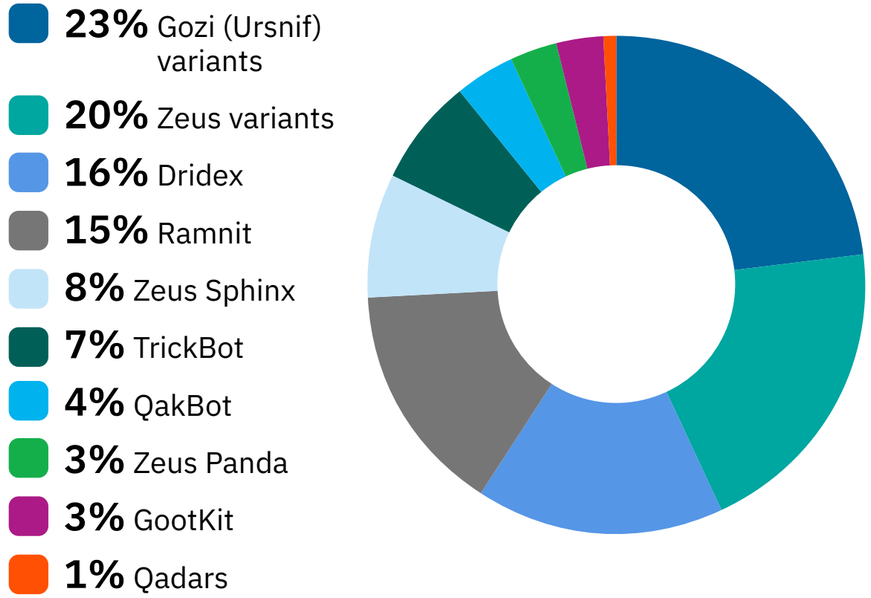


Figure 5: Most prevalent financial malware families – 2017.

TABLE OF CONTENTS

2017's newcomers

The banking Trojans that facilitate financial fraud are a pivotal part of the organized cybercrime supply chain. But writing sophisticated code is only the tip of the iceberg within the overall operation of organized cybercrime. Without the ability to fund the project and connect with other crime gangs, a gang will not be able to scale. It is therefore rather rare that entirely new gangs arise. Most years see one or two new malware codes at most, and that was case in 2017 as well with a new Trojan, IcedID, in the US and UK, and a new Ursnif (Gozi) iteration in Australia. Aside from those two global malware codes, Brazilian developers have been working to improve and spread the Client Maximus Trojan. More on each of these appears in the following sections.

IcedID emerges in the US and UK

In September 2017, X-Force research discovered and analyzed a new banking Trojan[30] that emerged in the wild. The malware was coined IcedID, and while the testing period started in September, actual infection campaigns did not take place until October 2017. X-Force researchers noted that IcedID features a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan.

IcedID targets banks, payment card providers, mobile services providers, and payroll, webmail and e-commerce sites in the US. Two major banks in the UK are also on the malware's target list.

One notable finding about IcedID is that it spreads via another Trojan—the Emotet malware. Emotet[31] was originally a banking Trojan itself, derived from the Bugat source code, which is also the core of the Dridex Trojan.

X-Force research indicates that a threat actor or a small cybergang has been operating Emotet as a distribution operation for banking Trojans, especially serving the cybercrime elite in Eastern Europe. Emotet's most prominent attack zone is the US. To a lesser extent, it also targets users in the UK and other parts of the world.

Emotet was one of the notable Trojan distribution methods in 2017, linked with groups operating QakBot[32] and Dridex,[33] both of which favor targeting business banking. It added IcedID[30] and Zeus Panda[34] as new payload drops in late 2017.

When it comes to tactics, techniques and procedures, IcedID has a few tricks up its sleeve. The malware features a network propagation module to allow it to spread to multiple users and terminal servers that share the same local area network/wide area network connection.

The malware monitors victims' online activity by setting up a local proxy for traffic tunneling, a concept used by the GootKit Trojan.[35] Its fraud attack tactics include both web-injection attacks and sophisticated redirection attacks similar to the schemes used by Dridex and TrickBot.[36]

TABLE OF CONTENTS

After X-Force published information about IcedID, it appears the group operating it has taken a step back and reduced its activity. Will IcedID be launched into wider campaigns? That is doubtful at this time since this malware started out in targeted fashion, electing the Emotet group as distributors, which makes it inherently much less aggressive in terms of attack scope.

Ursnif (aka Gozi) v3 emerges in Australia

Starting in August 2017, X-Force research began detecting a new variation of the Ursnif Trojan[37] that was being tested in the wild. Per X-Force analysis, the malware is entirely based on the same malcode as the original Ursnif Trojan (aka Gozi ISFB) but features some modifications on the code-injection level and the fraud-attack tactics.

Beyond the material modifications, the malware's developer also switched the internal build version, which now shows as v3 increments. The existing Ursnif variants are v2 builds, which would make this iteration new, and an upgrade of sorts that was most likely undertaken by a different malware developer and a different group.

Ursnif v3 first appeared in Australia, and the notable thing about it is that it featured some web-injection attacks, but it had separate configurations with redirection attacks[38] created to target Australian business and corporate banking services. Redirection attacks are a sophisticated tactic currently used by cybergangs such as Dridex, GootKit, TrickBot[36] and IcedID.

Ursnif v3 emerged in late 2017, and for now, X-Force research has detected its activity only in Australia and New Zealand. The malware may spread to other parts of the globe, but that would depend on its operators' resources and whether they plan to expand.

Client Maximus emerges, thrives in Brazil

In a niche of its own, Client Maximus is another malware code that emerged in 2017,[39] and has been growing and upgrading its capabilities in Brazil.

Unlike the plethora of Delphi-based malware in the region, Client Maximus caught X-Force researchers' attention for its relative sophistication, stealthy delivery tactics[40] and ongoing code development.[41]

The purpose of the Client Maximus malware is financial fraud, and as such, its code aspires to create the capabilities that most banking Trojans have: They allow attackers to monitor the victim's web navigation and to take control of the online banking session at will.

To do that, Client Maximus monitors open Internet tabs, and, if it matches them with a target on its list, an operator can launch real-time device takeover using a remote access tool to ride the authenticated banking session. The attacker displays pre-made fake overlay screens to users to keep them engaged and have them provide transaction authorization codes. The codes can ultimately allow the attacker to complete fraudulent transactions from that trusted device.

TABLE OF CONTENTS

X-Force research notes that, unlike other codes in Brazil, Client Maximus has been consistently evolving to evade anti-virus detection and update the code's capabilities. Moreover, the malware has been spreading in a rising number of campaigns in Brazil. Both these observations suggest that Client Maximus is a commercial offering being developed and sold to other criminals by its creators.

Overall in 2017, X-Force research indicates an ongoing escalation of malware codes in Brazil. After observed trending collaboration with external parties,[42] it appears there has been a permanent step-up in sophistication of malware codes that target online banking users in the country.

Notable or rising activity

Aside from the moving parts of the cybercrime arena in 2017, some of the existing constituents held steady, showing continued and rising activity. The top three in this category were Ursnif for its activity volume, TrickBot for its consistent activity bouts, and the QakBot Trojan for re-emerging and targeting businesses. A special mention in this section notes the activity of the Necurs botnet[43] as a major cybercrime group that distributes banking Trojans.

Ursnif v2 (aka Gozi)

By order of activity volume, X-Force research notes that Ursnif v2, a longstanding cybercrime group, has been 2017's most active operation in a few measures:

- Number of campaigns
- Code updates
- Geographic reach
- Attack volume

Aside from its usual targeting patterns, starting the third quarter in 2017, X-Force has observed Ursnif step up its focus on Japanese banks,[44] making activity in Japan, which was previously sporadic, more consistent. Ursnif targets Japanese banks and credit providers as well as e-commerce and popular cryptocurrency exchanges.

TrickBot

In terms of code updates and campaigns, TrickBot was one of the most consistent groups in 2017. During the third quarter of the year, when many people around the globe take summer vacation, other malware groups avoid wasting their efforts on emails that would not be opened before the malicious files were detectable and blocked. TrickBot, however, stood out as the one cyber gang that did not reduce volumes. It continued to distribute the malware through the Necurs botnet and via fake domains that were registered in order to target UK banks. TrickBot was second only to Gozi in terms of code updates and campaigns.

TABLE OF CONTENTS

Overall in 2017, TrickBot continued developing a global reach and building additional redirection attacks for many of its targeted entities. It regularly tests online banking procedures and continues to add to target lists. Specifically, it has added business banking, payment cards and cryptocurrency exchange platforms to those lists, which have grown to more than 1,000 URLs each.

QakBot (aka QBot)

QakBot[45] is an old financial Trojan that resurfaced in 2017. This gang-owned code has been around since 2009, at which point it was one of the only cybercrime operations that focused solely on US business banking accounts.

QakBot activity has been active on and off through the years, but it came back in 2017 with the same focus on North American business banking. Its modular, multithread code is designed to enable network propagation, security evasion, online banking fraud and data exfiltration.

QakBot works in limited scope. It is delivered in a targeted way by Emotet into already-infected endpoints. In 2017, X-Force observed QakBot in what might have been an operational glitch, causing mass Microsoft Active Directory lockouts[46] on compromised networks in an attempt to spread to other endpoints in the organization. Sporadic QakBot campaigns continue to target US financial entities.

Necurs botnet still hitting hard

The Necurs botnet, one of the biggest distributors of malware in 2016,[47] continued its reign in 2017 by distributing millions of emails containing malicious attachments in each of its aggressive campaigns. Despite a relatively inactive first quarter,[43] with the first rise in activity observed in late March 2017, Necurs campaigns sent millions of spam emails during the rest of the year. Over a two-day period in August, for example, X-Force research observed four separate Necurs campaigns spamming 22 million emails.

Necurs campaigns were diverse through the year, starting in the first quarter with a variety of so-called "penny stock"/pump-and-dump spam,[48] spewing emails that touted the supposed allure of low-value stock, attempting to influence the stock price over a short time to make a quick profit. In the second quarter, Necurs began to send out spam with malicious attachments such as Dridex and Locky alongside the penny stock spam. In May, Necurs operators focused on distributing Jaff ransomware, and by June they increased their efforts in sending out TrickBot-laden spam to email recipients across the globe. Necurs activity also included other malware campaigns, pushing GlobeImposter and Scarab ransomware later in the year.

Analyzing spam attachments shows that more than half of Necurs campaigns in 2017 delivered either Dridex, TrickBot or Locky attachments. Another 41 percent of Necurs campaigns distributed the Jaff and GlobeImposter ransomware codes.

TABLE OF CONTENTS

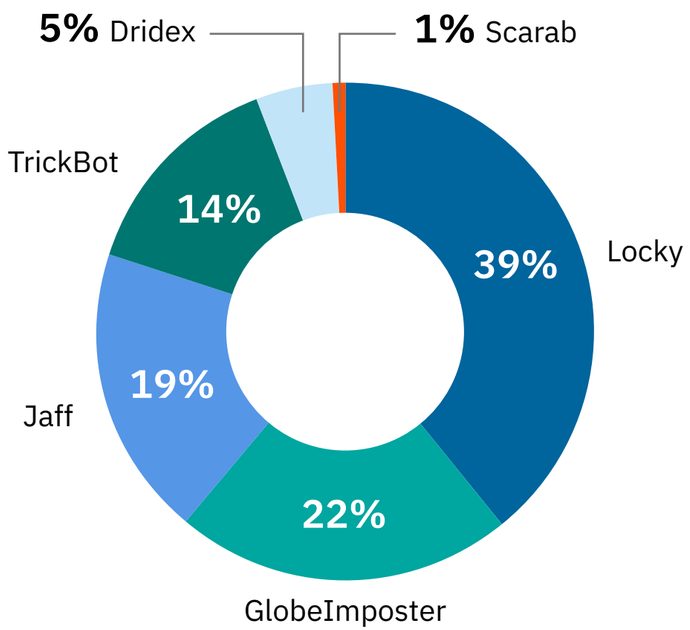


Figure 6: Necurs campaigns – Top malware families per spam count in 2017.

While Necurs activity kicked off 2018 with vast campaigns, the level of social engineering in some of these campaigns was rather basic.[49] The spammers attempted to trick recipients into opening malicious attachments with email subjects such as "Scan data" or "Invoice," and little effort has been made to make the email look realistic.

These campaigns were most likely gang-dependent because Necurs campaigns carrying TrickBot, for example, featured better social engineering ploys than the Necurs campaigns featuring other types of malware and scams.

2017's goners

Although 2017 was definitely a busy year for malware activity, some cybercrime groups—new and old—departed from the scene for various reasons, while others greatly reduced their activity volumes and scope.[50] Some of the notable departures were Neverquest, Shifu Trojan and GozNym.

Neverquest's 2017 exit

A very significant exit in 2017 featured the Neverquest Trojan[51]—a cybercrime-as-a-service gang that has been part of the crimeware arena since 2013. The malware was sourced from the Gozi ISFB code but evolved separately to feature its own modules and capabilities.

At its prime, Neverquest, aka Vawtrak, was a vast operation that touched many parts of the globe. Through their years of operation, Neverquest operators enabled their accomplices to target business banking accounts, allowing them to steal hundreds of millions of dollars from organizations every month. The operation was considered sophisticated and robust, and, in cybercrime terms, it was also long-standing. According to X-Force research, Neverquest has been on the top of the global malware chart since 2014.

TABLE OF CONTENTS

In late 2016, the group hit a road bump that shook it enough to disband. One of its key members, the person suspected to be the malware's author, was arrested in Spain.[52] By January 2017, X-Force saw Neverquest campaigns abruptly halt, and the attack pattern gradually died out.

Goodbye Shifu?

The Shifu Trojan's story is actually an unusual one in the cybercrime arena. Shifu emerged in Japan in 2015,[53] and, from the beginning, its code was considered to be quite sophisticated based on X-Force analysis. More than just a hybrid code, Shifu took best-of-breed parts of several banking Trojan codes in a way that could be crafted only by a malware-savvy developer who knew those codes and had access to them.

X-Force monitoring of Shifu's activity showed that it was quite active through much of 2016, leveraging the Angler exploit kit to spread around during the period following its release. However, by September 2016, X-Force saw a sharp drop in Shifu activity and a dying-out trend since.

What happened to Shifu? None but its own operators may know the reason, but the speculation is that the gang was simply not connected enough to operate globally and eventually disbanded. Shifu is still one of the most professional Trojan codes in existence, and it could be one that we will see in the future if another group takes over.

What to expect in 2018?

The financial cybercrime arena is not expected to slow down in 2018. Even with some groups gone, the ones that remain are those who manage complex operations that include the entire supply chain linked with financial crime, especially its money-laundering aspects.

Some of the trends X-Force expects to see in 2018 are:

Trojan codes will likely be exclusive to elite cybercrime and syndicates

Commercial codes are not likely to make it far in the 2018 security landscape. With rising awareness and bank controls, online fraud is becoming somewhat of a profession, and malware authors who sell their codes are not going to keep up with evolving security, machine learning and artificial intelligence controls. This suggests that well-funded elite cybercrime gangs and syndicates will be most likely to invest in commercial codes.

More destructive ransomworms

Destructive ransomworms WannaCry[54] and NotPetya[55] gave the world a glimpse into what attackers can achieve with sophisticated exploits. Drawing inspiration from those attacks, it was not long after that the TrickBot Trojan adopted network propagation based on the Server Message Block (SMB)[56] protocol.

In 2018, we expect to see more wide-spread vulnerabilities and sophisticated exploits in malware that target both the private and public sectors.

TABLE OF CONTENTS

A focus on businesses

Financial malware operators will most likely be focused on businesses, since compromised business accounts are more likely to yield higher profits than consumer accounts. This leaves most of the consumer base to the smaller cybercrime groups and mobile malware operators, who will likely be picking up the fraud slack in 2018. Mobile malware operators are less discriminating, spreading their malware far and wide, which typically results in more compromises to consumer accounts than to business accounts.

Bank heists

Groups that carry out attacks against banks' internal systems not only remained at-large after major heists in 2015[57] and 2016,[58] they also continued their activity in 2017.[59]

X-Force expects to see more attacks preying on banks' internal systems and processes in 2018, as well as a continuation of the focus on automated payment relays and ATMs used by the banking industry.

Mobile malware to drive rise in fraud

In 2017, mobile malware became a cross-channel fraud enabler.[60] With the increasing use of mobile payments, shopping applications and mobile banking, cybercrime is ready to take on the consumer market, and fraud cases are expected to increase via that channel in 2018.

Android banking Trojans have been spreading across the globe, and, reminiscent of the Zeus malware's spread, most of them are based on the same leaked source codes of malware such as GM Bot and BankBot. That does not stop these codes from making it into official application stores and ultimately compromising users' devices to take over their financial accounts.[61]

TABLE OF CONTENTS

RANSOMWORMS: MALWARE TO THE POWER OF DISRUPTION

If the security industry learned one thing in 2017, it was the dire need for incident response that followed the unprecedented and disruptive outbreaks of ransomworms on company networks across the globe midyear.

More than employing security basics, and even more important than having detection capabilities, those who had response plans in place and had trained staff to execute those plans were able to respond sooner and recover from the attacks with lesser impact, enjoying shorter downtimes and smaller related financial losses.

While many chief information security officers (CISOs) were already aware and concerned about **crypto-ransomware**—a 2016 IBM study found that nearly half of business executives surveyed had experienced ransomware attacks in the workplace[62]—organizations faced a new breed of crypto-ransomware in 2017, and X-Force projects that this is likely to happen again in 2018.

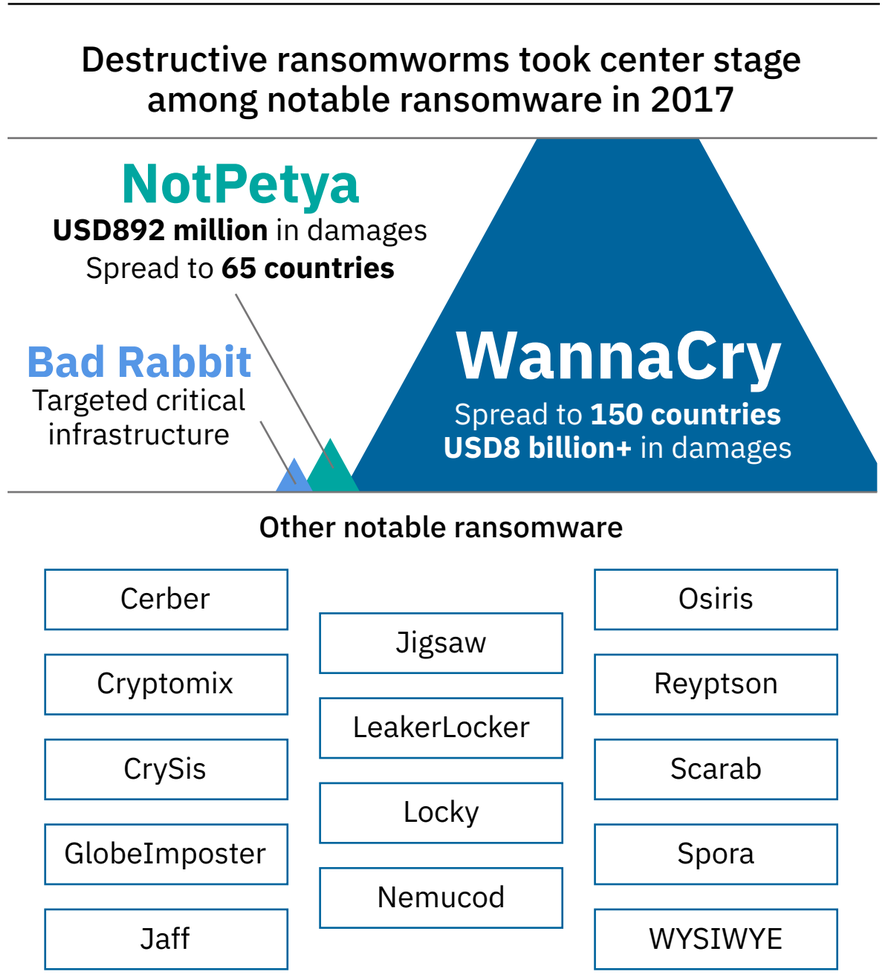


Figure 7: Destructive ransomworms took center stage among notable ransonware in 2017.

Crypto-ransomware: Malware that uses symmetric/asymmetric encryption to mass-lock files on the endpoint.

TABLE OF CONTENTS

Data loss and disruption

With the potentially irreversible encryption lock of crypto-ransomware, victims without up-to-date backups often choose to pay the ransom their attackers demand. Losing one's files on personal devices may cost a few hundred dollars, but that effect extends much further for organizations,[63] where infected users could cause the company to lose massive amounts of data, and possibly to have to pay the criminals[64] considerable sums of money to get it back. In some cases, financially motivated attacks on organizations become more targeted, forcing their way through networks to find and encrypt data tucked away on backup servers.[65]

This trend became a predominant threat for security leaders, and organizations hit with malevolent attacks were often caught off guard and forced to pay.[19] As a result, some are even said to keep some crypto coin on hand in order to pay more quickly in case of an unexpected outage due to an attack.[66] The practice of paying off the criminals, however, is discouraged by law enforcement agencies.[67]

Enter data destruction attacks

The ransomware problem was already riding a high wave in the past few years, with ransomware incident costs predicted to exceed USD11.5 billion annually by 2019,[68] when even more damaging versions hit organizations worldwide about halfway through 2017.

WannaCry

The first case that broke and that exercised the full power of mass data destruction was coined the WannaCry attacks.[56] WannaCry was a widespread crypto-ransomware attack that hit organizations in more than 150 countries within the span of 48 hours, spreading like wildfire through the Internet and hitting hundreds of thousands of endpoints on its way.

By coupling the malware with exploits leaked from the National Security Agency (NSA),[69] the operators of WannaCry/WanaCrypt0r 2.0[70] were believed to have caused the biggest attack of its kind ever recorded.

But while the attackers invested in modifying the exploits for attack on private enterprises, and in spreading the malware to ensure it wormed its way into organizational networks, they did not invest much in the mechanism that was supposed to gather payments and unlock files in return. That meant that payments could not result in the decryption of files.

That was probably the first indication of a ransomware attack that was not designed for financial gain. Instead, it seemed to be designed for disruption of operations[71] and destruction of data that would never be recovered from the attackers,[72] not to mention potential risk to human lives in cases where disruption affected critical infrastructure.

TABLE OF CONTENTS

WannaCry took place in May 2017, at which point voices in the security community already dreaded a sequel. And a sequel was soon to come, this time in the shape of the NotPetya attacks.[55]

NotPetya

NotPetya swiftly hit in June 2017, and while it was effective, it did not attain the same distribution as WannaCry had, since many organizations had already patched the vulnerabilities and were more vigilant after the first attack. Nonetheless, the attacks were noteworthy for their reach into critical infrastructure in Ukraine, paralyzing Ukrainian government resources, the National Bank of Ukraine, the country's transportation services and some of its largest power companies.[73]

The code was a play on the existing Petya ransomware.[74] However, the Petya spreading mechanism was refreshed, this time using a software update as a gateway, and the worming feature repeated the reliance on the same leaked NSA exploits.[75] Again here, the malware would demand payment, but the mechanism designed to collect payments was faulty and did not actually enable recovery of files to those who paid.

During analysis of the code, IBM X-Force Incident Response and Intelligence Services (X-Force IRIS) researchers found that the malware did not allow for data recovery even with access to the attacker's private encryption key. This observation would, by definition, turn NotPetya into a wiper malware and not ransomware.

After finalizing the analysis, X-Force IRIS concluded that the Petya variant attacks were intended as destructive attacks[76] against Ukraine and spread internationally due to the connectivity between businesses across the globe.[77]

TABLE OF CONTENTS

Bad Rabbit

Bad Rabbit[78] was the last ransomworm attack in 2017, arriving in October. It was yet another reminder to organizations that they must patch systems and prepare incident response and recovery plans for the ransomworm scenario.

Bad Rabbit attacks were once again focused in Eastern Europe, bringing Ukrainian infrastructure back to the arena. Sporadic cases were also recorded in Turkey, Germany, Bulgaria, the US, South Korea, Poland and Japan, according to reports from different sources.[79]

One of Bad Rabbit's victims was Odessa International Airport, which is located in the third-largest city in Ukraine, causing flight delays due to manual processing of passenger data. Ukrainians also saw their subway system affected, causing payment delays on customer service terminals, although trains continued to run normally.

Bad Rabbit's operators compromised news and media sites in a watering-hole type of scheme to have visitors redirected to malicious landing pages they controlled. On those pages, users were advised to install an Adobe Flash update, at which point a malicious download took place, delivering the malware dropper in what's called a drive-by attack.

Security analysts quickly drew links to previous attacks. According to information from the security community, some of the Bad Rabbit code was borrowed from Petya ransomware, which was also part of the NotPetya attacks. The same techniques were used for spreading the malware throughout corporate networks, relying on the Microsoft Windows Management Instrumentation Command-line (WMIC) and using the NSA's BlueRomance exploit. Also, websites used to propagate the malware were hosted on the same servers that distributed NotPetya infections back in June 2017.[80]

TABLE OF CONTENTS

INADVERTENT INSIDER: BILLIONS OF RECORDS EXPOSED

To err is human. Unfortunately, the lasting effects of a simple mistake in a digital world can be catastrophic. When it comes to data security, the potentially detrimental impact of an inadvertent insider on IT security cannot be overstated.

Sampling of publicly disclosed security incidents as a result of inadvertent actors, 2015 through 2017

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.

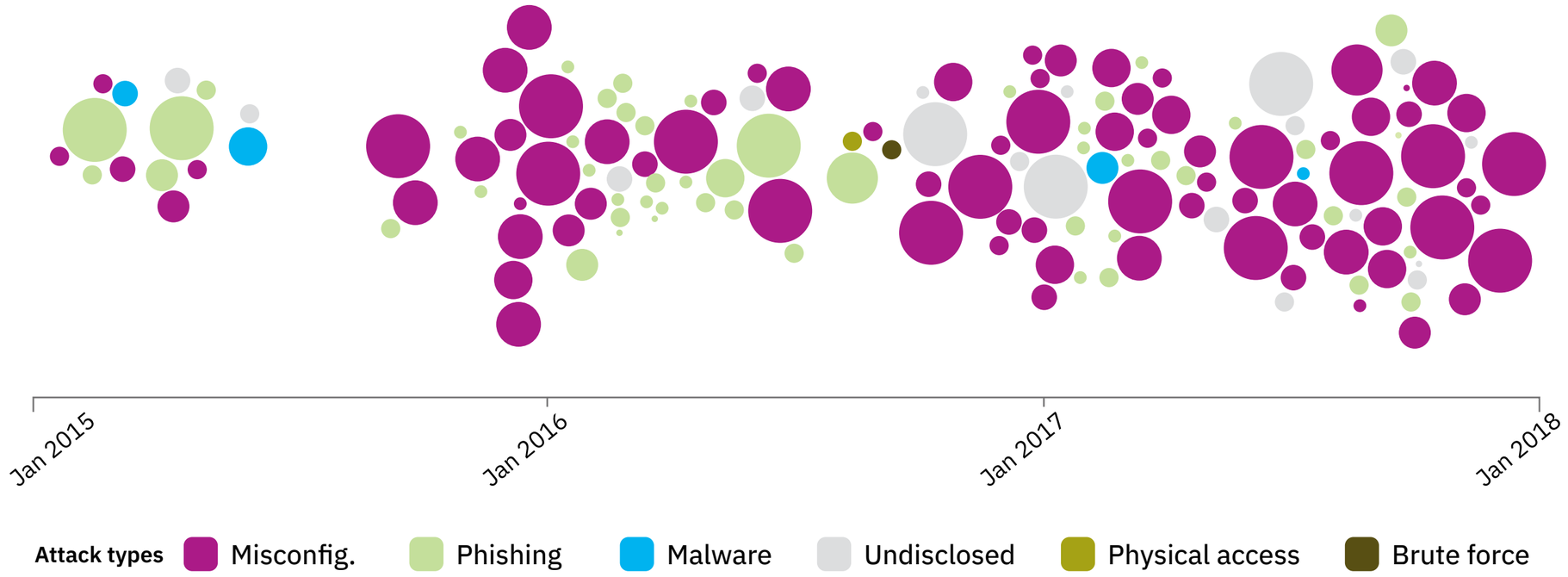


Figure 8: Sampling of publicly disclosed security incidents as a result of inadvertent actors, 2015 through 2017.

TABLE OF CONTENTS

MISCONFIGURED CLOUDS, PHISHING AND OTHER INSIDER-INFLICTED WEAKNESSES

With mobility and bring-your-own-device (BYOD) trends being the norm in today's workplace and productivity, many say that everyone is an insider threat. Does this outlook materialize in real-world security incidents? The numbers paint a grim picture.

As gleaned from information on publicly disclosed breaches in 2017, there were several high-profile breaches eventually attributed to the errors of inadvertent insiders.

Some of the most common scenarios included basic misjudgment. These include employees storing intellectual property on their own insecure personal devices and end systems and employees and insiders falling for phishing emails that resulted in account takeover or access to sensitive data. In addition, erroneous permission-level attribution on cloud services and networked backups exposed sensitive data through weak or non-existent authentication.

The following sections provide further details on the most prominent incident types attributed to inadvertent insiders affecting organizations in 2017.

Misconfigured clouds

Misconfigured cloud servers, networked backup incidents and other improperly configured systems were responsible for the exposure of more than 2 billion records, or nearly 70 percent of the total number of compromised records tracked by X-Force in 2017. There were 424 percent more records compromised as a result of these types of incidents in 2017 than the previous year.

Why the increase year to year, and why are these breaches so damaging? A large contributor is a growing awareness among the cybercriminal community of the existence of misconfigured cloud servers.

In 2015, using the Shodan search engine, a security researcher tapped into a number of misconfigured cloud databases that were world-readable without any form of username or password authentication required.[81] Since then, other researchers have uncovered these unprotected caches of data, using the same tools and techniques to uncover misconfigurations. Finding such servers can be as simple as entering a URL into a browser to see if it returns a directory listing. There are also open-source scripts that make scanning for open cloud storage much easier, drawing more attackers to look for vulnerable places.

By the end of 2016 and throughout 2017, attackers moved to criminal action, using those same tools to target open systems, and even stealing data from the databases before dropping all tables—thereby locking or preventing legitimate use of the database—and demanding a ransom payment. This kind of drop-locking attack impacted more than 45,000 databases during that time period.[82]

Cloud service misconfigurations can be further categorized into publicly accessible cloud storage,* unsecured cloud databases, and improperly secured rsync backups or open Internet-connected network area storage devices.

It is worth noting that in these cases, the error was not the fault of the cloud vendor, but rather the people implementing the services who did not properly secure their data.

TABLE OF CONTENTS

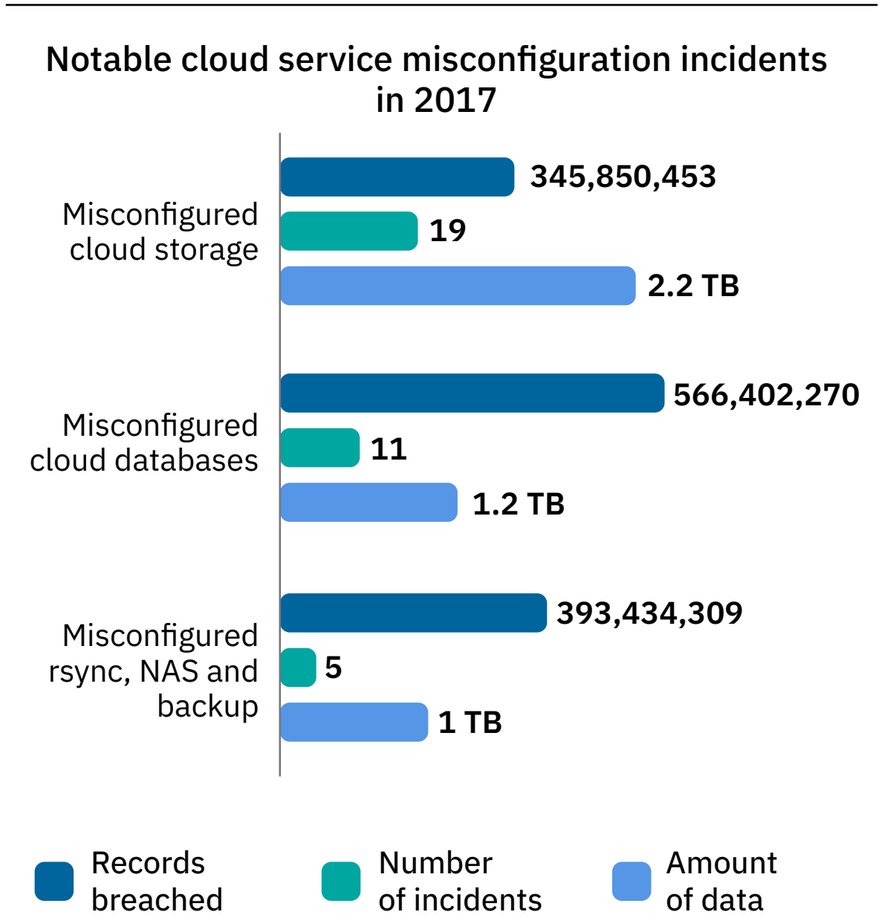


Figure 9: Notable cloud service misconfiguration incidents in 2017.

Records breached and amount of stolen data is based solely on public reports and may not represent a full accounting for all incidents.

Several of these incidents contained very sensitive data. In one of largest incidents—which involved 198 million registered US voters—personal information such as date of birth and address, political donations and views, as well as detailed marketing demographics were exposed.[83]

In one incident, a jobs database for military contractors exposed detailed information about people with US Special Forces backgrounds.[84] Another open system contained a 120-day history with detailed Global Positioning System (GPS) location data for individuals with a certain kind of tracker in their vehicles.[85]

Unsecured, publicly accessible data from a seemingly simple custom keyboard mobile application revealed that the application was logging keystrokes and private messages for users and storing this private data in the cloud without the users' knowledge.[86]

TABLE OF CONTENTS

Falling for the phish

Despite the increased use of chat and instant messaging applications, email continues to be one of the most widely used communication methods for any organization, and phishing attacks continue to be one of the most successful means of making unknowing insiders open the door to malicious attackers.

To create the initial compromise, phishing can be used effectively by attackers in a multitude of ways, including:

Compromised corporate credentials

A link or attachment inside a phishing email can lead employees to a web page where their credentials will be harvested, all while they think they are on a company-issued resource. By compromising credential sets for corporate networks, attackers can gain access to network resources and use additional schemes to compromise other users in the organization.

Dropping malware

Using email, attackers can simply send malicious files to a user in the hopes that the recipient will open attachments or visit malicious links. Unfortunately, more often than not, email recipients appear to be tempted to check unsolicited mail, or they are phished with highly customized formats that are harder to diagnose as malicious.

Account takeovers

Infection with malware is only one of the many dangers of a successful phishing campaign. Attackers who wish to further embed themselves into an organization can use phishing attacks to gain access to any web resource a company uses by creating fake login pages. The information harvested enables the attacker to take over user accounts and gain access to anything the user can access. For example:

- A popular video-hosting and media joint venture was targeted in a phishing attack that resulted in the compromise of 3.12 TB worth of internal files.[87]
- Several healthcare clinics were affected by data breaches in which an attacker was able to gain access to clinic employees' email accounts, which contained patients' protected health information (PHI).[88]

Business email compromise

When it comes to the most lucrative types of phishing attacks, business email compromise (BEC) has been a growing tide for several years.[89] Also known as "CEO fraud" or whaling attacks, BEC scams purport to originate from an owner, chief executive officer (CEO) or other high-ranking employee. These scams typically attempt to lure recipients into performing wire transfers or making large payments.

TABLE OF CONTENTS

BEC scams have plagued thousands of victims globally and have been responsible for the theft of more than USD5 billion over a three-year period between October 2013 and December 2016.[90] In one incident in 2017, a scammer tricked a Canadian university into wiring CAD11.4 million.[91]

Once again here, the entry point is email, and the door opener is an unwitting employee who may make the mistake of proceeding to act on the phish without checking internally with the supposed sender.

It seems that once a pattern of successful attacks such as these is established, attackers will attempt to use the same methods on multiple victims. Defending against these kinds of advanced targeted attacks will require more education and implementation of more stringent multi-factor procedures.

Use of weak passwords

The use of weak passwords has always been a concern for organizations, but today, as computing power grows and is available for lower costs, even passwords that were once considered complex can be easily deciphered through password-cracking hardware. In 2017, IBM X-Force Red, the IBM security testing specialists, debuted Cracken,[92] a powerful password-cracking rig, demonstrating the gravity of this problem.

When it comes to cracking passwords, attackers armed with only a few thousand dollars could build a password cracking tool that would decipher most Microsoft Windows passwords in a few days. This is bad news for organizations where many users hold privileged network accounts that can be compromised rather easily unless secured with additional factors.

While the death of the password[93] has been long predicted, passwords are still a core method of access for most systems. And although the rule of thumb for passwords in the past has focused on complexity, with at least eight characters combining letters, numbers and special characters, recent guidance suggests that longer passphrases—several unrelated words tied together, made up of at least 20 characters—are actually harder to crack and easier to remember.

Unsecured personal devices

There were several public security incidents in 2017 resulting from employees copying their company's intellectual property to their personal system. In one such case, a US government employee was running a case management system on an unsecured personal computer and inadvertently exposed the personal data of 247,167 individuals. Also exposed were confidential investigation reports from 2002 through 2014 that enumerated subjects, witnesses and complaints made to that employee's department.[94]

TABLE OF CONTENTS

Storing authentication credentials on open repositories

Insiders have also inadvertently exposed databases by placing authentication details on public code repositories. In one notable incident, a collection of corporate virtual private network (VPN) passwords, user names and operational details of a global accounting firm were found in a public-facing GitHub-hosted repository.[95] The exposure of user credentials in such a public way is a major risk to companies. Mitigation should include employee training, employee sign off on committing to company security policies and enforcement of password rotation. Also recommended is limiting user privileges to the minimum possible and deploying second-factor authentication.

Inadvertent insider threat as viewed from X-Force-monitored network activity

The percentage of monitored network activity by inadvertent insiders is derived by assessing all source and destination IP addresses identified in the attacks as well as in security incidents targeting the representative set of sensors that collected data throughout 2017.

Of the attack activity experienced by X-Force-monitored clients in 2017, 12 percent were the result of attackers attempting to exploit inadvertent weaknesses.

At 38 percent, the majority of the problematic inadvertent activity experienced by X-Force-monitored clients involved attackers attempting to trick users into clicking on a malicious link or attachment.

Types of exploitation targeting inadvertent weaknesses

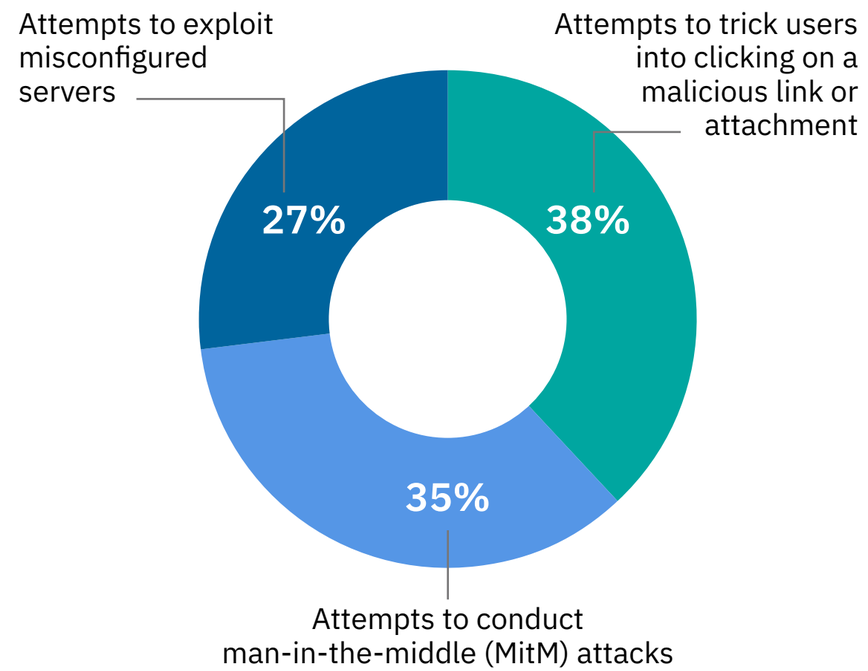


Figure 10: Types of exploitation targeting inadvertent weaknesses.

TABLE OF CONTENTS

Another 35 percent of exploitation activity involved attackers attempting to conduct man-in-the-middle (MitM) attacks. An example of this might be someone attempting to connect to a banking site via a rogue or compromised Wi-Fi router and ignoring the security certificate error upon visiting the site. If the victim logs in, that person's credentials would be sent to the attacker.

The remaining 27 percent involved attempts to exploit misconfigured servers—mostly through SQLi.

X-Force-monitored clients in the education, energy and utilities, and financial services industries experienced a notably higher percentage of inadvertent actor activity.

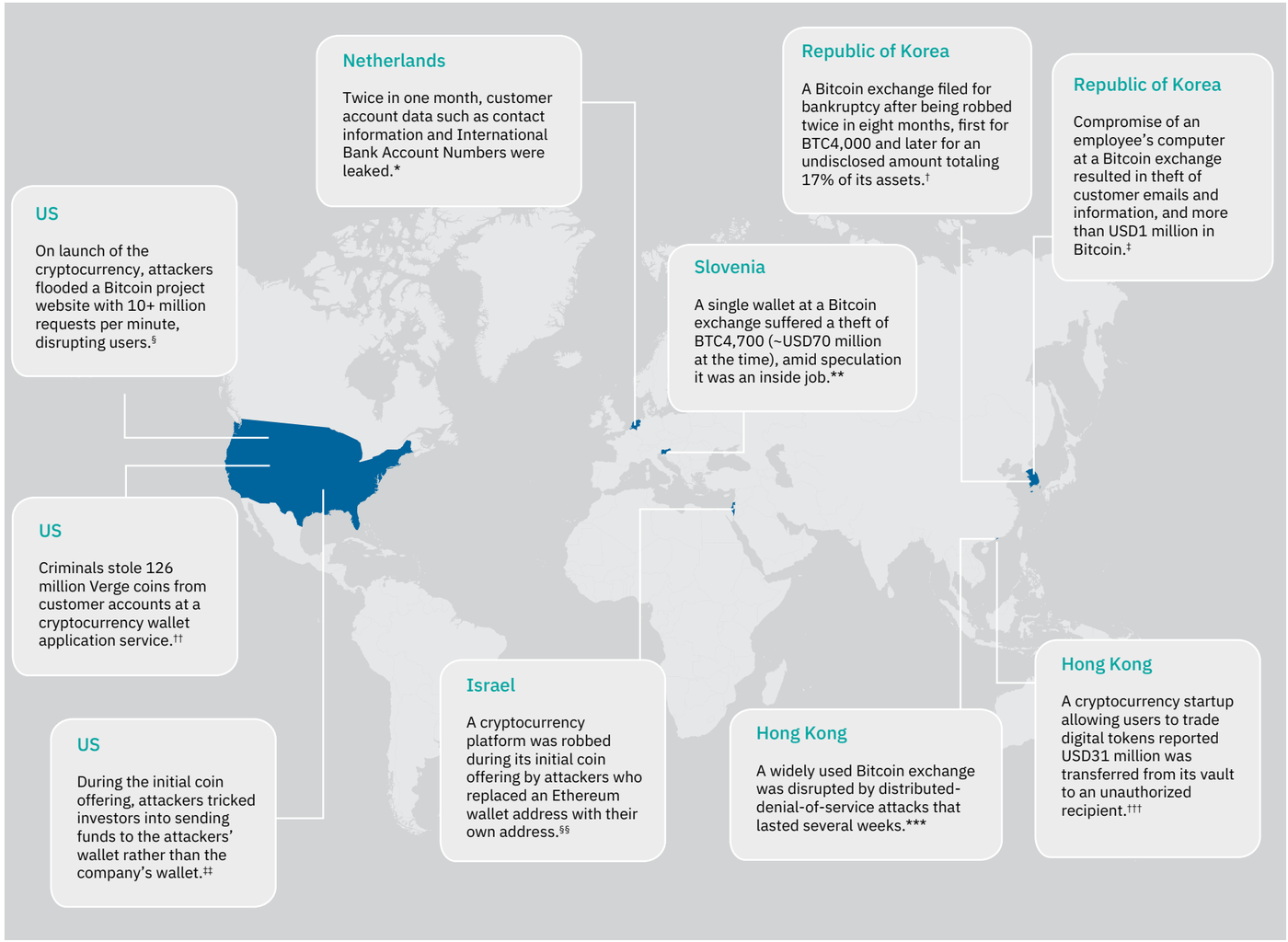
The reasons behind a higher percentage of inadvertent incidents in these industries is not readily apparent by examining event data. However, it is plausible that these industries may be experiencing a higher volume of targeted phishing emails, resulting in a higher rate among these organizations of individuals falling for phishing emails and clicking on malicious links. The education sector, for instance, was among the sectors most targeted with BEC scams reported by the US Internal Revenue Service (IRS).[96] In July 2017, reports surfaced regarding nuclear facilities in the US targeted with spear phishing, malicious Word documents and a watering-hole attack.[97]

Inadvertent security lapses could also be the result of a weak cybersecurity awareness culture. A third-party survey released in 2017 revealed that in the education sector 82 percent of IT professionals said they require students to take IT security training yearly, at a minimum, but only 35 percent of students noted their universities required such training.[98]

TABLE OF CONTENTS

UNDERGROUND CYBERCRIME ECONOMY THRIVES ON CRYPTOCURRENCY

Notable 2017 cryptocurrency-related incidents



* Raimund Bumblauskas, "Dutch Bitcoin Broker Litebit suffers second data breach in six seeks," HackedPress, 18 September 2017.

† "Bitcoin exchange Youbit shuts after second hack attack," *BBC News*, 19 December 2017.

‡ Raimund Bumblauskas, "Bithumb, Korean cryptocurrency exchange, hacked, $1 million stolen," *HackedPress*, 05 July 2017.

§ Rachel Rose O'Leary, "Bitcoin Gold Website Down Following DDoS Attack," *Coindesk*, 24 October 2017.

** Abhimanyu Ghoshal, "Bitcoin exchange Nice-Hash robbed of $64 million from its wallet," *TNW*, 06 December 2017.

†† India Ashok, "CoinPouch hack: Over $655,000 words of Verge cryptocurrency was stolen by hackers," *International Business Times*, 25 November 2017.

‡‡ Jeremy Nation, "Enigma Token Offering Eclipsed By Hacking Incident," ETHNews, 21 August 2107.

§§ Mohit Kumar, "Hacker Uses A Simple Trick to Steal $7 Million Worth of Ethereum Within 3 Minutes," *The Hacker News*, 17 July 2017.

*** Tomáš Foltýn, "Cryptocurrency exchange Bitfinex plagued by DDos Attacks," *WeLiveSecurity*, 06 December 2017.

††† Justina Lee, "Even a $31 Million Hack Couldn't Keep Bitcoin Down," *Bloomberg Technology*, 21 November 2017.

Figure 11: Notable 2017 cryptocurrency-related incidents.

TABLE OF CONTENTS

In the years since the rise of Bitcoin and other cryptocurrencies, it has become increasingly obvious that a steadfast connection has been formed between crypto coin and cybercrime. And while the result was surely not intentional, cryptocurrency currently reigns supreme in the world of online crime and can help criminals steal and move money in new ways that are harder than ever to detect or disrupt.

Cybercriminals and anonymized payment methods always kept a close relationship, since one of the most lucrative aspects of online crime is the ability to conceal one's identity. Cryptographic currencies gaining in value and popularity were thus a very meaningful and, unfortunately, welcomed development in crime underworlds.

The rush for crypto—From small fish to great white sharks

The anonymizing allure of cryptocurrency is not only the driver behind malware-wielding criminals; it has also attracted other kinds of financially motivated cybercriminals who are looking for ways to mine or steal crypto coins. As it goes with most types of crime, illicitly obtaining coins starts with small fish—actors who use low-grade attacks—and progresses to the great white sharks of the cybercrime world. Here are some examples:

Wallet phishers

One of the least-sophisticated ways of stealing crypto coin is through phishing attacks that target users of popular cryptocurrency exchange sites and attempt to steal access credentials to users' accounts in order to compromise their wallets.[99]

Phishing can usually be spotted by examining the sending email address, the site's URL and some look-and-feel variations of the website itself. This method is not considered an advanced attack, yet it can be convincing enough that many have fallen prey[100] to losing their access credentials on a copycat site. Activating second-factor authentication can protect users from most phishing attacks. It is important to activate a second factor that cannot fall into the attacker's hands as well, and to select it according to the account type being secured.

Coin-mining malware

The least advanced type of coin stealing happens via coin-mining malware. This malware is typically made up of basic pieces of malware designed to install a miner on the victim's endpoint and enslave it so that it slowly gathers coins for the attacker.† Miners in this category started appearing circa 2013 and have been evolving since their introduction. Jumping on the cryptocurrency bandwagon, banking Trojans were one of the first malware breeds that devised ways to steal coins.[101]

†It's worth noting that some sites actually use coin mining as a means of legitimately generating money and notify their users when this is the case, giving them the option to continue browsing or leave the site.

TABLE OF CONTENTS

These days, coin miners have been detected in malvertising, mining coins when website visitors merely reach an infected site.[102] They can be spread through mobile applications,[103] and can literally damage user devices by overheating smartphone batteries.[104]

Many coin-mining malware operators have moved away from Bitcoin since other, "younger" coins take less time and effort to gather. They therefore can use lower-end devices with lesser processing power, such as mobile phone and Internet-of-Things (IoT) devices,[105] to harvest coins, with the number of coins gathered growing as the value rises over time. One of the most popular targets is the Monero coin.

Similarly, banking Trojans historically attempted to hijack endpoints with Bitcoin-mining malware. However, within the past year there has been a rise in more sophisticated cryptocurrency theft through banking Trojans.[106]

Why mine coins when you can steal them?

Advanced malware codes are no longer in the business of mining crypto coins. Instead, they use their inherent capabilities to steal them. Currently, Trojans such as Dridex, TrickBot and Zeus Sphinx are only a few names of banking malware whose target lists feature cryptocurrency exchange sites.

In some cases, the malware may only steal wallet-access credentials, but in others, the Trojan can actually launch an MitM attack to divert cryptocurrency transactions.

Criminal hackers targeting businesses

Perhaps the most notable breed of attackers who prey on cryptocurrency are not those who gather it in small amounts, but rather, those who get the biggest bang for their crime: criminal hackers.

Targeted extortion attacks on enterprise networks became a rampant threat in the past few years, making businesses and security executives rethink business continuity and disaster-recovery plans. In some cases, the concern became so pressing that businesses prepared Bitcoin in advance to ensure their ability to pay if ever an attack were to paralyze their operations.[107]

The digital extortion picture in 2017 was rather grim. Attackers using ransomware to infect networks and lock up large amounts of data managed to hit companies and force them to pay anywhere from dozens[108] to hundreds of thousands[19] of dollars to recover. The worst case recorded thus far was one in which a web-hosting company in South Korea was forced to pay USD1 million in Bitcoin to have attackers halt an eight-day encryption siege that paralyzed its operations.[109]

X-Force researchers expect ransom attacks on businesses to continue rising in 2018, affecting any size of business and critical infrastructure organization, both for financial gain and potentially as part of nation-state-sponsored attacks.

TABLE OF CONTENTS

Criminal hackers targeting cryptocurrency exchange platforms

Another variety of criminal hackers targeting cryptocurrency are those who prey on exchange platforms to steal millions of dollars in coins at a time. This breed of attacks has been rising in the past few years and has frequently made headlines. In some cases, exorbitant amounts have been stolen from high-value individuals using exchange platforms to trade their coins. In other cases, the attack was against the exchange platform itself.

Those less skilled in the black hat practices of hacking the platform may opt for extortion by issuing a DDoS attack on the platform and demanding payment to stop the traffic flood and disruption.

What's next for cryptocurrency and cybercrime?

The more their value rises, the more lucrative cryptocurrencies become to both everyday people and those who place higher value on their anonymity. Unfortunately, the top anonymity seekers are people who have something to hide. From attackers who prey on other people, to cybercriminals, to actors with dubious business and intent,[110] the bond between ill-doers and cryptocurrency looks to be a permanent one.

Can those ties be loosened in the future? Possibly. Cryptocurrency may be good at anonymity, but it is not entirely opaque. "Even in the strange new world of Bitcoin," FBI Assistant General Counsel Brett Nigh said in September 2015, "investigators can follow the money."[111]

As the crypto coin stabilizes over time and gains an even larger foothold in the global economy, the world might be in for new challenges in this space. On the one hand, law enforcement is working to expose illicit crypto-activity; on the other, criminals are devising new ways to remain unnamed and continue to benefit from these global, decentralized currencies.

To see changes that drive criminals out while keeping legitimate users in, those who favor the use of cryptocurrency might have to give up some of their anonymity for more security—a reality that is already part of every other use of the World Wide Web.

TABLE OF CONTENTS

KEEPING PACE WITH THE CHANGING THREAT LANDSCAPE

The cyber threats of 2017 reminded enterprises of the continued need to practice security fundamentals such as effective patch management and the implementation of real-time systems and processes to monitor and detect breaches, coupled with machine-learning capabilities[112] to detect patterns and even predict attacks before they occur.

Throughout the past year, it became clear that threats are just as imminent from within as they are from external sources. Inadvertent insiders were found to be a major issue for security teams to reckon with, stressing that enterprises' cybersecurity awareness programs need to keep pace with the changing landscape and provide continued role-based training for all employees.

Seeing the sensitivity and variance of data that has been amassed and exposed from millions of individuals is a wake-up call for organizations to take steps to ensure that the data they collect in accordance with applicable privacy laws is also properly secured with controls that are tested over time. To discover data that could be stolen from unsecure assets, a minimum requirement should be to audit any cloud or network storage through scanning tools or professional penetration testing.

While all aspects of cybersecurity carry varying levels of urgency, utility and importance, the impactful nature of ransomware and data-wiping attacks has become very significant to ongoing operations. Affected organizations in such attacks suffered extensive and costly downtime,[113] reputational damage[114] and ongoing system mayhem[115] that took teams weeks to repair after the incident took place. As we move into 2018, incident response is where the growth of security investment could make a difference, along with the looming potential for combating not only ransomworm threats, but also the complete spectrum of cyber threats.

CONTRIBUTORS

Michelle Alvarez, *IBM X-Force IRIS*
Nick Bradley, *IBM X-Force IRIS*
David Bryan, *IBM X-Force Red*
Scott Craig, *IBM X-Force IRIS*
Limor Kessem, *IBM Security Global Executive Security Advisor*
Jason Kravitz, *IBM X-Force Research*
Dave McMillen, *IBM X-Force IRIS*
Johannes Noll, *IBM X-Force Content Security*
Megan Powell, *IBM Security Global Portfolio Marketing*
Mark Usher, *IBM X-Force Content Security*

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

FOOTNOTES

1 Luke Gallin, "Re/insurance to take minimal share of $8 billion WannaCry economic loss: A.M. Best," *Reinsurance News,* 23 May 2017.

2. Dave McMillen, "Network Attacks Containing Cryptocurrency CPU Mining Tools Grow Sixfold," *SecurityIntelligence*, 19 September 2017.

3. Michelle Alvarez, "Researchers Detect Second Wave of Shellshock Attacks Since Two-Year Anniversary," *SecurityIntelligence*, 21 October 2016.

4. "CAPEC VIEW: Mechanisms of Attack," *CAPEC*, 04 August 2017.

5. "Botnet Based LFI Attack," *IBM X-Force Exchange*, 12 October 2017.

6. Ivana Kottasová, "Bitcoin is too hot for criminals. They're using monero instead," *CNN*, 03 January 2018.

7. "CAPEC CATEGORY: Employ Probabilistic Techniques," *CAPEC*, 04 August 2017.

8. "CAPEC CATEGORY: Abuse Existing Functionality," *CAPEC*, 04 August 2017.

9. "CAPEC CATEGORY: Manipulate Data Structures," *CAPEC*, 04 August 2017.

10. "Several Polish banks hacked, information stolen by unknown attackers," *BadCyber*, 03 February 2017.

11. Zeljka Zorz, "Banks around the world targeted in watering hole attacks," *Help Net Security*, 14 February 2017.

12. Robert Hackett, "Equifax Underestimated by 2.5 Million the Number of Potential Breach Victims," *Fortune*, 02 October 2017.

13. Lily Hay Newman, "EQUIFAX OFFICIALLY HAS NO EXCUSE," *Wired*, 14 September 2017.

14. Janet Burns, "SEC Reveals Its EDGAR Database Was Hacked, Maybe Used For Illegal Trades," *Forbes*, 21 September 2017.

15. Renae Merle, "SEC reveals it was hacked, information may have been used for illegal stock trades," *The Washington Post*, 20 September 2017.

16. India Ashok, "Lloyds hit with massive DDoS attack by suspected hackers," *International Business Times*, 23 January 2017.

17. "Bitcoin exchange Youbit shuts after second hack attack," *BBC*, 19 December 2017.

18. "Security Incidents," *IBM X-Force*, Accessed 19 February 2018.

19. Howard Solomon, "Canadian firm pays $425,000 to recover from ransomware attack," *IT World Canada*, 13 July 2017.

20. Jason Kravitz, "X-Force 2017 Data Breach Review," *IBM X-Force Exchange*, 18 January 2018.

21. Katie Dangerfield, "Nissan Canada data breach may have exposed 1.1M finance customers' information," *Global News*, 21 December 2017.

22. Robert Abel, "Japanese Honda factory hit with WannaCry ransomware, halts production," *SC Media*, 21 June 2017.

23. Limor Kessem, "POS Malware Breach Sees Payment Cards Hit Underground Shops," *SecurityIntelligence*, 03 October 2017.

24. Mohit Kumar, "Forever 21 Warns Shoppers of Payment Card Breach at Some Stores," *The Hacker News*, 15 November 2017.

25. Zack Whittaker, "Clothing giant Brooks Brothers hit by year-long credit card data breach," *ZDNet*, 16 May 2017.

26. Dell Cameron and Kate Conger, "GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters," *Gizmodo*, 19 June 2017.

27. Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," *Forbes*, 17 January 2016.

28. Steve Morgan, "Cybercrime damages expected to cost the world $6 trillion by 2021," *CSO*, 22 August 2016.

29. Tracy Kitten, "Crimeware-as-a-Service Threatens Banks," *Information Security Media Group*, 18 December 2014.

30. Limor Kessem with Maor Wiesen, Tal Darsan and Tomer Agayev, "New Banking Trojan IcedID Discovered by IBM X-Force Research," *SecurityIntelligence*, 13 November 2017.

31. Paweł Srokosz, "Analysis of Emotet v4," *CERT Polska*, 24 May 2017.

32. "Malspam Leads to Malicous Word Document Which Downloads Geodo/Emotet Banking Malware," *Malware Breakdown*, 06 May 2017.

33. Bill Brenner, "Emotet's goal: drop Dridex malware on as many endpoints as possible," *Naked Security*, 10 August 2017.

34. Limor Kessem, "Panda Is One Hungry Bear! A Heavyweight Banking Trojan Rolls Into Brazil," *SecurityIntelligence*, 04 August 2016.

35. Gadi Ostrovsky with Limor Kessem, "GootKit Developers Dress It Up With Web Traffic Proxy," *SecurityIntelligence*, 01 March 2017.

36. Limor Kessem, "An Aggressive Launch: TrickBot Trojan Rises With Redirection Attacks in the UK," *SecurityIntelligence*, 08 November 2016.

37. Limor Kessem, "Ursnif v3 Emerges, Targets Australian Bank Customers With Redirection Attacks," *SecurityIntelligence*, 28 November 2017.

TABLE OF CONTENTS

38. Limor Kessem, "Dridex Launches Dyre-Like Attacks in UK, Intensifies Focus on Business Accounts," *SecurityIntelligence*, 19 January 2016.

39. Or Safran with Lior Keshet and Limor Kessem, "Client Maximus: New Remote Overlay Malware Highlights Rising Malcode Sophistication in Brazil," *SecurityIntelligence*, 10 January 2017.

40. Lior Keshet, "Exposing an AV-Disabling Driver Just in Time for Lunch," *SecurityIntelligence*, 04 January 2017.

41. Omer Agmon with Limor Kessem, "Brazilian Malware Client Maximus: Maximizing the Mayhem," *SecurityIntelligence*, 12 September 2017.

42. John Leyden, "Brazilian and Russian cybercrooks collaborating to create more potent threats," *The Register*, 01 April 2016.

43. Limor Kessem, "The Necurs Botnet: A Pandora's Box of Malicious Spam," *SecurityIntelligence*, 24 April 2017.

44. Limor Kessem, "Ursnif Campaign Waves Breaking on Japanese Shores," *SecurityIntelligence*, 26 October 2017.

45. "QakBot Ongoing Collection," *IBM X-Force Exchange*, 07 June 2017.

46. Mike Oppenheim with Kevin Zuk, Matan Meir and Limor Kessem, "QakBot Banking Trojan Causes Massive Active Directory Lockouts," *SecurityIntelligence*, 02 June 2017.

47. Pierluigi Paganini, "Necurs botnet: the resurrection of the monster and the rising of spam," *Security Affairs*, 29 September 2016.

48. "Necurs strikes again with New Penny Stock Campaign," *IBM X-Force Exchange*, 27 April 2017.

49. Robert Abel, "Necurs botnet launches massive 47 million emails per day campaign," *SC Media*, 28 December 2017.

50. Limor Kessem, "Where are They Today? Banking Trojans That No One Misses GozNym - Up a Storm Then Up in Flames," *SC Media*, 06 November 2017.

51. Limor Kessem, "Neverquest Gang Takes Leave — Is It the End of the Quest?," *SecurityIntelligence*, 04 May 2017.

52. Mohit Kumar, "Russian Hacker behind 'NeverQuest' Malware, Wanted by FBI, Is Arrested in Spain," *The Hacker News*, 21 January 2017.

53. Limor Kessem with Ilya Kolmanovich and Denis Laskov, "Shifu: 'Masterful' New Banking Trojan Is Attacking 14 Japanese Banks," *SecurityIntelligence*, 31 August 2015.

54. Limor Kessem, "WannaCry Ransomware Spreads Across the Globe, Makes Organizations Wanna Cry About Microsoft Vulnerability," *SecurityIntelligence*, 14 May 2017.

55. Diana Kelley, "Petya Weren't Expecting This: Ransomware Takes Systems Hostage Across the Globe," *SecurityIntelligence*, 27 June 2017.

56. Shane Schick, "TrickBot Learns From WannaCry and Petya by Adding Self-Spreading Worm Module," *SecurityIntelligence*, 31 July 2017.

57. Limor Kessem, "Carbanak: How Would You Have Stopped a $1 Billion APT Attack?," *SecurityIntelligence*, 23 February 2015.

58. Charlie Osborne, "Carbanak hackers pivot plan of attack to target banks, the enterprise," *ZDNet*, 10 October 2017.

59. Michael Mimoso, "THE CHANGING FACE OF CARBANAK," *Threatpost*, 19 January 2017.

60. Limor Kessem with Shachar Gritzman, "After Big Takedown Efforts, 20 More BankBot Mobile Malware Apps Make It Into Google Play," *SecurityIntelligence*, 27 July 2017.

61. Danny Palmer, "BankBot Android malware sneaks into the Google Play Store - for the third time," *ZDNet*, 09 November 2017.

62. "IBM Study: Businesses More likely to Pay Ransomware than Consumers," *IBM Press Release*, 14 December 2016.

63. Limor Kessem with Caleb Barlow, "Ransomware Report: Top Security Threat Expected to Continue Rising in 2017," *SecurityIntelligence*, 14 December 2016.

64. Limor Kessem, "Ransomware: How Consumers and Businesses Value Their Data," *SecurityIntelligence*, 14 December 2016.

65. Catalin Cimpanu, "Attackers Brute-Force Corporate RDP Servers to Spread Ransomware," *Softpedia News*, 03 May 2016.

66. Charlie Osborne, "UK firms 'stockpile' Bitcoin to pay off ransomware hackers," *ZDNet*, 18 December 2017.

67. Harold Stark, "When Attacked By Ransomware, The FBI Says You Shouldn't Pay Up," *Forbes*, 28 February 2017.

68. Steve Morgan, "Global ransomware damage costs predicted to exceed $11.5 billion annually by 2019," *Cybersecurity Ventures*, 14 November 2017.

69. Andy Greenberg, "Hold North Korea Accountable for WannaCry—And the NSA, Too," *WIRED*, 19 December 2017.

TABLE OF CONTENTS

70. "WCry2 Ransomware Outbreak," *IBM X-Force Exchange*, 30 May 2017.

71. Jamie Grierson and Samuel Gibbs, "NHS cyber-attack causing disruption one week after breach," *The Guardian*, 19 May 2017.

72. "Victims paid WannaCry ransom hackers less than $70k, no data recovered – White House," *RT*, 17 May 2017.

73. Thomas Fox-Brewster, "Another Massive Ransomware Outbreak Is Going Global Fast," *Forbes*, 27 June 2017.

74. Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," *CSO*, 17 October 2017.

75. Dan Goodin, "NotPetya developers may have obtained NSA exploits weeks before their public leak [Updated]," *Ars Technica*, 30 June 2017.

76. Mike Oppenheim, "A 'Wiper' in Ransomware Clothing: Global Attacks Intended for Destruction Versus Financial Gain," *SecurityIntelligence*, 29 June 2017.

77. Nicole Perlroth, Mark Scott and Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *The New York Times*, 27 June 2017.

78. Limor Kessem, "Bad Rabbit Ransomware Attacks Highlight Risk of Propagating Malware Outbreaks," *SecurityIntelligence*, 25 October 2017.

79. Selena Larson, "New ransomware attack hits Russia and spreads around globe," *CNN*, 25 October 2017.

80. Thomas Fox-Brewster, "Russian News Hacked To Launch Global Ransomware Attack," *Forbes*, 24 October 2017.

81. Darlene Storm, "13 million MacKeeper users exposed by Shodan search, no password or hacking required," *Computerworld*, 16 December 2015.

82. Catalin Cimpanu, "Massive Wave of MongoDB Ransom Attacks Makes 26,000 New Victims," *BleepingComputer*, 04 September 2017.

83. Dan O'Sullivan, "The RNC Files: Inside the Largest US Voter Data Leak," *UpGuard*, 20 December 2017.

84. Dan O'Sullivan, "Insecure: How A Private Military Contractor's Hiring Files Leaked," *UpGuard*, 26 December 2017.

85. Bob Diachenko, "Auto Tracking Company Leaks Hundreds of Thousands of Records Online," *MacKeeper Security*, 21 September 2017.

86. Jennifer Schlesinger and Andrea Day, "Hundreds of mobile websites and apps are found to leak personal info," *CNBC*, 03 March 2017.

87. Dell Cameron, "Welp, Vevo Just Got Hacked," *Gizmodo*, 15 September 2017.

88. Guy Boulton, "Confidential information of 9,500 patients at the Medical College of Wisconsin compromised," *Journal Sentinel*, 17 November 2017.

89. "FBI Says Business Email Compromise Scams Continue to Grow in U.S., Cost Companies More Than $1 Billion," *BBB*, 09 November 2017.

90. "BUSINESS E-MAIL COMPROMISE: E-MAIL ACCOUNT COMPROMISE: THE 5 BILLION DOLLAR SCAM," *FBI Public Service Announcement*, 04 May 2017.

91. Kaley Ramsay, "Clark Builders identified as company targeted in $11.8M MacEwan University phishing scam," *Global News,* 01 September 2017.

92. Security Intelligence Staff, "'Cracken' Passwords with EvilMog of IBM X-Force Red," *SecurityIntelligence*, 05 September 2017.

93. Limor Kessem, "IBM Study: Consumers Weigh in on Biometrics, Authentication and the Future of Identity," *SecurityIntelligence*, 29 January 2018.

94. Uzair Amir, "Private Details of 240,000 DHS Employees Accessed after Data Breach," *HackRead*, 04 January 2018.

95. Iain Thomsom, "Deloitte is a sitting duck: Key systems with RDP open, VPN and proxy 'login details leaked'," *The Register*, 26 September 2017.

96. Kelly Phillips Erb, "IRS Warns Again On Email Scam After FBI Reports Billions In Related Losses," *Forbes*, 23 August 2017.

97. Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," *The New York Times*, 06 July 2017.

98. David Raths, "Survey Hints at Cybersecurity Communications Gap," *Campus Technology*, 01 November 2017.

99. Tom Pritchard, "Bitcoin's Recent Shenanigans is Causing Cybercriminals to Ditch it for Competing Cryptocurrencies," *Gizmodo*, 03 January 2018.

100. Limor Kessem, "Hey Phishing, You Old Foe — Catch This Cognitive Drift?," *SecurityIntelligence*, 27 March 2017.

101. Urban Schrott, "Advanced Banking Trojan "Hesperbot" Can Also Steal Bitcoins," *ESET Ireland*, 10 December 2013.

102. Jonathan Keane, "Sneaky Crypto Malware Miners Are Targeting Ad Networks Next," *CoinDesk*, 04 January 2018.

103. Rob Thubron, "Hackers are spreading cryptocurrency mining malware through Facebook Messenger," *TechSpot*, 26 December 2017.

TABLE OF CONTENTS

104. James Sanders, "Cryptocurrency mining malware "Loapi" capable of physically damaging phones," *Android Police,* 20 December 2017.

105. Dave McMillen with Michelle Alvarez, "Mirai IoT Botnet: Mining for Bitcoins?," *SecurityIntelligence*, 10 April 2017.

106. "It's a Trap! Notorious Pony Loader Malware Updated to Steal Bitcoins," *Infosecurity Magazine*, 25 June 2014.

107. Margi Murphy, "British companies 'stockpile' Bitcoin to use as ransomware hush money," *The Telegraph*, 10 December 2017.

108. Catalin Cimpanu, "Los Angeles Valley College Pays a Whopping $30,000 in Ransomware Incident," *BleepingComputer*, 10 January 2017.

109. Richard Chirgwin, "South Korean hosting co. pays $1m ransom to end eight-day outage," *The Register*, 20 June 2017.

110. Jordan Pearson, "New Bill Asks Homeland Security to Investigate Whether Terrorists Use Bitcoin," *Motherboard*, 19 May 2017.

111. John Bohannon, "Why criminals can't hide behind Bitcoin," *Science*, 09 March 2016.

112. Lecia Papadopoulos, "How Watson AI is helping companies stay ahead of hackers and cybersecurity attacks," *IBM Watson, Discovery and Exploration*, 14 August 2017.

113. Iain Thomson, "NotPetya ransomware attack cost us $300m – shipping giant Maersk," *The Register*, 16 August 2017.

114. "Honda halts Japan car plant after WannaCry virus hits computer network," *Reuters*, 21 June 2017.

115. Damien Gayle, Alexandra Topping, Ian Sample, Sarah Marsh and Vikram Dodd, "NHS seeks to recover from global cyber-attack as security concerns resurface," *The Guardian*, 13 May 2017.

TABLE OF CONTENTS

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
March 2018

77014377-USEN-01