2018

TRUSTWAVE
GLOBAL
SECURITY
REPORT

Trustwave® | Singtel

INTRODUCTION

> **"The times they are a-changin'."**
>
> *—Bob Dylan*

Ten years ago, we published the first volume of the Trustwave Global Security Report. It was 11 pages long and focused exclusively on thefts of payment card data from point-of-sale and e-commerce environments. Trustwave has grown a lot since then and so has this report. Unfortunately, the threat landscape has grown, too.

In 2008, the biggest threats were opportunistic: Attackers distributed their threats indiscriminately to steal money, card data, login credentials and other valuable information from as many victims as possible. Fast forward 10 years, and we now live in a world of sophisticated assaults with targeted attacks and advanced persistent threats from criminal groups (and sometimes nation states). These skilled professionals have sufficient resources, time and patience to perpetrate against specifically chosen targets to breach nearly any network, however long it takes.

The 2018 Trustwave Global Security Report kicks off the next decade of cybersecurity by looking back at the last one. We begin by analyzing some of the data we collected over the past 10 years to understand how we arrived where we are now. From there, we move on to an analysis of data compromise incidents our incident response teams covered in 2017. If you wonder what kind of threats are emerging for frontline responders, you'll find it here.

In the Threat Intelligence section, Trustwave SpiderLabs, our elite team of security professionals, will share what they learned from the cybercriminal underground about everything from malware development to phishing trends to the underground economy of exploit kits and traffic trading. Lastly, we survey the state of database, network and application security with the aid of telemetry from Trustwave's state-of-the-art vulnerability scanning and testing services.

No one can know for sure what the next 10 years hold for tech professionals or security responders. One thing we can tell you, though, is that Trustwave will be there with you throughout, helping you fight cybercrime, protect data and reduce risk from threats known and unknown. What does the future hold? Join us for the next 10 years to find out.

DATA SOURCES

Trustwave's large, global client base offers unmatched visibility into security threats. We gain key insights from our analysis of hundreds of data-breach investigations, threat intelligence from our global security operations centers, telemetry from security technologies and industry-leading security research.
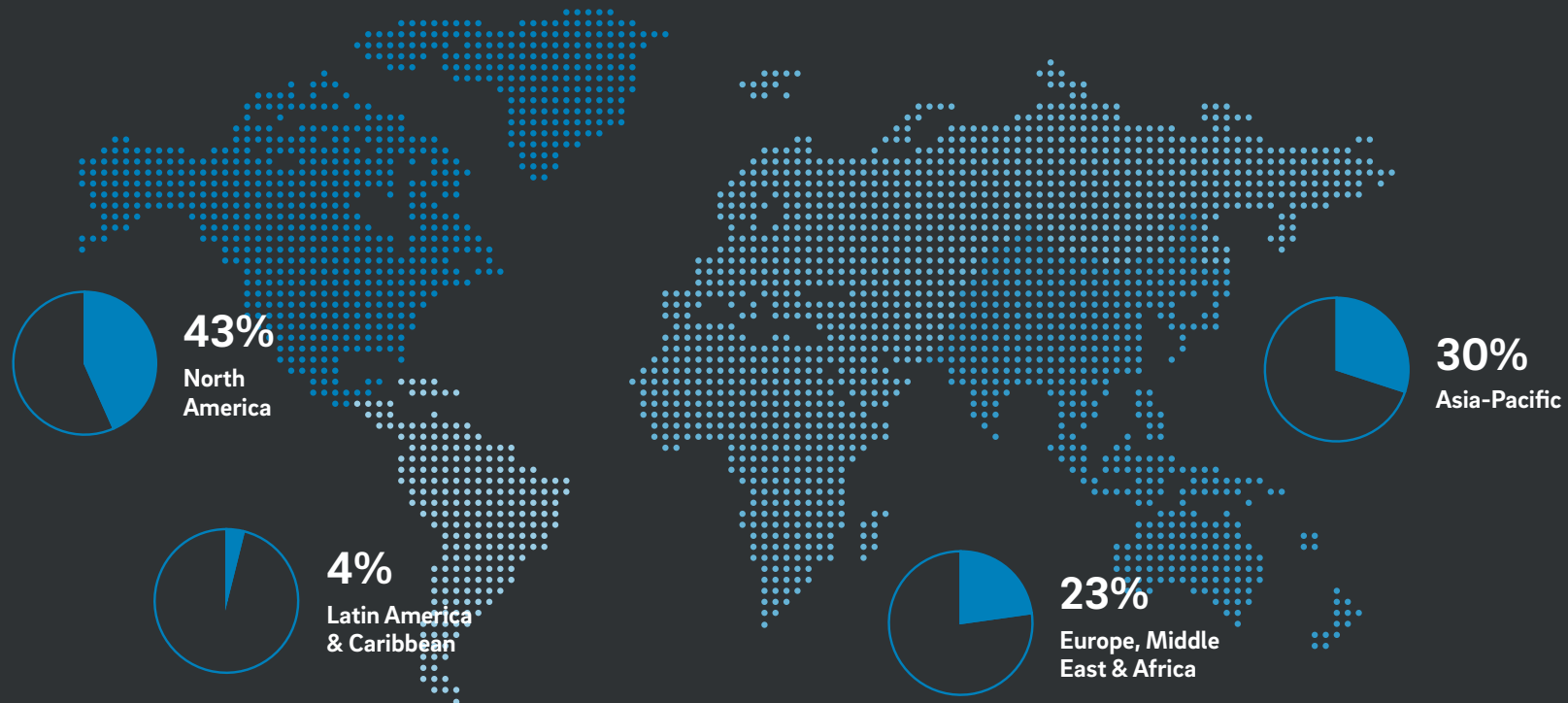
THIS YEAR, TRUSTWAVE:

- Investigated compromised locations in 21 countries

- Logged billions of security and compliance events each day across our 10 Advanced Security Operations Centers (ASOCs)

- Examined data from more than tens of millions of network vulnerability scans

- Accumulated results from thousands of web application security scans

- Analyzed tens of millions of web transactions for malicious activity

- Evaluated tens of billions of email messages

- Blocked millions of malicious websites

- Conducted thousands of penetration tests across databases, networks and applications.

EXECUTIVE SUMMARY

43%
North
America

4%
Latin America
& Caribbean

30%
Asia-Pacific

23%
Europe, Middle
East & Africa

Trustwave investigated breaches affecting thousands
of locations across 21 countries in 2017.

DATA COMPROMISE

Industries most affected

17%
Retail

13%
Finance & Insurance

12%
Hospitality

40%

of breaches targeted
payment card data
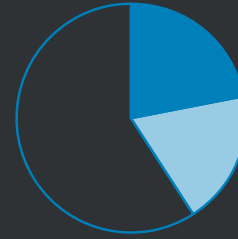
22%
Magnetic stripe

18%
Card-not-present

Incidents involving point-of-sale systems were most common in North America, which has been slow to adopt the Europay, MasterCard and Visa (EMV) chip standard for payment cards

Median number of days between intrusion and detection for detected incidents

0
INTERNAL

83
EXTERNAL

WEB ATTACKS

Targeted attacks have become more common and are becoming more sophisticated: Many high-profile breach incidents show signs of significant preplanning by attackers who carefully identify weak packages and tools on the targeted servers before making a move.

Attacks on networked devices have increased significantly over the past decade. Devices are particularly vulnerable due to lack of hardening in their software and the difficulty of distributing software updates to the them. For example, Trustwave SpiderLabs published two security advisories in 2017 about weaknesses in Netgear routers and Brother printers. These weaknesses can allow attackers to compromise the devices or networks and take malicious actions against them.

40%

of all web attacks Trustwave researchers observed in 2017 involved cross-site scripting

OWASP **TOP 10**

The Open Web Application Security Project (OWASP) updated its list of the 10 most critical web application security risks in 2017. The new list ranks sensitive data exposure more highly and introduces four new entries, including XML external entities (XXE), broken access control (created by a merger of two entries in the 2013 list), insecure deserialization and insecure logging and monitoring.

EMAIL THREATS

Percentage of all inbound email that was spam

2008	85%
2016	59%
2017	39%

Percentage of spam messages that contained malware

35%
2016

26%
2017
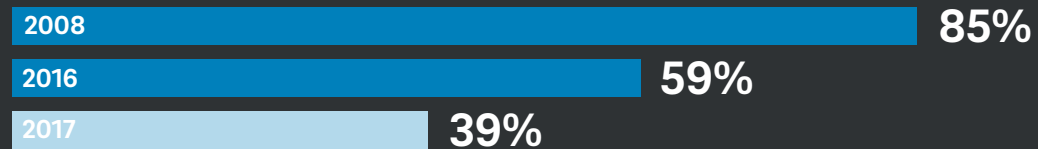
The Necurs botnet

Malware is on the rise, mostly due to the Necurs botnet. It typically operates in short bursts of intense spamming activity, followed by periods of dormancy.

At its peak, Necurs sends spam from between 200,000 and 400,000 unique IP addresses per day.

Major Necurs campaigns in 2017 delivered ransomware, banking Trojan and other botnet malware using several different delivery mechanisms and file types.

PDF FILES

are gaining traction as a delivery method for phishing lures. An attacker tricks the victim into clicking a link in the PDF to supposedly view secure content, but the link leads instead to a URL of the attacker's choosing.

EXPLOITS

Trustwave researchers tracked the following exploit kits and zero-day vulnerabilities:

34
Exploit kits that first appeared in 2012 and 2013

06
Web-based, client-size, zero-day vulnerabilities exploited in 2017

04
Exploit kits involved in incidents in 2017

The exploit kit market was much quieter in 2017 following 2016's disappearance of Angler and Nuclear, two of the most common exploit kits in the world.

CRYPTOCURRENCY AND CRIME

The characteristics that have made cryptocurrencies, such as bitcoin, an increasingly popular alternative medium of exchange have also made them highly attractive for cybercriminals.

- Transactions are fairly anonymous
- Proof of ownership is relatively basic
- Currencies are global and not government-controlled
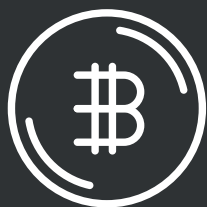
Cryptocurrencies are a popular medium of exchange for ransomware attacks. Attackers behind WannaCry ransomware, which caused widespread damage in 2017, demanded payment in bitcoin.

Mining—performing calculations to create new cryptocurrency coins—is so resource-intensive that criminals developed ways to make website visitors' and botnet victims' computers mine coins for them.

$15 BILLION

Cryptocurrency stolen from online cryptocurrency exchanges between 2012 and 2017 (in USD)

MALWARE

Percentage of malware samples Trustwave examined that used...

● ● ● ▶

30% Obfuscation to avoid detection
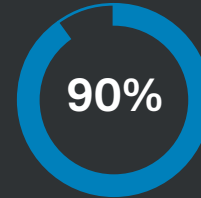
90% Persistence techniques to reload after a reboot

DATABASE AND NETWORK SECURITY

Number of vulnerabilities patched in five of the most common database products

170
2016

119
2017

53%

The percent of computers with SMBv1 enabled that were vulnerable to MS17-010 "ETERNALBLUE" exploits, used to perpetrate the widespread WannaCry and NotPetya ransomware attacks.

APPLICATION SECURITY

Percentage of web applications Trustwave application scanning services tested in 2017 that displayed at least one vulnerability

100%

11 Median number of vulnerabilities detected per application

Vulnerabilities Trustwave Managed Security Testing detected in 2017

86%
involved session management

8%
were classified as high-risk or critical

TEN YEARS OF SECURITY

In the 10 years we've been publishing the Trustwave Global Security Report, we've seen a lot of changes in the security landscape. The criminal gangs that dominated the space in the 21st century transitioned from hawking fake anti-spyware programs and blanketing the world with spam to persistently attacking individual targets until they succeed. In this special section, we look back at the data our technologies and security experts accumulated over the past decade and speculate about what these trends might mean for the next 10 years.
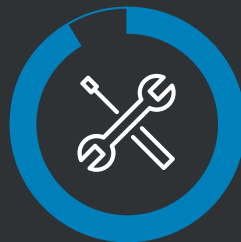
TEN YEARS OF EMAIL THREATS

As long as the internet has been open to private and commercial activity, there has been spam. In the late 1990s and early 2000s, spam was largely the domain of small-time operators who used bulk-email programs on their home computers to send pitches for weight-loss creams, pyramid schemes and, occasionally, legitimate products to email addresses harvested from Usenet and early web-based forums. Though small-scale compared to what would come later, the lack of effective filtering technologies made the problem a highly visible one for most email users.

Today a small number of criminal gangs, who pump out billions of unsolicited messages a day from large botnets composed of malware-infected computers, control most spam. The good news is that intended recipients don't see most of this spam because of multiple layers of filtering at the network edge and in client email programs and services. The bad news is that, as it did many years ago, spam is again rivaling the web as a delivery mechanism for dangerous malware.

IN 2004...

Bill Gates famously said "Two years from now, spam will be solved." Two years later, the spam problem was significantly worse and continued to worsen for several years. The worst year for spam that we observed came in 2009, when spam was more than 87% of the incoming mail Trustwave filters analyzed.

Fortunately, just when it seemed that the problem was here to stay, things started getting better. Attention from law enforcement and changing economics for the underground spamming ecosystem contributed to an overall decline in spam volumes. Since 2009, we've seen a decrease in spam activity every year, with the exception of 2016 when the Necurs botnet caused a momentary uptick in spam volumes that reversed itself in 2017. (See the **Email Threats** section for more information about Necurs.) In 2017, less than 40 percent of the email stream was spam for the first time since we began publishing the Trustwave Global Security Report.

Spam As a Percentage of Total Inbound Mail

SIGNIFICANT DEVELOPMENTS IN SPAM AND EMAIL THREATS OVER THE PAST 10 YEARS:

Spam advertising fake anti-virus programs began to take off in earnest. These programs claim to diagnose multiple infections and other problems on the infected computer and demand the computer user pay money for the "full version" of the program to remove them.

Attackers used large-scale campaign of link spam to spread the Blackhole exploit kit. (See the **Ten Years of Exploit Kits** section for more information about Blackhole.)

2009

2011

2008

One of the first really big botnets was the so-called Storm botnet, which distributed spam and malware in the form of infected e-cards and messages with provocative subject lines tied to current events. The Srizbi botnet, which produced half of all spam until the takedown of the hosting provider for its command-and-control (C&C) apparatus late in the year, rivaled Storm's impact.

2010

The Lethic spam botnet hit its peak, generating 20 percent of all spam. A series of takedowns of the Lethic infrastructure in January and February effectively neutralized Lethic as a significant threat. Eighty percent of all spam was ads for fake or dubious pharmaceutical products.

2012

A series of hosting provider takedowns in July dealt a fatal blow to the Grum botnet.

SIGNIFICANT DEVELOPMENTS IN SPAM AND EMAIL THREATS OVER THE PAST 10 YEARS:

Spam campaigns distributed CryptoLocker ransomware and malware to steal banking credentials.

2013

FBI estimates that business email compromise (BEC) and CEO fraud scams cost businesses more than USD $200 million in 2014. (See the **Email Threats** section for more information about CEO fraud.)

2015

Necurs launched several high-volume campaigns to deliver ransomware. See the **Email Threats** section for more information.

2017

2014

Malware distributed through Microsoft Word documents containing malicious macros, which had nearly dissipated by 2008, began reappearing in significant numbers.

2016

The Necurs botnet caused spam volumes to rise for the first time in several years. The percentage of spam in Trustwave's spam traps that contained malware rose to 35 percent in 2016 from 3 percent in 2015. Most of the malware came in the form of small, highly obfuscated downloader scripts that download and execute other malware from the web.

TEN YEARS OF VULNERABILITIES

Telling a complete story about the network security landscape over the past 10 years is difficult. Security tools and event loggers have evolved so much that many of the metrics we take for granted today simply did not exist in 2008. Nevertheless, the data available to us provides enough information to spot significant trends and make a few educated guessed about the future.
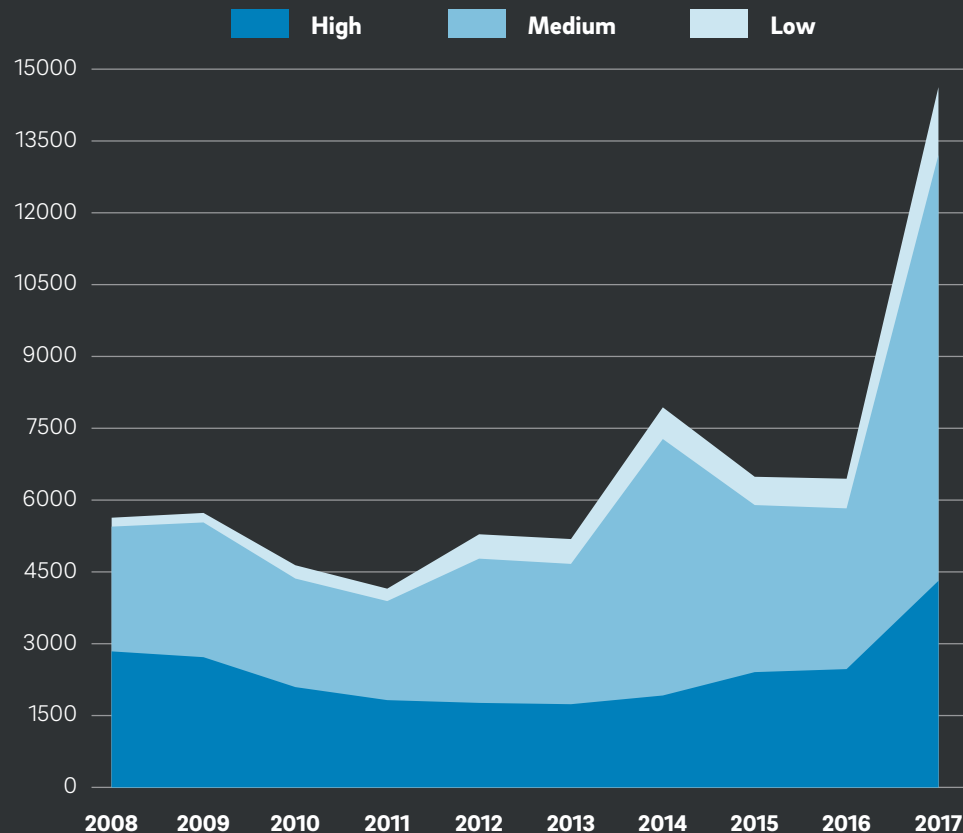
Vulnerability Disclosures Per Year

Source: nvd.nist.gov

The most obvious trend, based on sources like the National Vulnerability Database (NVD), CVE Details, Exploit-DB.com and our own security data, is that security incidents and individual vulnerabilities have been increasing.

For example, the chart to the left shows a significant increase in vulnerabilities the NVD cataloged beginning in 2012, with a particularly large increase in 2017. (Although administrative backlogs may account for some of the 2017 increase, it's indicative of a recent sharp upturn in vulnerability disclosures.)

Does the increase in vulnerability disclosures mean software is getting less safe, or are there other reasons? We can probably attribute at least part of the increase to simple population increases overall and in the digital world.

Internet Users Worldwide – In Millions

| | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |

While the world population increased by about 10 percent from 2008 to 2017, the number of internet users worldwide more than doubled during the same period. Many of those new users are "digital natives" of the millennial generation who have never known life without the internet. More technically savvy people mean more eyes on security issues, including "white-hat" researchers who share vulnerability reports with vendors and "black-hat" criminals who sell zero-day vulnerabilities and exploits on the dark web.

Even if software developers are becoming more security conscious—and there is considerable evidence suggesting they are—higher vulnerability disclosure rates are inevitable given the increasing number of people looking for vulnerabilities. In the end, the result, of course, is the same: More vulnerabilities means greater potential for exploitation.

World Population – In Billions
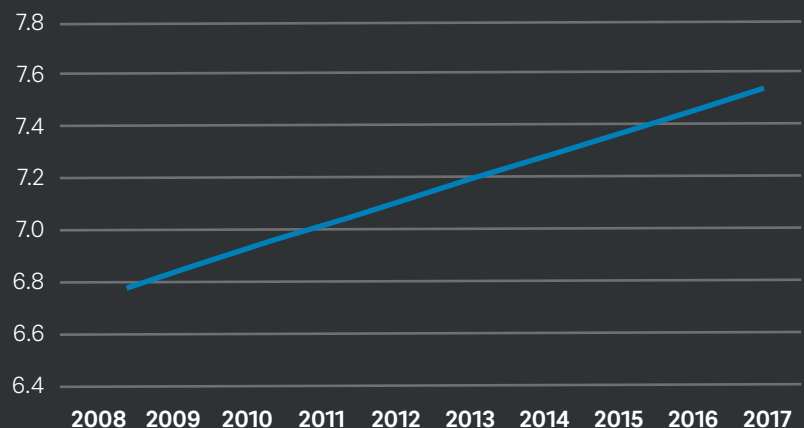
Just as troubling as the increase in vulnerability disclosure rates is the evolution in the types of vulnerabilities being reported. In recent years, Trustwave researchers are seeing increasing numbers of cipher- and SSL-based vulnerabilities, which have become significantly easier to exploit with the increasing availability of affordable mass-computing power. In the past, website operators might have reasoned the risk from a newly discovered cryptographic weakness was too small to justify the trouble of ending support for older, less-secure protocols and ciphers. As cloud computing platforms make it possible to easily and inexpensively harness the kind of computing power that would have been unimaginable a few short years ago, this is no longer a safe assumption.

Although the number of exploits published each month has increased since 2014, the rate of publication in 2017 pales in comparison to years like 2009 and 2010. This is less likely due to a genuine decline in exploits than to a shift to more surreptitious mechanisms for trading and using valuable exploits.

Exploits by Date

Source: Offensive Security, January 2018, offensive-security.com/offsec/decade-of-exploit-database-data/

With the rise of targeted attack groups that place a premium on zero-day exploits for undiscovered vulnerabilities, many black-hat exploit developers now sell their wares privately on dark-web markets or work for customers directly. The targeted attack groups that purchase these exploits are likely to use them sparingly, in extremely limited attacks, thereby preventing or delaying the widespread awareness of such exploits.

As a result, over the past several years, the primary contributors to Exploit-DB have been white-hat researchers who not only develop proof-of-concept exploit code but also engage in remediation and patch development. And, of course, the higher trend seen over the past three years serves as a reminder that exploits have not gone anywhere.

More vulnerabilities mean greater potential for exploitation.

TEN YEARS OF EXPLOIT KITS

Exploit kits, which provide a means for technically unsophisticated attackers to infect thousands of computers via an easy-to-use package or interface, formed a crucial step in the evolution of malware from the domain of hacker pranksters to a tool that criminals used to steal money and information from victims. The exploit kits of 2008 were primitive compared to the ones in use a decade later, but even the earliest kits displayed characteristics we still see today.

Exploit kits as we know them today first appeared in 2006 with a basic kit, called Web Attacker, which its creators sold on underground websites for USD $15-$20, source code included. MPack, a better-known, more full-featured kit discovered later the same year, carried a more typical price tag of USD $1,000, also including source code. Buyers could use the kit to deploy a landing page that detected the browser a visitor was using and served up exploits to infect the browser. It was up to the buyer to attract traffic to the landing page, typically through spam or by loading the page into an inline frame on a compromised website. Kit creators offered tech support and updated the kits periodically with new exploits, although existing buyers did not receive free access to newly added exploits. Though not very sophisticated by today's standards, the early kits were instrumental in creating a do-it-yourself culture that reduced the relationship between malware author and malware user to a transactional one, enabling criminals to launch campaigns and target populations as they saw fit.

A do-it-yourself culture enabled criminals to launch campaigns and target populations.

Exploit Kits by Year

Year	Exploit Kits
2008	Fiesta, AdPack, FirePack
2009	CrimePack, Eleonore, Fragus, Liberty, JustExploit, MyPoly, LuckySploit, Neon, Nuclear, Spack, Siberia, Unique, Yes
2010	Blackhole, BleedingLife, Dragon Pack, SEO, Papka
2011	Best Pack, G01Pack, OpenSource, Katrin, Sava
2012	Alpha Pack, CK, Cool, CrimeBoss, CritXPack, GrandSoft, Impact, KaiXin, Kein, NucSoft, ProPack, RedKit, Sakura, Serenity, Sibhost, Styx, Sweet Orange, Techno Xpack, Yang Pack, ZhiZhu
2013	Angler, Anonymous, DotkaChief, GongDa, HiMan, LightsOut, Magnitude, Neutrino, Private, RedDot, SafePack, White Lotus, WhiteHole, Zuponcic
2014	Niteris, RIG, HanJuan, Astrum, Archie
2015	Nuclear, Flash, Sundown, Hunter, Spartan
2016	Empire
2017	Terror/Blaze/Neptune, Eris, Nebula

2006-2009: EARLY DEVELOPMENTS

Even the earliest landing pages used basic obfuscation techniques like JavaScript loops and *eval ()* statements to avoid security scan detection. As exploit kits became more mainstream, their hiding mechanisms became more sophisticated. LuckySploit, which first appeared in 2009, was the first kit to use encryption for communication between the malicious server and the browser. The encryption method LuckySploit used was rudimentary, somewhat unwieldy and not copied by other kits. However, it presaged the far more sophisticated encryption methods that many of the most successful kits of the following decade used.

2010-2012: EXPLOIT KITS AS A SERVICE

A major step forward for the exploit kit ecosystem came in 2010 with the release of the first version of the Blackhole exploit kit, which replaced the normal fee-for-product business model with two different subscription services. One service allowed customers to download and install the kit on their own, but the encrypted software would stop working when the subscription ran out. More significantly, the other subscription option was a software-as-a-service (SaaS) model, where customers would pay a subscription fee to rent access to an online Blackhole installation. Subsequently, most of the major exploit kits would adopt this SaaS approach in the same way that legitimate web-based services have largely supplanted desktop software in many areas.

Blackhole was also one of the first kits to tackle the problem of delivering high-quality traffic to landing pages. Whereas early kits largely left that job up to the customer, exploit kit developers and users quickly realized that filtering out undesirable traffic—such as visitors from particular countries or those invulnerable to the kit's exploits—could reduce the risk that a landing page would be detected and taken down without significantly lowering the number of successful infections. While many customers used commercial traffic distribution systems (TDSes), like Sutra TDS, to bring in high-quality traffic, Blackhole offered built-in TDS features that allowed customers to write rulesets to redirect traffic to different landing pages based on specific characteristics. Blackhole 2.0, which appeared in 2012, introduced a feature that would check the landing page URL against a number of underground websites to determine whether anti-malware vendors identified the URL as malicious and change it if too many vendors discovered it.

Introduced in 2012, the Cool exploit kit is the most expensive kit we've ever seen. Dmitry "Paunch" Fedotov, the malware author who also created Blackhole, designed Cool to be a premium kit with exclusive exploits not available elsewhere, thereby greatly reducing exposure and increasing potential infection rates. Aimed at the most serious players in the market, Cool came with a price tag to match: Renting the kit cost a whopping USD $10,000 per month, compared to $50, $200 or $500 to rent access to Blackhole for a day, a week or a month, respectively. The Blackhole/Cool era ended on October 4, 2013, when Russian authorities arrested Paunch on multiple counts of computer fraud. Declared guilty in 2016, he received a seven-year prison sentence.

Significant Exploit Kit Technological Developments, 2008-2018:

YEAR	FEATURE	FIRST EXPLOIT KIT TO USE
2009	Basic encryption used in obfuscation	LuckySploit
2010	SaaS model	Blackhole
2011	Use of external, underground-developed TDS for channeling traffic into exploit kits	Blackhole
2012	Domain rotation based on underground AV checks	Blackhole 2
2014	Flash as delivery method	RIG
2015	Domain shadowing	Angler
2015	EK using zero-day	Angler
2015	EK using Diffie-Hellman key exchange for obfuscation	Angler/Nuclear
2015	Heavy use of malvertising to channel traffic into exploit kits	Angler

2013-2015: THE LAND RUSH

As Blackhole disappeared from the scene, other exploit kits rushed to fill the gap in the market. Trustwave tracked at least 34 exploit kits that first appeared in 2012 and 2013, including Angler, which would dominate the market a few years later in part because of its reputation for adopting high-quality exploits quickly. In 2015, Angler would be the first exploit kit to use a previously unknown zero-day exploit, targeting a remote code execution (RCE) vulnerability in Adobe Flash Player. The same year, Angler began using a technique dubbed domain shadowing to deter security scans. Domain shadowing involves compromising a legitimate domain and establishing a new subdomain under it that redirects users to the exploit kit. Many security products take domain reputation into account when determining whether a URL is malicious. Therefore, the blacklisting process for a new subdomain of a legitimate domain tends to be much slower.

This period also saw the introduction of several other familiar exploit kits, including Magnitude, Neutrino and RIG. Angler reintroduced encryption to the exploit kit landscape in 2015 when it began using the Diffie-Hellman key exchange method to deliver encrypted malware from its landing pages. Also in 2015, we began to see attackers use malvertising—ads that point to compromised pages or contain malicious scripts that automatically redirect visitors to landing pages—as a major vector for delivering traffic to landing pages.

2016-PRESENT: THE DECLINE?

The disappearance of three of the biggest kits—Angler, Nuclear and Neutrino—upended the exploit kit market in 2016. Nuclear shuttered operations in April after researchers published a detailed technical analysis of its software and infrastructure. Angler disappeared in June following the arrest of the Lurk gang, believed to be behind Angler. Neutrino activity declined to negligible levels beginning in September, possibly to go private for the benefit of a single criminal group. In contrast to the rush of activity seen after the disappearance of Blackhole in 2013, a period of much quieter activity followed this round of disappearances. RIG, the sole remaining major player in the space, continues operating at reduced levels, with lower-end kits like KaiXin and Magnitude mounting brief campaigns every few months. None of the kits picked up the zero-day exploits revealed since the disappearance of Neutrino in late 2016. (See the **Exploits** section for more information about exploit kit developments in 2017.)

While exploit kit development could easily pick up again, the exploit kit landscape is displaying the characteristics of a mature software market, in which the turbulence and flurry of innovation seen in the early years has given way to a stable space with a few significant players occupying specific market niches.

THE NEXT 10 YEARS

We wish we could be optimistic about what the future holds, but we've never seen the threat landscape get better over time and see no reason to believe that will change in the future.

One might believe the spam problem has been effectively "solved," inasmuch as blocking and filtering solutions have become sophisticated enough that the average email user may see few if any spam messages in a week. But the rise of Necurs and its focus on malware spam to the exclusion of other types is a troubling development that suggests that attackers find email to be an effective vector for distribution of malware. Fortunately, history tells us that coordinated takedown actions can cause major botnets to vanish in a single day, and we wish our colleagues in industry and government well in pursuing Necurs and any of its successors that may spring up.

The vulnerability and exploit trends we investigated suggest that exploits, especially technically sophisticated ones, are likely to increase in 2018. It's reasonable to expect that we will find more serious vulnerabilities sooner and with greater frequency as time progresses. This means that companies and individuals will have to install patches more rapidly if they expect to stay safe and incident-free. Frequent system upgrades and robust patch-management policies will need to become the norm across the industry or system breaches will continue to occur at an ever-increasing rate.

The decline of exploit kits in 2017 is a good omen, but compromised web pages are too tempting a vector for exploitation for attackers to ignore it for long; and, inevitably, serious players will perceive a gap in the "market" and fill it. High-profile arrests of figures have had a positive impact, but we are certain there are many players who have largely gone quiet, perhaps in an attempt to not become the next target of law enforcement. However, we would not be surprised to see them re-emerge.

Overall, targeted attacks are on the rise, and attackers continue to grow more sophisticated, attracted by the lucrative possibilities of a world that increasingly conducts its business in the cloud. It is clearer than ever that everyone who relies on today's technology—not just security and IT professionals—must adopt an informed defensive stand to protect themselves from attack.

01

DATA COMPROMISE

In this section, we discuss our findings from the analysis of Trustwave investigations of security compromises and data breaches affecting enterprise environments in 2017. While these statistics are highly dependent on the details of each investigation, we find they provide an interesting picture of where and how attackers concentrated their efforts and provide useful clues as to what the future might hold.

One worrying recent trend has been the rise in targeted attacks that mature and technically competent threat actors performed.

Today's biggest threats come not from scattershot opportunistic attackers but from highly competent, professional criminals and state actors. These professionals are targeting a wider range of targets, resulting in breaches that put more devices at risk. Organizations of all sizes now must think about security and incident response in fundamentally different ways than they did 10 years ago.

2017 COMPROMISE DEMOGRAPHICS

The observations in this section are from Trustwave SpiderLabs investigations of malicious data breaches affecting thousands of locations in 21 different countries.

2017: **43%**
2016: **49%**

North America

2017: **4%**
2016: **10%**

Latin America & Caribbean

2017: **30%**
2016: **21%**

Asia-Pacific

2017: **24%**
2016: **20%**

Europe, Middle East & Africa

Compromises by Region

COMPROMISES BY INDUSTRY

The incidents were across many economic sectors: The largest single share of incidents involved the retail industry, at nearly 17 percent of the total, followed by finance and insurance at 13 percent and the hospitality industry at nearly 12 percent. Several other sectors each comprised less than 10 percent of the total.

Of particular concern is the large increase in service-provider compromises, which includes any business that provides IT services to other businesses. This industry can be an attractive proposition for targeted attacks as a successful compromise can give an attacker access to numerous businesses. We assisted a variety of service providers, including web-hosting providers, point-of-sale (POS) integrators and help-desk providers, in responding to breaches in 2017. In 2016, service-provider compromises did not even register in our statistics.

2017   **2016**

Industry	2017	2016
Retail	16.7%	22.2%
Finance & Insurance	13.1%	13.6%
Hospitality	11.9%	12.3%
Food & Beverage	9.5%	19.8%
Service Provider	9.5%	0%
Professional Services	6.0%	1.2%
Payment Services	4.8%	2.5%
Health Care	3.6%	0%
Other	25.0%	28.4%

COMPROMISES BY ENVIRONMENT

Half of the incidents we investigated involved corporate and internal networks, up from 43 percent in 2016, followed by e-commerce environments at 30 percent. Incidents affecting Point-of-Sale (POS) systems decreased by more than a third to 20 percent of the total. Historically, we saw large volumes of smaller breaches; now we are seeing breaches affecting multiple businesses because of compromises to service providers and franchise head offices.

2017

- POS
- 2017: 20%
- 2016: 31%
- Corporate/Internal Network
- 2017: 50%
- 2016: 43%
- 2016: 26%
- 2017: 30%
- E-Commerce
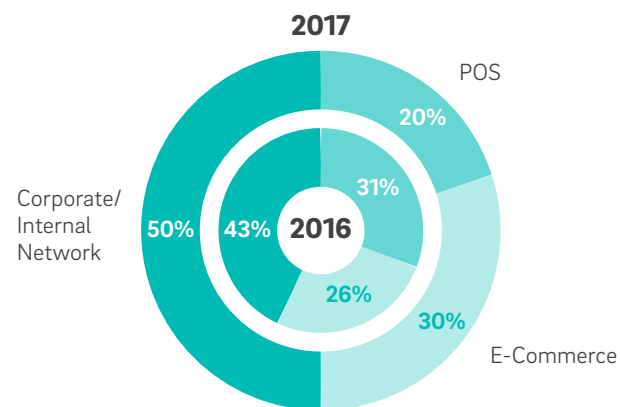
COMPROMISES BY TYPE OF DATA TARGETED

Threat actors targeted payment card data in the majority of incidents, with card-track (magnetic stripe) data making up nearly 23 percent of incidents and card-not-present (CNP) data, which is mostly used in e-commerce transa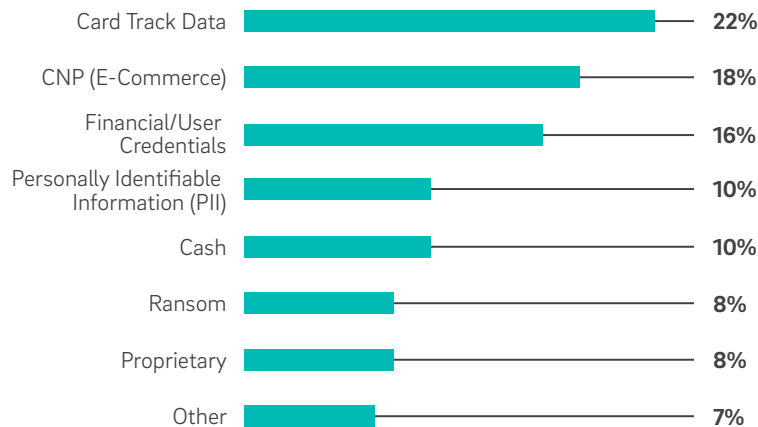ctions, comprising nearly 20 percent. This is a significant decline from 2016, when attackers targeted card data in almost two-thirds of incidents. But at the same time, there is a rise in incidents targeting cash (11 percent), mostly due to fraudulent ATM transaction breaches enabled by vulnerable account management systems at financial institutions.

Card Track Data	22%
CNP (E-Commerce)	18%
Financial/User Credentials	16%
Personally Identifiable Information (PII)	10%
Cash	10%
Ransom	8%
Proprietary	8%
Other	7%

See the **Trustwave SpiderLabs Advanced Threat Reports** section for the results of our investigation into these operations.

There have also been noticeable increases in breaches targeting personally identifiable information (PII) and proprietary data. A study Trustwave commissioned in 2017 investigated the values of stolen data on the dark web and public internet. Criminals could acquire most of the PII categories we examined for less than USD $1 per record, due to the sheer volume of data available for purchase and the varying quality of the offerings. For example, a large collection of payment card data may be next to useless if the records are not recent.

At the same time, however, some data categories command premium prices that incentivize attackers to focus their efforts on particular industries. At the top of the list, a health care record for a single targeted individual fetched an average USD $250, with some offerings going for significantly more. The values of other kinds of proprietary data can be more difficult to categorize and assess.

Visit **https://www2.trustwave.com/Value-of-Data-Report_LP.html** to download a copy of the study.

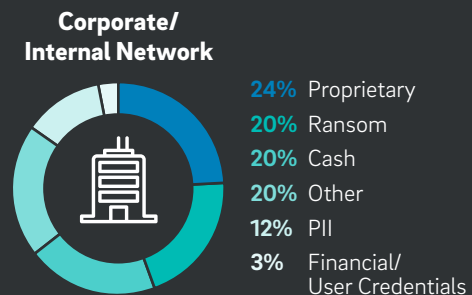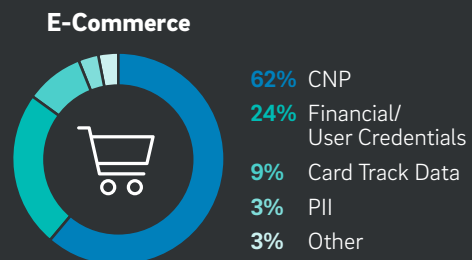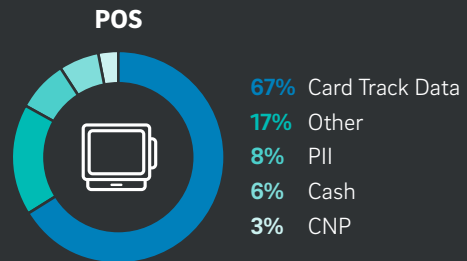> (i) Trade secrets, classified intelligence and other highly sensitive data types can be priceless to an organization.

Mean Prices for One PII Record (USD)

Health Care Record

$250.15

Payment Card Details

● **$5.40**

Banking Record

● **$4.12**

Access Credentials

● **$0.95**

Social Security number

● **$0.53**

Credit Record

● **$0.31**

Basic PII

· **$0.03**

TYPES OF DATA COMPROMISED BY ENVIRONMENT

We classify the IT environments in which breaches occur in the following categories:

- **POS environments** include dedicated "cash registers" where businesses accept payment for in-person retail transactions. POS terminals process payment cards using magnetic-stripe scanners and EMV chip-card readers. (EMV stands for Europay, MasterCard and Visa, the companies responsible for developing the chip standard.) Most run versions of the Windows Embedded or Linux operating systems customized for POS devices, and their networks usually transmit card and sales data to a centralized location and/or a financial institution.

- **E-commerce** environments include web-server infrastructures dedicated to websites that process payment information and/or PII.

- **Corporate- and internal-network environments** comprise enterprise networks in general and can include sensitive data originally collected in a POS or e-commerce environment.

POS

67%	Card Track Data
17%	Other
8%	PII
6%	Cash
3%	CNP

E-Commerce

62%	CNP
24%	Financial/ User Credentials
9%	Card Track Data
3%	PII
3%	Other

Corporate/ Internal Network

24%	Proprietary
20%	Ransom
20%	Cash
20%	Other
12%	PII
3%	Financial/ User Credentials

2017 saw a surprising trend away from payment card data as an attacker's primary objective, even in POS compromises. In e-commerce environments, we have seen attackers focusing less on stealing payment card data in favor of seeking to use the compromised website to commit fraud or theft against website owners. We have also seen an increase in ransomware attacks, sometimes to the exclusion of data that attackers previously targeted. Some of the cases we investigated involved attackers that gained root- or administrative-level access to a company's network but only used the access to install ransomware, even though there was valuable data available for the taking.

ENVIRONMENTS COMPROMISED BY INDUSTRY

Different industries face different kinds of attacks. Most of the incidents affecting the retail industry, which includes e-commerce sites as well as brick-and-mortar stores, involved e-commerce platforms. By contrast, the hospitality and food-and-beverage industries, which predominantly conduct business through POS terminals, experienced high occurrences of POS-related incidents. The largest share of incidents in health care and service-based industries were attacks on corporate and internal networks.

Legend: ■ Corporate/Internal Network ■ E-Commerce ■ POS

Industry	Corporate/Internal Network	E-Commerce	POS
Retail	1.25%	16.25%	
Hospitality	5.00%		7.50%
Finance & Insurance	10.00%	1.25%	
Food & Beverage	1.25%		8.75%
Service Provider	7.50%	1.25%	
Professional Services	5.00%	1.25%	
Payment Services	1.25%	2.50%	
Health Care	3.75%		
Other	15.00%	7.50%	3.75%

One common attack vector used to target hotels and restaurants last year was telephone-initiated spear phishing. The caller, who often was associated with the Carbanak-targeted attack group, would complain about being unable to make a reservation on the victim's website and ask to email his details to the staff member. The attacker then emailed a message with a malicious file attached, waited until the victim confirmed they opened the attachment and then hung up the phone.

The retail industry processes a lot of payment card data at POS terminals and on e-commerce platforms; consequently, most of the incidents in the retail industry involved compromised card track and CNP data. The hospitality and food-and-beverage industries, as noted earlier, conduct much of their business at POS terminals, so threat actors heavily targeted card track data in breach incidents affecting those industries.

Last year saw an increase in attacks targeting restaurant and hotel chains where threat actors used the same attack vector and malware at multiple locations. These were really an extension of a targeted attack, where criminals developed and refined an attack process for a specific merchant but gained access to multiple locations because of identical operating environments. Financial institutions faced significant cash losses from criminal operations involving fraudulent ATM transactions with this approach.
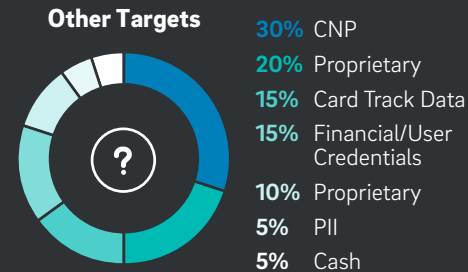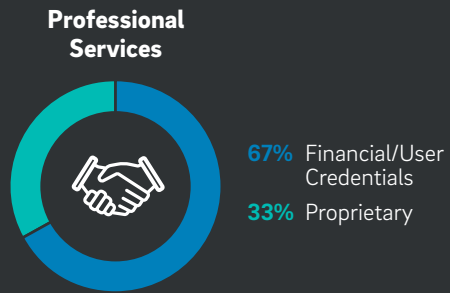
See the **Trustwave SpiderLabs Advanced Threat Reports** section for the results of our investigation into these operations.

CASE STUDY — BREACH FOR RANSOMWARE

In one case last year, an attacker gained remote access to the targeted client environment by exploiting a default administrator account for specialist software. Although the compromised account had minimal privileges, a weak password allowed the attacker to gain control of a local administrator account. Unfortunately, the same account and password was on every workstation within the environment, and event logs showed the attacker accessing multiple systems using the account. Surprisingly, although the attacker had access to all data in the environment, including sensitive financial and customer information, all they did was install ransomware.

IT Environments Compromised by Industry
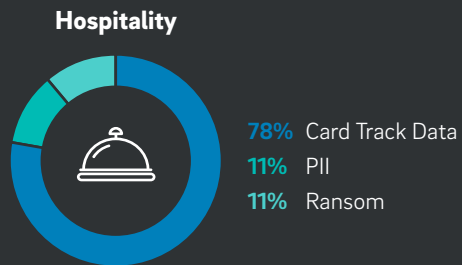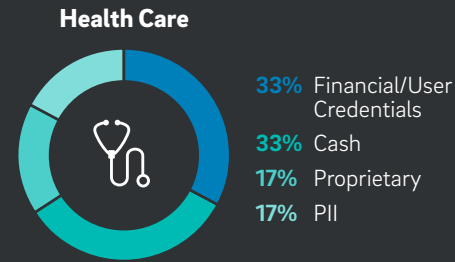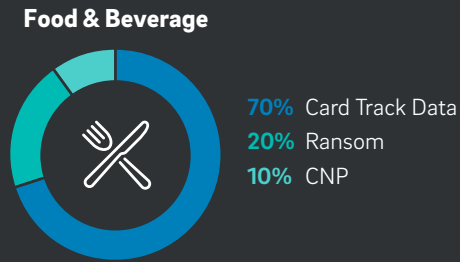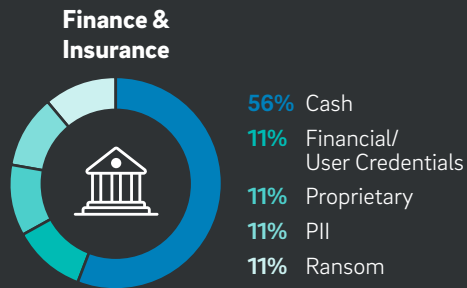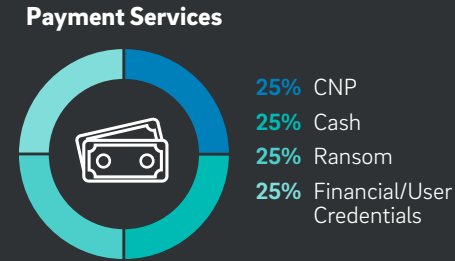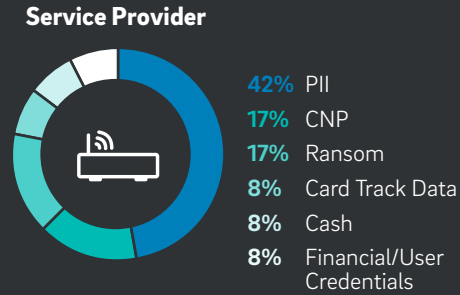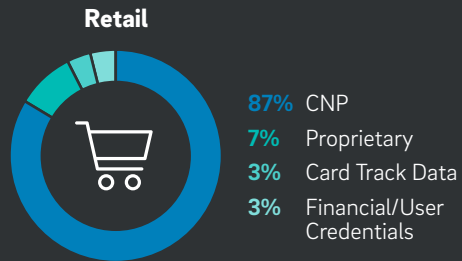
Retail

87%	CNP
7%	Proprietary
3%	Card Track Data
3%	Financial/User Credentials

Service Provider

42%	PII
17%	CNP
17%	Ransom
8%	Card Track Data
8%	Cash
8%	Financial/User Credentials

Payment Services

25%	CNP
25%	Cash
25%	Ransom
25%	Financial/User Credentials

Finance & Insurance

56%	Cash
11%	Financial/User Credentials
11%	Proprietary
11%	PII
11%	Ransom

Food & Beverage

70%	Card Track Data
20%	Ransom
10%	CNP

Health Care

33%	Financial/User Credentials
33%	Cash
17%	Proprietary
17%	PII

Hospitality

78%	Card Track Data
11%	PII
11%	Ransom

Professional Services

67%	Financial/User Credentials
33%	Proprietary

Other Targets

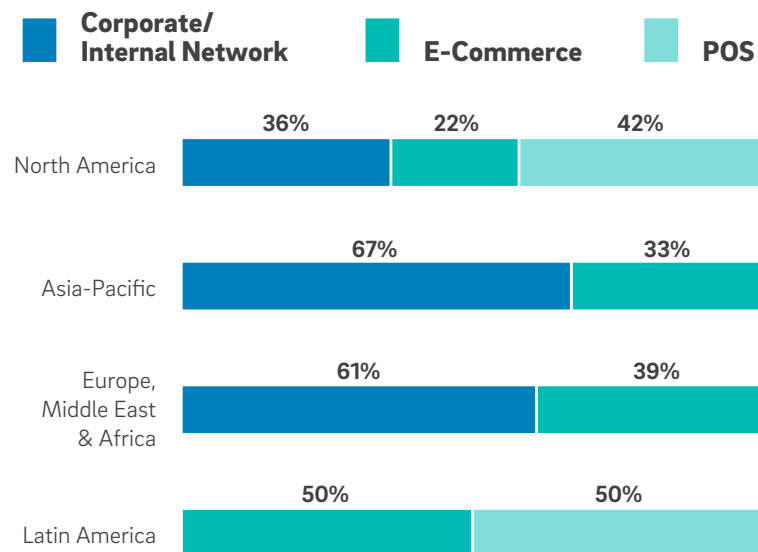|	
30%	CNP
20%	Proprietary
15%	Card Track Data
15%	Financial/User Credentials
10%	Proprietary
5%	PII
5%	Cash

ENVIRONMENTS COMPROMISED BY REGION

Again this year, POS compromises decreased across the board. In fact, we did not see a significant number of POS breaches in the Asia-Pacific region (APAC) or Europe, the Middle East and Africa (EMEA). This is likely because of the widespread adoption of the EMV payment card standard (often called "chip-and-PIN," although the standard also supports authentication mechanisms other than PINs). Unfortunately, the Americas, which do not use PIN authentication, are still lagging behind the rest of the world in EMV deployment—exemplified by a recent MasterCard and Visa decision to delay compliance for automated fuel pumps for three more years, from 2017 to 2020. Slow chip card adoption may be a factor in the larger POS compromises for North and Latin America shown in the graphs to the right.

The persistence of attacks on track data is troubling; however over the past 10 years, POS environments have become vastly more capable of protecting cardholder data. Today, an attacker is more likely to find card data stored securely, which explains why authors design most POS malware to collect track data directly from memory. While the Payment Card Industry Security Standards Council recommends three technologies—EMV chip, tokenization and point-to-point encryption—to help organizations make their customer data less valuable to criminals, 69 percent of the cases we investigated involved track data stored in plain text.

Corporate/ Internal Network   **E-Commerce**   **POS**

North America: 36% | 22% | 42%

Asia-Pacific: 67% | 33%

Europe, Middle East & Africa: 61% | 39%

Latin America: 50% | 50%

COMPROMISE DURATION

To understand how long it takes businesses to detect a breach and how long affected data records stay exposed, Trustwave investigators record the dates of three milestones in a compromise's duration. They are:

- Initial intrusion
- Detection
- Containment (wherever possible).

In some cases, the date of containment can occur before the date of detection. An example is when a software upgrade halts an attack before discovery or when investigators determine the attacker left the network before detection of the breach.

COMPROMISE MILESTONES

INITIAL INTRUSION

The day the attacker gained unauthorized access to the victim's systems, as determined by Trustwave investigators.

DETECTION

The day the victim or another party identified a breach occurred.

CONTAINMENT

The day administrators cleaned the compromise and records no longer remain exposed.

You must be able to detect a breach to respond to one. We have seen a marked reduction in the time needed to detect a breach, which is consistent with the recent advancements in detection mechanisms, including tools such as endpoint detection and response (EDR) solutions.

The message from the figures below is that attackers often have access to a compromised environment for a long period, often measured in months and, in some cases, years. Thus, attackers have ample time to obtain sensitive data and even set up mechanisms to collect and exfiltrate new data as it is added. This also means they have opportunity to install multiple backdoors, significantly increasing the difficulty of removing them from the network.

The longer a data compromise lasts, the more harm the attacker can do and the costlier the breach can be. When victims are capable of detecting compromises internally, they generally do so quickly. The median time between intrusion and detection for internally discovered breaches was zero days in 2017, meaning businesses discovered the majority of such breaches the same day they happened. In cases where the victims did not learn of the breach before regulatory bodies, law enforcement or other third parties notified them, breach duration was usually much longer. The median time between intrusion and detection for externally detected compromises was 83 days in 2017, an increase from 65 days in 2016.

Median Time Between Compromise Milestones

Intrusion to Detection

49 days
2016

26 days
2017
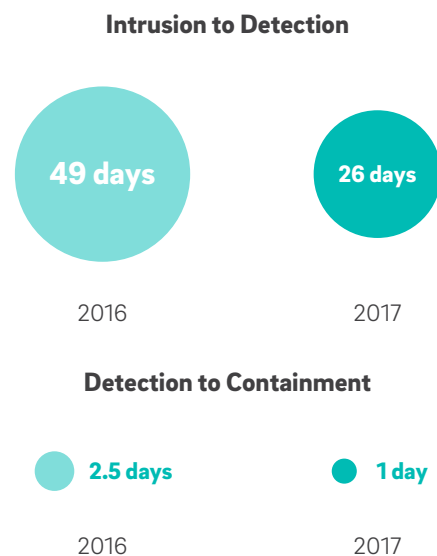
> Typically businesses only retain operating system and application event logs, which often provide critical information regarding attacker activity, for seven days or less—making them largely useless when investigating an intrusion that happened months ago.

Detection to Containment

2.5 days
2016

1 day
2017

Median Time Between Intrusion and Detection

Externally Detected

65 days
2016

83 days
2017

Internally Detected

16 days
2016

0 days
2017

Even more interesting is that businesses also contained internally detected compromises more quickly than externally detected ones. In cases where containment occurred after detection, the median duration between the two milestones was just one day for internally detected breaches compared to 21 days for externally detected breaches. The same tools and techniques that enable businesses to detect breaches on their own or in partnership with a managed security services provider (MSSP) often make it possible to respond to them within days or even minutes. By contrast, a business that must rely on breach information from an outside party is often not in a position to contain it quickly, so the compromise continues—sometimes for several crucial days.

Attackers often have access to a compromised environment for months and, in some cases, years.

METHODS OF COMPROMISE

Phishing and other social engineering facilitated almost half of the POS-system compromises we investigated. These can happen when administrators don't properly segregate the cardholder data environment from the rest of the network. As mentioned, groups targeting the hotel and restaurant sector extensively exploited this attack vector.

Compromises of service providers often enabled most remote access attacks, the second most common method of compromise for POS attacks. Often, the attacker gained remote access to multiple locations by obtaining service-provider remote access credentials, either by compromising the service-provider network (and thus VPNs) or by simply obtaining default passwords in cases where remote access tools were internet accessible.

The human factor is still the highest source of weakness for corporate environments, with phishing contributing to more than half of such compromises. We have also seen an increase in threats from malicious insiders, the second most common source of compromise in corporate environments.

Disappointingly, code injection and file upload are still the two most common methods of compromise affecting e-commerce websites. File upload attacks occur when threat actors upload a web shell to the server and get the server to execute the shell. Exploits are available for file-upload vulnerabilities in a number of popular content management systems (CMSes), and unpatched systems are still vulnerable to exploit. (See the **Web Attacks** section and **Malware** section for the results of our investigation into these operations.)

POS
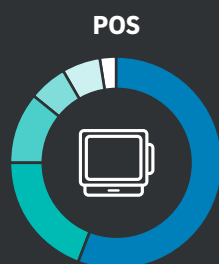
%	Method
47%	Phishing/Social Engineering
23%	Remote Access
13%	Malicious Insider
7%	Weak Password
7%	Other
3%	Misconfiguration

Corporate/ Internal Network
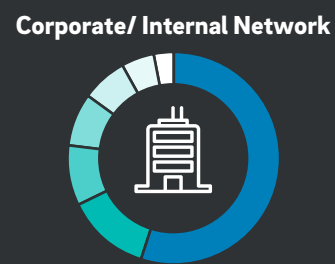
%	Method
55%	Phishing/Social Engineering
13%	Malicious Insider
9%	Remote Access
8%	Misconfiguration
7%	Other
5%	Code Injection
3%	Weak Password

E-Commerce
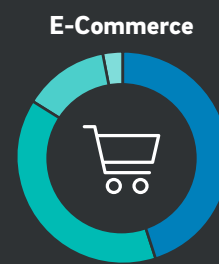
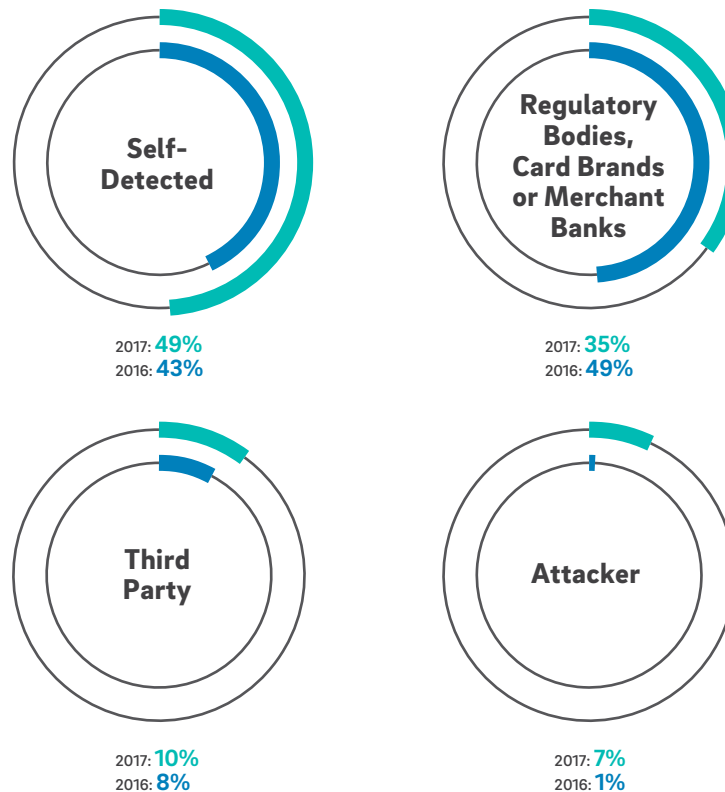| %	Method
45%	File Upload
39%	Code Injection
13%	Remote Access
3%	Weak Password

METHODS OF DETECTION

Breaches that victims detected themselves comprised nearly half of 2017 incidents, followed by breaches that regulatory bodies, card brands and merchant banks detected. The increase in attacker notification this year was largely due to the rise in ransomware attacks.

As noted, organizations that self-detect compromises can typically contain them quicker than organizations that use outside parties to detect compromises, so the prevalence of self-detections this time is a welcome development. The true rate of internal detection is also probably higher than our data suggests because many companies that have effective internal-detection systems do not need to hire external investigators. Nevertheless, it still indicates that many organizations do not have the appropriate systems in place to effectively defend against or detect a breach.

Self-Detected

2017: **49%**
2016: **43%**

Regulatory Bodies, Card Brands or Merchant Banks

2017: **35%**
2016: **49%**

Third Party

2017: **10%**
2016: **8%**

Attacker

2017: **7%**
2016: **1%**

TRUSTWAVE SPIDERLABS ADVANCED THREAT REPORTS

Trustwave publishes multiple, in-depth reports each year on topics of particular interest in the security world. Two 2017 Trustwave Advanced Threat Reports detailed Operation Grand Mars and post-Soviet bank heists.

OPERATION GRAND MARS: DEFENDING AGAINST CARBANAK CYBER ATTACKS

Several leading organizations from the hospitality sector in Europe and the United States consulted the Trustwave SpiderLabs team to analyze suspicious and potentially malicious activity on their networks, which included servers, point-of-sale terminals and client workstations spread across different locations.

Financial gain and a desire to take total control of the victims' infrastructures and establish bots within their networks appear to be the motivation behind the malicious activities. Forensic investigation and analysis indicated different individuals or groups performed these activities, leading us to conclude that several malicious factions cooperated in a single, larger operation with each group performing its own role and tasks. It soon became obvious that we were dealing with an organized crime operation. The attack characteristics of the malware used share several common traits with the Carbanak financial cybercrime network.

Enterprise anti-malware services or suspicious indicators in Windows event logs alerted the victimized organizations of the attacks. Intelligence sharing among the Trustwave teams that responded to the incidents uncovered similarities in several attacks, which affected multiple, unrelated businesses. Initially, we believed that a formal criminal operation was targeting the hospitality sector in Europe and the U.S. However, the findings suggest other sectors, such as e-commerce and retail, are equally at risk, and the campaign could easily spread to other parts of the world.

The common successful entry point in the attacks was an email message containing a Microsoft Word document attachment. Once the target opened the attachment, malicious macros created or downloaded multiple files, allowing the attackers to gain some level of access into the victim's infrastructure. In some cases, the attackers actually called the victims on the phone, a social engineering tactic, to trick them into opening the attachments.

Next, attackers used pass-the-hash techniques to escalate privileges and they achieved persistence by using scheduled tasks and several of the operating system's auto-start locations. When successful, these actions allowed attackers to gain domain-level or even enterprise admin-level access to the network. The attackers used cloud services, such as Google Docs, Google Forms and pastebin.com to keep track of infected systems, spread malware and perform additional malicious activities. Attackers used such services since many enterprise networks allow access to them and it can be challenging to blacklist them without disrupting business operations.

Attackers split malicious code used in these operations among memory resident code; scripting code, such as PowerShell, JavaScript and VBS; executables, often variants of existing malware; and customized versions of toolkits, such as Metasploit, PowerSploit and Veil Framework. The core tools used in these activities appear to comprise a variant of Anunak malware and a remote backdoor, along with a Visual Basic script (VBS) specially crafted with data-exfiltration features.

Notably, attackers signed some of the executables using valid certificates from a trusted root certification authority in most browsers. Based on the analysis of the certificates, we believe the attackers purchased and used fake identities to bypass additional security controls. The name of this operation, called "Grand Mars," comes from a name the attackers used in one of the digital signatures. While the name and some of the details used in the certificate are probably fake, the fact that someone actually paid for these certificates is a strong indicator we are dealing with organized crime activities.

The majority of IP addresses used as command-and-control (C&C) points were unknown systems located within Europe (United Kingdom, France, Sweden, etc.), indicating attackers were trying to bypass network security controls by using seemingly innocuous servers as malicious endpoints. We monitored access to these C&C servers during the investigation and found attackers occasionally changed their C&C server and took the previous one offline. We believe this alternating use of C&C servers helped attackers remain as stealthy as possible.

DOWNLOAD THE GRAND MARS REPORT FOR IN-DEPTH INFORMATION ABOUT:

- Our analysis and findings of malicious activities, the tactics and tradecraft attackers used, possible motives and the attribution of the threat actors behind these attacks.

- Remediation actions and advice to organizations targeted by this attack campaign or those willing to take proactive countermeasures.

- Indicators of compromise (IOCs) that benefit organizations seeking to undertake a compromise assessment on their own—or with the help of a team, such as Trustwave SpiderLabs, that specializes in threat hunting and compromise assessments—or to proactively implement detection mechanisms that provide early warnings if and when the organization is targeted.

DOWNLOAD NOW:
https://www2.trustwave.com/
Operation-Grand-Mars.html

POST-SOVIET BANK HEISTS: A HYBRID CYBERCRIME STUDY

In mid-to-late 2017, the Trustwave SpiderLabs team investigated a series of bank breaches originating from post-Soviet states. The actual amount of money stolen was different in each case, ranging from USD $3 million to $10 million, with the average amount around $5 million. The investigations showed the attacks shared several common features, including a large monetary loss originating from what initially appeared to be legitimate bank customer accounts.

Additionally, in all cases, the theft took place via normal cash withdrawals, using legitimate bank-issued debit cards, from various ATM terminal locations outside the bank's originating country. In some cases, the victimized banks didn't even realize a breach and theft had taken place until well after the attack. In a few cases, third-party processors responsible for processing the bank's debit and credit card transactions reported the malicious activity to the banks.

The attacks included physical and network-based components. For network-based components, attackers used spear phishing and social engineering to gain initial entry to the banks' networks. From there, they captured credentials for a third-party service and compromised it as well, ultimately gaining access to functions for modifying customer accounts.

For the physical component, the criminals used "mules," people who performed various in-person tasks on behalf of the attackers. The mules personally visited various bank branches, opened new accounts with minimum or zero-initial deposit amounts and requested debit cards for the accounts. Debit cards draw on funds deposited in bank accounts, not lines of credit. At first glance, it may seem as if the criminals would only be able to use them to withdraw their own money;

however, many banks offer overdraft protection for some checking accounts, allowing a qualified customer to temporarily withdraw more funds from an account than are on deposit. Typically, banks conditionally offer overdraft protection to customers based on factors known as risk levels, and the accounts the mules opened would not have qualified for overdraft protection to any significant degree. Having compromised the banks' systems, however, the attackers were able to manipulate the debit cards' features to enable high overdraft amounts and remove anti-fraud protections that ordinarily would detect suspicious card activity.

For the final stage, the criminal group collected the debit cards from the mules and distributed them outside their originating countries to international conspirators. Afterward, the conspirators used the debit cards to perform cash withdrawals from different ATMs. When the operation concluded a few hours later, the conspirators had successfully withdrawn up to USD $10 million from each bank.

We believe the attack represents a clear and imminent threat to financial institutions in European, North American, Asian and Australian regions in 2018. While the activity we analyzed took place exclusively in Russia and Eastern Europe, these regions often prove to be the canary in the cybercrime mineshaft, signaling possible upcoming threats affecting other parts of the world. Our investigations revealed victim losses totaling around USD $40 million. When possible, we consider the undiscovered or uninvestigated attacks along with investigations internal groups or third parties are undertaking. In this case, we estimate that losses could be in the hundreds of millions of U.S. dollars. All global financial institutions seriously should consider and take steps to mitigate this threat.

...victimized banks didn't even realize a breach and theft had taken place until after the attack.

$40 MILLION

VICTIM LOSSES DUE TO POST-SOVIET BANK HEISTS

All global financial institutions seriously should consider and take steps to mitigate this threat.

02

THREAT INTELLIGENCE

Every day, Trustwave products, systems and security response professionals monitor the internet and customer networks for threats. In this section, we examine the insights our findings provided about the trends, techniques and developments we uncovered in 2017.

In the first part of this section, we discuss attacks on web applications, focusing on the methods and mechanisms attackers used to compromise web servers. Next, we discuss email threats, such as spam, phishing and malware attachments, with a focus on the Necurs botnet that distributes malware through spam. This section also includes an example of a CEO fraud conversation a scammer successfully used to steal a large sum of money from a targeted corporation.

From there, we discuss significant exploits that emerged during the year and examine the state of the exploit kit landscape in 2017, following the high-profile disappearance of several major kits the previous year. In a sidebar, we look at cryptocurrencies, such as bitcoin, and how criminals use, steal and mine them for their own purposes. Finally, we take inventory of the malware we encountered during investigations into data compromise incidents and explore the similarities and differences between malware families.

WEB ATTACKS

Much has changed across the attack landscape in past 10 years, with many alterations in the top actors, their motives, toolsets, attack frameworks and targeted exploits. Targeted attacks have become more common and are becoming more sophisticated: Many high-profile breach incidents show signs of significant preplanning by attackers who carefully identify weak packages and tools on targeted servers before making a move. At the same time, the basic attack techniques attackers use tend to be the same ones they've been relying on for years, including cross-site scripting (XSS), SQL injection (SQLi) and so on.

TOP WEB ATTACKS

- Other **22%**
- XSS **40%**
- DDoS **3%**
- LFI **4%**
- Path traversal **7%**
- SQLi **24%**
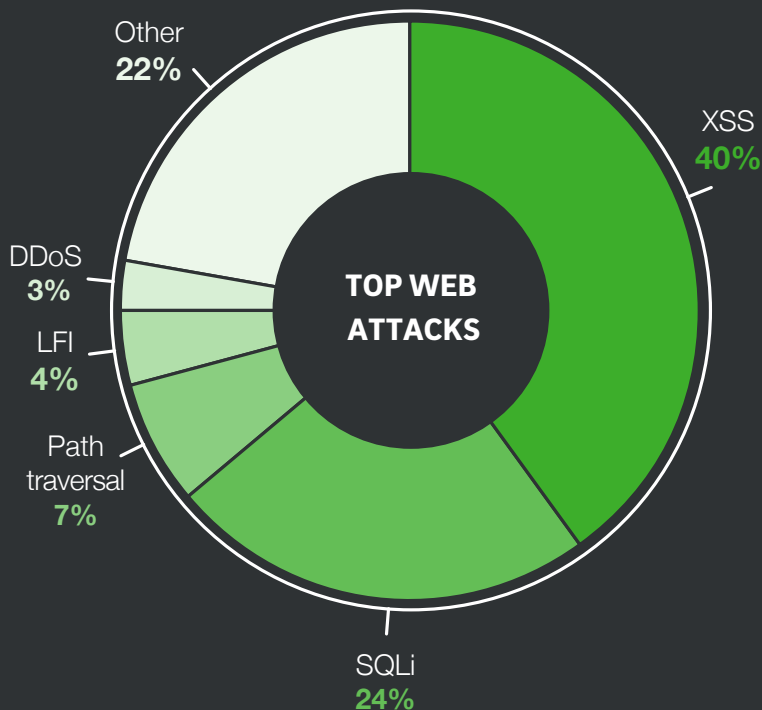
Analysis of web-application attacks and compromises helps identify the top attack methods cybercriminals used in 2017. Our data set includes multiple sources:

- Alerts from Trustwave Managed Web Application Firewall
- Web-specific alerts from Trustwave Managed IDS/IPS
- Web alerts from testing environments
- Web honeypot systems
- Cyber intelligence from public resources
- Logs from ModSecurity Web Application Firewall instances deployed as part of the OWASP Web Application Security Consortium Distributed Web Honeypots project
- Trustwave Advanced Security Operations Centers
- Trustwave incident response and forensic investigations
- Telemetry data from customers.

TOP WEB ATTACKS IN 2017

The top web attacks we observed include:

Cross-site scripting (XSS), involved in about 40 percent of attack attempts last year, remains the most common attack technique we see. XSS typically involves inducing a web site to execute arbitrary or malicious script code an attacker uploaded, usually because the site fails to properly sanitize user-submitted inputs. If another visitor loads the malicious or compromised web page, their browser may execute the malicious code, infecting the victim. Most XSS attacks are not particularly sophisticated, and we see a lot of attacks come from "script kiddies," inexperienced attackers using scripts and tools others wrote.

SQL injection (SQLi), at about 24 percent, was the second most common attack technique we witnessed. The most common form of SQLi occurs when an attacker enters malicious SQL code into a field on a web page and the server-side code submits it to the database without properly sanitizing it first. A successful SQLi attack can delete or change sensitive data or reveal it to the attacker.

Path traversal attacks were in about 7 percent of cases we examined. These attacks attempt to access unauthorized files or directories outside the web root folder by injecting patterns such as "../" to move up in the server directory hierarchy. Successful path-traversal can allow attackers to improperly access site or user credentials, configuration files, databases or other sites co-located on the same physical machine.

As with XSS and SQLi, successful path traversal attacks usually result from inadequate input sanitization and often are combined with other attacks, such as local file inclusion, to steal the targeted data or credentials.

Local file inclusion (LFI), observed in about 4 percent of attacks, is where the attacker uses directory traversal or a similar mechanism to induce the web application to execute a file residing elsewhere on the server.

Distributed denial of service (DDoS) attacks accounted for about 3 percent of attacks we examined. DDoS involves commanding numerous computers, typically compromised computers in a botnet, to bombard a targeted web server with requests, overloading its resources and rendering it unavailable to legitimate visitors. While DDoS alone does not provide an attacker with improper access to any resources, in 2017 we saw a trend of attackers increasingly using DDoS alongside other attacks to distract automated defense systems from responding to a more serious and dangerous attack.

Two security advisories Trustwave SpiderLabs researchers published in 2017 highlight the risk internet-connected devices can introduce to an environment. Trustwave SpiderLabs Security Advisory TWSL2017-003, published in January 2017, addresses CVE-2017-5521, which covers multiple vulnerabilities in several popular models of Netgear routers that can lead to administrative password disclosure via a simple crafted request. Attackers can exploit the bug remotely if the remote management option is set and locally with access to the router over LAN or WLAN. If attackers gain access to a router's administrative password, they can potentially take a wide range of malicious actions against the network, including lowering security settings and exposing computers on the network to external attacks. Trustwave disclosed the vulnerability to Netgear privately in 2016 and worked with the company to coordinate public disclosure with the release of firmware updates that addressed the vulnerability for the affected routers.

Trustwave SpiderLabs Security Advisory TWSL2017-017, published in November 2017, addresses CVE-2017-16249, a vulnerability in the embedded HTTP server in some Brother network-connected printers. The embedded server is vulnerable to a denial-of-service attack wherein a single malformed HTTP POST request can cause the server to hang until it times out, in approximately 300 seconds, with an HTTP 500 error. While the server hangs, network print jobs are unavailable and the web interface is inaccessible. An attacker can continuously send this malformed request to keep the device inaccessible to legitimate traffic. Trustwave disclosed the vulnerability privately to Brother in September and, after receiving no response, published the security advisory two months later. As of this writing, no patch is known to exist. Brother recommends mitigating the vulnerability by activating the printer password feature and using IPsec, SSL, TLS, SNMPv3 and other industry standard protocols to further secure the printing environment if necessary. To limit exposure, we recommend limiting access to the affected devices to authorized personnel through the use of access control lists and proper network segmentation.

...hackers issued a points system for independent attackers willing to help conduct DDOS attacks...

The nature and circumstances of these vulnerabilities remind us that the update mechanisms for most devices continue to lag far behind those of traditional computers, smartphones and tablets. Even when firmware updates are available, the onus is on the customer to be aware they exist and to have the technical ability to implement them—a reasonable expectation for IT staff, perhaps, but not for most home users. Even worse, updating device firmware often erases user configuration changes, so even knowledgeable users may choose to assume the risk of exploitation rather than re-implement what may be a time-consuming and poorly documented series of customization options. Making the update process easier and less painful should be a top priority for device manufacturers.

POINTS FOR ATTACKING

We've noted in the past how the underground economy of attackers and those who pay for their products and services have taken on many of the trappings of legitimate enterprise. A curious news item from December 2016 underlines the point nicely: A group of Turkish hackers had issued a points system for independent attackers willing to help conduct DDoS attacks against targets the group selected, all of which were associated with opponents of Turkey's current government. For every 10 minutes spent attacking a target, attackers would receive points they could trade in for rewards, such as bots and hacking tools. Participants could even keep track of their rankings on a live scoreboard. We wonder how many potential participants chose to hold out for an Xbox Live-style achievement system.

ATTACKS ON DEVICES

In the past decade, there has been a rise in attacks on internet-connected devices, such as network infrastructure hardware, peripherals and the web of connected smart devices colloquially called the internet of things (IoT), which include home appliances, vehicles, wearable fitness devices and many other technologies that have not traditionally been part of the internet. Many such devices run unique embedded systems not hardened through years of responding to attacks. Hackers have been quick to respond to the attack surfaces these devices introduced into the network ecosystem.

OWASP UPDATES THE TOP 10

In 2017, the Open Web Application Security Project (OWASP) updated its "Top 10" list of the most critical web application security risks for the first time in four years. The list includes four new entries and reorganizes several others.

OWASP Top 10 Lists for 2013 and 2017

RANK	2013	2017
A1	Injection	Injection
A2	Broken Authentication and Session Management	Broken Authentication
A3	Cross-Site Scripting (XSS)	Sensitive Data Exposure
A4	Insecure Direct Object References	External Entities (XXE)
A5	Security Misconfiguration	Broken Access Control
A6	Sensitive Data Exposure	Security Misconfiguration
A7	Missing Function Level Access Control	Cross-Site Scripting
A8	Cross-Site Request Forgery (CSRF)	Insecure Deserialization
A9	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
A10	Unvalidated Redirections and Forwards	Insufficient Logging & Monitoring

Injection flaws, including SQLi, led the OWASP list again, as they have since 2010. Injection vulnerabilities are easy to detect and exploit, and exploitation can cause major damage. OWASP reports that injection vulnerabilities remain prevalent in legacy code, and attackers use scanners and fuzzers to find vulnerabilities automatically.

Sensitive-data exposure moved up to third place in 2017 from sixth place in 2013 due to the increased prevalence of attacks targeting sensitive attacks. The most common flaw in this category is simply a lack of encryption for data at rest or in transit.

XML external entities (XXE), in fourth place, is a new entry on the list. The XML standard allows a document to define an external entity, referenced by a uniform resource identifier (URI), the parser should dereference and evaluate. Modern XML processors typically disable external entities by default; but many older processors continue to allow them, which can enable attacks through local or remote file inclusion.

Broken access control, in fifth place, is a new entry created by the merger of insecure direct object references (#4 in 2013) and missing function level access control (#7 in 2013). Access control weaknesses are common due to a lack of automated detection and effective functional testing by application developers. Broken access control allows attackers to access functions normally only available to authenticated users or administrators, placing vital resources at risk.

XSS moved to seventh place in 2017 from third place in 2013. XSS attempts remain common, as we explored earlier; but most popular frameworks automatically sanitize inputs, which helps mitigate the risk.

Insecure deserialization, in eighth place, is new to the list. Insecure deserialization of entities such as JSON objects can permit remote code execution or sensitive object manipulation on affected platforms.

Insufficient logging and monitoring, in 10th place, is also new. Well-designed systems should log high-risk events, such as login attempts and high-value transactions, and transmit alerts when they detect suspicious activity. The chance that an attack will succeed dramatically increases if inadequate logging and monitoring delay incident response.

CMSES REMAIN TEMPTING TARGETS

In last year's report, we discussed how popular content management systems (CMSes), such as Joomla and WordPress, represent potentially lucrative targets for attackers. When they discover a significant weakness in a widely adopted CMS, it places every installation of that CMS at risk for exploitation not only before the fix is available but also for considerable time afterward. Attackers use automated tools to find CMS installations to target. WPScan (for WordPress), JoomScan (for Joomla) and Jaidam (for multiple CMSes), for example, are penetration testing tools owners use to scan their own sites for vulnerabilities. Like most pen testing tools, they can attack sites as well as defend them.

> Site administrators should be aware of the risks and take security seriously, including frequently checking for updates for core installations and plugins and themes. They should also install security updates quickly and attend to security warnings immediately.

Typical security issues that affect CMSes include:

- **Failure to update:** Although the most popular CMSes regularly publish security fixes, most installations aren't updated quickly, and many are out of date by a year or more. Some administrators delay or avoid upgrading for fear of losing customizations they made to their site, themes or plugins.

- **Default configurations:** Many CMS administrators make few changes to the default configuration after installation, which gives attackers a significant advantage when looking for weak points.

- **Vulnerable plugins and themes:** Even when the core CMS itself is reasonably secure, plugins can introduce vulnerabilities. Enthusiasts with inadequate knowledge of secure development techniques, and who may use open-source components with known vulnerabilities, write many plugins and themes. Even when plugins and themes receive security updates, users may need to install them separately from core CMS updates, creating another risk.

- **Lack of security awareness:** Inadequate security awareness on the part of site owners, often small companies or community organizations without dedicated IT staff, often exacerbate these issues.

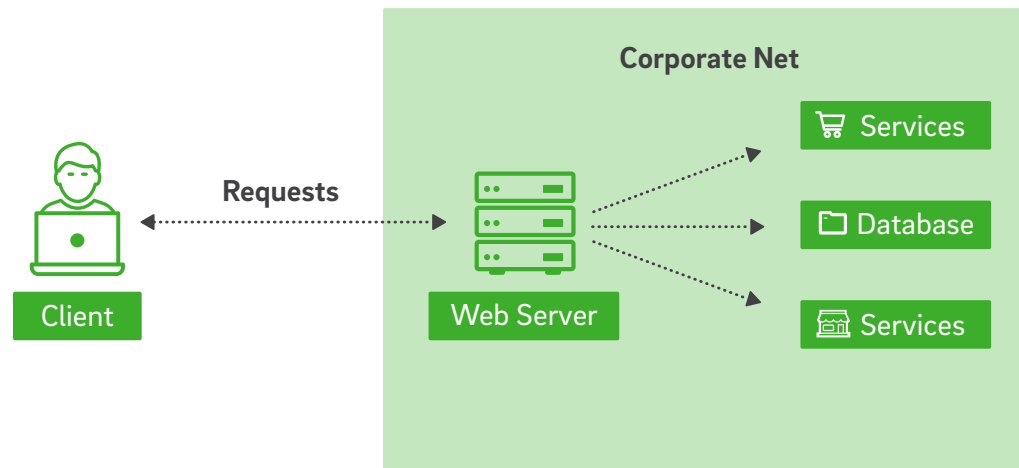- **Shared storage:** CMSes are often co-hosted on shared storage, which can place them at risk of cross-infection by compromised sites located on the same server.

WEB APPLICATION FIREWALLS IN ACTION

WAFs provide an important line of defense for critical applications and data. Unlike traditional firewalls, which mainly control traffic based on the ports and protocols they use, a WAF controls access to web applications using rules designed to recognize and restrict suspicious activity, such as SQLi, XSS and exploitation of vulnerabilities. WAFs, such as Trustwave Web Application Firewall, are updated continuously with new rules designed to catch the latest attack and exploitation techniques before they can harm important resources. WAFs operate on the application layer, the highest level of the OSI model, and have access to all protocols on all networking layers. This gives them the power to protect websites from a wide range of attacks.

This illustration shows a traditional commercial web infrastructure with no WAF, where visitors connect directly to a web server that provides controlled access to data and other resources.

Client — **Requests** — **Corporate Net** — **Web Server** — 🛒 **Services**, 🗀 **Database**, 🏦 **Services**

The illustration to the right shows how a malicious visitor can attack the web server and compromise it, allowing attackers to access sensitive data and resources or infect other visitors with malware.
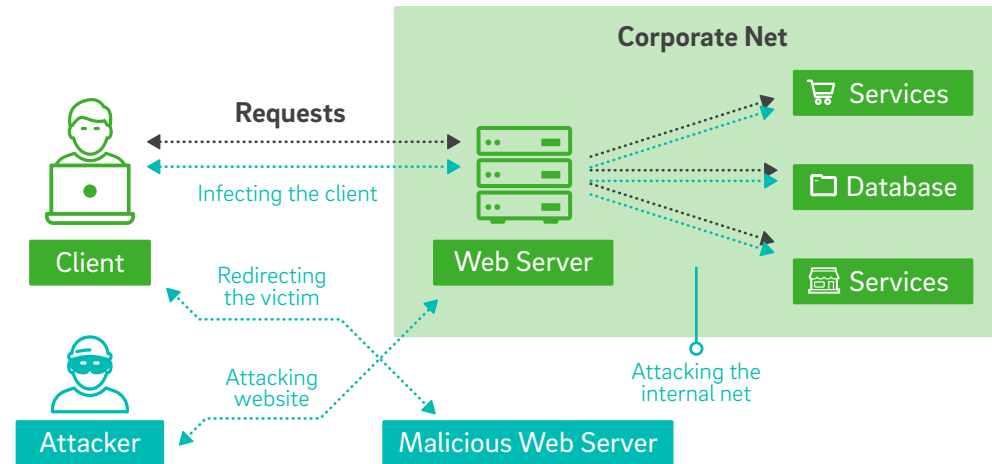
When, as in this following illustration, clients connect to the web server through the WAF, legitimate visitors see no difference, and the system detects and blocks attack attempts before they can do damage.
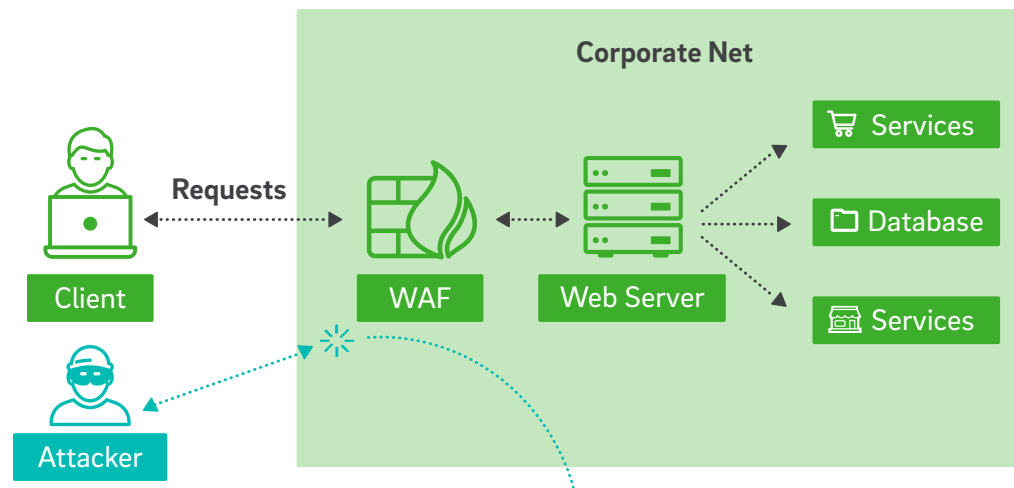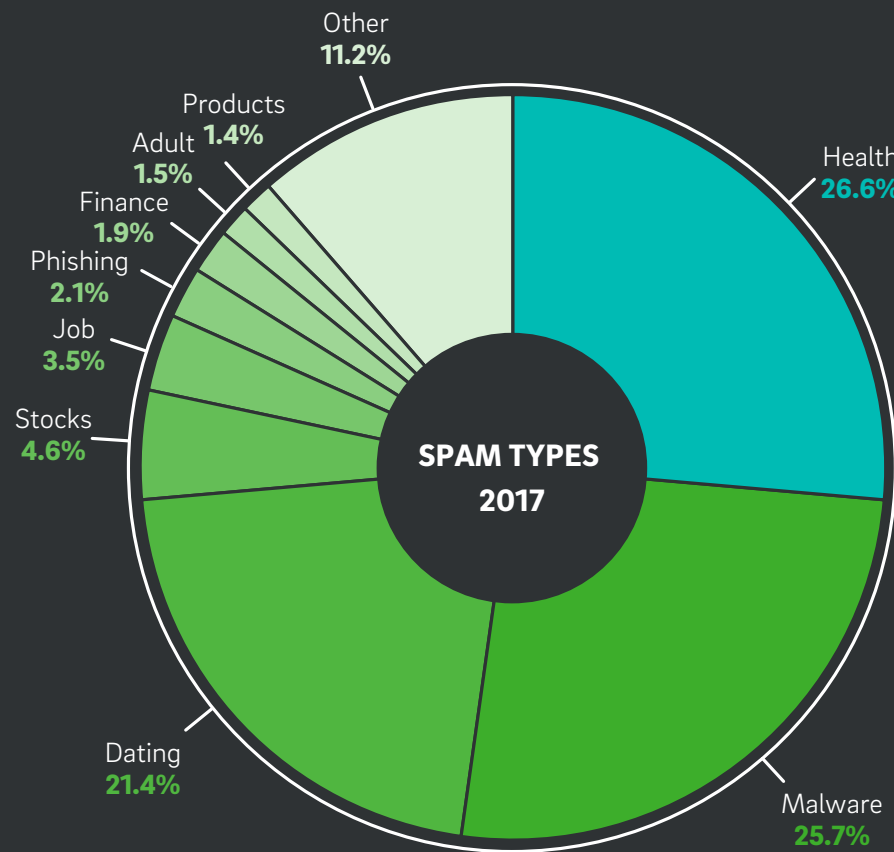
EMAIL THREATS

The story of the year in email security was the resilience of the Necurs botnet, which continued to pump malware-laden messages into inboxes and email filters throughout 2017. The good news is that overall spam volumes, which increased in 2016 due to Necurs' influence, fell again in 2017 to the lowest level in a decade.

SPAM TYPES

This figure shows the subject matter of spam messages Trustwave observed in 2017. The data reflects spam caught in Trustwave's spam traps and may not be representative of spam that makes it to mailboxes, which often sit behind spam-blocking services that filter out unwanted messages before delivery.

Three categories comprised almost three-fourths of the spam Trustwave analysts saw in 2017. Health-related spam—advertisements for phony cures and other illegitimate or dubious pharmaceutical products—accounted for 26.6 percent, followed closely at 25.7 percent by spam delivering malware and spam advertising, and online dating sites at 21.4 percent. Categories beyond the top three include stock spam, phony job offers, phishing attempts, financial spam and others, none of which comprised more than 5 percent of the total.

Other
11.2%

Products **1.4%**

Adult
1.5%

Finance
1.9%

Phishing
2.1%

Job
3.5%

Stocks
4.6%

Health
26.6%

**SPAM TYPES
2017**

Malware
25.7%

Dating
21.4%

See the **Ten Years of Security** section for long-term trend information about email-borne threats, such as spam and malware.

NECURS AND MALWARE SPAM

Spam containing malware accounted for less than 3 percent of the spam Trustwave analysts saw each year until 2016, when it jumped to almost 35 percent. Malware spam declined a bit in 2017 but was still high.The elevated levels of spam-borne malware in 2016 and 2017 are almost entirely due to Necurs, a prolific botnet that typically operates in short bursts of intense spamming activity followed by periods of dormancy. At its peak, the botnet sends spam from between 200,000 and 400,000 unique IP addresses daily. Necurs activity decreased in 2017 compared to the previous year, but the start-and-stop nature of the botnet makes it difficult to conclude the decline represents an actual decrease in activity or shrinkage of the botnet.

Malware Detected in Trustwave Spam Traps
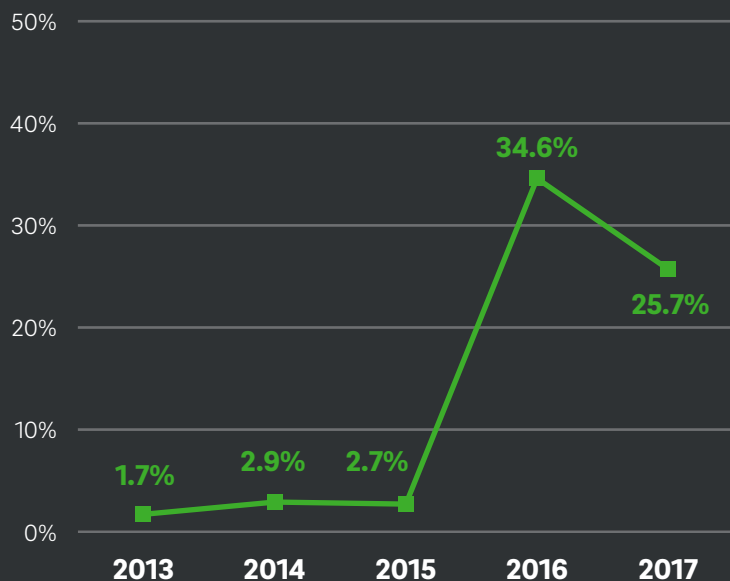
MONTH	PAYLOAD
April	PDF with embedded Word Doc containing a macro that downloads Jaff ransomware
July	PDF with embedded Word Doc containing a macro that downloads a loader for Nitol or TrickBot
August	JavaScript attachment that downloads Locky ransomware
Octoboer	JavaScript attachment that downloads Locky ransomware
November	Word Docs using Dynamic Data Exchange (DDE) to execute script; Word Docs with embedded OLE VBS object script that downloads Locky

Necurs operators constantly experiment with different attachment types and methods for getting code to run on victims' computers. This table shows some of the larger spam campaigns Necurs waged in 2017 and how operators delivered their payloads.

Attackers deliver more than 90 percent of spam-borne malware inside archive files, such as .zip or .7z, typically labeled as invoices or other kinds of business files. The malicious file itself is typically a small script file or a document that contains embedded code, such as a Microsoft Word file with macros.

When users open the file, the malicious code runs. The sole purpose of this code, which typically is highly obfuscated, is to download and execute additional malware. In some cases, the script fetches another download script, often of a different file type, which then downloads the ultimate payload. Common payloads encountered include:

- Banking Trojans, such as **Ursnif**, **Emotet** and **Trickbot**, which steal online credentials for banking websites.

- **Kovter**, a fileless malware family that performs multiple malicious actions. (See the **Malware** section for more information about fileless malware.)

- Ransomware families including **Cerber, FakeGlobe** and **Locky.**

RAR
15%

**EMAIL
MALWARE
CONTAINER
FILES**

ZIP
25%

7z
60%
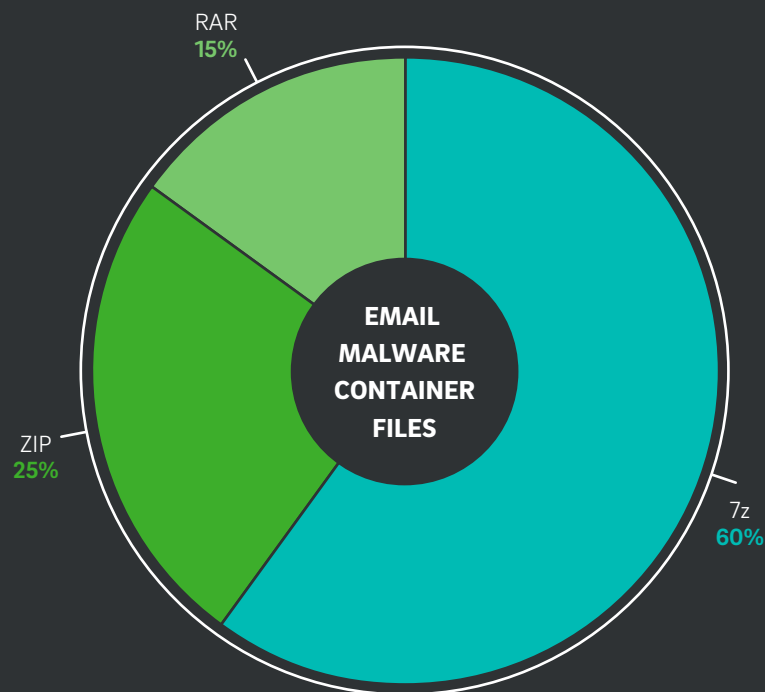
Attackers deliver more than 90% of spam-borne malware inside archive files.

The majority of the spam-delivered malware we observed in 2017 came in the form of .vbs files, many of which contained embedded PowerShell code. JavaScript .js files were the second most common file type, followed by PDF files and Microsoft Word documents. Late in the year, we saw Necurs begin to exploit a newly discovered technique for exploiting Word's Dynamic Data Exchange (DDE) protocol to execute malicious code, which means attackers can craft malicious documents using the macro-less .docx file type usually deemed safer than the older .doc binary format. All Word users should ensure they apply the latest security updates to defend against this exploit.
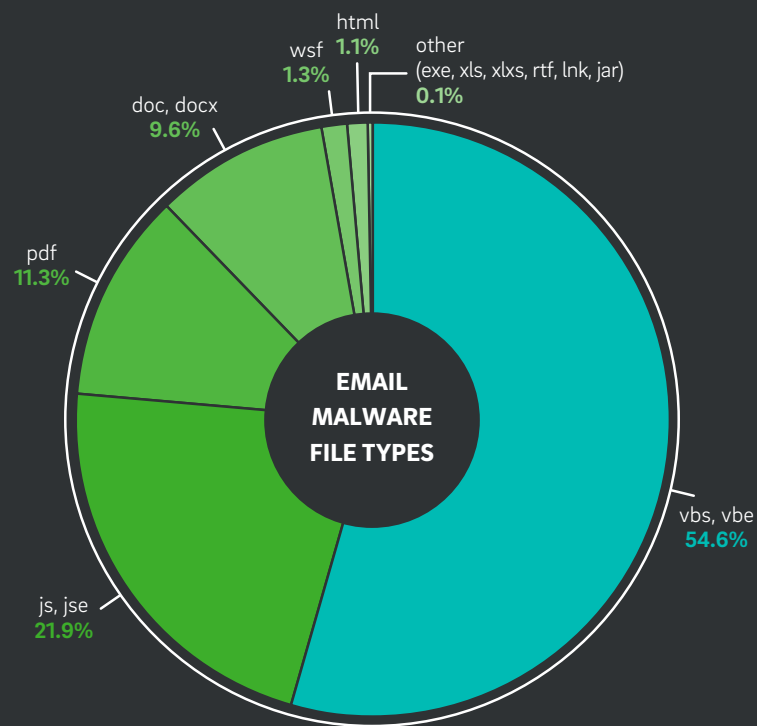
Other Vulnerabilities Spam-Borne Malware Commonly Exploited in 2017

CVE REFERENCE	PRODUCT/COMPONENT
CVE-2017-0199	Microsoft Office/WordPad Remote Code Execution Vulnerability
CVE-2014-6352	Windows OLE Remote Code Execution Vulnerability
CVE-2015-1641	Microsoft Office Memory Corruption Vulnerability
CVE-2012-0158	MSCOMCTL.OCX RCE Vulnerability with Microsoft Office
CVE-2015-2545	Microsoft Office Malformed EPS File Vulnerability
CVE-2017-8759	.NET Framework Remote Code Execution Vulnerability
CVE-2017-11882	Microsoft Office Equation Editor Stack Buffer Overflow

EMAIL MALWARE FILE TYPES

- html **1.1%**
- wsf **1.3%**
- other (exe, xls, xlxs, rtf, lnk, jar) **0.1%**
- doc, docx **9.6%**
- pdf **11.3%**
- js, jse **21.9%**
- vbs, vbe **54.6%**

PHISHING TRENDS

Phishing activity remained strong in 2017. The story is always the same: Users received realistic-looking email messages that mimic real emails from real organizations. In some cases, the attackers base their templates on actual messages, just changing a few words and the underlying links. Below are some of the major themes we encountered in 2017:

CVE REFERENCE	PRODUCT/COMPONENT
Bank	Fake landing page harvesting online banking credentials
Amazon	Fake Amazon receipts that lead to a variety of landing pages, including malware credentials and junk products
Courier	Fake parcel deliveries and receipts from shipping companies. Links lead to malware downloads, such as ransomware or banking Trojans
Apple	Fake Apple store receipts or password "resets." Harvests Apple credentials
Utility	Fake bills from energy utilities or telecoms, with links leading to ransomware or banking Trojans
Finance Software	Fake emails ostensibly from accounting providers, such as MYOB, Quickbooks, Xero or Intuit, leading to Dridex banking Trojan
Tax Return	Fake tax return; e.g., a message from the IRS leading to Java-based remote access Trojan (RAT)
Mail Quota	Fake email quota or email password "reminders" that seek to gain the user's domain login credentials

PDF PHISHING

A continuing development that first came to our attention last year is the PDF phishing document. The target receives an email message with an attached PDF file. When opened, the file displays blurred text along with a message that the PDF is secure and must be viewed online. Clicking the link loads a URL of the attacker's choosing, leading to either a phishing credentials page or a malware download.

A CEO FRAUD CONVERSATION

"CEO fraud" (or "CEO wire transfer fraud") is a technique that attackers use to steal money from companies. In this scam, the target is typically a mid-level executive or financial officer with the authority to send money on behalf of a company. It often is not difficult for the scammer to find the name and email address of a suitable candidate by perusing the company's website, or other public information, along with the identity and email address of the company's chief executive officer. The scammer then sends the target an email message to another employee purporting to be from the company's CEO, asking them to send a payment to a vendor or other party. In one common approach, the message appears to originate from the CEO's account, but the Reply-To message header is set to a different account to ensure that replies or follow-up messages from the target reroute to the scammer and not the CEO.

We recently received a copy of an email thread showing a CEO fraud operation action. The conversation reproduced here actually happened in November 2017 between a CEO scammer and the victim he successfully ripped off, although the names and other identifying details have been changed.

LANGUAGE FLUENCY

One notable thing about this conversation is that the scammer is reasonably fluent in English, which is often not the case with phishing messages. CEO fraud is a one-to-one operation conducted individually by con artists targeting specific companies and all but requires the perpetrator be highly conversant in the victim's language.

From: John Smith
Sent: Monday, 13 November 2017 11:27 AM
To: Susan Brown
Subject: Urgent Attention

Are you available to handle an international payment this morning? Have one pending, let me know when to send bank details.

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 1:33 AM, Susan Brown wrote:

Hi John,

Sorry was caught up with a project – I'm here now – can I still help?

Susan Brown
Director

Note that the scammer did not need to use specific information about the company other than the names and email addresses of the targeted individual and the executive he pretended to be.

On Mon, Nov 13, 2017 at 4:29 PM,
John Smith wrote:

Can you still handle this right now? was very busy earlier.

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 6:01 AM,
Susan Brown wrote:

Hi John,

Just back – can do it for you now if that will help.

Cheers,
Susan Brown
Director

On Mon, Nov 13, 2017 at 5:48 PM,
John Smith wrote:

Yes it seem to be a very busy day. The amount is for $30,120 i am guessing it is very late already for the transfer or can you still get it done today?

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 6:50 AM,
Susan Brown wrote:

Hi John,

Is it set up ready to go in PC banking?
I can't see it there to authorise under international?

Cheers,
Susan Brown
Director

On Mon, Nov 13, 2017 at 5:56 PM,
John Smith wrote:

Oh ok, please find a way around it, my day is really tied. Can i send you the bank details today still? Can the payment still go out?

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 6:58 AM,
Susan Brown wrote:

Hi John,

I can do my best but will do it from home tonight as have to leave the office now. Think they still go to 8 pm or so.

Send me all the details and I'll try but usually Mary sets them up and we just authorise them.

Will see what I can do – it's no trouble as I know I can ask Mary from her home if necessary.

Leave it with us.

Regards,
Susan Brown
Director

On Mon, Nov 13, 2017 at 7:02 AM,
John Smith wrote:

Ok then. Thanks

    NAME: Acme
    SORT CODE: 12341234
    ACCOUNT: 123412341234
    IBAN: ABCD1234123412341234123412341234
    SWIFT ABC:ABCD1234
    BANK: SOME BANK
    ADDRESS: 3 Somewhere Place

Send me payment slip once it is completed.

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 7:14 AM,
John Smith wrote:

Please use this IBAN number for the account.
IBAN:ABCD1234123412341234123412341

Ensure to send me the slip once its done. Thanks

N.B: confirm receipt of the new IBAN number.

Regards
John Smith
Sent from my iPhone

EXPLOITS

Last year was a mixed year for exploits. High-profile zero-day exploits leaked by the Shadow Brokers hacking group enabled the widespread WannaCry and Petya ransomware attacks. At the same time, the exploit kit landscape came out of a turbulent 2016 into a much quieter period—symbolic, perhaps, of a general shift in the cybercriminal underground from widespread exploitation to narrower targeted attacks.

ZERO-DAY EXPLOITS IN 2017

Trustwave researchers tracked six web-based, client-side vulnerabilities that vendors patched in 2017 that contained exploit code in the wild prior to patching. Attackers used all six sparingly in targeted attacks, and, at the time of publication, exploit kits have not picked up any of them.

- CVE-2017-0199 is a remote code execution (RCE) vulnerability in Microsoft Office and WordPad that attackers can exploit using a specially crafted document containing an embedded object that contacts a malicious web server.

- CVE-2017-0261 and CVE-2017-0262 are RCE vulnerabilities in the Encapsulated PostScript (EPS)-processing feature of Microsoft Office. CVE-2017-0263 is an escalation of privilege (EoP) vulnerability in the kernel-mode drivers in Microsoft Windows. Attackers used it alongside CVE-2017-0262 to elevate privileges on the targeted system and allow the RCE exploit to execute malicious code.

- CVE-2017-8759 and CVE-2017-11292 are RCE vulnerabilities in the Microsoft .NET Framework and Adobe Flash Player, respectively. We believe targeted attack groups have used each in cyber-espionage activities.

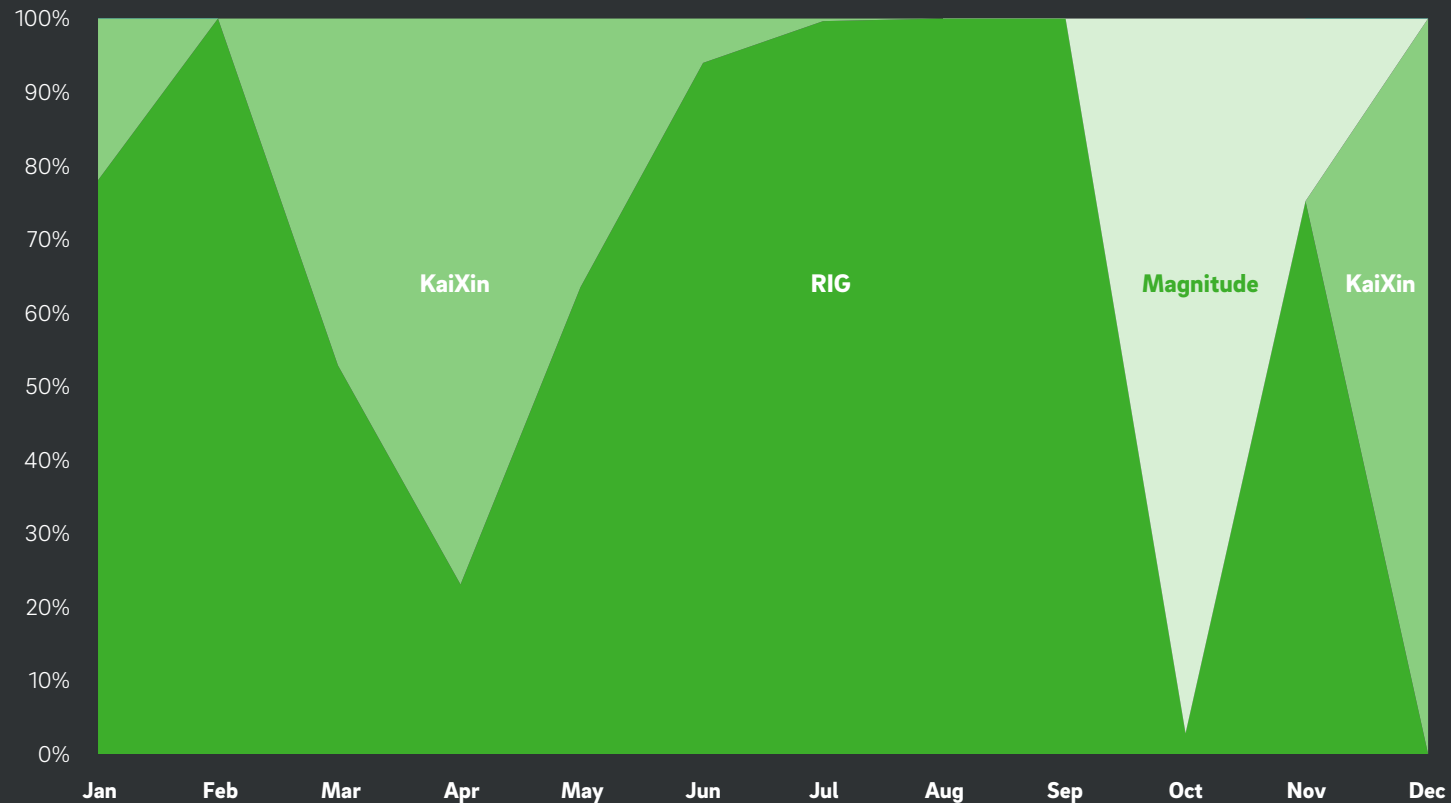| CVE REFERENCE	PRODUCT OR COMPONENT AFFECTED	IMPACT	DATE PATCHED	CVSS V3 SEVERITY
CVE-2017-0199	Microsoft Office	RCE	Apr. 11	7.8 (High)
CVE-2017-0261	Microsoft Office	RCE	May 9	7.8 (High)
CVE-2017-0262	Microsoft Office	RCE	May 9	7.8 (High)
CVE-2017-0263	Microsoft Windows	EoP	May 9	7.8 (High)
CVE-2017-8759	Microsoft .NET Framework	RCE	Sept.12	7.8 (High)
CVE-2017-11292	Adobe Flash Player	RCE	Oct.16	8.8 (High)

RETURN OF THE SHADOW BROKERS

The Shadow Brokers hacking group gained notoriety in 2016 when it disclosed a number of tools and exploits, including ETERNALBLUE—subsequently used in the widespread WannaCry and Petya ransomware attacks.

See the **Network Security** section for more information about ETERNALBLUE and the subsequent ransomware attacks.

EXPLOIT KITS IN 2017

The following chart examines exploit kit-related incidents Trustwave responded to in 2017 and the exploit kits responsible for those incidents. Patterns in the data are highly dependent on the specific incidents Trustwave investigated and may not be indicative of actual trends in exploit kit activity. Nevertheless, the data provides a useful look at which kits are currently active and used to attack computer users around the world.

Exploit Kit Distribution

Last year was quiet for exploit kits compared to the chaos of 2016, when the exploit kit market went into turmoil after the sudden disappearance of several major exploit kits, including Angler, which had been the biggest player in the space by far. If anything, however, 2017 was too quiet: The shutdown of Angler and the others left a gap in a high-end part of the market that we expected at least one major new player to fill. Instead, 2017 amounted to a holding pattern with substantially reduced overall activity and none of the remaining kits doing much to change the market. Notably, none of the most popular exploit kits adopted the zero-day exploits we tracked in 2017; although that is likely due in part to the fact that most of the exploits must be delivered through malicious documents or applications and are therefore poorly suited to exploit kit landing pages.

RIG

RIG, the biggest remaining player following the 2016 shakeout, remained the kit we heard from the most in 2017. Although the activity we observed decreased greatly from the previous year.

KaiXiN

KaiXin has been around since at least 2012, making it positively ancient in exploit kit terms. KaiXin is a low-end kit that usually targets Asian countries; although it doesn't check the browser's configured locale and will serve up landing pages to visitors anywhere.

MAGNITUDE

Magnitude, which we thought disappeared in mid-2016, reappeared in 2017 as a kit that targets Asia specifically and South Korea in particular. Unlike KaiXin, Magnitude checks locale and clearly targets according to geography. A couple of additional small exploit kits drew attention in 2017. We wrote about the **Terror** exploit kit on the Trustwave SpiderLabs blog in January 2017, drawing a taunting Twitter reply from the kit's developer. Nevertheless, the Terror kit was only involved in a small number of incidents we examined in June. **Astrum** is another old kit that reportedly sprang back to life in 2017, delivering ransomware. We didn't encounter Astrum in the incidents we investigated during the year; however, if its activity continues to increase, it may be in a position to fill at least part of the existing vacuum.

CRYPTOCURRENCY AND CRIME

Cryptocurrencies are forms of digital money used to buy and sell anonymously on the internet and in other environments in which physical currency exchange is impossible or impractical. Since the creation of bitcoin in 2009, dozens of other cryptocurrencies arose based on the same general principle. Users store virtual "coins" in digital wallets, and transfers between users are recorded in the blockchain, a distributed virtual ledger that ensures no one can spend the same money twice. Users create coins through mining, in which third parties receive compensation for performing blockchain calculations. Thus the prospect of financial gain incentivizes cryptocurrency users to keep the blockchain running smoothly.

The characteristics that have made cryptocurrencies an increasingly popular alternative medium of exchange have also made them highly attractive to cybercriminals who risk shutdown or arrest when using traditional payment services like payment card processors. Transactions are fairly anonymous, proof of ownership is relatively basic, and currencies are global and not government-controlled.

`

...the prospect of financial gain incentivizes cryptocurrency users...

**CRYPTOCURRENCY ACCEPTED,
NO QUESTIONS ASKED**

Among the early adopters of cryptocurrencies are ransomware creators who typically allow or require payment from victims in cryptocurrency. For example, the WannaCry ransomware attack that caused widespread damage in 2017 demanded payment in bitcoin, then "helpfully" explained to victims what bitcoin was and how to obtain bitcoins to pay the ransom.

Just because cryptocurrency transactions are anonymous does not mean they are not traceable. Bitcoin has a completely open blockchain, which means someone can follow money as it transfers from wallet to wallet, and having access to a wallet makes it possible to trace every transaction in which that wallet has been used. After the 2013 arrest of Ross Ulbricht, the proprietor of the notorious Silk Road online black market, Ulbricht's bitcoin wallet provided U.S. federal prosecutors with more than enough evidence to send him to prison for life for money laundering, narcotics trafficking and other offenses. As a result of this and other arrests, criminals are moving away from bitcoin to other cryptocurrencies, such as Monero, which uses an obfuscated blockchain to disguise the source and destination of transactions.

See the **Network Security** section for more information about WannaCry.

PICKING VIRTUAL POCKETS

Criminals also take advantage of the anonymous nature of cryptocurrency transactions and wallets to simply steal money directly. While the extensive fraud-prevention measures that traditional payment services, like credit card issuers, implemented usually make it possible for victims to cancel fraudulent transactions and recover most or all of their money, coins stolen from a digital wallet are likely gone for good. Like physical coins and notes, criminals can launder digital money to conceal its source and keep it hidden from prying eyes. Even knowing the address of the wallet to which the user transfers the money is usually of little use in light of anonymity and jurisdictional issues.

Bitcoin Price in U.S. Dollars (2016-2017)

Source: data.bitcoinity.org

When cryptocurrencies first became well known, a number of authors began to create malware that searched for wallets on compromised computers and stole from them. In 2014, for example, we discovered an instance of the Pony botnet that targeted wallets for bitcoin, Litecoin and other currencies that collected coins worth approximately USD $22,000 at the time. While this kind of individual-level theft still takes place, it can be much more profitable and less labor-intensive to target online exchanges, the cryptocurrency equivalent of banks and financial markets. By design, many cryptocurrencies are scarce commodities, and the potential for appreciation offered by popular currencies—such as bitcoin, which increased in value by almost 38,000 percent over the past two years—has brought cryptocurrency speculators to online trading platforms in droves. To trade at an exchange, a trader must establish a wallet at the site into which they initially transfer funds and which holds coins they are trading. The safety of money in a trader's account, therefore, depends almost entirely on the security of the exchange itself, and any security weaknesses put every trader's funds at risk of theft.

Traditional financial institutions that allow banking and trading online have made security a top priority for years and have pioneered the widespread acceptance of security best practices, such as strong password requirements and multifactor authentication. But the rapid rise in popularity of cryptocurrencies like bitcoin has led to an equally rapid rise in the profile of numerous online exchanges, many founded as little more than personal hobbies that are inadequately prepared to deal with the kinds of security challenges faced by the financial sector. (For example, MtGox.com, a major early bitcoin exchange that collapsed in 2014 after a large-scale theft, originally was founded as Magic the Gathering Online eXchange, a trading platform for the popular collectable card game.) Since 2012, at least two dozen hacking incidents at online exchanges have led to the theft of cryptocurrency funds (mostly bitcoin but other currencies as well) worth more than USD $15 billion at late 2017 prices—and that doesn't include more than $500 million in NEM coins stolen from the Coincheck cryptocurrency exchange in January 2018.

The most common obfuscation techniques were packing and crypting.

MINING WITH MALWARE

With cryptocurrencies such as bitcoin, the mining process that creates new coins intentionally produces fewer coins over time. Initially, when the currency has few users and the blockchain is small, mining coins is relatively easy. As the blockchain grows, it becomes increasingly computationally expensive to perform the calculations necessary to generate new coins. Today, for example, professional miners who run enormous farms of high-speed computers, dominate bitcoin mining, making it extraordinarily difficult for smaller operators to see any profit from the process.

As cryptocurrencies have increased in value and popularity, a number of mechanisms now enable people to parcel out mining work, at varying levels of legality and morality, to thousands of desktop computers. Malware that steals cryptocurrency is only effective on computers storing such currency, but malware that mines currency can run on any computer it infects. Criminals increasingly use such "miners" as payloads in malware attacks, slowing the computer's performance and wasting electricity for the benefit of the attacker. Other attackers pursue dedicated mining operations themselves, developing malware and exploits for weaknesses in purpose-built mining hardware and software to steal from them or sabotage their machines.

One interesting development along these lines likely doesn't involve criminality at all. Coinhive claims to provide a way for website owners to monetize visits without resorting to intrusive advertising. When someone visits the website, their browser executes the Coinhive JavaScript code embedded in the page, causing the visitor's CPU to mine the Monero cryptocurrency and deliver coins discovered to the site owner's wallet and to Coinhive. Positioned as a win-win solution for site owners and visitors, this approach ran into significant problems almost as soon as it

first appeared. One of the first prominent sites to employ Coinhive was the infamous file-sharing website The Pirate Bay, which briefly tested the Coinhive code in September. Though one can customize the Coinhive script to limit the impact on the computer's CPU, an apparent typo in the code that The Pirate Bay used caused the miner to use all available processor cores, causing CPU utilization to rise to 100 percent, slowing the computer to the point of inoperability in some cases—which many angry users of the site quickly noticed.

Cybercriminals were quick to notice the potential of Coinhive, and JavaScript-based miners in general, for ill-gotten gains. A few days after The Pirate Bay ended its Coinhive experiment, the Coinhive code briefly showed up on the website of a premium cable network in the United States, which some attributed to a hack. We've also seen instances of pop-up ads, typically hosted on adult sites, that include Coinhive code— an interesting development for a service developed to help site owners get rid of ads altogether.

While the approach Coinhive uses seems to be completely legal and even ethical if employed in such a way as to require informed consent from the website visitor, Coinhive's implementation leaves much to be desired. The service's terms of service do not require visitors' consent to using their computers for mining or even that Coinhive notifies visitors. The inevitable result for end users is computers that suddenly and randomly slow to a crawl with no obvious reason, leading to more calls to IT, more hassle and lost productivity. While the people behind Coinhive may have launched their service with good intentions, it turned out to be a losing proposition for everyone else.

SECURITY IN THE AGE OF CRYPTOCURRENCY

The best advice for protecting physical money applies to cryptocurrency as well: Keep it someplace safe and guard it well. Anything that's connected to the internet can become a target for compromise, which is why many people store the majority of their digital cash offline, on external hard drives or on USB devices. Several manufacturers sell hardware wallets, custom-built devices designed for storing cryptocurrency securely with encryption and PIN number access. For large sums, using multiple wallets stored in different places can mitigate the risk of compromise or loss. Cryptocurrency traders should avoid storing more money at online exchanges than they need for trading and download the rest to a personal wallet. For their part, exchanges need to start thinking of themselves as akin to banks and do a lot more to provide secure storage options for traders.

Enjoying the benefits of transacting anonymously online means sacrificing many of the protections traditional financial institutions offer. Ultimately it's up to every individual to take the steps necessary to keep their cryptocurrency safe. As is usually the case, there's a balance between cryptocurrency security and usability, and each person must conduct their own risk assessment and consider what security measures are reasonable.

DETECTION LOGIC

We released detection logic for Trustwave Secure Web Gateway to block miners, such as Coinhive.

> Many people store the majority of their digital cash offline, on external hard drives or on USB devices to avoid compromise.

MALWARE

Trustwave researchers conduct deep analysis of and reverse engineer malware samples encountered during investigations into data-compromise incidents. This section presents some of the aggregated malware statistics collected during Trustwave 2017 investigations. Most of the information presented comes from examinations of compromise incidents affecting point-of-sale (POS) environments and the specialized equipment employed to collect payment card data from customers. As a result, most of the malware families discussed here are specifically for stealing and exfiltrating data from POS systems, although we also collected some malware samples from general-purpose computers in such environments.

TYPES OF MALWARE ENCOUNTERED IN 2017

The top 5 categories comprised more than half of the malware samples we encountered. The largest category consisted of memory scrapers and dumpers that POS malware often used to grab payment card numbers and then transmitted them to an attacker or stored them for later exfiltration. Downloaders that fetch other malware from malicious servers are the second largest category, followed by remote access Trojans (RATs) that open a backdoor for attackers to access the system, injectors that attempt to hide malware within existing processes running on the computer and keystroke loggers.

Dropper **3%**
Webshell **3%**
Reverse Shell **4%**
Memory Scraper/Dumper **16%**
Privilege Escalation **4%**
Ransomware **4%**
Anti-Analysis **5%**
Downloader **14%**
Password Utility **5%**
Installer **5%**
RAT **9%**
Remote Admin **6%**
Injector **9%**
Bot **7%**
Keystroke Logger **8%**

OVER 50% OF ALL MALWARE ENCOUNTERED CAME FROM 5 SOURCES

POINT-OF-SALE (POS) MALWARE

Point-of-sale malware targets POS systems that handle payment card data in retail establishments. POS malware families typically include memory scraping/dumping and keystroke-logging functionality to capture as much card data as possible. The Top 5 POS malware families we encountered were:

- **FastPOS:** Discovered in March 2015, this family has a modular architecture with separate keylogger and memory-scraper components, which makes it harder to detect. FastPOS stores its stolen data using a mailslot, a location in Windows memory that attackers can engage for one-way communication with the process that owns the mailslot. For FastPOS, that process is a separate service running in the background that retrieves the stolen data and transmits it to a remote server the attacker controls.

- **Alina:** One of the oldest POS-focused malware families still active, Alina has evolved since its source code was leaked in 2014. Another memory scraper with command-and-control (C&C) features that exfiltrates data using HTTP POST, Alina utilizes simple XOR encryption to deter casual monitoring. A variant we encountered in 2017 uses SSL to transmit card date to the attacker.

- **PoSeidon/FindStr:** PoSeidon is a multi-stage attacker consisting of components apparently developed semi-independently from one another. In the first stage, a loader component sets up the malware and communicates with the C&C server. In the second, a file called FindStr performs keylogging and memory scraping for card data and exfiltrates the stolen data to the attacker. (See the **Trustwave SpiderLabs** blog for more information about this malware.)

- **FrameworkPoS:** Investigators attribute this well-documented family of malware to at least one high-profile retail breach. FrameworkPoS targets POS systems using PowerShell scripts for execution and obfuscation methods for cardholder data.

- **Project Hook:** Project Hook has been one of the most prevalent POS malware families for the past four years. At one time advertised for sale for USD $1,000 on underground forums, attackers have since customized Project Hook into a number of different variants.

REMOTE ACCESS TROJANS (RATS)

RATs accounted for 9 percent of the malware samples Trustwave investigated in 2017, making it one of the most common types of malware we saw. RATs provide a mechanism for remotely accessing and controlling a computer. Remote access programs are common and have many legitimate uses, but the "RAT" terminology generally refers to malware. Often written in Java, threat actors can use many RAT families to attack computers running numerous operating systems.
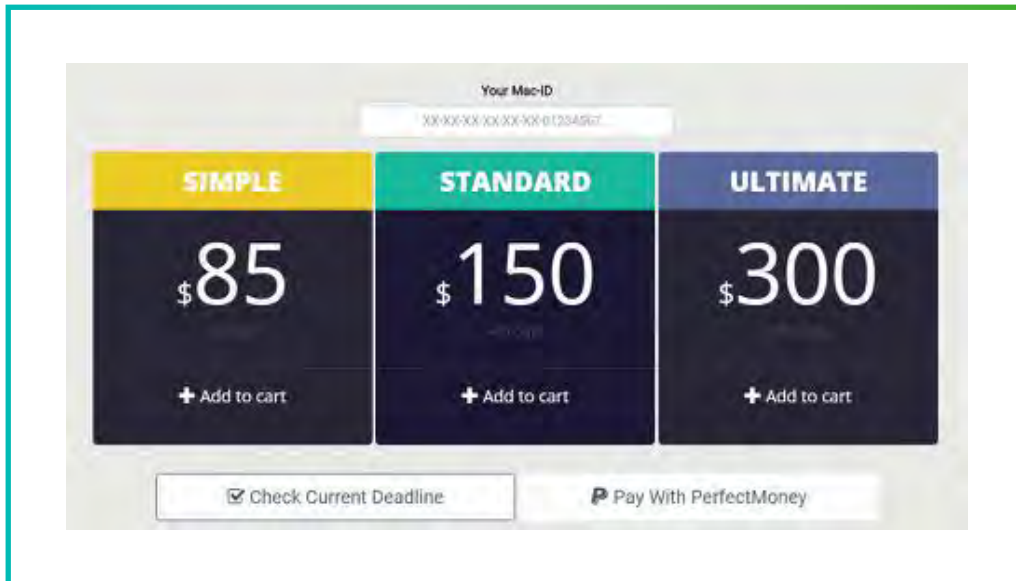
The RAT families we encountered most in 2017 were:

- **jRat** (also known as **Adwind**): jRat is among the most popular Java-based RATs criminals employed. Trustwave encountered this family in incident-response investigations and as a malware attachment in spam. It is inexpensive to buy and supports multiple operating-system platforms, including Windows, macOS and Linux.

- **Netwire:** Around for several years now, attackers recently repurposed Netwire as a tool for scraping cardholder data from POS systems. Its integrated keylogger feature makes it particularly suited for the task.

- **QRAT** (also known as **QuaRAT**): Another Java-based RAT, QRAT is capable of dumping passwords from browsers, keylogging, taking screen captures and acting as an agent to receive and execute files. We discovered QRAT for sale as software-as-a-service, with prices ranging from USD $85 for a one-month subscription to USD $300 for one year. Purchasing a subscription requires the attacker to submit his or her computer's MAC address as a customer identifier.

TROJANIZED MICROSOFT REMOTE DESKTOP PROGRAM

Remote Desktop Services is a Microsoft Windows component that attackers can use to remotely access and control a computer over a network connection. During an incident-response investigation in 2017, we encountered malware piggybacking on a legitimate copy of the Microsoft remote-desktop client program, mstsc.exe. This targeted attack worked by patching a small block of code into the entry point of the otherwise non-malicious mstsc.exe file. This code block decrypts the payload, a UPX-compressed Dynamic-link library (DLL) embedded in the host file's resources section, and injects it into the memory space of the running host file. The payload was a Cobalt Strike beacon, a toolkit mostly used by penetration testers that opens a backdoor in the victim's system.
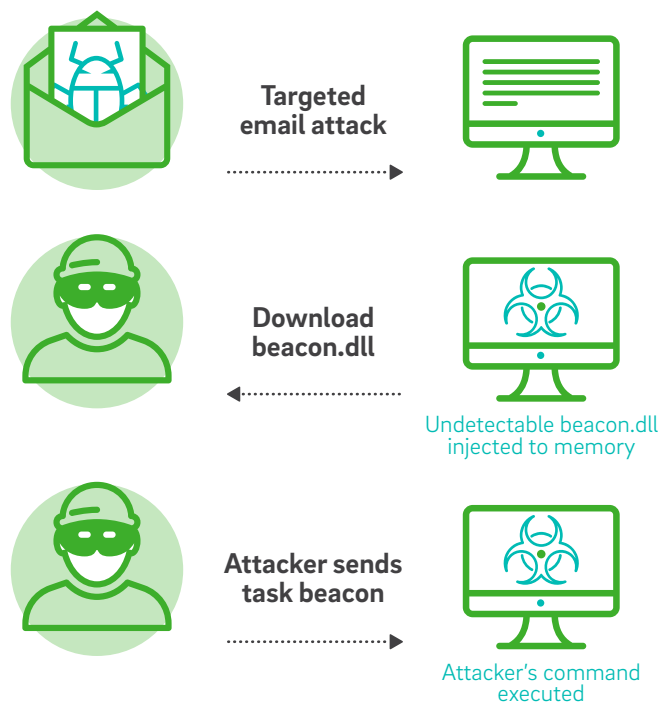
POST-EXPLOITATION AND PENETRATION-TESTING TOOLKITS

Attackers often use penetration testing tools to compromise computers. Penetration testing is a standard tactic that security professionals use to test the security of a computer system. Unfortunately, because pen testing tools, by design, discover vulnerabilities and other weaknesses, the same tools white-hat security experts use to harden systems are the same tools black-hat attackers frequently use to compromise them. The top pen testing tools we saw attackers use in 2017 include:

- **Cobalt Strike Beacon:** Targeted attackers—including the well-known Carbanak crime group and the attackers behind the post-Soviet bank heists detailed in the **Trustwave SpiderLabs Advanced Threat Reports** section—use Cobalt Strike, a commercial suite of pen testing tools, to steal from banks. They employed the beacon.dll payload included with Cobalt Strike to access compromised computers through a backdoor and move laterally through the network. It uses a fileless persistence mechanism to avoid antivirus software detection by injecting into the memory space of a targeted process without saving to disk. (See the **Persistent "Fileless" Malware** section for more information about this technique.) In a typical example, the attacker sends an email message with attached malware to an employee of the targeted bank. When the employee opens the attachment, it downloads beacon.dll and injects it to memory where it can receive the remote attacker's commands.

- **Metasploit Meterpreter:** Meterpreter is a payload included with the widely used Metasploit Framework, an open-source, pen testing project. Meterpreter is primarily a backdoor that engages in-memory, DLL-injection stagers to download additional components and extend its capabilities. The toolkit connects to its C&C server through

a reverse TCP shell tunnel to receive the attacker's commands. A popular alternative to Meterpreter is TinyMet, a customized version that is only 4K in size.

- **Empire PowerShell:** An open-source, post-exploitation agent for Windows PowerShell, Empire PowerShell uses an encrypted staging process to bypass network firewalls.

- **Mimikatz:** Mimikatz is a post-exploitation tool for gathering credential data from Windows computers. Because it is open source, threat actors employ customized versions of Mimikatz in targeted attacks as well as in ransomware worms like WannaCry and NotPetya.

Targeted email attack

Download beacon.dll

Undetectable beacon.dll injected to memory

Attacker sends task beacon

Attacker's command executed

RANSOMWARE

Ransomware, which encrypts the files on an infected system and demands the victim pay the attacker to receive the decryption key, remained a major threat in 2017 with a pair of high-profile ransomware worms causing havoc worldwide in May and June. These are the most prominent ransomware families we encountered in 2017:

- **WannaCry:** First appearing in May 2017, this was the first major malware family to self-propagate via the ETERNALBLUE exploit. In April, the Shadow Brokers hacker group alleged the U.S. National Security Agency (NSA) originated the exploit. (See the **Network Security** section for more information about ETERNALBLUE and the subsequent ransomware attacks.) Although Microsoft released a patch for the vulnerability in March, there were enough remaining unpatched systems—many running no-longer-supported operating systems such as Windows XP and Windows Server 2003—for WannaCry to infect hundreds of thousands of computers in more than 100 countries, causing crucial shutdowns at institutions such as hospitals and major manufacturers.

- **NotPetya:** NotPetya is a variant of Petya, an older ransomware family that threat actors updated to make the ETERNALBLUE exploit self-propagate. In addition, NotPetya spreads across a network using shared folders and uses legitimate Windows components and tools, such as Windows Management Instrumentation (WMI) and PsExec, to remotely execute copies of itself. NotPetya first appeared in June 2017 and quickly spread to numerous computers, most located in Ukraine. A highly destructive worm, NotPetya and related variants overwrite the computer's master boot record with a custom bootloader that displays its ransom notes, making full recovery difficult or impossible.
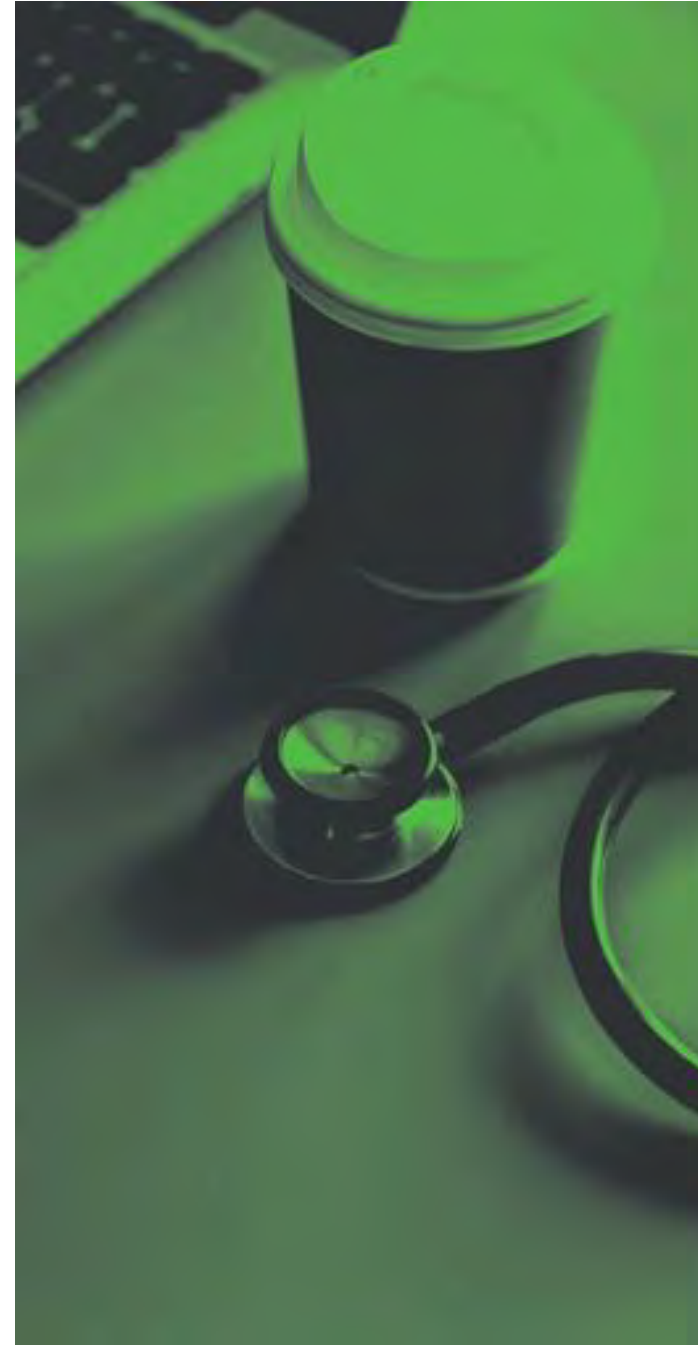
WEB SHELLS

Web shells are malicious scripts uploaded to web servers to gain persistent access and enable remote administration of an already compromised server. Systems infected with web shells are typically legitimate web servers that attackers compromised by exploiting vulnerabilities in components, such as plugins for WordPress or other CMSes. (See the **Web Attacks** section for more information about attacks on CMSes.) Attackers use web shells to obtain backdoor access to the web server and sometimes to move across the network to find assets and sensitive data to steal.

The web shells we encountered most during forensic investigations in 2017 included:

- **WSO** (short for *Web shell by oRb*): Attackers write WSO in PHP and generally obfuscate it using simple techniques, such string replacement, gzip and Base64. It avoids web crawlers from search engines, such as Google, Bing, Yandex and Rambler, so it won't appear in search results. Threat actors can use WSO—which includes a file manager, a remote shell, a password brute-force tool and a SQL browser—to view host server information.
- **phpFileManager:** This simple, PHP-written, web-based file manager for web servers is a legitimate program, but its open-source license makes it a handy tool for malicious adversaries.
- **P.A.S. Web Shell**: This is a full-featured PHP web shell with similar WSO capabilities, including a basic file browser, file-search functionality and a client for accessing databases and downloading data. A password protects this web shell that attackers use to encrypt the PHP script itself, making it one of the hardest shells to crack unless someone captures the password while the attacker is in the session.
- **Simple ASP File Manager:** This is the only web shell we encountered written in the ASP scripting language. Unlike its PHP counterparts, it only has basic file-manager features, such as copy, move, delete, rename, download, zip, unzip, view properties and change attributes.

HIDING IN PLAIN SITE

Attackers embedded many of the web shell backdoor codes we encountered in image files, such as the one shown above. They embed web shell code within a JPEG image file as EXIF metadata to evade detection when they upload the "image" file to the web server.
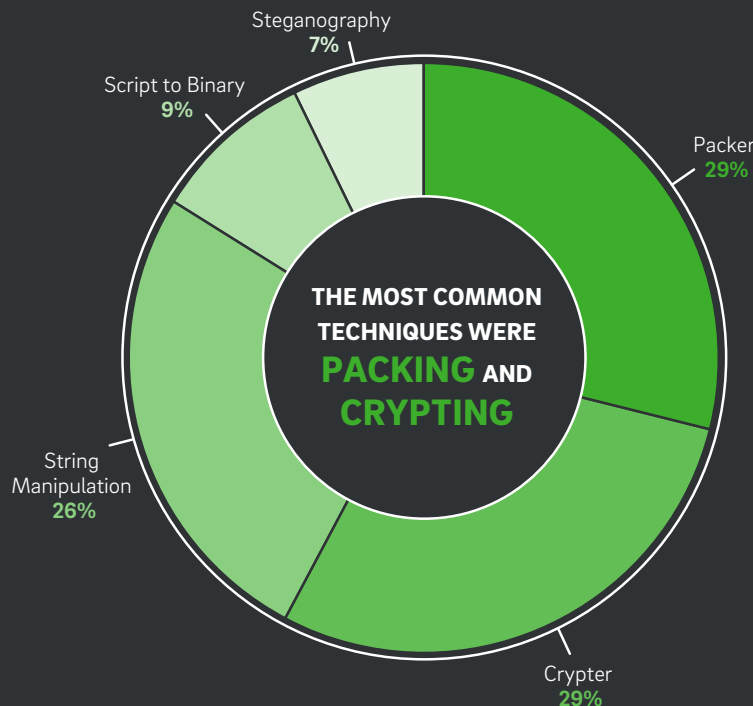
MALWARE OBFUSCATION

Malware developers often use obfuscation techniques, hiding the true nature of their code's functionality from security tools, to avoid detection.

More than 70 percent of the malware we investigated in 2017 did not use obfuscation techniques. Of the samples that did, the most common techniques were packing and crypting. A packer is a utility that bundles program files and resources into a single, compressed executable file. Packing is a common technique for legitimate software developers that malware authors also use. Attackers commonly use popular packers, such as UPX, MPRESS, ASPack and PECompact, to try to make their code unrecognizable to security software.

A crypter, by contrast, is a specialized tool malware authors use to obfuscate their code, typically by encrypting certain strings or adding superfluous behaviors to mislead security software and researchers about the purpose of the software. Another common technique is string manipulation, which uses simple functions and escape sequences to render parts of the code unrecognizable until it is deobfuscated. A few of the cases we investigated involved scripts formatted as binary files to deter text scanners or steganographic techniques used to hide information inside other media, such as an image file in which attackers manipulated the least significant bits to contain a malicious script.

Methods of Obfuscation

Steganography
7%

Script to Binary
9%

Packer
29%

THE MOST COMMON
TECHNIQUES WERE
PACKING AND
CRYPTING

String
Manipulation
26%

Crypter
29%

MORE THAN
70%
**OF MALWARE DID NOT USE
OBFUSCATION TECHNIQUES**

MALWARE PERSISTENCE

Attackers usually employ techniques to ensure their malware executes every time the computer reboots. Ninety percent of the samples we investigated in 2017 used some mechanism to persist between reboots.

Most of the samples that persisted added or changed Windows registry entries, such as the Run key that contains lists of programs that start automatically. Other samples persisted by creating a service and setting its start type to "Automatic" or by adding items to the startup folder.

Methods of Persistence

No Persistence
10%

Other
1%

Startup
Folder
14%

90%
OF SAMPLES USED
SOME MECHANISM TO
PERSIST BETWEEN
REBOOTS

Registry
56%

Service
18%

PERSISTENT "FILELESS" MALWARE

We found one interesting use in which a POS malware family called PowerShellTea stores its binary data in the registry. Lately, we've seen an increase in fileless malware such as this, which tries to avoid detection by security software that scans files on disk.

The Autorun key contains a PowerShell script that loads another script in a second key. The second script decompresses and executes a binary shellcode stored in a third key, which injects a small DLL into memory that opens a backdoor an attacker can use to download and execute arbitrary programs.

Autorun executes a PowerShell script in another registry key

A PowerShell script is a second stage loader that decodes and executes the malicious shellcode residing in another registry key

A small shellcode decompresses and executes the malware and DLL in the memory
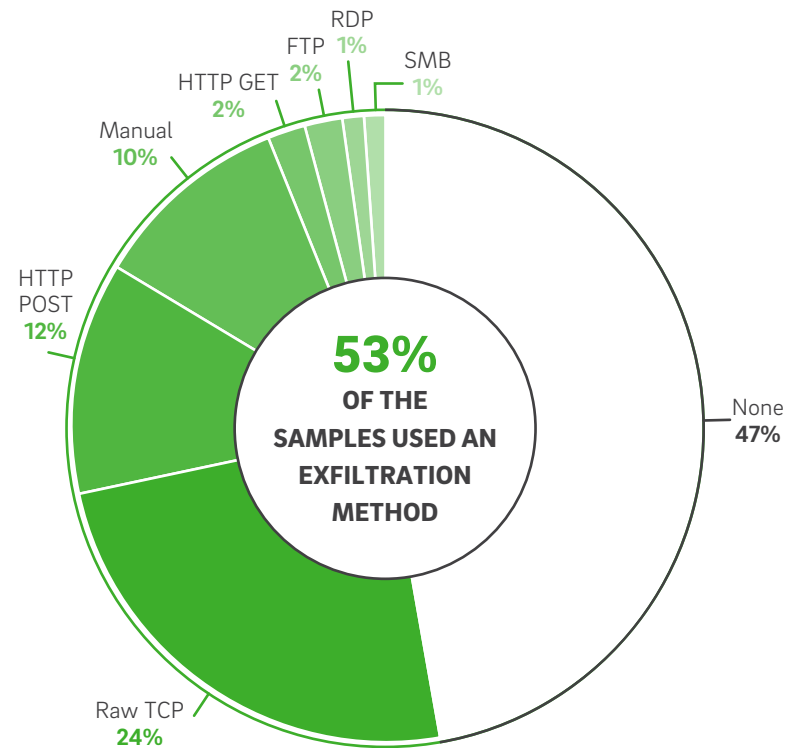
MALWARE EXFILTRATION

Stealing data doesn't do much good unless the attacker can get the stolen data out of the infected computer. Here are the exfiltration techniques used by the malware samples we investigated in 2017.

Nearly half of the samples did not use an exfiltration method, probably because exfiltration can create a trail that helps investigators identify the malware's source. In these cases, an attacker typically connects remotely to the computer to exfiltrate the data. In other cases, they have another malware component handle exfiltration.

Of the samples that did exfiltrate, the largest percentage used raw TCP socket connections to communicate with the attacker, a method RATs and bots frequently use to transfer data to C&C servers. Others, including Alina, used HTTP POST to exfiltrate data. The remainder employed standard internet protocols, such as FTP and SMTP.

Methods of Exfiltration

RDP **1%**
FTP **1%**
HTTP GET **2%**
SMB **1%**
Manual **10%**
HTTP POST **12%**

53%
OF THE SAMPLES USED AN EXFILTRATION METHOD

None **47%**

Raw TCP **24%**

03

THE STATE
OF SECURITY

The power of web applications to connect outside users to data and services easily makes them big targets for attackers. Scanning and testing databases, networks and applications gives us a unique perspective on where the vulnerabilities are, how dangerous they are (and for whom) and how to mitigate them.

In "Database Security," we look at the vulnerabilities disclosed in 2017 that affect five widely used database platforms and the kind of impact they can have on your data. "Network Security" discusses the most common security issues our network-scanning systems encountered, most notably weaknesses in the TLS and SSL protocols that underlie secure web traffic. We also examine one of the biggest network security stories of the year, the ETERNALBLUE exploit leaked by the Shadow Brokers hacker group and its subsequent use in the WannaCry and Petya ransomware attacks that wrought havoc around the world in May and June. Finally, "Application Security" looks at the most common weaknesses Trustwave discovered in web applications, focusing on critical and high-risk vulnerabilities.

DATABASE SECURITY

Most common web applications use database management systems (DBMS) on the back end. Like the applications themselves, databases can have vulnerabilities that attackers can exploit under the right conditions to steal or damage sensitive information or gain control of the underlying operating systems. Databases hold a treasure trove of assets that is only getting larger as digital information grows at record rates. Examining vulnerabilities patched in several of the more widely used database systems provides insight into the state of database security in 2017.

MySQL ■ **Oracle** ■ **DB2 LUW** ■ **SQL Server** □ **SAP ASE** ■
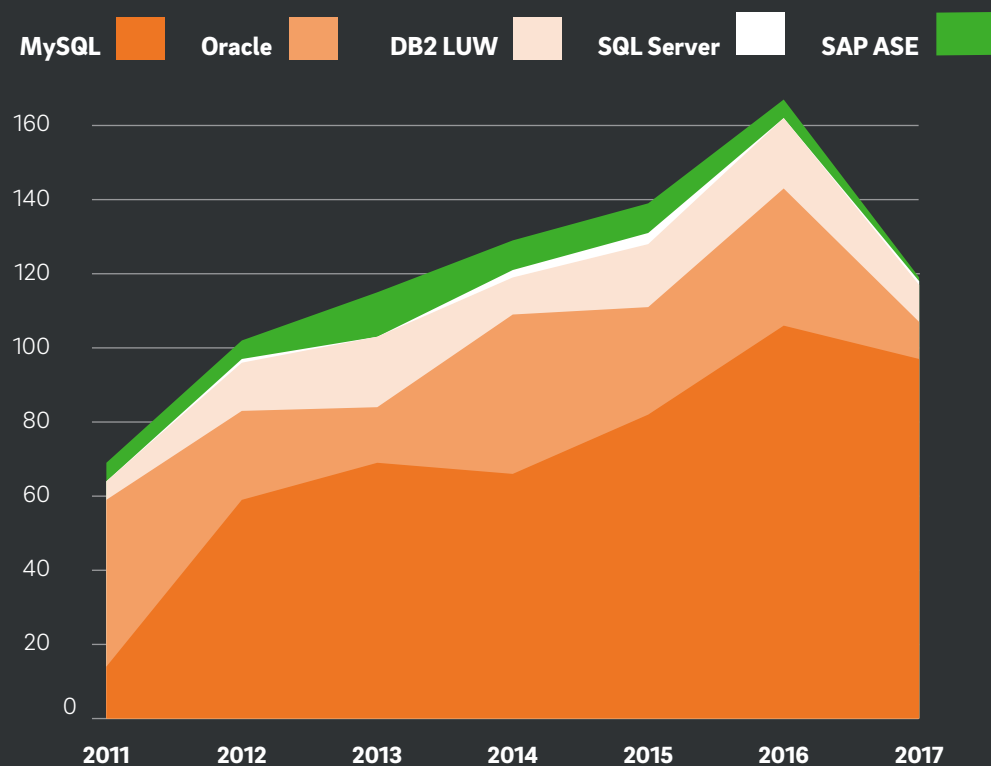
SOME OF THE MORE COMMON VULNERABILITIES FOUND IN DATABASES FALL INTO THE FOLLOWING CATEGORIES:

■ **Privilege-escalation flaws** allow an unprivileged, or low-privileged, user to gain administrator-level read and/or write access to tables or configuration settings.

■ **Buffer overflow vulnerabilities** allow an attacker to crash the database server and cause a denial-of-service condition or, in some cases, execute arbitrary code.

■ **Advanced but unused features**, such as reporting services or third-party extensions, can leave a database vulnerable even if the flaw is not in the core database management system (DBMS) service itself or in other essential components.

■ **Default credentials** still present an opportunity for attacker abuse. In our penetration testing engagements, we often find default administrator-level accounts with default passwords.

As in each of the preceding four years, Oracle's MySQL database led the way in patched vulnerabilities with 97, compared to 10 each for Oracle Database and IBM Db2 for Linux, Unix and Windows (LUW), and one each for Microsoft SQL Server and SAP's Adaptive Server Enterprise (sometimes referred to as "Sybase").

We noted in the past that having a large number of vulnerabilities disclosed and fixed does not mean a product is less secure than a comparable product with fewer known vulnerabilities, as the number is usually heavily influenced by how much time and effort researchers and other experts expend trying to find vulnerabilities in each product. Of the five widely used databases discussed in this section, MySQL is the only one with an open-source license, and it has a large and active community of developers who contribute code to the project. The more people with access to a code base, the more likely researchers will find a given vulnerability, which not only gives attackers more opportunities for exploitation but also means the product becomes safer as administrators find and fix the vulnerabilities.

By contrast, independent researchers must use techniques such as fuzz testing to locate vulnerabilities in closed-source software, which makes them harder to find. Moreover, some security vulnerabilities in proprietary software may never be identified and disclosed as such. Developers might simply take care of them as part of the normal testing process, with the fix rolling out as part of a routine maintenance release.

DATABASE PATCH TRENDS

All of the database products we examined had fewer security patches in 2017 than in 2016, with the exception of Microsoft SQL Server, which went from zero patches to one—hardly a cause for alarm. Although vulnerability disclosures and patches can rise and fall for a variety of reasons, as a general rule, a decline in patches is a positive development. It suggests development practices may be getting better and more secure, leading to vulnerabilities becoming rarer and more difficult to exploit. That said, it's important to remember that what goes down may go up again, and product vendors owe it to their customers and themselves to remain vigilant about finding and patching vulnerabilities.

Vulnerabilities by Type – 2017

	SAP ASE	SQL Server	DB2 LUW	Oracle	MySQL
Buffer overflow			2		
Code execution	1			2	
Information disclosure		1	1		10
DoS			2	1	11
Privilege Escalation			2	5	19
Unspecified/Other			3	2	57
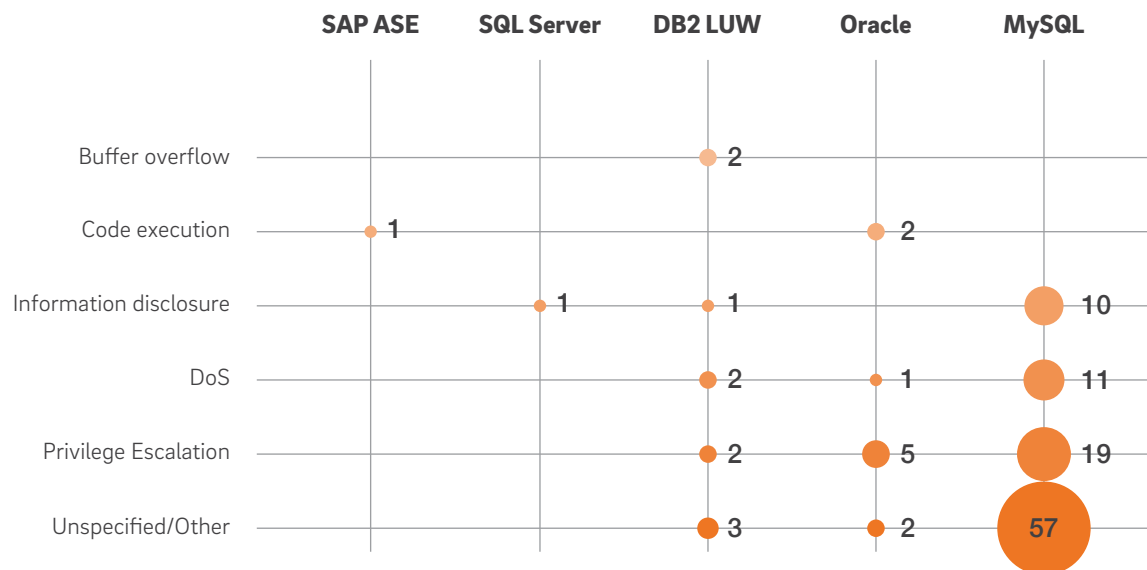
DATABASE PATCHING BY VULNERABILITY TYPE

We classified more than half of the MySQL vulnerabilities as "Unspecified/Other" because Oracle reported less information about the MySQL vulnerabilities it patched in 2017 than it reported in past years. Fortunately, MySQL's open-source code base makes it possible to investigate the nature of any vulnerability by examining the code changes introduced by the associated patch. However, this process is time-consuming and requires a deep understanding of the MySQL code base and of vulnerabilities in the C and C++ programming languages, which not everyone with an interest in assessing vulnerabilities is likely to have.

Over the past few years, the vast majority of MySQL vulnerabilities patched were denial-of-service (DoS) vulnerabilities, and we have seen no reason to believe that is not likely to be the case for most of the unspecified MySQL vulnerabilities reported in 2017. Oracle Database and IBM Db2 also introduced patches for DoS vulnerabilities in 2017. Successful exploitation of a DoS vulnerability enables the attacker to freeze or crash the database or otherwise deny access to some or all database users. DoS vulnerabilities are relatively minor compared to other types because they typically don't allow the attacker to read or alter the contents of the database.

Privilege-escalation vulnerabilities are more serious because they enable an unprivileged database user to run commands as administrators and gain access to data or actions. Even if the user encrypts the data, an attacker may be able to execute functions not available to other unprivileged users, which can potentially include destroying data. Privilege-escalation vulnerabilities comprised the largest share of patched MySQL vulnerabilities for which there was a report on the nature of the vulnerability. However, as stated earlier, it is likely that DoS vulnerabilities were the largest total share. Privilege-escalation vulnerabilities also made up half of the vulnerabilities patched in Oracle Database, and they were a significant category for IBM Db2 as well.

Information vulnerability disclosures are also quite serious as they can, in some cases, lead to the disclosure of sensitive information to unauthorized parties. The database products Trustwave examined patched 12 information-disclosure vulnerabilities in 2017, all but two of which affected MySQL.

DATABASE CHANGES AND MILESTONES

- **Microsoft SQL Server:** Microsoft released SQL Server 2017 on Sept. 25 (for Linux) and Oct. 2 (for Windows). Notably, this is the first version of SQL Server to run on Linux; the supported distributions are Red Hat Enterprise Linux, SUSE Enterprise Linux and Ubuntu.

  Mainstream support for Microsoft SQL Server 2012 Enterprise Core ended on July 11.

- **Oracle Database:** Released on March 1, 2017, Oracle Database 12.2 adds support for new Transparent Data Encryption (TDB) algorithms, full database encryption, Real Application Security (RAS) enhancements, default strong-password verifiers and many other features and improvements.

  Premier support for Oracle Database Enterprise Edition 12.1 and Standard Edition 2 (SE2) 12.1 ends in July 2018.

- **IBM Db2 LUW:** Base support for IBM Db2 LUW 9.7 and 10.1 ended on Sept. 30.

  Extended support for IBM Db2 LUW 9.5 ends April 30, 2018.
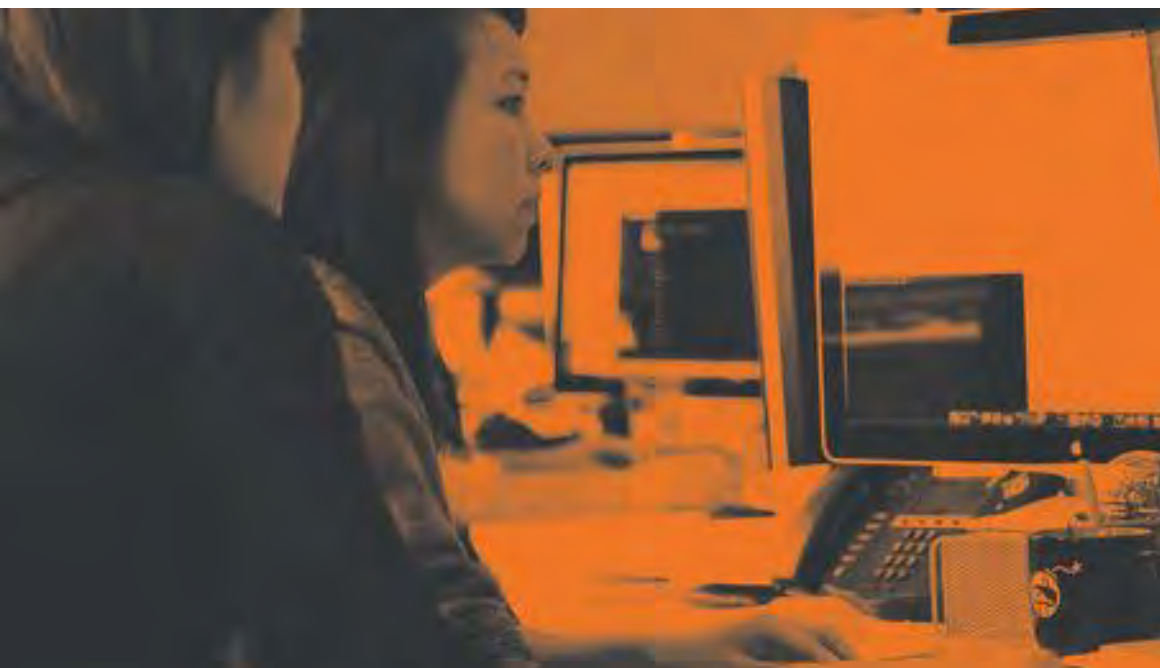
NETWORK SECURITY

Our internal and external network vulnerability scanning systems, which inspect servers for insecure configurations that could increase the risk of attack, provide insight into the most frequent network vulnerabilities.

Top 5 Security Findings by Occurrence

NAME	OCCURRENCE IN 2016	OCCURRENCE IN 2017
TLSv1.0 Supported	6.01%	5.00%
Block-cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack (known as Sweet32)	0.39%	3.67%
SSL/TLS Weak Encryption Algorithms	2.53%	1.42%
Web Page Transmits Login Credentials without Encryption	0.31%	1.07%
SSL version 3 protocol padding-oracle attack (POODLE)	1.51%	0.75%

In the table above, the figures indicate the percentage of detections by our scanner that are likely attributed to that vulnerability. For example, 5 percent of the vulnerability detections we recorded in 2017 may be due to the "TLSv1.0 Supported" finding.

June 30, 2018, is the deadline the Payment Card Industry Data Security Standard (PCI DSS) set for organizations that handle credit and debit cards to disable support for the insecure SSL 3.0 and TLS 1.0 protocols and implement more secure versions of TLS (version 1.1 or higher, though it strongly encourages 1.2) in all environments, except payment terminals. Despite this, support for TLS 1.0 and SSL 3.0 remain two of the five most common security vulnerabilities our scanner found in 2017. Companies clearly are making efforts to move away from insecure protocols—support for TLS 1.0 dropped by 20 percent in 2017, while support for SSL 3.0 dropped by half—but these transitional efforts need to accelerate considerably, lest numerous organizations find themselves in violation on July 1.

The other four vulnerability detections on the list have to do with weak or missing encryption. Support for block-cipher algorithms that use 64-bit blocks, such as DES and Triple-DES (3DES), are vulnerable to the Sweet32 attack, a proof-of-concept birthday attack security researchers demonstrated in 2016. (The apparent increase in this vulnerability in 2017 is partly because threat actors first demonstrated the Sweet32 attack in August 2016. So, our scanners only checked for it for part of that year.) Attackers use these obsolete, block-cipher algorithms in a small minority of HTTPS connections. Server administrators should discontinue support in favor of more modern encryption schemes, such as AES.

See the **Ten Years of Security** section for an overview of network security over the past decade.

Weak SSL/TLS encryption algorithms were the third most common weakness we found. This includes cipher suites that have key lengths of less than 128 bits, older algorithms such as RC4 and MD5, pre-shared keys and anonymous Diffie-Hellman algorithms.

Somewhat surprisingly, web pages that still transmit login credentials without encryption comprised the fourth most common security vulnerability we observed in 2017. It is trivially easy to eavesdrop on unencrypted traffic over unsecured wireless connections, which are ubiquitous in public spaces in much of the world. Most popular websites transitioned to HTTPS for sessions that involve personal account data, but the best encryption in the world is for naught if a visitor is able to log in over an ordinary HTTP connection before the secure session begins.

Notably, 2017 also saw a rise in malicious content being delivered over SSL/TLS. With more enterprise traffic encrypted, attackers submitted more malicious payloads over encrypted connections to try to foil detection.

VULNERABILITIES AND EXPLOITS IN THE NEWS—AGAIN

Exploits made the headlines again in 2017, with the biggest story being the public disclosure in April of several new and significant exploits, apparently stolen from the U.S. National Security Agency (NSA), which led to the highly damaging WannaCry and Petya ransomware outbreaks. A few months later, attackers employed a different exploit to attack a U.S. credit reporting agency, creating one of the largest breaches of personal financial information in history.

High-Profile Vulnerabilities and Exploits

CVE IDENTIFIER	EXPLOIT	NAME	TIMELINE
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	ETERNALBLUE ETERNALSYNERGY ETERNALROMANCE ETERNALCHAMPION	Microsoft Windows SMB Remote Code Execution and Information Disclosure Vulnerabilities (MS17-010)	**March:** Microsoft publishes MS17-010 security update **April:** Shadow Brokers disclose exploits **May:** WannaCry **June:** Petya/NotPetya
CVE-2008-4250	ECLIPSEDWING	Vulnerability in Server Service Could Allow Remote Code Execution (MS08-067)	**April 2017**
CVE-2009-2526 CVE-2009-2532 CVE-2009-3103	EDUCATEDSCHOLAR	Microsoft Windows SMB2 _ Smb2ValidateProviderCallback() Vulnerability	**April 2017**
CVE-2017-7269	EXPLODINGCAN	Microsoft IIS WebDAV Buffer Overflow Vulnerability	**April 2017**
CVE-2017-5638	EXPLOIT-DB-41570	Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability (S2-045)	**March:** S2-045 published **May–July:** U.S. credit reporting agency

SMB VULNERABILITIES AND THE RANSOMWARE SAGA

Since 2016, a hacking group calling itself the Shadow Brokers has published several sophisticated exploits, some for previously unknown vulnerabilities. In April 2017, the Shadow Brokers leaked several hundred megabytes of alleged NSA material, including multiple significant Windows exploits and a framework called FuzzBunch that attackers could use to load the exploit binaries onto computers. Several of the most serious exploits targeted vulnerabilities in the ServerMessage Block (SMB) protocol used for local network communication in various versions of Microsoft Windows. Two of these exploits (called ECLIPSEDWING and EDUCATEDSCHOLAR) only affected older versions of Windows that Microsoft in previous years addressed with patches. But others—ETERNALBLUE, ETERNALSYNERGY, ETERNALROMANCE and ETERNALCHAMPION—affected recent versions of Windows (up through Windows 10 and Windows Server 2016). Microsoft patched the vulnerabilities in March 2017, a month prior to the Shadow Brokers leak. (Some believe the NSA notified Microsoft about the vulnerabilities after learning about the data breach.) Because the fix hadn't been in the field for long at the time of the leak, it was a virtual certainty that numerous computers around the world remained unpatched, making them ripe for exploitation. A month later, that was exactly what happened.

In May, a new ransomware family spread across the globe at nearly unprecedented speed rocking the world. Dubbed WannaCry, the ransomware used the ETERNALBLUE exploit along with other leaked tools, allegedly from the NSA, to propagate itself to more than more than 200,000 computers that still lacked the MS17-010 security update in more than 150 countries. Among the largest victims of the attack was a health service in the U.K., which lost control not only of desktop workstations but also of critical medical equipment. In response to the WannaCry attack, Microsoft took the exceptional step of releasing patches, MS17-010, for Windows XP and Windows Server 2003, operating systems Microsoft stopped supporting years before.

A month later, a second ransomware attack used the ETERNALBLUE exploit to cripple thousands of computers, mostly in Ukraine. This time the culprit was an updated version of Petya, an older ransomware family that attackers modified so they could use ETERNALBLUE for self-propagation. Dubbed "NotPetya" for its differences from the original Petya, this new variant is a highly destructive worm that overwrites the computer's master boot record with a custom bootloader that displays its ransom notes, making full recovery difficult or impossible.

Percent of Computers With SMBv1 Enabled

Allow SMB null session/anonymous access

64%

Vulnerable to MS17-010 exploits

53%

These attacks were possible because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code. SMB version 1 is almost 30 years old, and many consider it inefficient and insecure; however, it remains enabled by default for the use of legacy applications. In addition, as the chart above shows, many computers with SMBv1 enabled allow anonymous login and null-session connections: and many are available over the internet, exposing them to further attacks.

We observed spikes in our scanner findings for MS17-010 when the WannaCry and Petya/NotPetya outbreaks happened, which suggested that customers were actively scanning for (and presumably patching) the MS17-010 vulnerabilities. In the weeks following, we observed a drop in MS17-010 findings, which is likely indicative of more patched systems.

Attackers used EXPLODINGCAN, another Shadow Brokers exploit linked to the NSA, to target Microsoft Windows 2003 servers running version 6.0 of the Internet Information Services (IIS) web server. This exploit sends a long request to the WebDAV PROPFIND function triggering a buffer overflow, resulting in remote code execution on the target machine. Microsoft initially did not issue a patch for the exploit, as it no longer supports Windows Server 2003; however, after the WannaCry and Petya/NotPetya attacks, the company relented and published a security update for EXPLODINGCAN just as it did with the MS17-010 update for Windows Server 2003 and Windows XP.

### STRUTS REMOTE CODE EXECUTION VULNERABILITIES

Another noteworthy exploit from 2017 is CVE-2017-5638, a critical zero-day vulnerability affecting the Jakarta Multipart parser in Apache Struts 2, a web application development framework. This vulnerability allowed remote-command-injection attacks through incorrectly parsing an attacker's invalid Content-Type HTTP header. Apache issued emergency security patch S2-045 for this vulnerability, shortly after its March disclosure. (Trustwave added coverage for S2-045 and other Apache Struts 2 remote code execution vulnerabilities to our network scanner.)

In September, a U.S.-based credit-reporting agency announced that hackers gained access to company data, potentially compromising sensitive information, including driver's license and Social Security numbers, for 143 million people in the U.S., U.K. and Canada. Later analysis of the attack revealed hackers accessed the compromised systems from May to July, using CVE-2017-5638 as the initial attack vector.

APPLICATION SECURITY

Securing a web application without help is difficult. Even if you build your application using secure platforms, technologies and development principles, a single, obscure misconfiguration or vulnerability can open a door for an attacker to compromise your system. One thing we've learned from scanning thousands of applications is that almost all web apps have weaknesses, ranging from mostly harmless to potentially devastating, and all can and should be addressed. In 2017, in fact, 100 percent of the applications we tested displayed at least one vulnerability.

Percent of Applications with Vulnerabilities
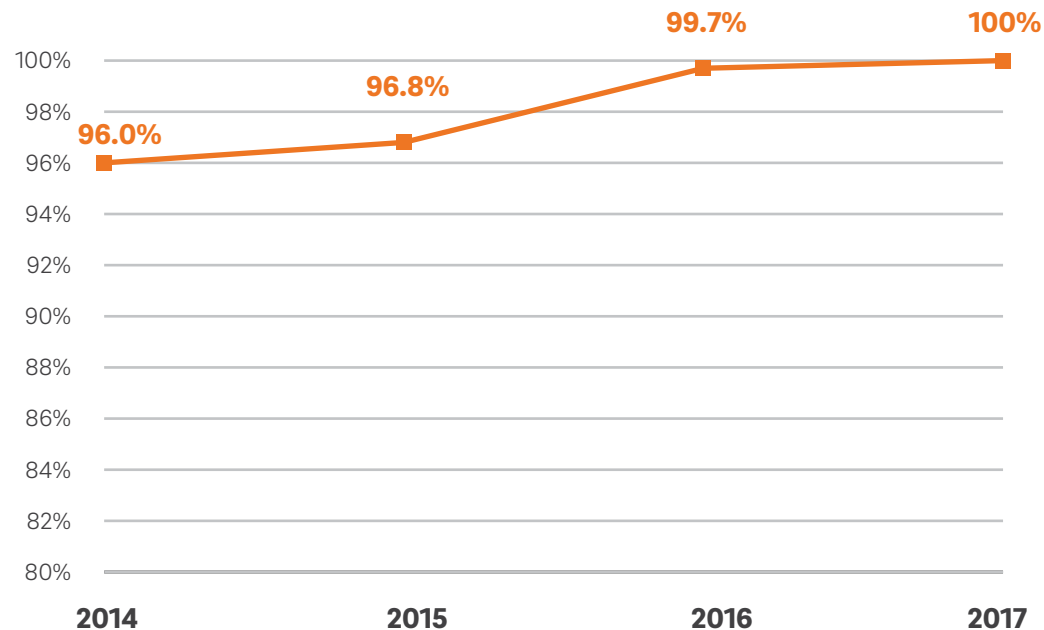
Median Vulnerabilities Per Application
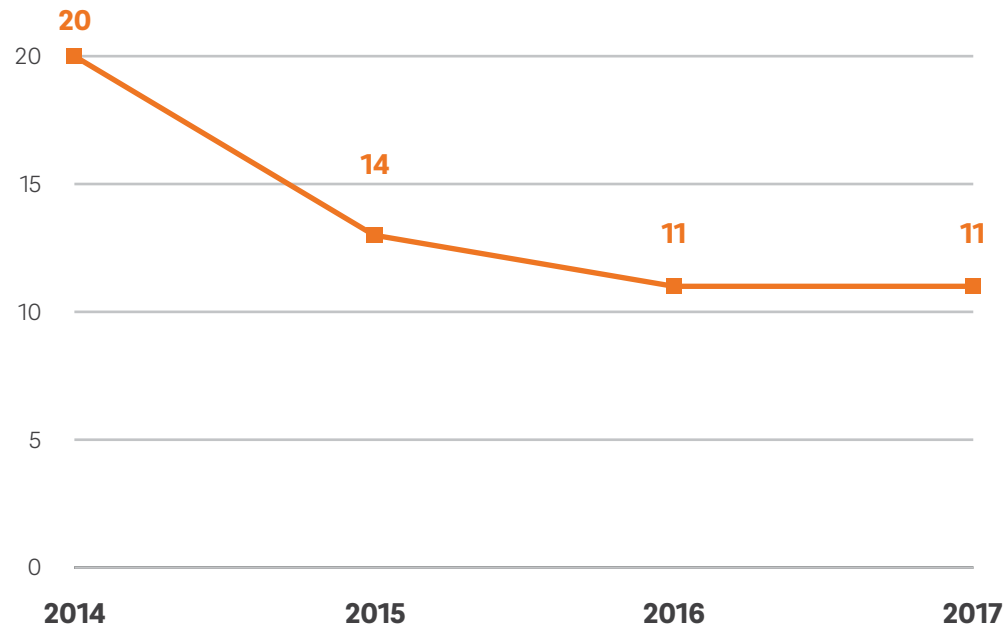
The median number of vulnerabilities detected per application in 2017 was 11, the same as in 2016 and down from 14 in 2015. The largest number of vulnerabilities we found in a single application was 154.

APPLICATION VULNERABILITY CATEGORIES

Session-management vulnerabilities remained the most common category of weaknesses in 2017, being present in nearly 86 percent of the applications we tested. Session-management vulnerabilities allow an attacker to take over or eavesdrop on a user session, placing sensitive information at risk. Most of the session management vulnerabilities we identified involved improper handling of HTTP cookies, which help preserve state across inherently stateless web connections.

Cookies are an integral part of almost all web applications, and we consistently find cookie-handling vulnerabilities to be widespread across applications we test. In fact, 80 percent of the applications we examined in 2017 displayed one or more such vulnerabilities that, in some cases, can expose session tokens, authentication information or other sensitive information that can facilitate session hijacking if compromised.
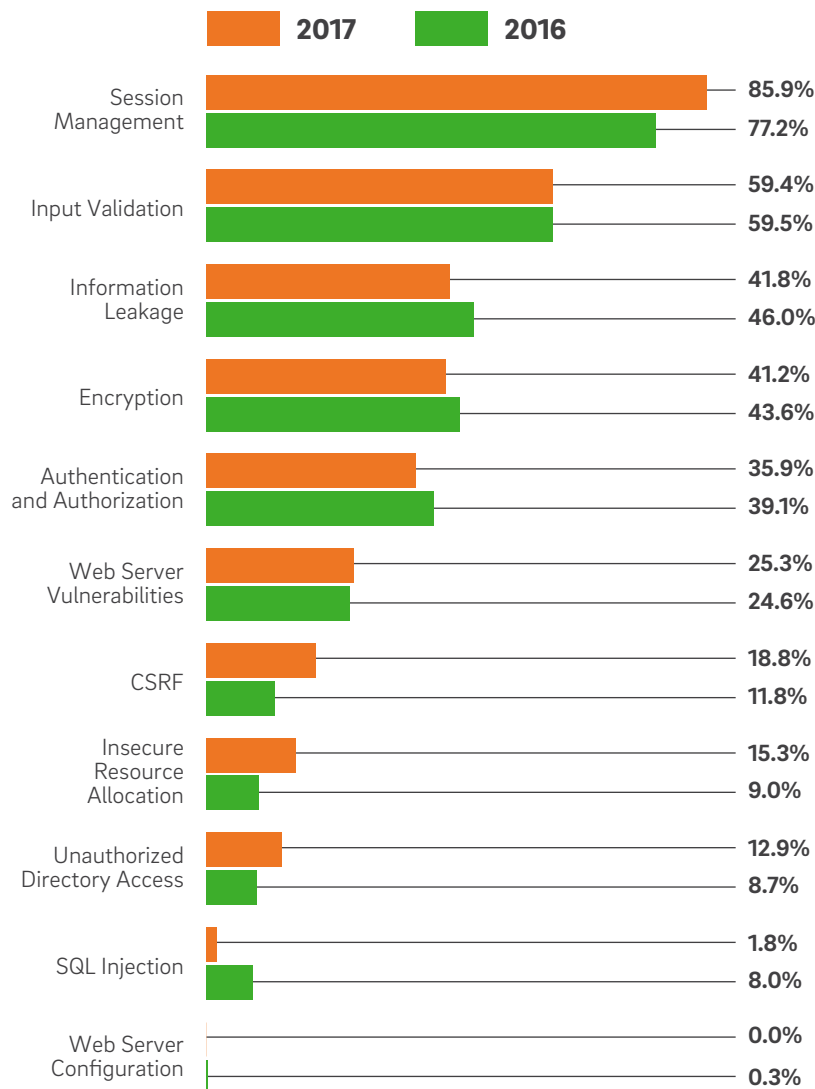
Input validation vulnerabilities (i.e. improper or inadequate validation and sanitization of user input) affected more than 59 percent of the applications we tested. More than 25 percent of these failed to encode browser output to safely filter entities like HTML tags, which can facilitate cross-site scripting (XSS) and similar attacks. An XSS attack allows an attacker to relay malicious scripts from an otherwise trusted URL to compromise information maintained within the victim's browser.

We found XSS vulnerabilities themselves in 21 percent of applications. Cross-frame scripting (XFS) vulnerabilities, present in 24 percent of applications, were another significant category. In an XFS attack, the attacker lures a victim to a malicious page that has a legitimate page—such as a login page for a social network or email service—embedded in an inline frame and uses a malicious script to eavesdrop on the victim's keystrokes. Administrators can mitigate XFS attacks by setting the X-Frame-Options HTTP header to prevent application pages from loading into frames.

Information leakage vulnerabilities were in nearly 42 percent of applications tested. These vulnerabilities can directly expose sensitive data to unauthorized visitors, making them potentially dangerous. The largest subset of information leakage weaknesses involved forms that allow the browser to cache sensitive data, which can lead to improper disclosure of the information to unauthorized people through examination of the browser's cache.

Application Vulnerability Categories

Legend: ■ 2017 ■ 2016

Category	2017	2016
Session Management	85.9%	77.2%
Input Validation	59.4%	59.5%
Information Leakage	41.8%	46.0%
Encryption	41.2%	43.6%
Authentication and Authorization	35.9%	39.1%
Web Server Vulnerabilities	25.3%	24.6%
CSRF	18.8%	11.8%
Insecure Resource Allocation	15.3%	9.0%
Unauthorized Directory Access	12.9%	8.7%
SQL Injection	1.8%	8.0%
Web Server Configuration	0.0%	0.3%

APPLICATION SECURITY

Trustwave's on-demand, security scanning and testing service, Trustwave Managed Security Testing, uncovered more than 37,000 vulnerabilities in web applications in 2017. Of these, we classified 84 percent as informational or low-risk. Medium-risk vulnerabilities comprised 9 percent of the vulnerabilities identified, and 5 percent were high-risk vulnerabilities. We classified 2 percent of identified vulnerabilities as critical, the most severe category.

Frequency of Vulnerabilities Identified by Risk Level

Critical
2%

High
5%

Medium
9%

Informational
39%

84%
OF VULNERABILITIES
CLASSIFIED AS
INFORMATIONAL
OR LOW RISK

Low
45%
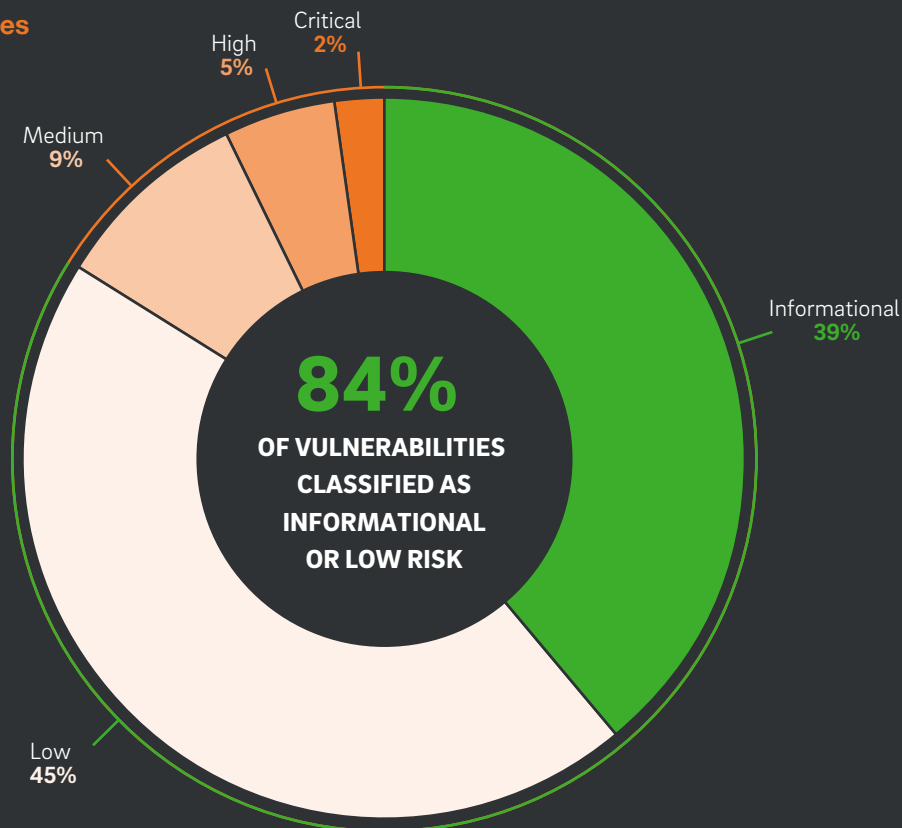
TOP 10 CRITICAL VULNERABILITIES IDENTIFIED THROUGH PEN TESTING

The most common critical weakness identified in 2017 involved Windows systems that were missing Microsoft Security Update MS17-010, which fixes the ETERNALBLUE vulnerability in the Server Message Block (SMB) protocol used for local network communication. Several high-profile malware families, including the WannaCry ransomware family that caused widespread disruptions in 2017, exploit the ETERNALBLUE vulnerability to propagate from computer to computer on their own, making it highly dangerous. Systems vulnerable to ETERNALBLUE exploitation comprised 15.6 percent of critical vulnerabilities found in 2017.

VULNERABILITY	% OF ALL VULNERABILITIES	% OF CRITICAL VULNERABILITIES
Unpatched Windows Systems (Missing MS17-010)	0.34%	15.6%
Authentication Bypass	0.30%	13.8%
Cisco Smart Install Configuration File Exposure and Remote Code Execution	0.15%	6.9%
Weak Administrator Password	0.10%	4.7%
Local Network Poisoning	0.09%	4.1%
Vertical Privilege Escalation	0.09%	4.0%
JBoss Administrative Console Access	0.08%	3.8%
NetBIOS Name Service Poisoning	0.07%	3.0%
(tie) Cross-Site Scripting (XSS), Persistent	0.05%	2.1%
(tie) SQL Injection	0.05%	2.1%
(tie) Sensitive Data Stored Unencrypted	0.05%	2.1%

Nearly 13.8 percent of critical vulnerabilities came from web pages intended for authenticated users that attackers nevertheless accessed without a valid session identifier. In some cases, these pages exposed sensitive information, such as user data and credentials, source code or public and private encryption keys.

See **Network Security** section for more information about ETERNALBLUE and WannaCry.

TOP 10 HIGH-RISK VULNERABILITIES IDENTIFIED THROUGH PEN TESTING

The largest share of high-risk vulnerabilities, at 8.9 percent, were applications vulnerable to XSS. These vulnerabilities arise when web applications do not properly validate user-supplied inputs before including them in dynamic web pages. An attacker can exploit the vulnerability by entering special characters and code into the application, which users can then execute. Threat actors can use this type of attack to steal information, such as usernames and passwords and sensitive information; remotely control or monitor the victim's browser; or impersonate a web page used to gather order information, including payment card numbers.

VULNERABILITY	% OF ALL VULNERABILITIES	% OF CRITICAL VULNERABILITIES
Cross-Site Scripting (XSS), Persistent	0.47%	8.9%
Default Credentials Identified	0.36%	6.7%
Vertical Privilege Escalation	0.34%	6.4%
Horizontal Privilege Escalation	0.33%	6.1%
SQL Injection	0.26%	4.8%
Shared Password for Local Administrator with Remote Logon	0.20%	3.8%
Sensitive Data Stored Unencrypted	0.20%	3.7%
LLMNR Name Service Poisoning	0.18%	3.4%
Secure Connection Not Enforced	0.18%	3.3%
Sensitive Data Stored Unencrypted	0.05%	2.1%

Systems that used default credentials for administrative access were the second highest share of high-risk vulnerabilities, at 6.7 percent. These can allow unauthorized users to access or modify sensitive systems or information without specialized skills or tools.

Vertical- and horizontal-privilege-escalation weaknesses comprised 6.4 and 6.1 percent of high-risk vulnerabilities, respectively. Privilege escalation occurs when systems don't properly enforce authorization controls, allowing unauthorized access to resources or functions.

With vertical-privilege escalation, a user can improperly access information or functions typically restricted to higher-privilege users. With horizontal-privilege escalation, a user can improperly access information or functions restricted to other users at the same privilege level.

Other high-risk vulnerabilities uncovered through penetration testing include systems vulnerable to SQL injection, administrator passwords shared among machines, unencrypted sensitive data and LLMNR name-service poisoning.

Systems that used default credentials for administrative access were the second highest share.

CONTRIBUTORS

- Chris Bielinski
- Vlad Bukin
- Anirban Chowdhuri
- Anat Davidi
- Christophe De La Fuente
- Mangesh Dhumne
- Dixie Fisher

- Rob Foggia
- Phil Hay
- Dan Kaplan
- Simon Kenin
- Jeff Kitson
- Ziv Mador
- Rodel Mendrez

- Prutha Parikh
- Cas Purdy
- Martin Rakhmanov
- John Randall
- Alex Rothacker
- Karl Sigler
- Todd Wilson

**2018 TRUSTWAVE
GLOBAL SECURITY REPORT**

WWW.TRUSTWAVE.COM

Trustwave®

Smart security on demand