

REPORT



Table_of_contents

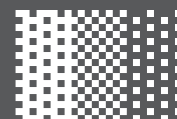
> INTRODUCTION	1
> EXECUTIVE SUMMARY	3

DATA COMPROMISE

> DATA COMPROMISE	5
> COMPROMISES BY ENVIRONMENT	9
> COMPROMISES BY INDUSTRY	13
> COMPROMISES BY REGION	15
> METHODS OF COMPROMISE	19
> METHODS OF DETECTION	21
> STOPPING DATA COMPROMISE NOW AND IN THE FUTURE	23
> SCADA SYSTEMS: AN ONGOING THREAT	25



THREAT INTELLIGENCE



> THREAT INTELLIGENCE	27
> WEB ATTACKS	29
> CMS PROS AND CONS	32
> EMAIL THREATS	37
> EXPLOITATION TRENDS	43
> EXPLOIT KITS	51
> THREE VERSIONS OF RIG	55
> MALWARE	57
> MALWARE FUNCTIONALITY	59

THE STATE OF SECURITY

> THE STATE OF SECURITY	67
> DATABASE SECURITY	69
> NETWORK SECURITY	73
> THREAT HUNTING	77
> APPLICATION SECURITY	79

Be Prepared. The Scout motto

An increasingly common mindset in the cybersecurity field often is summed up with the phrase assume breach. In other words, rather than focusing your efforts on keeping criminals out of your network, it's better to assume they will eventually breach through your defenses or may already be in your network. Therefore, it's more important to concentrate on quickly identifying intruders and limiting the damage they can do.

While that sounds pessimistic, it's also realistic. If you manage an internet-facing infrastructure of just about any size, a cybercriminal will attack and probably will breach your systems.

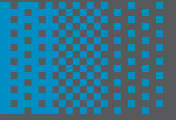
The world is changing rapidly, and cybercriminals are adapting to it more quickly in some cases than are legitimate organizations. Black marketers trade zero-day vulnerabilities for tens of thousands of dollars. The growing network of connected devices in the internet of things means coping with a new class of attack vectors, from smart thermostats to flying drones. And targeted attacks by highly competent and persistent cybercriminals are now a fact of life for many organizations.

Ten years ago, the prevailing information security paradigm was, fundamentally, still a reactive one focused on using anti-malware and IDS/IPS systems to defend the network against known threats. However, today's world can't afford that mindset. The time for reactive thinking is over; it's time to be proactive.

The 2017 Trustwave Global Security Report is part of our contribution to that paradigm shift. To help customers and the public better understand the nature of the threats we face, Trustwave compiled intelligence and statistics from Trustwave researchers working in highly varied disciplines. Our incident-response specialists provided valuable information about data compromise investigations they conducted for our customers around the world. Researchers for Trustwave SpiderLabs, our elite team of security professionals, shared a wealth of data and analysis about how cybercriminals operate, from malware development to phishing trends to the underground economy of exploit kits and traffic trading.

Lastly, Trustwave surveyed the state of network, database and application security with the aid of telemetry from Trustwave's state-of-the-art application and vulnerability scanning services. Along the way, our researchers took a comprehensive look at content management system (CMS) security, the zero-day vulnerability marketplace and a major exploit kit.

Assuming a breach doesn't have to mean pessimism. Trustwave has learned a great deal about the value of approaching cybersecurity proactively, and we're happy to share that knowledge with you in our latest Global Security Report.

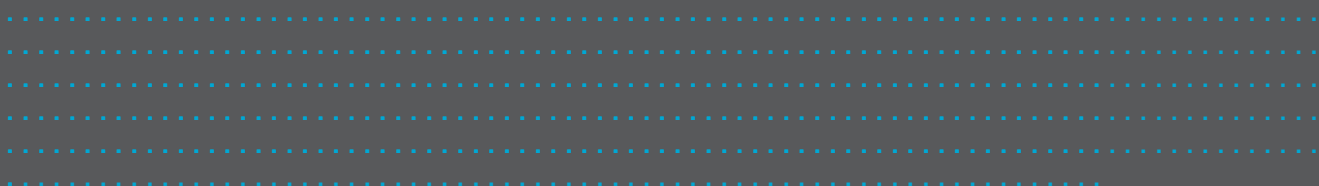


DATA SOURCES

Enhanced by our applied research and field experiences, Trustwave's 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.

For example, in 2016 Trustwave:

- Investigated compromised locations in 21 countries
- Logged billions of security and compliance events daily throughout our advanced security operations centers (ASOCs)
- Examined data from 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



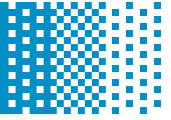
EXECUTIVE SUMMARY

DATA COMPROMISE

- Trustwave investigated breaches affecting thousands of locations throughout 21 countries in 2016
 - 49% of incidents were in North America
 - 21% were in the Asia-Pacific region
 - 20% were in Europe, the Middle East and Africa
 - 10% were in Latin America and the Caribbean
- 22% of incidents affected the retail industry, followed by food and beverage at 20%
- 63% of breaches targeted payment card data, with magnetic stripe data at 33 percent and card-not-present (CNP) data at 30%
- 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.
- 16: The median number of days between intrusion and detection for internally detected incidents
- 65: The median number of days between intrusion and detection for externally detected incidents

EXPLOITATION

- 9: The number of zero-day vulnerabilities exploited in the wild Trustwave researchers tracked in 2016
 - 5: The number of zero-day vulnerabilities that targeted Adobe Flash Player
 - 3: The number that targeted Microsoft Internet Explorer
 - 1: The number that targeted Microsoft Silverlight
- \$5: The estimated cost for cybercriminals to infect 1,000 vulnerable computers with malvertisements
- \$95,000: The initial price advertised on an underground website for an undisclosed zero-day Windows vulnerability and accompanying exploit code
- The most common exploit kits in the world — Angler, Magnitude and Nuclear — disappeared or went private in 2016, leading to a shakeup of the exploit kit market.



WEB ATTACKS

- In 2015 and 2016, Trustwave security researchers discovered significant vulnerabilities in Zen Cart and Joomla, the most commonly used open-source web applications. Trustwave worked with the development teams to patch each application's vulnerabilities and added new detection patterns to the Trustwave Web Application Firewall (WAF) products to mitigate the danger to customers.
- 13%: The percentage of web attacks Trustwave researchers observed involving cross-site scripting (XSS)

SPAM AND PHISHING

- 60%: The percentage of all inbound email that was spam, up from 54 percent in 2015
- 35%: The percentage of spam messages containing malware, up from 3 percent in 2015

MALWARE

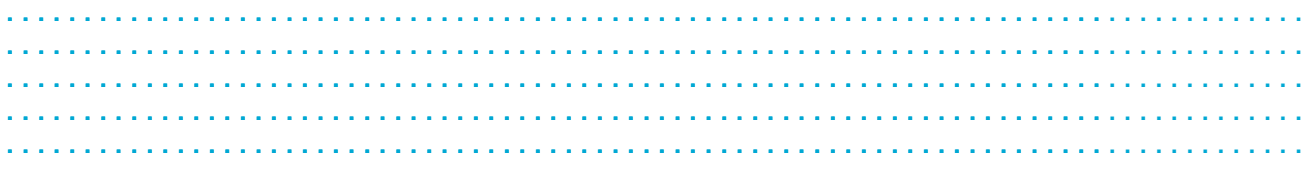
- 83%: The percentage of malware samples Trustwave examined that used obfuscation
- 36%: The percentage of malware samples that used encryption

DATABASE AND NETWORK SECURITY

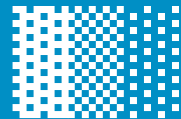
- 170: The number of vulnerabilities patched in five of the most common database products in 2016, up from 139 vulnerabilities in 2015
- 11%: The percentage of network vulnerabilities Trustwave scanners detected involving servers with insecure SSL/TLS configurations

APPLICATION SECURITY

- 99.7%: The percentage of web applications Trustwave application scanning services tested that displayed at least one vulnerability
- 11: The median number of vulnerabilities detected per application
- 77%: The percentage of vulnerabilities detected involving session management
- 10%: The percentage of vulnerabilities Trustwave detected and classified as high-risk or critical



COMPROMISE



■ At the end of 2016, the global data compromise landscape looked much the way it did a year earlier. Organized criminal gangs sought low-hanging fruit, such as deployments of widely used software platforms with known vulnerabilities. In some cases, as with content management systems (CMSes) and online shopping cart platforms, finding vulnerable systems to exploit was as easy as performing a Google search.

```

:::codxddxxdol:
co0000000000KKKX0:
dk0KXXXKx:lk000o:ldk00000l
kKXNNXXKc ck0000xodk0000000000ko:
dkKXXNNd:0KKkddccxdolcc:
odk0XNNc owXKxllllc:
ddx0XWNl dwK00kxxk000kxdol:clc:
cclx0NNc dwKdccccldddx00K0000o:
::o0Ko.00o:cllooxKX0000x:
::,cOX0:dXx,::,cok000kdc,
::,lOX0:oXd':::c:
::cdx0Kd,o0c:::cc:
xkKwWkL'c:lc:ok0XNNNXK0ko:
KXXNW0'loX::cc:dkWMMMMMMMMMMKo
NNNXKl.loX:::kNMMMMMMMMMXKX:
KX0d:odxxxxxl::dXWMMMMMMMMKoIxdol
K0000l.oXNNNNNN0o:OXWMMMMMMMMXK0l
KK000l.oKXXXX0xl,o0XNNXKKXNN0lcc
NNXx'cx000kdo:0000000kxolc:lx:
NNXc cKNNNK0kdo:cldk000kdl:
NNKc.cXWNX00kdolo0kxdol:cccclc:
MW0:KWNX00kooo::lodxkkoxxxxxxxcc:
MMd:WNWNX00kdldxl:cldxk000000dccc::ccc:
MX:kWwNX00kdolx0xcldxk000KK000000kxc:
0:xWwWwX00kxdollox0KKKKK000kxxdol:
.l0wMMwNX00kxdoodxk000kxdlc:
.dXWMMMMWNK00kxxdoodxdoc:cl:
cd0NMMMMMMWNK00kxxdolc:cdxxdol:
NWMMMMMMWNXK0kxddoc:cloddl:
KXXNNNNXK0kxdoc:
xxdddoc:

```

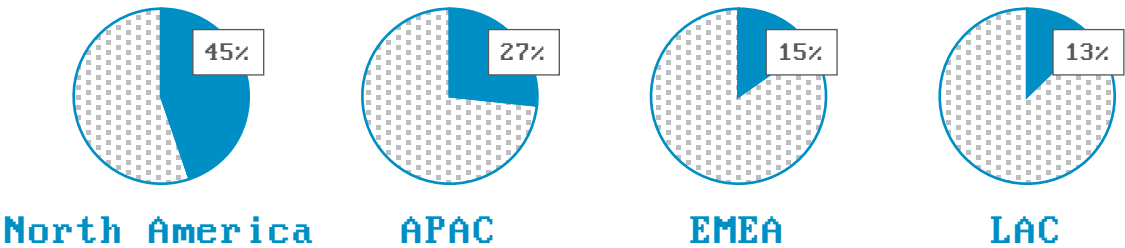
Again, the hospitality industry faced significant challenges. Trustwave investigated cases involving hotels and hotel chains hit by the notorious Carbanak crime gang, which is best known for attacking banks but has clearly broadened its scope over the past year. (See the “Malware” section for more information about Carbanak.)

Merchants’ slow adoption of EMV chip card readers in the United States again resulted in point-of-sale (POS) attacks accounting for the largest share of occurrences in North America. (EMV stands for Europay, MasterCard and Visa, the companies responsible for developing the chip standard.) Researchers expect those attacks to diminish as more merchants adopt the technology and consumers grow more familiar with it. In the meantime, North American shoppers should always choose the chip when possible.

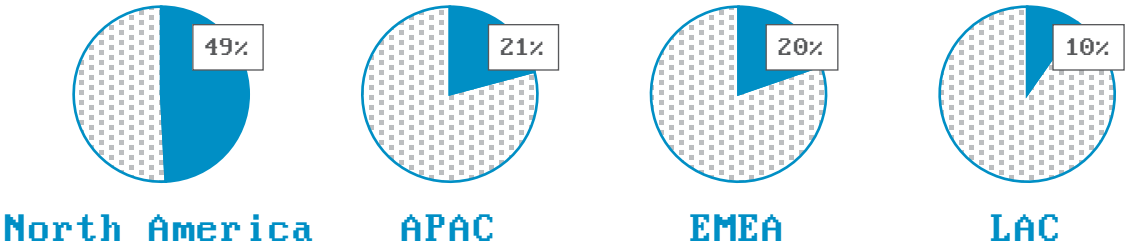
In this section, researchers discuss Trustwave investigations into security compromises and data breaches affecting enterprise environments in 2016. While these statistics depend on the details of each investigation, they provide an interesting picture of where and how attackers concentrated their efforts and useful clues as to what the future might hold.

COMPROMISES BY REGION

2015

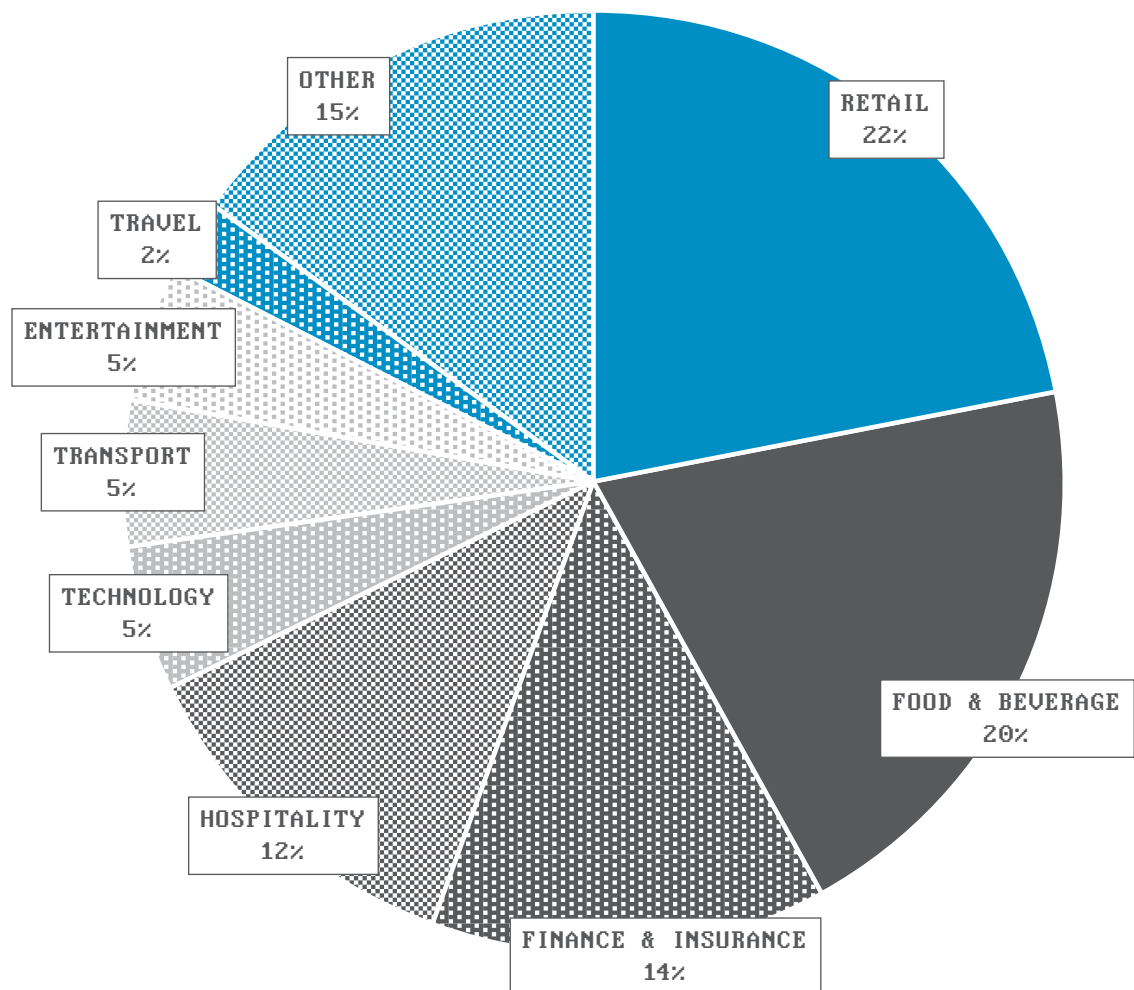


2016



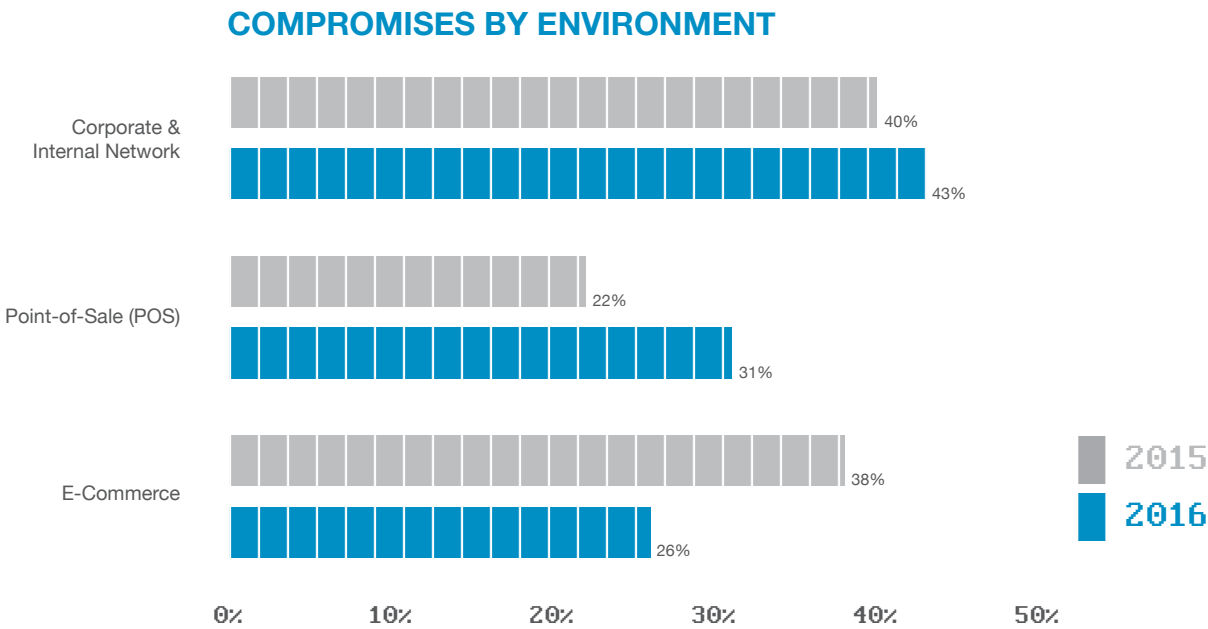
The observations in this section originate from 2016 Trustwave SpiderLabs investigations into data breaches affecting thousands of locations in 21 countries. The regional distribution was like previous years, with nearly half of incidents taking place in North America, followed by roughly 20 percent each in the Asia-Pacific region (APAC) and in Europe, the Middle East and Africa (EMEA) and 10 percent of incidents in Latin America and the Caribbean (LAC).

COMPROMISES IN 2016 BY INDUSTRY

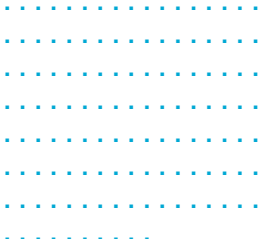


The incidents spread across economic sectors. The largest single share of incidents involved the retail industry, at 22 percent, followed by the food and beverage industry, at nearly 20 percent. Finance and insurance, 14 percent, and hospitality, 13 percent, were the next hardest hit, with other sectors accounting for fewer than 5 percent of incidents apiece.

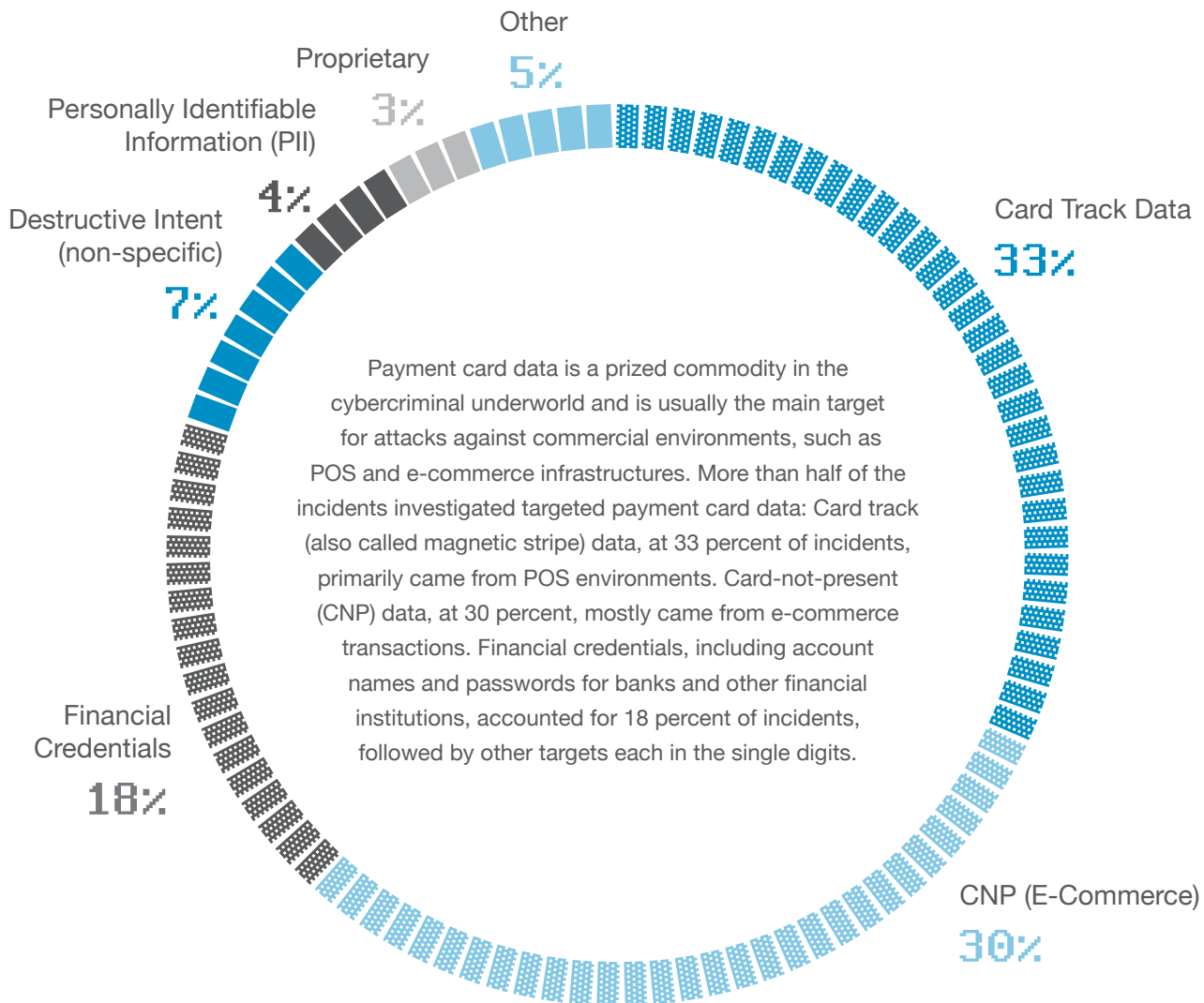
COMPROMISES BY ENVIRONMENT



Environments most breached in 2016 again consisted of corporate and internal networks, at 43 percent. Incidents affecting POS systems increased significantly to 31 percent in 2016, from 22 percent in 2015, while incidents affecting e-commerce environments fell to 26 percent from 38 percent. The decrease in e-commerce investigations could be due to e-commerce providers adopting more secure infrastructures and eliminating components with known vulnerabilities. In some cases, banks are mandating the changes.

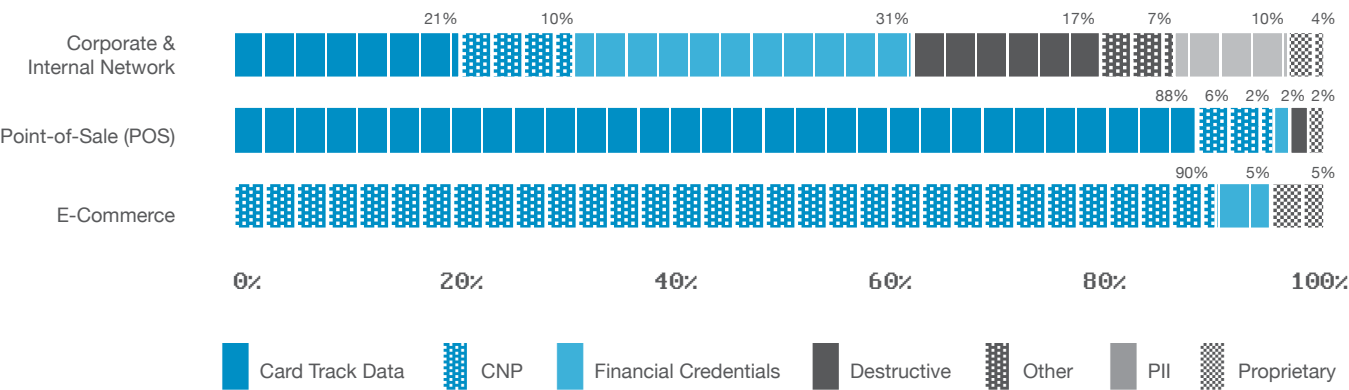


PRIMARY TYPES OF DATA TARGETED



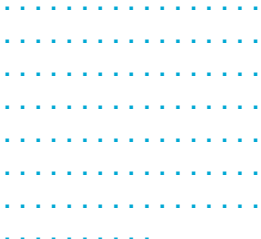
Note: Organizations often forgo a full investigation and deal internally with destructive intent cases, including ransomware; so, the incidences reported here are not necessarily representative of their true scope. In some cases, attackers exposed and targeted multiple types of data, meaning the exposure of any one data type does not reflect the totality of the breach. For this statistic, researchers reported the primary data type targeted.

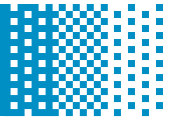
TYPES OF DATA COMPROMISES BY ENVIRONMENT



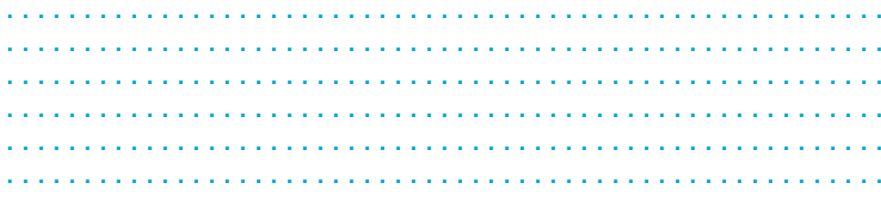
Researchers organize the IT environments in which breaches happen in the following categories:

- **Corporate/Internal Networks:** 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:** 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. Most run versions of the Windows Embedded or Linux operating systems customized for POS device, usually networked to transmit card and sale data to a centralized location and/or a financial institution.
- **E-commerce:** E-commerce environments include web-server infrastructures dedicated to websites that process payment information and/or personally identifiable information (PII).



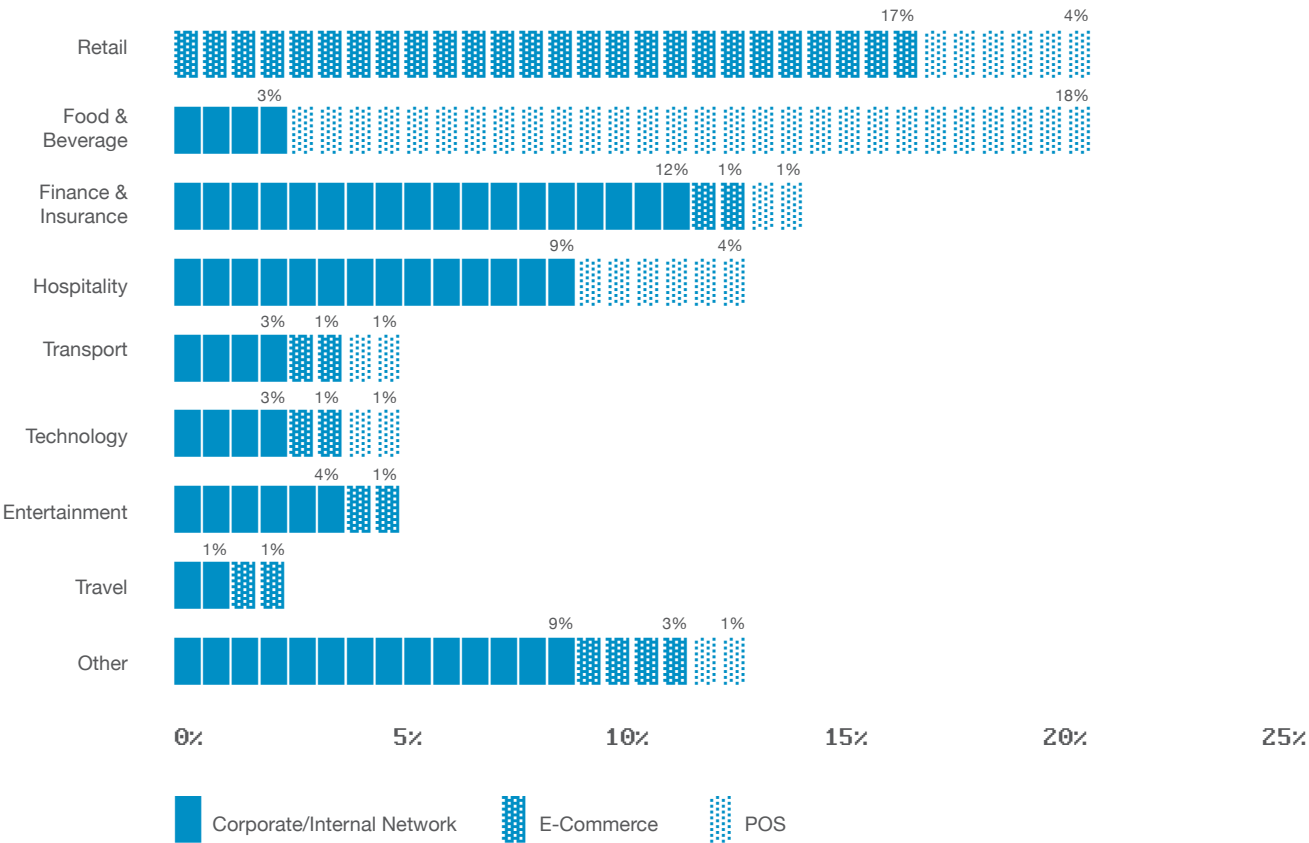


As expected, the types of data cybercriminals sought strongly correlated with the type of environment attacked. Most of the incidents affecting POS environments targeted track data, the information encoded on a payment card's magnetic stripe but not on the EMV cards used in chip-and-PIN transactions, which are significantly more secure. Similarly, most of the incidents affecting e-commerce environments targeted CNP data, used to process payments made over the internet. Incidents involving corporate and internal networks targeted a range of different data types.



COMPROMISES BY INDUSTRY

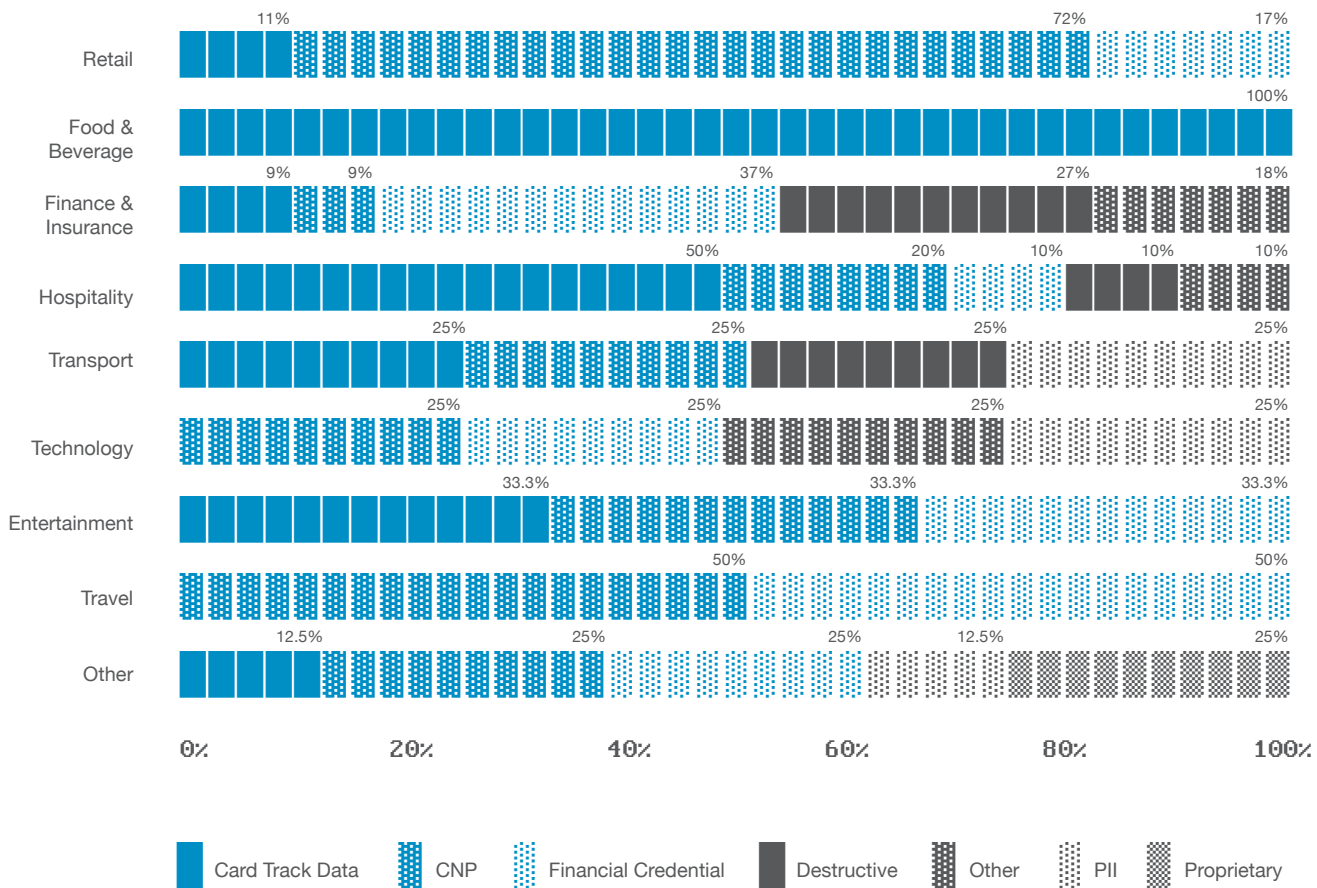
IT ENVIRONMENTS COMPROMISED BY INDUSTRY



Different industries face different kinds of attacks. Most incidents affecting the food and beverage industry targeted POS infrastructures, which are ubiquitous in food service establishments. Similarly, the largest retail industry, which includes e-commerce sites and brick-and-mortar stores, experienced the greatest share of incidents affecting e-commerce assets. Attacks on corporate and internal networks accounted for the largest share of incidents in all the other industries.

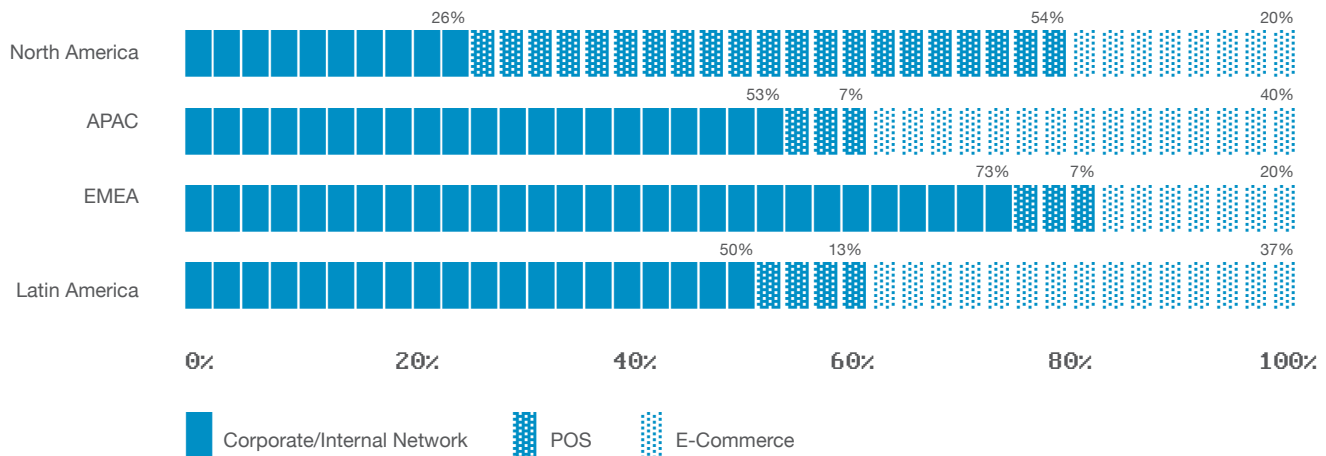
Many of the same correlations are visible in the breakdown of the types of data compromised per industry. The food and beverage industry frequently processes payment cards at POS terminals; and indeed, all the incidents Trustwave investigated in that industry in 2016 involved attackers seeking card track data. Attacks on the retail industry, with its prevalent e-commerce presence, likewise focused on seeking CNP data. The hospitality industry, which not only uses POS terminals extensively to check travelers in but also processes reservations online, was targeted heavily for both card-track and CNP data. Other industries faced a wider range of attacks.

TYPES OF DATA COMPROMISED BY INDUSTRY



COMPROMISES BY REGION

ENVIRONMENTS COMPROMISED BY REGION



Incidents involving POS environments were most common in North America, which has been slower than much of the world to adopt the EMV payment card standard (often called chip-and-PIN, although the standard also supports authentication mechanisms other than PINs). The continued prevalence of POS compromises in North America is disappointing given the October 2015 industry-imposed deadline for businesses to install EMV-compatible equipment or assume liability for card fraud themselves. EMV adoption has grown significantly since then; yet even as of November 2016, only 38 percent of U.S. storefronts were capable of processing chip card transactions, according to Visa. POS environments are likely to remain a tempting target for attackers while magnetic-stripe transactions remain pervasive in North America, and it may be another few years before POS-related incidents become as rare there as they are in the rest of the world.

US adoption
of EMV was
only 38% as of
November 2016

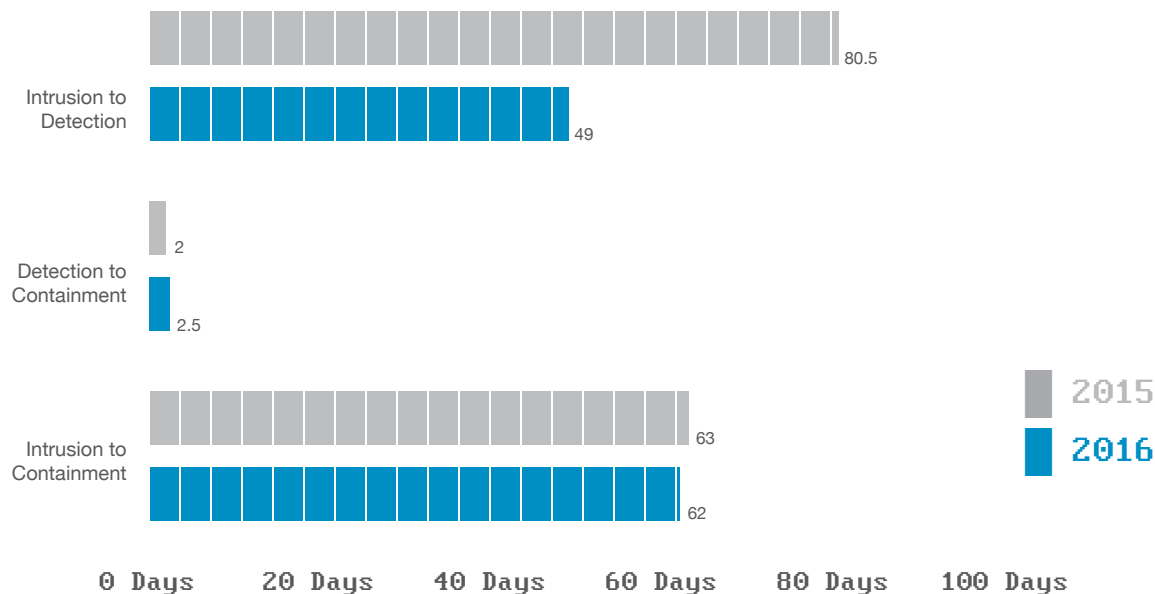
COMPROMISES BY DURATION

To understand how long it takes businesses to detect a breach and how long affected data records remained exposed, Trustwave investigators record the dates of three milestones in a compromise's duration: initial intrusion, detection and containment (wherever possible).

- **Intrusion:** The date of initial intrusion is the day Trustwave investigators determined the attacker gained unauthorized access to the victim's systems.
- **Detection:** The detection date is when the victim or another party identifies a breach occurred.
- **Containment:** The containment date is when a security professional cleans the compromise and records no longer remain exposed.

In some cases, the containment date can occur before the detection date, as when a software upgrade halts an attack before discovering it, or when investigators determine the attacker left the network before the victim or investigator detected evidence of the breach.

MEDIAN TIME BETWEEN COMPROMISE MILESTONES

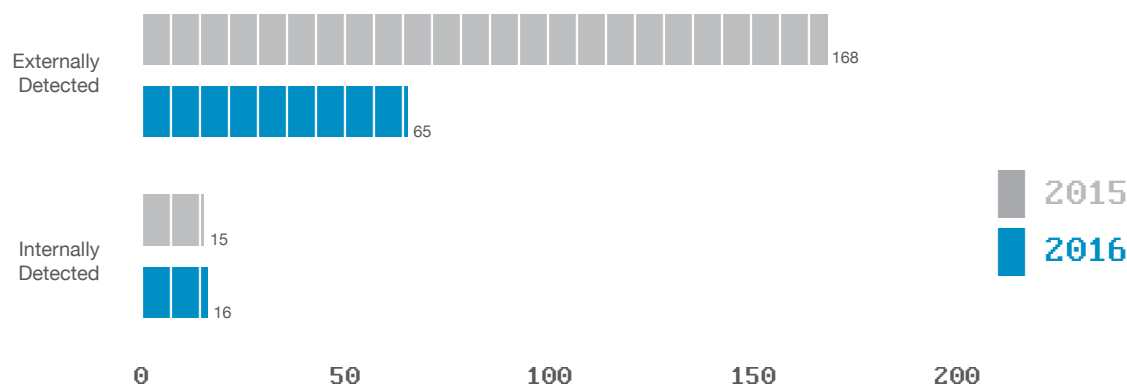


Durations varied greatly in the incidents investigated. The median number of days from the first intrusion to detection of the compromise decreased to 49 days in 2016 from 80.5 days in 2015, with values ranging from zero days to almost 2,000 days (more than five years).

Once detected, victims usually contained intrusions quickly. The median number of days from detection to containment was 2.5 in 2016 with values ranging from -360 days, meaning the intrusion ended 360 days before detection, to 289 days. In cases where containment occurred after detection, the median duration was 13 days from detection to containment.

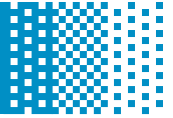
The median total duration between intrusion and containment was 62 days in 2016, almost the same as in 2015

MEDIAN TIME BETWEEN INTRUSION AND DETECTION



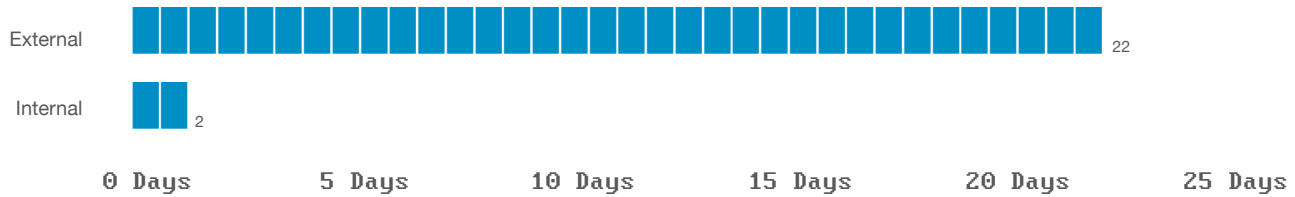
The longer a data compromise lasts, the more harm the attacker can do and the costlier the breach can be. When victims can detect compromises internally, they generally do so quickly: The median time between intrusion and detection was just 16 days for internally detected incidents, compared to 15 in 2015. In cases where victims did not learn of the breach until regulatory bodies, law enforcement or other third parties notified them, the duration was usually much longer. The median time between intrusion and detection for externally detected compromises was 65 days in 2016 — much less than the 168-day figure in 2014 but significantly more than for self-detected incidents.

Containment is
60% quicker when
a breach is
self-detected



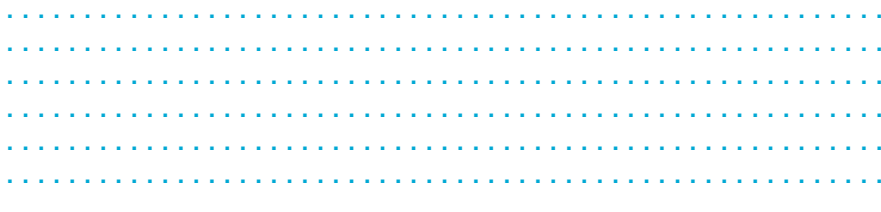
MEDIAN TIME BETWEEN DETECTION TO CONTAINMENT

(excluding incidents in which containment preceded detection)



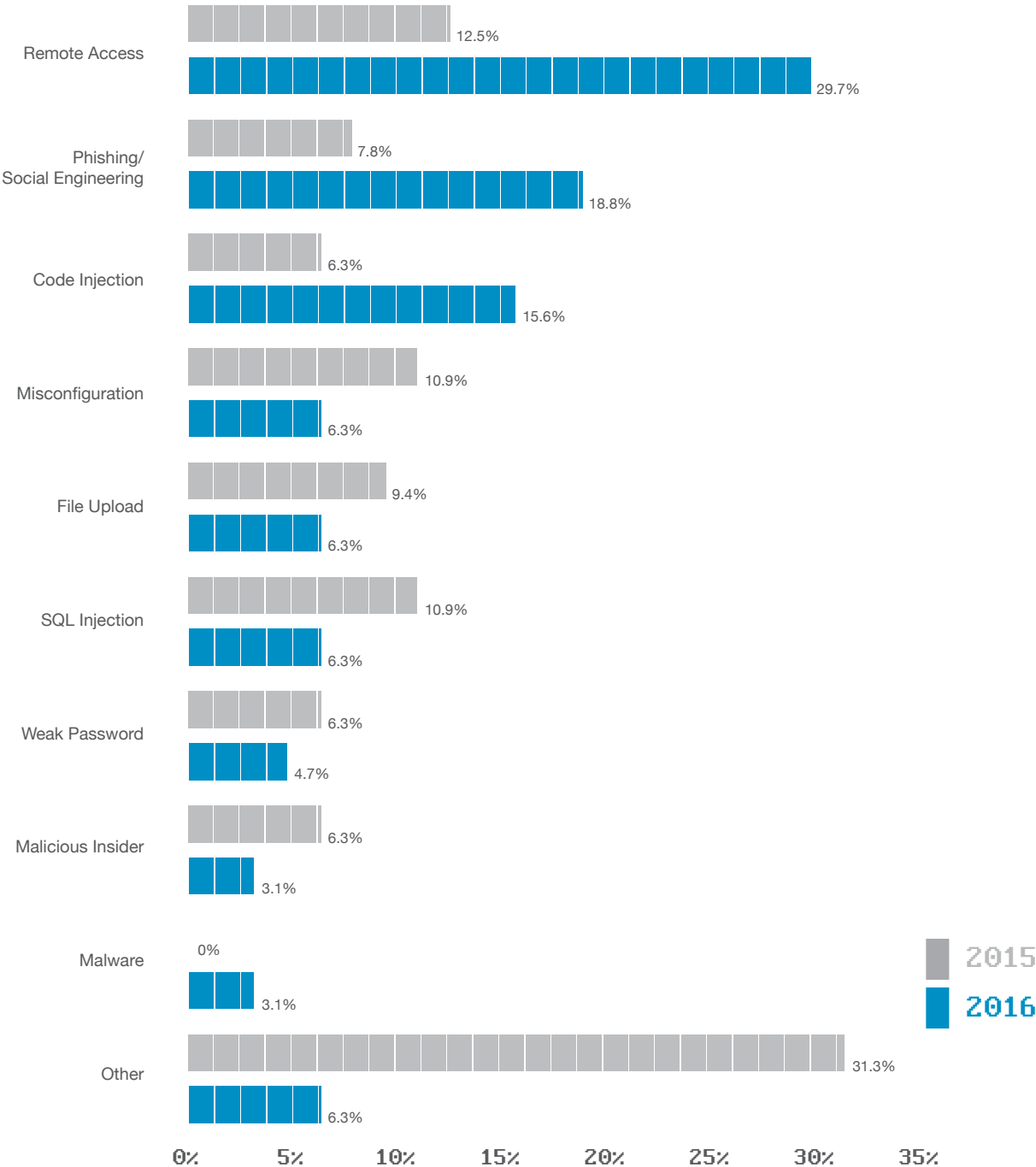
Perhaps more interesting is that victims or other parties contained internally detected compromises more quickly than externally detected ones. In cases where containment occurred after detection, the median duration between the milestones was just two days for internally detected breaches compared to 22 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 often make it possible to respond to them within days or even minutes. By contrast, a business that requires an outside party to inform it of a breach often is unable to contain it quickly, and the compromise continues, sometimes for several crucial days.

Compromise durations varied significantly by region. Latin America had the longest median times from intrusion to detection and intrusion to containment, at 151 and 154.5 days respectively. In Europe, the Middle East and Africa, the median time between detection and containment was zero days, meaning containment of more than half of intrusions in the region occurred the same day as detection or earlier.



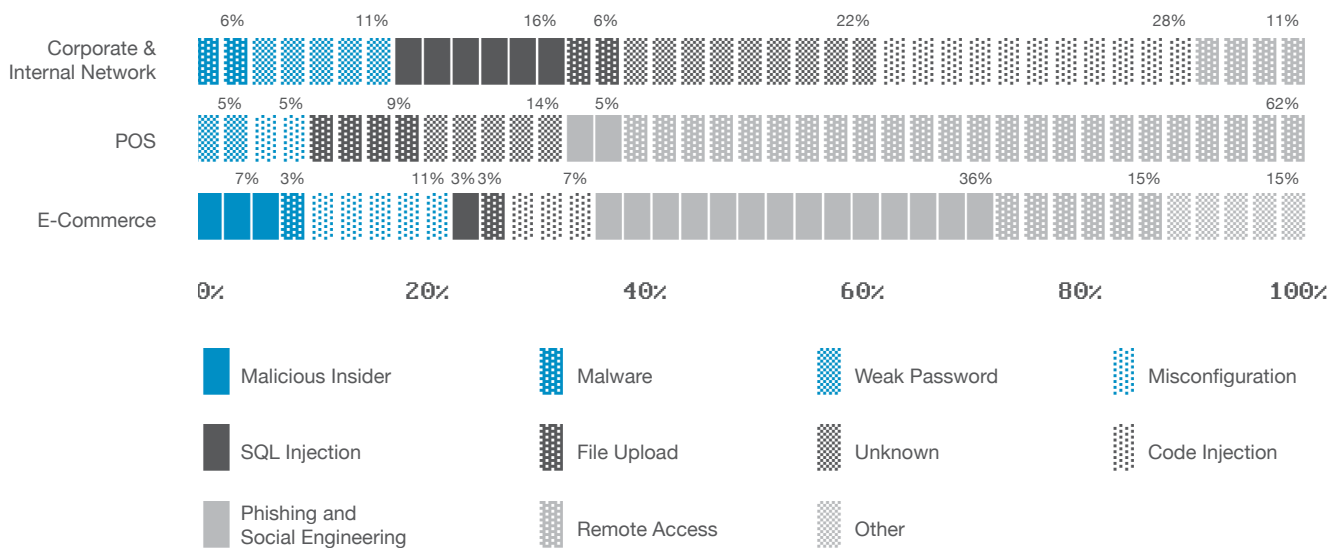
METHODS OF COMPROMISE

TOP FACTORS CONTRIBUTING TO COMPROMISE



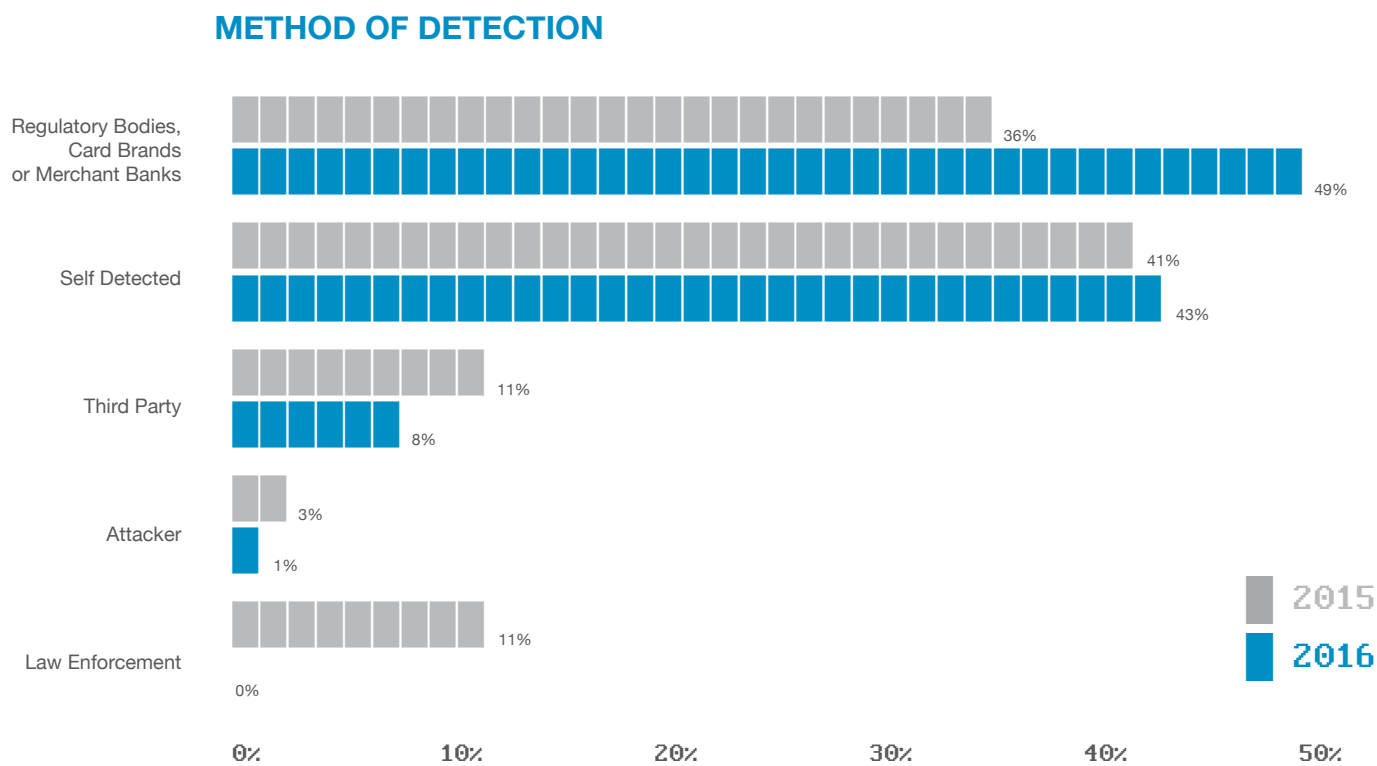
Nearly half the compromises investigated in 2016 were due to insecure remote-access software and policies (30 percent) or phishing and social engineering (19 percent). Remote access and phishing/social engineering nearly doubled since in 2015. Factors contributing to significantly fewer incidents in 2016 included server misconfigurations, SQL injection, malicious insiders and browser exploits.

CONTRIBUTING FACTORS BY COMPROMISE TYPE

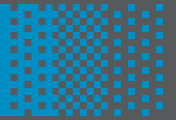


The nature of the incidents investigated in 2016 differed significantly depending on the type of environment affected. Sixty-two percent of intrusions affecting POS environments involved malicious remote access — a significant hazard with networked POS devices but much less common in other environments. By contrast, phishing and social engineering were involved in most (36 percent) corporate and internal networks but only a small portion of POS incidents and did not contribute to e-commerce incidents at all.

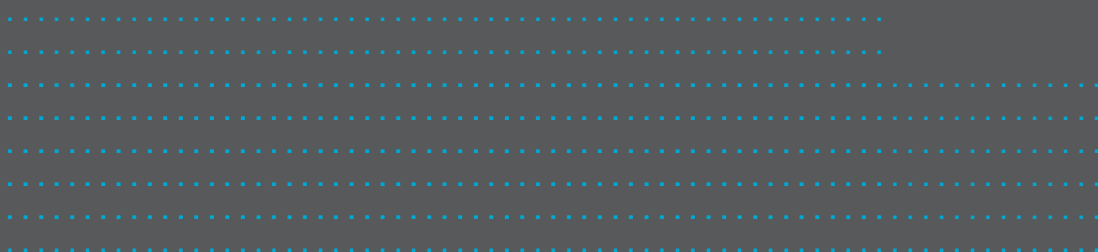
METHODS OF DETECTION



In 2016, compromises detected by regulatory bodies, card brands and merchant banks accounted for nearly half of incidents, followed by self-detected compromises. As noted previously, victims that self-detect compromises typically identify and contain them more quickly than compromises outside parties detect; so, it's good to see the share of self-detected incidents increasing.



It's good to see
the share of self
detected incidents
increasing. 📊



STOPPING DATA COMPROMISE NOW AND IN THE FUTURE

The cost and effort of securing a network against a data compromise pales in comparison to the cost and effort of cleaning up after a breach. The following list includes security measures Trustwave investigators recommend customers take to mitigate risks. Though based on the Payment Card Industry Data Security Standard (PCI DSS) for merchants handling payment card data, any organization handling sensitive data can adapt these steps for use.

■ Firewall Configuration

- Restrict inbound and outbound access to and from the network. Confine inbound access only to those services (open ports) necessary to conduct business. Restrict outbound traffic to only trusted sites or IP addresses.
- Prohibit systems connected to a payment processing environment to “surf” the web.
- Do not locate systems that are not part of the payment-processing environment or required to conduct business within the same network segment.
- Audit all firewalls for accessible ports and services.
- Ensure all firewalls are hardware-based and provide stateful packet inspection (SPI) capabilities.

■ Passwords

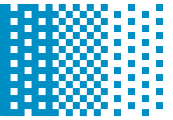
- Follow password complexity requirements for all personal computers, servers, firewalls, routers and other network devices. Require users to change passwords at least every 90 days.
- Render all passwords either stored or transmitted unreadable using strong encryption.
- Require each user to have a unique account so systems personnel can track activities on a system. Avoid using generic or default account names.
- When an employee leaves the company, change all passwords to which the employee had access.

■ System Configuration

- Ensure system-hardening guidelines are in place to address known vulnerabilities and security threats. Base system configuration on industry-standard best practices.
- For Windows environments, configure the operating system (OS) to clear the pagefile.sys upon reboot.
- For Windows environments, configure the OS to disable restore points.
- Ensure there are no unauthorized modifications to systems in the environment (i.e. use of external storage, TrueCrypt volumes, unsupported software).
- Implement a strong change-control process to track all changes made to systems in the environment.

■ Remote-Access Solution

- Use two-factor authentication for all remote access into the environment. Two-factor authentication normally is a method requiring something a user knows (password) and something the user has (token, certificate).
- Third-party remote access must be an on-demand solution. Ensure third-party remote access turns off by default and authorized users only enable it when needed.
- Enable auditing and logging for remote access into the environment.



■ Malware Removal

- If you suspect malware is, or was, on a system, rebuild the system to fully confirm the removal of the threat.
- Ensure anti-virus software is current on all systems and configure it to update virus definitions. Also, ensure there is a valid virus definition license and the software is properly accessing new definitions.

■ Logging and Monitoring

- Configure Windows event logs to capture security, application and system events on all systems.
- Retain logs for at least 90 days on the system and one year offline.
- Conduct a daily review of the logs from all devices. Procedures should be in place for escalations of critical alerts.
- Implement an intrusion detection system (IDS).
- Implement file-integrity monitoring (FIM) software.

■ Patch Management

- Patch the operating system within 30 days of vendor-released security patches/hotfixes.
- Keep applications up to date with the latest vendor-supplied security patches.

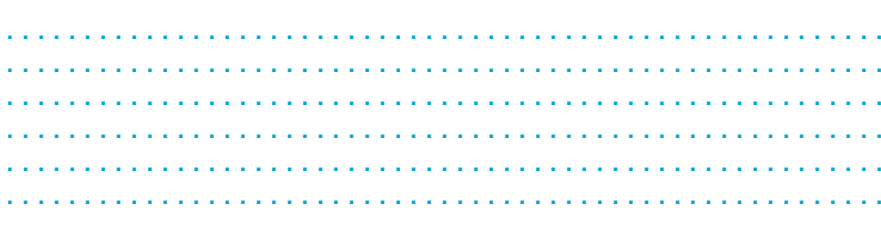
■ External and Internal Scanning

- Regularly conduct external and internal scanning to proactively find and remediate vulnerabilities.
- Conduct external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade.

■ Policy and Procedures

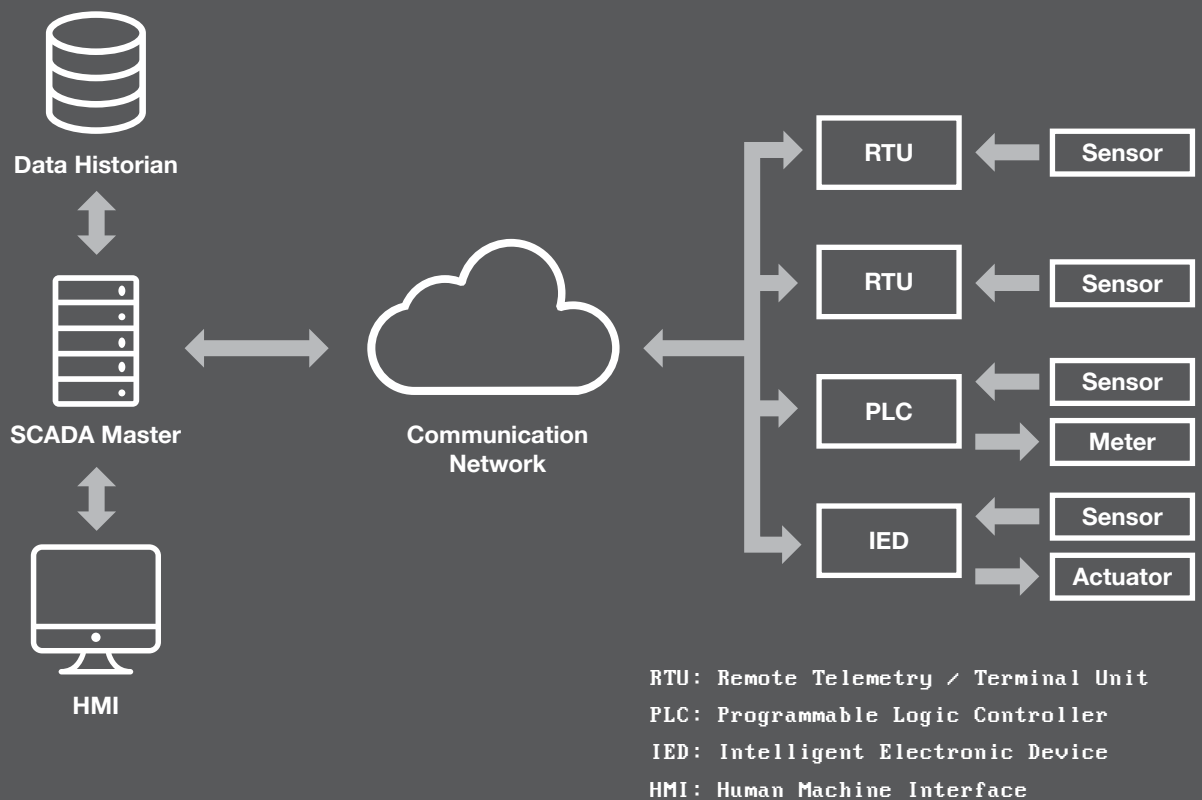
- Conduct employee security-awareness training at least annually to educate employees on information security best practices.

Only use systems that handle sensitive data for business purposes. Implement policies and procedures, along with strict monitoring, to ensure misuse (i.e. installing computer games or unlicensed software) does not occur.



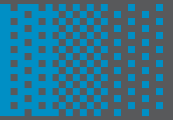
SCADA SYSTEMS: AN ONGOING THREAT

Supervisory Control and Data Acquisition (SCADA) is software, hardware and communication architecture enabling remote monitoring and control of physical (industrial control) systems.



The SCADA system uses data received from sensors to affect signals output to control elements under the supervision of the SCADA software and control programs in the programmable logic controllers (PLCs) and intelligent electronic devices (IEDs).

Federal, state and local governments use SCADA systems to help operate and control municipal infrastructure, and many businesses, especially those involved in manufacturing, use SCADA systems as well.



An unsecure SCADA system can lead to service disruption and negatively affect the environment as well as the health and safety of people. Typically, IT professionals concern themselves with protecting data. In a SCADA system, however, the emphasis is on protecting the process because there is a very real possibility that people may die if someone compromises the process.

Some of the security challenges in securing SCADA systems are as follows:

- Designed without security in mind, many SCADA systems have been around for decades.
- Nation states are very interested in SCADA infrastructure.
- SCADA software often runs on obsolete operating systems.
- The SCADA Strangelove project, an independent group of information security researchers, identified more than 150 zero-day vulnerabilities in SCADA, ICSes and PLCs.
- Many still mistakenly believe security through obscurity protects SCADA systems.
- Shodan, a search engine that locates web interfaces, reveals webcams, traffic light controllers, SCADA systems, HVAC, routers and much more.

Taking the following steps can improve SCADA security.

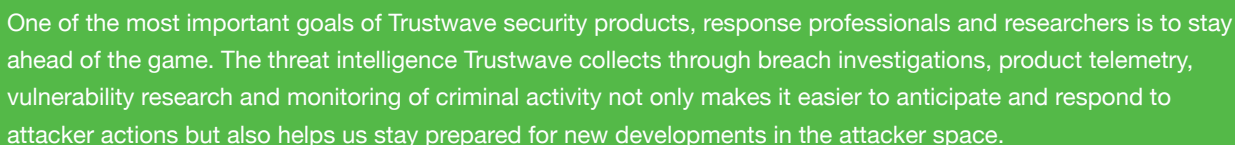
1. Assess existing systems.
2. Document policies and procedures.
3. Train staff and contractors.
4. Segment the control-system network into zones:
 - a. Supervisory / HMI zone
 - b. Production (RTU, PLC, IED) zone
 - c. Data Historian zone
5. Control physical and logical access to the system.
6. Harden the components.
7. Monitor and maintain the system.
8. Test and audit the system.



11/02

THREAT INTELLIGENCE

[illegible]



From there, the report turns to exploits, including a fascinating look at a zero-day exploit auction Trustwave monitored on an underground marketplace site. Leaving turmoil and uncertainty in their wake, the disappearance of three major kits in 2016 rocked the exploit kit ecosystem. Researchers discuss what happened and which kits survived the shakeout and take an in-depth look at RIG, the new big bully on the block.

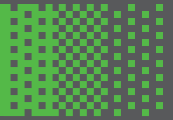
WEB ATTACKS

It has never been easier or less expensive to develop and deploy a great website. The easy availability of web applications and services makes it possible for individuals, small businesses and enterprises to assemble rich, full-featured platforms from components in a way that was unimaginable a decade ago. Unfortunately, the widespread use and availability of these tools makes them attractive to hackers who can compromise hundreds or thousands of sites by seeking out and attacking vulnerable web application deployments.

Analysis of web application attacks and compromises helps identify the top attack methods cybercriminals used in 2016. Our data set includes multiple sources:

- Alerts from Trustwave Managed Web Application Firewall (WAF)
- Web-specific alerts from Trustwave Managed IDS/IPS
- Web alerts from testing environments
- Web honeypot systems
- Cyber-intelligence from public resources
- Logs from ModSecurity WAF instances deployed as part of a project by OWASP Web Application Security Consortium Distributed Web Honeypots
- Trustwave global Advanced Security Operations Centers (ASOCs)
- Trustwave incident response and forensic investigations
- Telemetry data from Trustwave security technologies





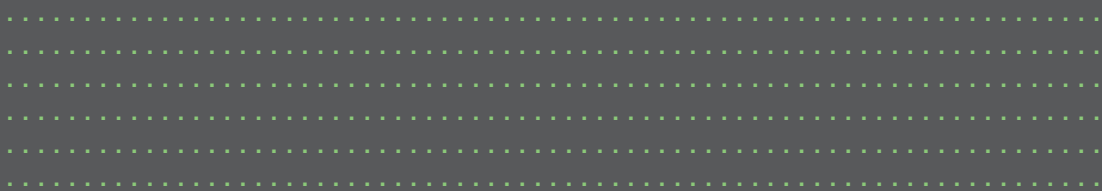
CMS VULNERABILITIES: TEMPTING TARGETS

Security professionals distinguish between opportunistic attacks, in which attackers generally try to infect as many computers as possible for various unlawful purposes, and targeted attacks, in which attackers select a specific business or organization to compromise, typically so they can steal or damage valuable data. For opportunistic cybercriminals, vulnerabilities in content management systems (CMSes) represent an express lane to their destination. A single reliably exploitable vulnerability in a popular CMS can enable an attacker to compromise hundreds or even thousands of web servers for purposes such as stealing user data or hosting exploit kit landing pages. CMSes such as WordPress, Joomla and Drupal underlie many of the most popular sites on the web and have the trust of countless internet users. When a new vulnerability crops up in a widely used CMS or web application, it's no surprise attackers tend to jump on it right away.

The following are five of the most significant vulnerabilities Trustwave saw cybercriminals exploiting against popular CMSes and associated components in 2016.

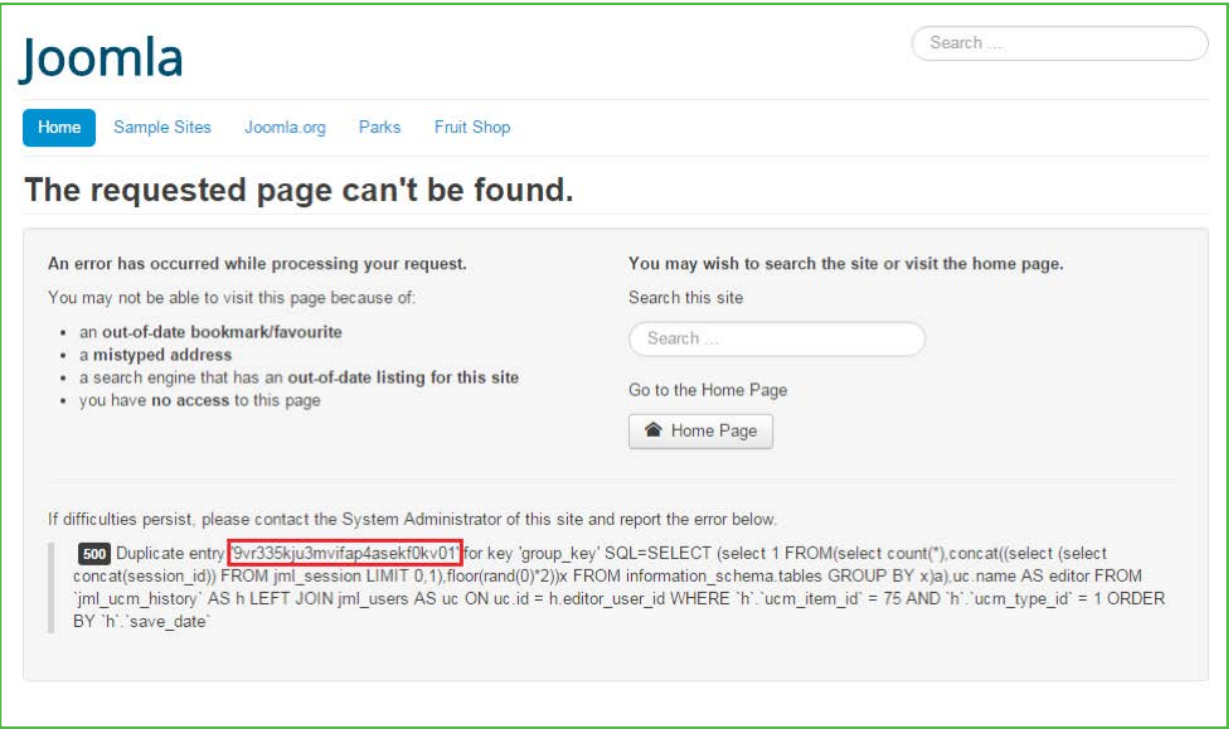
ZEN CART: MULTIPLE XSS VULNERABILITIES

Zen Cart is a popular open-source shopping cart application many web sites use to process e-commerce sales. In March 2016, Trustwave researchers discovered several reflected cross-site scripting (XSS) vulnerabilities in Zen Cart 1.5.4, the latest released version at the time. A reflected XSS vulnerability is one in which a web page takes input from the user via a GET or POST request and then displays all or part of it to the user without filtering out potentially dangerous strings, such as <script> tags. A reflected XSS attack cannot steal or alter information on the server, but an attacker can use it to create a link that will execute malicious script code for anyone who opens it. Most of the XSS vulnerabilities Trustwave discovered involved the Zen Cart administrative interface; although, one issue affected the payment information page, which does not require authentication. Trustwave researchers reported the vulnerability to the Zen Cart development team and helped them develop mitigations for the issue. Because of this collaboration, Zen Cart released version 1.5.5 on March 17, 2016, with new code providing global admin request sanitization.

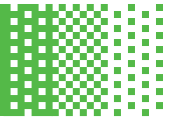


Joomla: SQL Injection Vulnerability (CVE-2015-7857)

Joomla is the second most popular CMS in the world, according to most market-share estimates. In October 2015, Trustwave researchers discovered an SQL injection vulnerability in a Joomla core module vulnerable to exploits via a GET request to return an administrative session ID while an administrator is logged in to the system during the attack. This attack is an example of error-based SQL injection, a technique in which an attacker extracts information from a database by submitting a string to the website designed to produce an SQL error and then observing the resulting error message for useful data.



If the attack successfully returns an administrative session ID, the administrator can use it in a subsequent GET request to gain access to the Joomla administrative interface, where they can perform malicious actions like deleting data and creating new super-user accounts. Because the vulnerability affects a core Joomla module, all websites using Joomla versions 3.2 through 3.4.4 are vulnerable to attack. Trustwave reported the issue to the Joomla team, which patched the vulnerability in version 3.4.5, released on October 22, 2015. Trustwave also updated WAF products, Trustwave Web Application Firewall and ModSecurity with new pattern checks that detect and mitigate attempts to exploit this vulnerability and similar attacks.



CMS PROS AND CONS

Open-source CMSes are popular with website owners and developers, but that popularity has long made them a target for attackers who can get more bang for their buck by successfully pursuing a frequently used platform. The following are some advantages and disadvantages of using a popular CMS rather than a custom-developed platform.

PROS:

- The top CMS platforms have large communities of developers contributing to them, which leads to ecosystems full of creative enhancements and add-ons that site owners can adopt for little or no cost. The large user base also makes it easy to seek help for problems encountered or for tasks such as migrating from one platform to another.
- Many hosting providers offer inexpensive hosting solutions for popular CMSes that simplify installation and upkeep.
- Anyone can review the code running each of the top CMS platforms. In addition to making customization relatively easy, this also makes it easy for “white-hat” security researchers to find and fix vulnerabilities in the code before attackers can exploit them.

CONS:

- Dedicated support for CMS platforms can be difficult to find, as is often the case with open-source software. As a result, website developers frequently find themselves with few options for solving problems beyond looking for help on the internet.
- Just as white-hat researchers spend a lot of time inspecting CMS code for flaws, so do “black-hat” researchers and attackers. A criminal who finds an exploitable vulnerability in a popular CMS platform could use it to compromise thousands of websites and victimize millions of people — creating a strong profit motive to find new vulnerabilities before anyone else does.

IMAGEMAGICK: “IMAGETRAGICK” RCE VULNERABILITY (CVE-2016-3714)

ImageMagick is an open-source suite of image processing and manipulation tools that CMSes and web components frequently use to handle graphics. ImageMagick is one of the most widely deployed server-side code libraries in the world due to its integration with languages such as PHP, Python, NodeJS and Ruby, and the web sites using it likely number in the tens or even hundreds of millions. In May 2016, researchers discovered a critical remote code execution (RCE) vulnerability in the way ImageMagick processes user-submitted images. Insufficient filtering of filenames passed to an ImageMagick command can allow an attacker to inject shell commands at the end of a filename, which the server then executes. The attacker can exploit this vulnerability by adding a malformed filename to a file that supports linking to external resources, such as scalable vector graphics (SVG), and uploading it to the target server. If the server attempts to process the uploaded file in certain ways, it will execute the attacker’s shell code. Shortly after disclosing the vulnerability, ImageMagick developers released an updated version resolving the issue. Website administrators can also mitigate the vulnerability by disabling the vulnerable ImageMagick coders using a policy file.

JOOMLA: ZERO-DAY RCE VULNERABILITY (CVE-2015-8562)

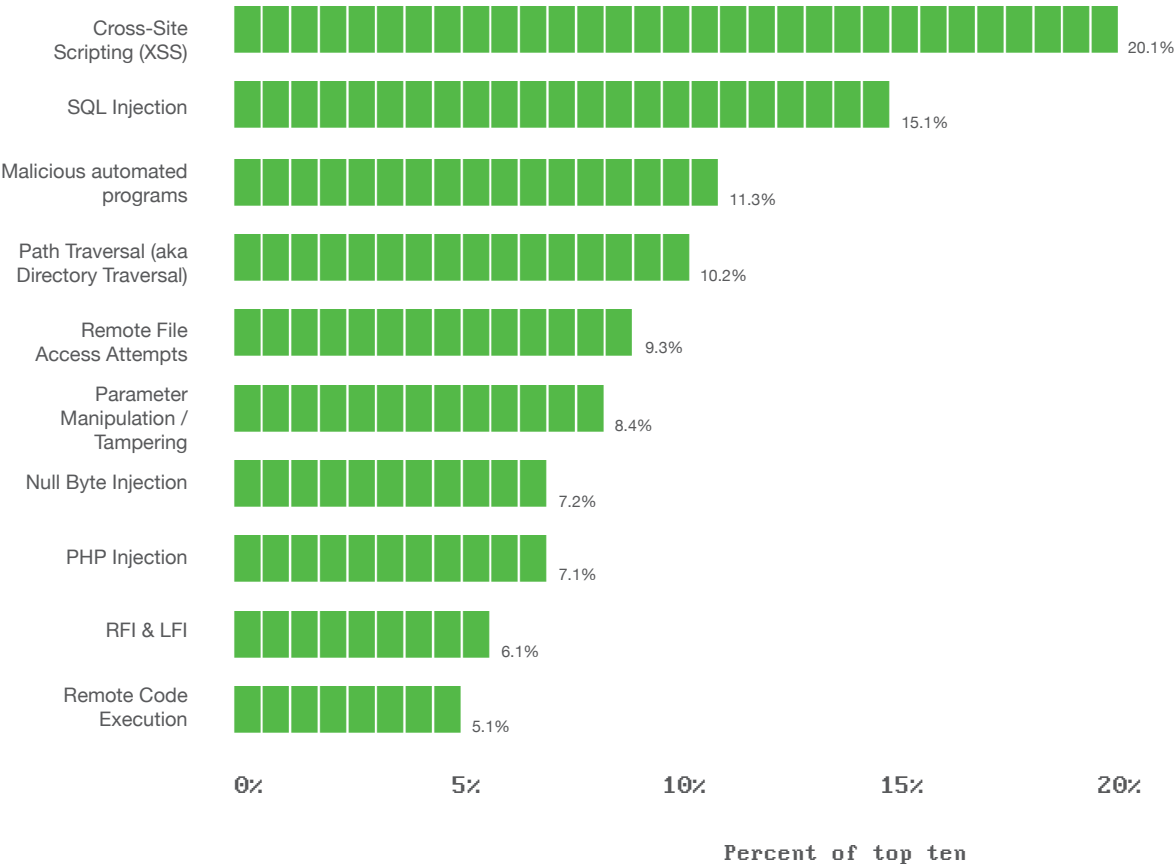
On December 14, 2015, the Joomla team published a security fix for a critical RCE vulnerability that affects all versions of Joomla from 1.5 to 3.4. The vulnerability allows an attacker to perform an object-injection attack against the Joomla database, leading to remote-command execution. After learning of the vulnerability, Trustwave researchers found evidence that attackers used the exploit at least two days before the patch was available. With attacks already taking place in the wild, the Trustwave SpiderLabs security team swiftly developed detection patterns for WAF products to detect and mitigate exploitation attempts.

GNU BASH: “SHELLSHOCK” CODE INJECTION VULNERABILITY (CVE-2014-6277 AND OTHERS)

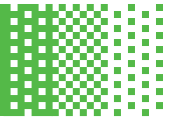
Shellshock is a group of related vulnerabilities in the GNU Bash command shell often installed on Unix and Linux computers. Successful exploitation can allow an attacker to run arbitrary code on the server. In some cases, an attacker can exploit the vulnerability remotely via a malformed HTTP request. Researchers began observing widespread exploitation. The GNU Project quickly issued patches addressing the vulnerabilities, and Trustwave developed a comprehensive set of patterns for WAF products to detect and mitigate Shellshock exploitation attempts.

TOP WEB ATTACKS IN 2016

These are the top ten categories of web attacks researchers observed in 2016. Together, they account for about two-thirds of all web attacks.



- XSS: These were the most common type of web attacks Trustwave observed in 2016, representing 20.1 percent of the top ten attacks, or about 13 percent of all attacks. As explained above, XSS typically involves inducing a website to execute an attacker’s arbitrary or malicious script code usually because the site fails to properly sanitize user-submitted inputs. Patterns for detecting XSS attempts often include strings such as “alert”, “confirm”, “script” and other tags and commands and can become quite complicated for sophisticated attacks that often depend on code obfuscation and unusual JavaScript constructions.



- **SQL injection:** Generic SQL injection attempts comprise the second largest share of web attacks, with 15.1 percent of the top ten attacks, or about ten percent of all attacks. Patterns for detecting simple attacks can include strings such as “SELECT” and “‘ OR ‘1’=’”. Here, too, patterns can become complicated when detecting attacks that use obfuscation methods like percent encoding and random comment characters.
- **Malicious automated programs (reconnaissance scans):** Automated programs that scan web servers for weaknesses, such as vulnerabilities and open ports, make up the third most common type of web attack researchers observed in 2016. One or more attack attempts associated with the source of the scan often follow reconnaissance scans.
- **Path traversal (directory traversal):** 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 attacks usually result from inadequate input sanitization. Attackers often combine these with other assaults, such as local or remote file inclusion, remote file access attempts and RCE. Remote file access attempts: Cybercriminals often try to access important files on the server, such as executable files in /usr/bin; account information in /etc/passwd; and boot.ini, which contains BIOS boot options for Windows systems.
- **Parameter manipulation or tampering:** These attacks target parameter information exchanged between client and server, such as cookies, form field contents, URL query strings and HTTP headers. The attacker attempts to modify and manipulate the parameter values to obtain different responses from the application, such as error messages or sensitive information, or to force the application to act differently than designed.
- **Null byte injection:** High-level programming languages, such as C and C++, use null bytes to indicate the end of a string. An attacker may attempt to use a URL-encoded null byte character (typically “%00”) to force a string to terminate abnormally and possibly trigger a vulnerability and gain access to unauthorized information.
- **PHP injection:** These attacks attempt to exploit vulnerabilities in server-side PHP code by passing serialized PHP code to an application that does not properly sanitize inputs. Frequently, cybercriminals heavily obfuscate PHP injection attempts.
- **Remote file inclusion (RFI) and local file inclusion (LFI):** RFI and LFI are similar attacks; each involves forcing a web application to accept and execute a malicious file as an input. With RFI, the attacker uploads a file containing shell or other malicious code. With LFI, the attacker selects an existing server file, often through directory traversal or a similar mechanism, and induces the web application to execute it.
- **Remote Code Execution (RCE):** This happens when an attacker exploits a vulnerability in the web application or component in a way that causes it to execute code of the attacker’s choosing. In the worst cases, a successful RCE exploit can allow an attacker to take over the entire server.



GUARDING AGAINST INFORMATION LEAKAGE WITH A WEB APPLICATION FIREWALL

Information leakage occurs when a web application transmits sensitive information about users or the application environment, typically because of a vulnerability or insecure configuration. WAFs provide protection against information leakage by monitoring HTTP requests and responses for anomalous behavior using features such as rulesets and active learning. By performing a little detective work, system administrators can use WAF leakage alerts to identify zero-day exploits and other unknown threats, find and fix vulnerabilities in web applications and more.

Here’s an example of a Trustwave WAF uncovering a compromised website. It began with several alerts from the WAF suggesting possible information leakage.

Security Events								
Group View - <Technical information retrieval>								
Host	Destination Port	Sensor	Date/Time	Entry/Informative Event	Result	Exit Event	URL	Source IP
www.trustwave.com	80	SENSOR	5/25/2016 1:48:00 PM		InfoLeak	Technical Information Retrieval - Server Parameters	http://www.trustwave.com/	10.0.0.1
www.trustwave.com	80	SENSOR	5/25/2016 1:47:59 PM		InfoLeak	Technical Information Retrieval - Server Parameters	http://www.trustwave.com/	10.0.0.1
www.trustwave.com	80	SENSOR	5/25/2016 12:18:52 PM		InfoLeak	Technical Information Retrieval - Server Parameters	http://www.trustwave.com/	10.0.0.1
www.trustwave.com	80	SENSOR	5/25/2016 10:08:52 AM		InfoLeak	Technical Information Retrieval - Server Parameters	http://www.trustwave.com/	10.0.0.1
www.trustwave.com	80	SENSOR	5/25/2016 10:08:51 AM		InfoLeak	Technical Information Retrieval - Server Parameters	http://www.trustwave.com/	10.0.0.1

Upon examining the request, researchers discovered the query string included what looked like a password in clear text, which is unusual. This was part of what caused the WAF to flag the request as suspicious.

InformationAnalysisRequestWeb Server ResponseBrowser View

Show All [WD-ID = 6288530805151555707]

POST /filesman HTTP/1.1
Host: www.trustwave.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36
Accept: */*
Cache-Control: no-cache
Content-Length: 64
Content-Type: application/x-www-form-urlencoded

a=filesman&c=/&p1=&p2=&p3=&charset=windows-1251&pass=ryfgddjs1

Visiting the URL revealed it to be c99madshell, a malicious web shell an intruder installed on the server.

Details

Information

Analysis

Request

Web Server Response

Browser View

Name: Linux server1 [redacted] 2.6.32-358.el6.x86_64 #1 SMP Tue Jan 29 11:47:41 EST 2013 x86_64
User: 48 (apache) **Group:** 48 (apache)
Php: 5.5.30 **Safe mode:** OFF [phpinfo] **Datetime:** 2016-05-25 16:47:59
Hdd: 92.18 GB **Free:** 46.65 GB (50%)
Cwd: / dr-xr-xr-x [home]

[Sec. Info]

[Files]

[Console]

[Sql]

[Php]

File manager

```
p1_=p2_=p3_="";
```

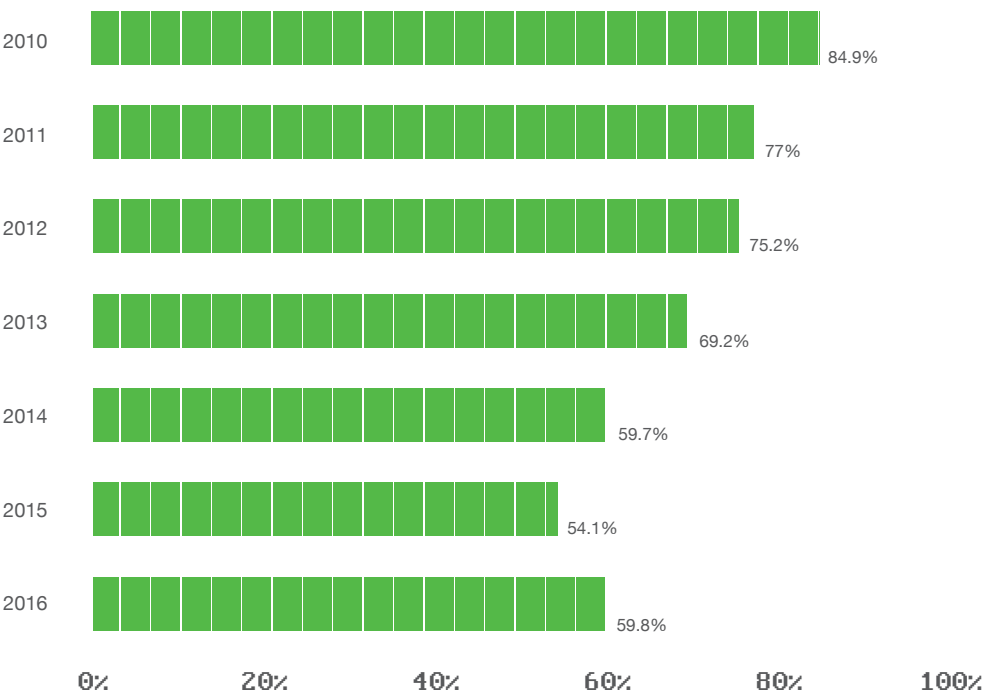
<input type="checkbox"/> Name	Size	Modify
<input type="checkbox"/> [.]	dir	2016-05-09 09:37:57
<input type="checkbox"/> [..]	dir	2016-05-09 09:37:57

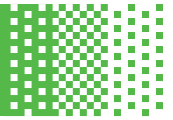
Without a WAF, the victim might not have detected this intrusion for quite some time. Over the past year, Trustwave has seen many examples of a WAF protecting customers from a wide range of attack techniques, emphasizing the importance of a comprehensive, multi-layer defense strategy.

EMAIL THREATS

For most of this decade, spam volumes decreased every year as law enforcement disrupted several prolific spamming operations and others voluntarily ceased operations. Unfortunately, this trend reversed itself in 2016 and volumes rose to back to 2014 levels. We can attribute this reversal almost entirely to Necurs, a botnet responsible for a troubling increase in the amount of spam sent with malicious attached files.

SPAM AS A PERCENTAGE OF TOTAL INBOUND EMAIL

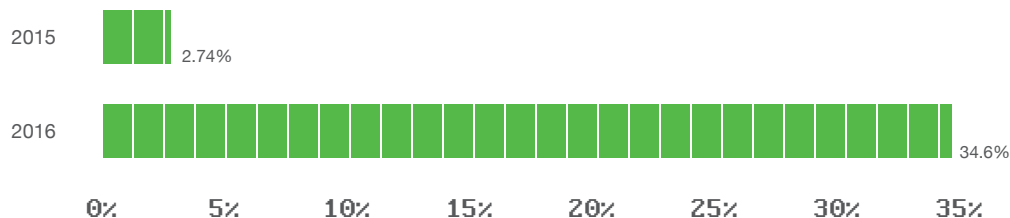




MALWARE SPAM, COURTESY OF NECURS

The Necurs malware has been around since at least 2012; however, it was only in mid-2015 that Necurs became associated with large-scale distribution of malware, particularly the banking Trojan Dridex and the Locky ransomware, which encrypts its victim's files and demands payment to decrypt them. Necurs typically operates in short bursts of intense spamming activity followed by lower activity. The botnet sends spam from between 200,000 and 400,000 unique IP addresses per day at its peak and often ceases activity on weekends. Much of Necurs spam comes from IP addresses in four countries — India, Vietnam, Mexico and Iran — with the top 10 countries representing 70 percent of all spam the botnet sends. Notably, Necurs clearly avoids sending spam from IP addresses in Russia.

MALWARE DETECTED IN TRUSTWAVE SPAM TRAPS

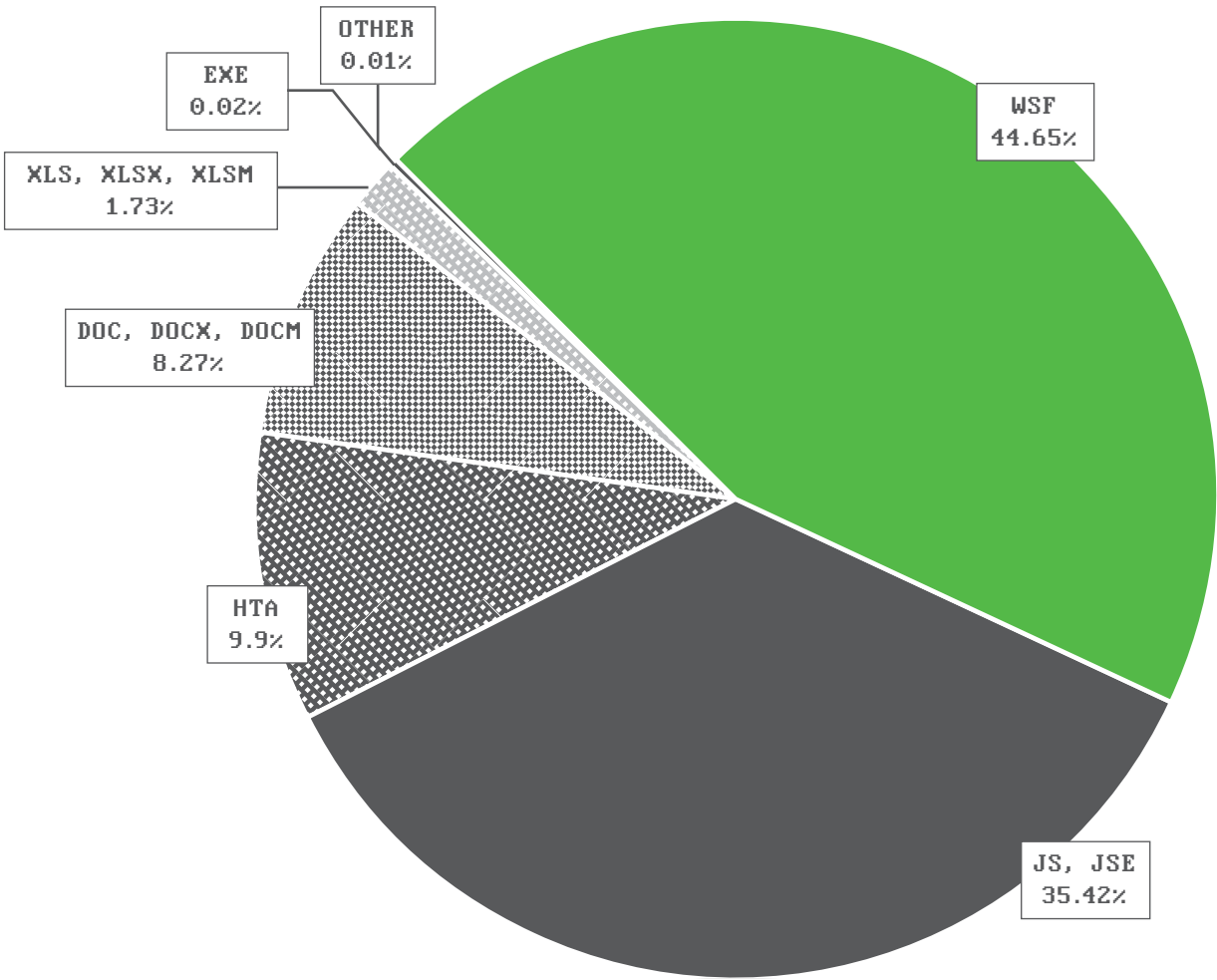


This chart reveals Necurs' influence, showing spam messages containing malware as a percentage of all messages hitting Trustwave's spam traps. In 2015, only 3 percent of spam messages contained malware. In 2016, this figure rose to almost 35 percent, with Necurs being responsible for most of the increase. Fortunately, this does not mean organizations were victims of this level of malicious spam. Attackers target some domains more heavily than others, and filtering at the SMTP connection level keeps a significant amount of spam from entering an organization's network.

Most Necurs attachments are inside .zip files. The typical payload is a small, highly obfuscated downloader script, the sole purpose of which is to download malware from the web and execute it. The type of file used to download the malware varies daily. Usually Necurs uses JavaScript (.js, .jse) and Windows Script (.wsf) files; but recently, Trustwave observed increasing use of .hta, a format used to package HTML files as Microsoft Windows applications. The outsized influence of Necurs on the malicious spam landscape again is apparent in the breakdown of malware file attachments in Trustwave's spam traps — executable Windows applications with the .exe extension that predominated in previous years comprised just 0.02 percent of the 2016 total.



EMAIL MALWARE FILE ATTACHMENTS



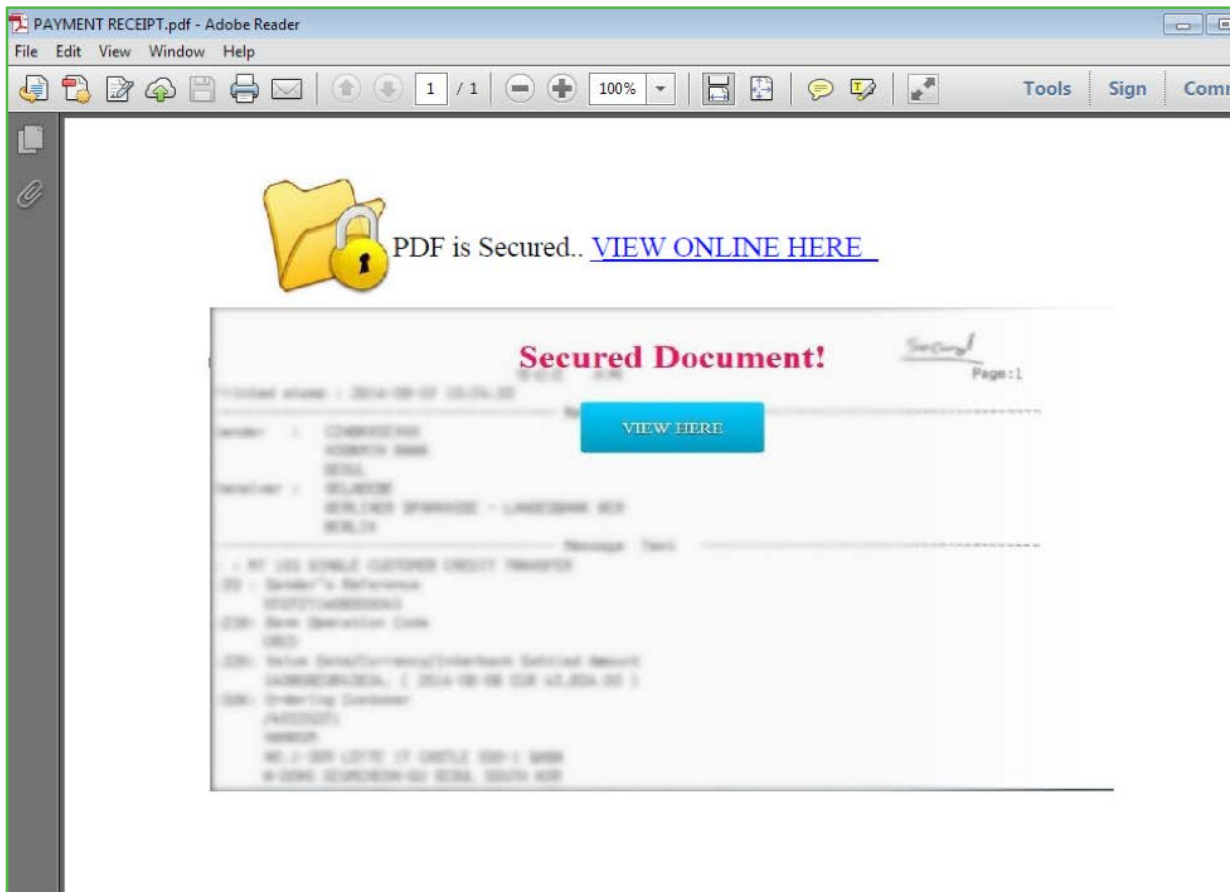
MALICIOUS EMAIL TRENDS AND THEMES

While the rise of the Necurs' botnet was probably the biggest email-related story of the year, several other developments attracted researchers' attention as well.

PHISHING DEVELOPMENTS

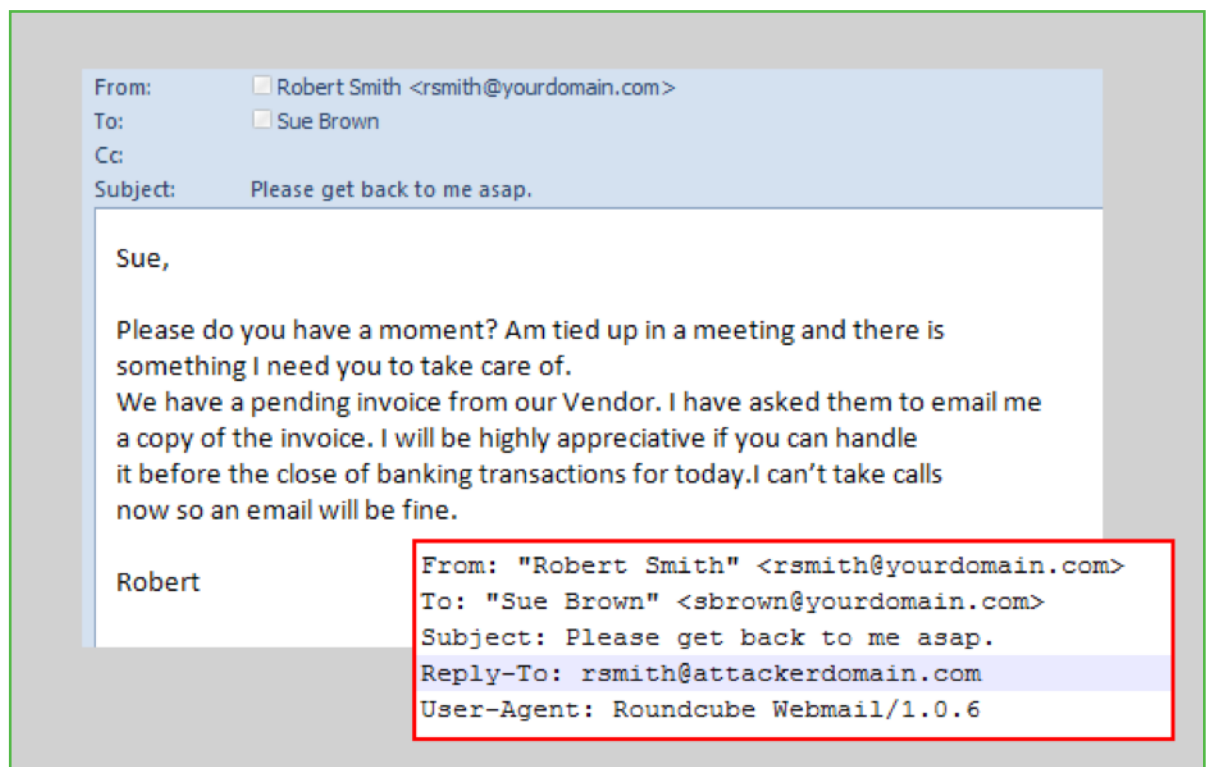
Phishers continued branching out from their focus on financial institutions to targeting other types of accounts, like Apple and Adobe IDs. One tactic that remained popular in 2016 was mail-quota phishing, in which targets receive messages telling them their email quota is full and giving them a link to follow to resolve the problem. The phisher, of course, controls the link, and victims who attempt to log in will have their domain credentials stolen.

Another case Trustwave investigated displayed aspects of phishing and malware delivery. In this case, 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 secured” and only viewable online. When clicked, the link leads to a fake Adobe ID sign-in page. When the user clicks “View File,” the page downloads a Microsoft Word binary file (.doc) that includes an image of more blurred text and instructions to enable macros for the file. If the user complies, malicious macros in the document download and install a rootkit and remote access Trojan (RAT).

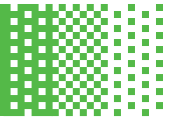


“CEO WIRE TRANSFER” FRAUD

Scammers increased use of the CEO wire transfer fraud tactic to steal money from victims in 2016. 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. Often, the scammer peruses the company’s website or other public information to find the name and email address of a suitable candidate along with the identity and email address of the company’s CEO. The scammer then sends the target an email purporting to be from the company’s CEO, asking the target 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 for a different account to ensure replies or follow-up messages from the target redirect to the scammer and not to the CEO.



CEO fraud scams are big business: The U.S. Federal Bureau of Investigation (FBI) estimated these and related scams cost companies \$3.1 billion from 2013 to 2016.



OFFICE DOCUMENT MALWARE

Malicious Microsoft Office files are a perennial favorite for delivering malware through email. The Necurs botnet was the main source of these in 2016 but not the only source. Malicious Office documents typically come in two forms: those with malicious macros that download malware and install malware from a remote site and files crafted to exploit a vulnerability. In some cases, a cybercriminal will send a message containing a Microsoft Word file and a PDF file with each file designed to deliver malware through exploits targeting their respective applications. Attackers sending malicious Office and PDF files seek to take advantage of the ubiquity of the file formats in business environments. However, the macro protections built into the last several versions of Office significantly hinder them, and Microsoft and Adobe patched most of the vulnerabilities they seek to exploit long ago.

DEFENDING THE EMAIL ATTACK SURFACE

To protect against the impact of email attacks, organizations should:

- Deploy an email security gateway. The security gateway should be on premises or in the cloud with multiple layers of technology, including anti-spam, anti-malware and flexible policy-based content filtering capabilities.
- Lock down email traffic content as much as possible. Carefully consider your organization's inbound email policy. Quarantine or flag all executable files, including Java, JavaScript, .vbs and .wsf attachments, as well as all suspicious and/or unusual file attachments, such as .cpl, .chm, .hta and .lnk files. Create plans for how to handle these potentially dangerous files coming into your organization.
- Block or flag macros in Office documents. At the least, organizations should enable macro protection in Office while making users aware of the threats.
- Keep client software fully patched and promptly up to date. Many email attacks succeed because of unpatched client software, such as Microsoft Office and Adobe Reader.
- Ensure ability to check potentially malicious or phishing links in emails. Perform checks with the email gateway, a web gateway or both.
- Deploy anti-spoofing technologies on your domains. Do this at the email gateway and deploy techniques to detect domain misspellings that may indicate phishing.
- Educate users. Everyone, from the rank and file up to the C-suite, needs to comprehend the nature of today's email attacks. Conducting mock phishing exercises against your staff shows employees phishing attacks are a real threat and they need to be wary.



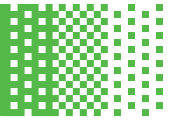
EXPLOITATION TRENDS

When Trustwave security professionals discuss changes in exploitation techniques, tools and trends, it's important to remember the cybercriminals responsible for these changes have one primary goal — to increase profits. That not only can mean finding ways to innovate their distribution methods, such as traffic trading, but can also mean going after the low-hanging fruit, like vulnerabilities in Adobe Flash Player, that previously served them well.

ZERO-DAY EXPLOITS IN 2016

Trustwave tracked nine web-based, client-side vulnerabilities that vendors patched in 2016 that had exploit code in the wild prior. Five of the vulnerabilities affected Adobe Flash, three affected Microsoft Internet Explorer and one affected Microsoft Silverlight.

CVE	PRODUCT OR COMPONENT AFFECTED	DATE PATCHED	CUSS V3 SEVERITY
CVE-2016-0034	Microsoft Silverlight	January 12	8.8 (High)
CVE-2016-1010	Adobe Flash	March 10	9.8 (Critical)
CVE-2016-1019	Adobe Flash	April 7	9.8 (Critical)
CVE-2016-0189	Microsoft Internet Explorer	May 10	7.5 (High)
CVE-2016-4117	Adobe Flash	May 12	9.8 (Critical)
CVE-2016-4171	Adobe Flash	June 16	9.8 (Critical)
CVE-2016-3351	Microsoft Internet Explorer	September 13	3.1 (Low)
CVE-2016-3298	Microsoft Internet Explorer	October 11	5.3 (Medium)
CVE-2016-7855	Adobe Flash	October 26	9.8 (Critical)



MORE FLASH, MORE PROBLEMS

Despite the numerous high-profile mitigations Adobe recently built into Flash, attackers continue to target its technology most often. Of the seven new exploits integrated into exploit kits in 2016, one targeted Microsoft Silverlight, two targeted Internet Explorer and five targeted Flash, including one (CVE-2016-1019) that was a zero-day exploit when it appeared in the Magnitude kit. Exploit kit writers rush to add useful new exploits to their kits as soon as someone discloses vulnerabilities, knowing it takes a few days for institutions and individuals to apply patches after release. Six new Flash vulnerabilities, for example, means six windows of opportunity in which attackers can expect higher-than-normal rates of successful infection. Whatever the reason, the kits are seeing some successes with these exploits. In Trustwave's analysis of statistics from the RIG exploit kit, researchers found an infection rate of about 7 percent of visitors to the landing page for both Flash and Internet Explorer, which is good for the attackers, considering the six-figure volumes of traffic the kit processed.

THE BUSINESS OF MALVERTISING

Malicious advertising remains the number one source of traffic to exploit kit landing pages. Large malvertisement campaigns several of the top exploit kits launched in March and April 2016 snared unsuspecting visitors to some of the top sites on the internet. Likely, attackers placed most of these ads with small, low-cost advertising networks that sell ad placements for as little as \$0.20 or less per 1,000 impressions. Ordinarily, such inexpensive ads run on low-end sites; however, they can bubble up to more popular sites when larger ad networks, such as those run by Google and Microsoft, buy traffic from smaller networks to cover shortfalls in their own targeted ad inventories. This strategy can be surprisingly cost-effective for malvertisers.

Trustwave conducted an experiment in 2016 running online ads that tested for vulnerable versions of Flash to gauge the cost of spreading exploits through malvertising. Researchers estimate an attacker could reach approximately 1,000 computers with exploitable vulnerabilities for about \$5 — less than \$.01 per vulnerable machine — far less than the \$80 to \$400 per 1,000 computers attackers pay for access to infected machines, depending on geolocation.

One tactic Trustwave researchers discovered used by the Angler exploit kit in March involved taking over an expired domain from a small, but apparently legitimate, website design and marketing company and using it as a conduit for malvertisements leading to Angler landing pages. The original registration for the domain, brentsmmedia.com, expired in January 2016. Subsequently, in March, someone in Russia reregistered the domain and began serving malicious ad content within a week. Further investigation revealed several other recently expired domain names containing the word “media” that the same registrant or associated parties acquired around the same time. It's likely the people behind this operation are trying to exploit the established history and reputation of these formerly legitimate, innocuous-sounding domains and use them to trick ad companies into publishing their malicious ads.



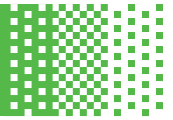
TRADING TRAFFIC FOR FUN AND PROFIT

The conventional wisdom for several years was opportunistic attackers, such as exploit kit customers, wanted to maximize their impact by exposing their malware to as many potential victims as possible. As attackers become more sophisticated, however, they increasingly target specific types of visitors, to maximize their chances of a successful infection while minimizing the likelihood that security tools and researchers will identify the landing pages and browsers and search engines, subsequently, will flag them as malicious.

For several years, exploit kits have been tailoring their landing pages to each visitor and allowing attackers to configure campaigns to target visitors matching certain characteristics, such as country of origin or browser used, as determined by the HTTP headers the browsers send. For example, a visitor running Internet Explorer 6 with several out-of-date plugins might expose himself to a dozen exploits for known vulnerabilities, whereas a visitor running the latest version of Chrome or Firefox might not face exposure at all. A while back, attackers extended this concept by using traffic distribution systems (TDSes), software designed to funnel different types of traffic down different “paths.”

TDSes function as gateways between a web page and additional content, directing visitors to ads or other links based on factors such as geolocation and browser characteristics. In this way, they function similarly to ad networks or content discovery networks, although the TDS label generally applies to systems geared toward illegitimate or shady traffic, such as pornography, gambling, grey market pharmaceuticals and malware distribution. In the early days, these systems were usually stand-alone products, like Sutra TDS, SimpleTDS and Keitaro TDS. Designed for purchase by a prospective traffic trader for installation on the trader’s server, these products typically dealt with the lower-end of traffic, redirecting most of their visitors to adult sites and fake pharmaceuticals, with only a small portion of traffic redirecting to exploit kit landing pages. In 2016, there was a rise in TDS services designed to funnel high-quality traffic to exploit kits from higher-end cybercrime groups, such as ElTest, Pseudo-Darkleech and Afraidgate.

Two factors largely determine traffic quality: the likelihood of a successful infection and the potential profits from infecting the computer. To boost the likelihood of infection, high-quality traffic includes a high percentage of machines with vulnerable browsers or components. Attackers filter out computers with certain security products installed or those that show signs of use for security testing. Attackers value computers in wealthy regions, like North America, for installing banking malware and ransomware, which encrypts computer data, because these regions tend to have more money to pay the ransom for the decryption key. On the other hand, botnet operators find satisfaction with traffic from just about anywhere because botnets typically depend on volume, not wealth to send spam. And clean machines, those without other pre-existing infections, can command a higher price than machines already infected with malware.



Prior to 2016, consistently high-quality traffic such as this was rarely available, if at all. Illicit traffic trading has been around in some form for at least a decade. However, it has been relatively primitive, with traders running Sutra TDS or another package as little more than a forwarding service for traffic priced out by source.

In 2016, though, evidence revealed TDSes were becoming more sophisticated in providing their customers with steady streams of high-quality traffic ripe for exploitation not only by filtering out low-quality traffic but also by detecting honeypots and virtual machines run by security researchers and filtering them out as well. Providing a service at this level requires an active investment of time, money and effort on the part of the TDS, and the availability of such services is testament to the value attackers place on high-quality traffic.

Participants in the traffic-trading industry tend to break down into four general roles:

- Traffic sellers get traffic via links distributed through compromised websites, malvertisements, spam, botnets and other such sources that have been serving as sources for exploit distribution for a long while. Whereas in previous years, a malicious inline frame placed on a compromised site might have led directly to an exploit kit landing page, today, it is likely to lead to a TDS that redirects visitors based on who buys the traffic.
- The TDS receives traffic from its customer (the attacker) and refines this traffic, filtering only desired traffic based on various characteristics defined by the customer. This enables the creation of traffic streams that are more specialized than what the attacker could obtain from random visitors to a widely distributed exploit kit landing page. For example, an attacker could choose to redirect traffic from North America or Europe to a ransomware payload and traffic from other regions to a botnet payload.

- Attackers buy traffic according to their needs and direct it to or away from exploit kits using a TDS easier than if they were to manage the traffic funneling on their own. Traffic trading also enables attackers to switch freely between different exploit kits to distribute their payloads simply by configuring the TDS to direct traffic to a different landing page link.
- Exploit kits rent out landing pages to attackers who supply the traffic and malicious payloads and configure the kits to connect visitors to malware as desired.

In practice, actors often play multiple roles: A group running a TDS might run occasional attack campaigns; an exploit kit operator might go into the traffic-trading business by setting up a TDS, and so on. Overall, though, the trend has been componentizing the exploitation process into multiple independent roles, each looking for a share of the illicit profits.

SHINING A LIGHT ON THE ZERO-DAY MARKETPLACE

The underground economy for computer crime in many ways resembles the legitimate economy, with sellers offering products and services to buyers willing to pay for them and the highest-value offerings commanding a premium price. In May and June 2016, Trustwave SpiderLabs researchers were first hand witnesses to a cybercriminal offering an unknown Microsoft Windows zero-day exploit for sale to the highest bidder. What ensued was a fascinating, if incomplete, picture of the underground malware marketplace in action.

The offer first appeared on a website that serves as an underground marketplace for Russian-speaking cybercriminals to buy and sell coding services, access to exploit kits and botnet resources, and other illegitimate products and services. A user going by the name “BuggiCorp” posted a message on May 11 offering to sell a local privilege escalation (LPE) exploit for the Windows kernel for \$95,000. In part, the translated message reads:

Dear friends, I offer you a rare product.

Description:

Exploit for local privilege escalation (LPE) for a 0day vulnerability in win32k.sys. The vulnerability exists in the incorrect handling of window objects, which have certain properties, and [the vulnerability] exists in all OS [versions], starting from Windows 2000. [The] exploit is implemented for all OS architectures (x86 and x64), starting from Windows XP, including Windows Server versions, and up to current variants of Windows 10.

[...]

The buyer will receive:

- 1. Source code project based on MSVC2005, with all the source code of the exploit and a demo for the exploit.*
- 2. Free of charge updates to address any Windows version that the exploit might not work on (Might be the case with Windows 10 as there is a large number of different builds).*
- 3. A detailed write up of the vulnerability details (including the specific vulnerable code in win2k).*
- 4. Complementary consultation on integrating the exploit according to your needs (within reason).*
- 5. On request – convert the source code project to a different MSVC version.*

Prices:

Willing to accept offers starting from 95k [USD]

Do not offer revenue sharing as payment. Respect your and my time.

Payment transaction:

BTC [Bitcoin]

Escrow – the forum admin.

Win LPE 0 day, All Win ver

01.08.2016, 11:31

Дорогие друзья, предлагаю Вам редкий продукт.

Описание:
экспloit для локального повышения привилегий (LPE) для 0-day уязвимости в win32k.sys. Уязвимость заключается в некорректной работе с оверлейми, обладающими определенными свойствами и существует во всех ОС, начиная с Windows 2000. Экспloit реализован для всех ОС (x86 и x64), начиная с Windows XP, включая серверные системы и эквивалент всем упомянутым вариантам Windows 10. Уязвимость относится к классу cirta-wiki-eflags и, таким образом, позволяет осуществить запись определенного значения на любую адресную, чего оказывается достаточно для успешной эксплуатации. Экспloit успешно осуществляет выходы из Jit/Arithmetic (JIT), обходит (в том числе, не затрагивает) все существующие механизмы защиты вроде ASLR, DEP, SMEP etc, не требует никаких библиотек кроме KERNEL32 и USER32. Проект эксплойта и тестового примера написан в MSVC 2005 на C и ассемблере. На выходе получается IS-файл, который может быть проинжектан в другую программу и тестовый exe, осуществляющий запуск opt.exe и повышение ему прав до SYSTEM. Размер готового exe колеблется от 7 до 12kb в зависимости от разрядности ОС и используемого варианта эксплойта. Экспloit тестировался на всей линейке Windows, начиная с XP, более чем на 20 вариантах ОС, как пользовательской, так и серверной.

Экспloit предоставляется в двух вариантах:
1. Просто повышение прав до SYSTEM любой программой.
2. Повышение прав любой программе и возможности выполнения стороннего кода в prog. Эксплуатируемый уязвимость может передавать и функцию локализации привилегий указывать на код, который должен быть выполнен в prog (режиме адми). Примененный метод заключается в модификации PTE пользовательской страницы, в конкретный флаги оверлея, что позволяет изменить владельца конкретной страницы с User на Kernel. Далее, одним из стандартных методов управления передается на код в этой странице, который выделит неподключенный путь в адрес, скопирует в него пользовательский код, передаст управление ему и восстановит измененный PTE. Таким образом, примененный метод не использует потенциально ненадежных трюков с ROP и не конфликтует со SMEP и прочими защитными механизмами ОС.

Покупатель получает:
1. Проект со всеми исходными кодами в MSVC2005, включающий в себя исходный код эксплойта и пример эксплуатации.
2. Эксплуатационные скрипты и доработки в случае обнаружения ОС, на которой эксплойт не работает (может быть актуально для Windows 10 с большим количеством обновлений).
3. Подборку исходных уязвимостей (с указанием конкретного места в оверлее win32k) и принципы работы эксплойта.
4. Бесплатные консультации по работе эксплойта (в разумных пределах).
5. По желанию - сконвертированный в другую версию MSVC проект эксплойта.

Видео:
Код

Цена:
Выпускается предложение от 90k.
Работа под % не интересует. Укажите и код, и свое время.

Сделка
Расчеты в BTC
Гарантия - админ ресурса.

Сайт: buggicorp.com

23.05.2016, 11:10
Цена снижена до 90k.
Продажа в 1 руки.

Update (May 23rd):
- Price lowered to 90K (USD)
- Offer is exclusive and will be sold to a single buyer

ZERO-DAYS COME OUT OF THE SHADOWS

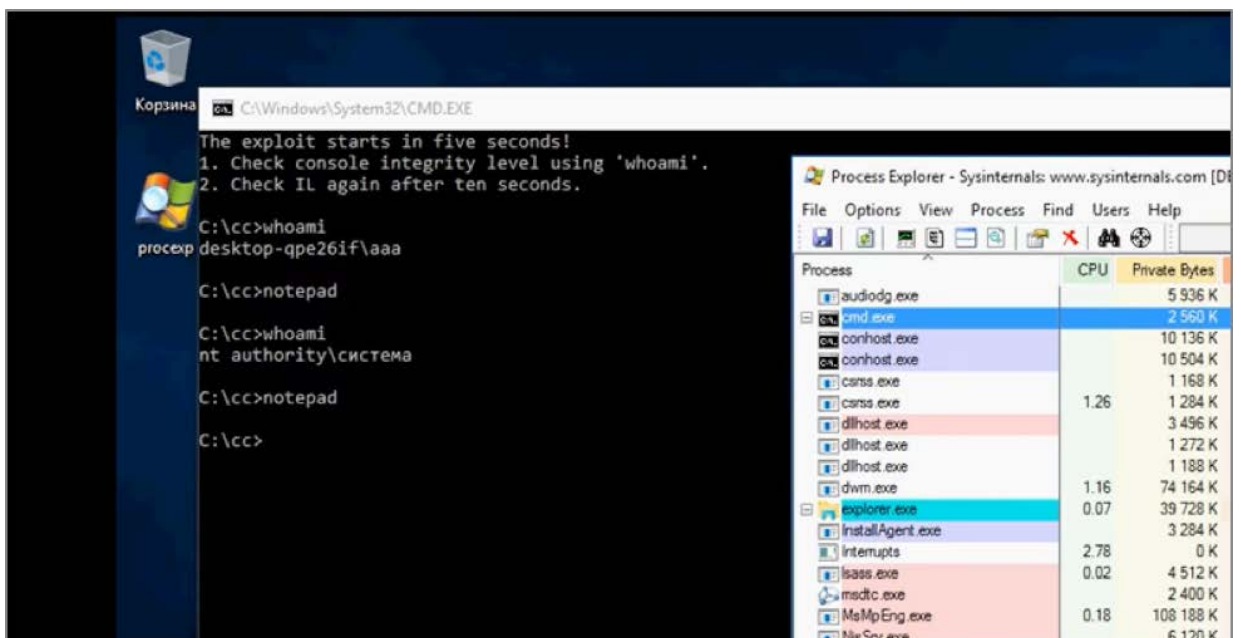
Zero-day exploits are among the most prized commodities in the cybercriminal underground, as they offer the prospective attacker a greater chance of a successful compromise than an exploit for which a patch is already available. The market for zero-day exploits has been around for several years, and will continue to be around as long as there is money to be made, as black-hat security researchers discover previously unknown vulnerabilities, develop exploit code for them and offer them for sale, usually to advanced persistent threat (APT) groups. Usually, though, these transactions take place privately, with one party contacting the other directly or through an intermediary. To see a zero-day offered for sale on a forum — and a publicly available forum, rather than a dark-web forum accessed through the anonymous Tor network — is rare and suggests zero-days might be coming out of the shadows and becoming a commodity for criminal masses.

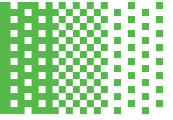
Although the product for sale was atypical, the offer displayed characteristics typical of those in forums where buyers and sellers have plenty of reasons to distrust one another. Most notably, BuggiCorp insists on using the forum's administrator as an escrow party, indicating it wanted potential buyers to perceive it as a trustworthy seller. Escrow services are common on cybercrime forums. To ensure neither the buyer nor the seller can rip the other off, the escrow provider holds the buyer's money until the seller delivers the product and the buyer verifies it. The escrow requirement suggests the offer was real: If BuggiCorp could not deliver the exploit as promised, it would not get paid. The offer specified payment in bitcoins, the anonymous digital currency that has become the preferred payment method on cybercrime forums, and included multiple perks (consultation services, free updates and so on) befitting the premium nature of the product for sale.

SETTING — AND RESETTING — THE PRICE

LPE exploits are less valuable to attackers than the more dangerous remote code execution (RCE) class of exploits because attackers can't use them alone to compromise a computer; although, attackers often use them in conjunction with other exploits to hijack machines. For example, an attacker can pair an RCE zero-day that only works when the user has administrative privileges with an LPE zero-day to provide those privileges. Information about the zero-day economy is hard to come by because of the deeply private nature of most transactions. Therefore, it's difficult to know what an exploit like the one BuggiCorp described would be worth to a prospective buyer, but the limited information available suggests \$95,000 was a lot to charge. A 2015 breach episode revealed HackingTeam, an Italian company that sells zero-day vulnerabilities and exploits to governments and law enforcement agencies, paid one Singaporean researcher about \$80,000 for a working zero-day LPE exploit affecting Windows. Zerodium, a company in a similar line of business, takes the unusual step of publishing a list of the sums it's willing to pay for different kinds of exploits. Prices range from \$10,000 to \$1.5 million, but Windows LPE zero-days are in the "up to \$30,000" category near the low end of the scale, nowhere near the \$95,000 price BuggiCorp quoted.

A few weeks later, on May 23, BuggiCorp posted another message lowering the price to \$90,000 and making the offer exclusive to a single buyer. Exclusive zero-days are significantly more valuable than non-exclusive ones because the purchaser has more opportunities to use the exploit without having to worry the actions of another buyer will tip off the vendor of the vulnerable product. The seller also published a pair of videos supposedly showing the exploit in action. One video apparently shows the exploit active on a computer running Windows 10; the other appears to show it bypassing Microsoft's Enhanced Mitigation Experience Toolkit (EMET), which adds mitigations to Windows to prevent exploitation of some vulnerabilities. BuggiCorp demonstrates both videos on the Russian-language edition of Windows 10.





On June 6, the seller lowered the asking price to \$85,000. On June 16, BuggiCorp posted that the exploit still worked despite Microsoft's "Patch Tuesday" round of security updates, which occurs on the second Tuesday of every month. Finally, on July 4, the seller posted that the discussion thread for the offer was no longer relevant. Because it posted the July 4 message before July's Patch Tuesday, the seller likely came to terms with a customer and sold the exploit.

PROTECTING YOURSELF AGAINST ZERO-DAY EXPLOITS

There's a lot we don't know about this exploit. The buyer, if there were one, may have used it or may be keeping it in reserve. Microsoft already may have patched the vulnerability. Or, it's possible, this was simply a well-designed hoax, and the exploit never existed. Whatever the truth is, this isn't the first and unfortunately isn't the last zero day. Still, lessons learned from previous cases provide general guidance that has proven itself over the years:

- **Keep your software up to date.**

As discussed, an attacker can only use an LPE exploit as one component of several that constitute a successful compromise. If you can break one link in the chain, you will probably thwart the entire attack. Consider a scenario where the cybercriminal uses this LPE exploit in tandem with an RCE exploit to break out of a sandbox. Your machine may not have a patch against the zero day LPE, but it may very well have a patch against the RCE component of the attack, which should be enough to stop the attempt.

- **Security works in layers.**

Following the above logic, you can break links in the chain in various parts of your security infrastructure. Deploying a full stack of intelligent security products will increase the odds of breaking one of these links.

- **Use common sense and be aware.**

These days, many attacks begin with and depend on user interaction, such as clicking a link or opening an attachment. Avoid clicking suspicious links or opening attachments from unsolicited sources.



EXPLOIT KITS

Last year was a roller coaster year for exploit kits and the people tracking them. Chaos in the market ensued in June 2016 when Angler, the most popular exploit kit by a wide margin, disappeared suddenly leaving several other kits vying for supremacy. Combined with the temporary or permanent departure of several other prominent kits, the exploit kit environment looked very different at the close of 2016 than a year earlier.

EXPLOIT KIT TECHNIQUES

Exploit kits enable criminals to infect computers without having the technical sophistication necessary to develop and deploy exploits on their own. Now they can simply purchase access to a kit and configure it to meet their needs. Exploit kits work by generating special web pages, called landing pages, which contain exploits for vulnerabilities in popular browsers, browser plugins and other software. When a prospective victim loads a landing page using a computer vulnerable to one of the exploits, the computer can become infected. Customers can typically configure the kit to target computers based on specific criteria, such as:

- Geographic region
- Specific operating system or browser versions
- The presence or absence of specific browser plugins
- The presence or absence of specific anti-malware software or other security countermeasures.

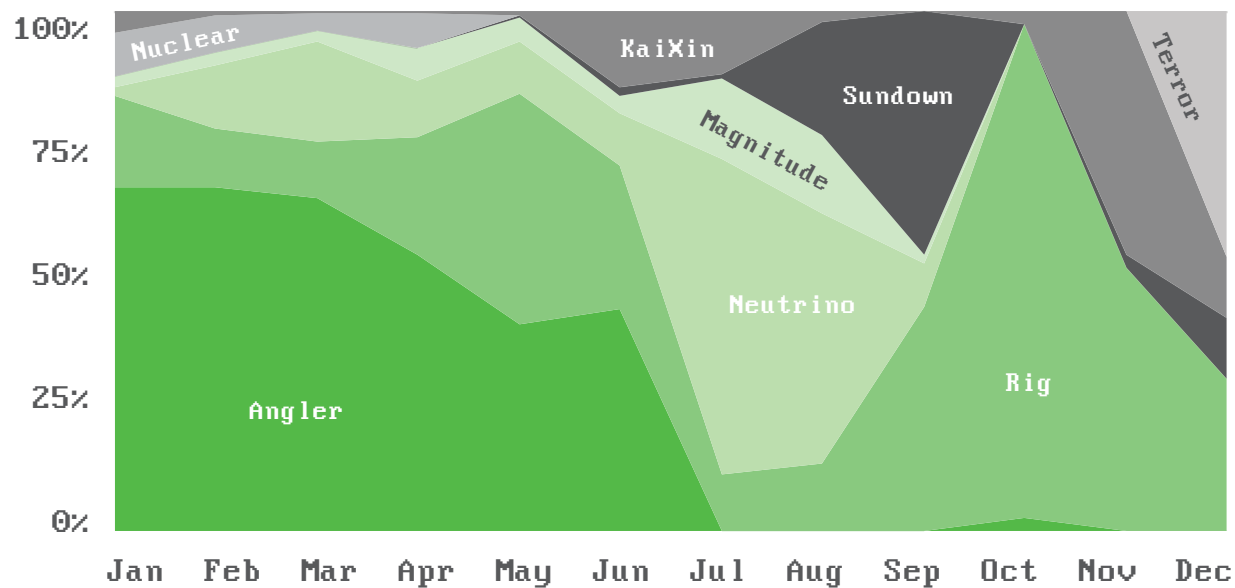
Exploit kit makers face a running battle with security professionals and design their kits to minimize the likelihood anti-malware software or intrusion detection system and intrusion prevention system (IDS/IPS) solutions will detect or block attempts. Popular kits compete to provide access to the newest exploits before patches become widely available. Some security products recognize exploit attempts by monitoring web traffic for characteristic URL patterns used by landing pages generated by different kits, so kit makers frequently change these markings. Some of the more advanced kits include features that attempt to detect when they are executing in a virtualized or laboratory environment, which can indicate a security gateway product or research lab, and avoid running in such environments.

EXPLOITS THAT EXPLOIT KITS ADOPTED IN 2016

Exploit kits in 2016 integrated several new exploits, including two that were zero-day at the time of adoption.

CVE	DATE DISCLOSED	PRODUCT OR COMPONENT AFFECTED	CVSS V3 SEVERITY	FIRST KIT TO ADOPT EXPLOIT
CVE-2015-8651	December 28, 2015	Adobe Flash Player	8.8 (High)	Angler
CVE-2016-0034	January 13, 2016	Microsoft Silverlight	8.8 (High)	Angler
CVE-2016-1001	March 12, 2016	Adobe Flash Player	9.8 (Critical)	Angler
CVE-2016-1019 (zero-day)	April 7, 2016	Adobe Flash Player	9.8 (Critical)	Magnitude
CVE-2016-4117	May 10, 2016	Adobe Flash Player	9.8 (Critical)	Magnitude
CVE-2016-0189	May 10, 2016	Microsoft Internet Explorer	7.5 (High)	Neutrino
CVE-2016-3298 (zero-day)	October 13, 2016	Microsoft Internet Explorer	5.3 (Medium)	Neutrino

EXPLOIT KIT PREVALENCE IN 2016

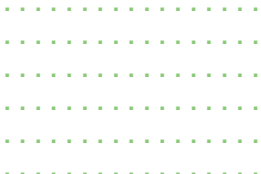


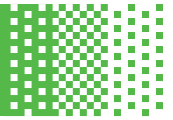
JANUARY-APRIL: EARLY STABILITY

The year began much as 2015 ended, with Angler commanding the exploit kit market and the other players far behind. Angler, which charged handsomely for its services, built a reputation as a technically sophisticated kit that often adopted a new exploit or technique first. Dominating most of the rest of the market in 2016 were four other kits — RIG, Nuclear, Neutrino and Magnitude — with KaiXin, a Chinese kit, occasionally having a small impact.

Angler figured prominently in several aggressive actions attackers took in early 2016. In February, Trustwave researchers discovered a redirect to an Angler landing page on extendoffice.com, a moderately popular website offering add-ins and tips for Microsoft Office programs, that attempted to install the TeslaCrypt ransomware on visitors’ machines. (See the “Web Attacks” section for information about CVE-2015-8562, the Joomla exploit researchers believed compromised the site.)

In March, a large-scale malvertising campaign resulted in placements of Angler landing page redirects on some of the most popular sites on the web. (See “The Business of Malvertising” section in “Exploitation Trends” for more information about these techniques.)





MAY–JUNE: ARRESTS AND DISAPPEARANCES

The landscape began to change at the end of April when Nuclear, one of Angler's largest competitors in 2015 and early 2016, abruptly disappeared. Researchers first observed Nuclear in 2009, making it the oldest active exploit kit at the time. Earlier that month, a group of security researchers published a major technical analysis of the Nuclear software and infrastructure, leading many to associate the two events.

On June 1, Russian federal authorities announced the arrest of the so-called Lurk gang, a group of about 50 accused of using the Lurk banking Trojan to steal more than 1.7 billion rubles (\$25 million) from customers of Russian banks. The next week, on June 7, activity associated with the Angler kit disappeared nearly as abruptly as Nuclear activity. Security researchers generally agree Angler's disappearance was not a coincidence; the Lurk gang was probably responsible for the development and distribution of Angler and the arrests made it impossible for the kit to continue operating.

JULY–DECEMBER: MORE TURMOIL

The disappearance of Nuclear and Angler had a huge effect on the exploit kit ecosystem. The volume of exploit kit-related incidents Trustwave tracked in June was 95 percent lower than in April. Activity bounced back somewhat in the following months but never to the levels seen in the first half of the year.

The exploit kit that seemed to benefit the most in the wake of Angler's disappearance was Neutrino, which was responsible for the lion's share of activity Trustwave monitored in July and August. Beginning in September, however, Neutrino activity declined to negligible levels as did that of Magnitude, a longtime competitor. Some evidence suggests one or both kits may have reinvented themselves as private exploit kits that a single criminal group used rather than exploit kits rented to many different customers.

With the disappearance of Neutrino and Magnitude, the exploit kit market largely dropped to two major players: RIG is a full-featured kit aimed at high-end customers. (See page 55 for more information about RIG). Sundown is a less expensive kit that offers fewer features than RIG and steals exploits from other kits.

By the end of the year, it was clear these upheavals had a lasting effect on the exploit kit space. The large gap Angler and the other withdrawn kits left in the marketplace tempted small independent groups of cybercriminals into building and selling their own exploit kits, such as Terror, which Trustwave first saw in December. Terror, a variant of Sundown, is a rudimentary kit that makes naïve mistakes, such as using an unobfuscated landing page and serving up exploits directly without performing referrer checks.

Despite the partial respite computer users have enjoyed for the past few months, it would be unwise to assume disruption to the exploit kit landscape is permanent. If exploit kits are profitable, there will be kit developers trying to fill the demand. The only safe assumption is that the landscape will look as different a year from now as it did a year ago.



THREE VERSIONS OF RIG

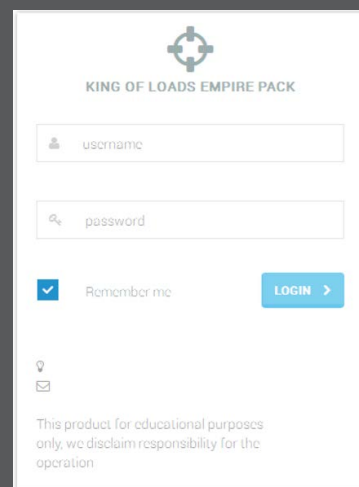
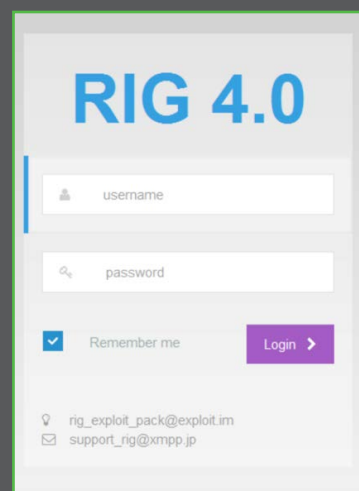
The clearest beneficiary of the exploit kit market shakeout in 2016 has been RIG, a full-featured kit aimed at high-end customers that previously struggled to compete with former market leaders Angler and Neutrino. RIG's operators stayed busy throughout the year by debuting not only an updated and improved version of the kit for its customers but also a private version for its own use. This section covers Trustwave researchers' investigations of the three distinct versions of RIG active in 2016 and discusses their similarities and differences in terms of construction, traffic and payloads.

RIG 3

Version 3.0 of the RIG kit was active from mid-2015 to around October 2016. Deployed a few months after a disgruntled reseller leaked the source code for previous version of the kit, RIG 3 featured several security improvements over its predecessor along with a more polished user interface.

RIG 4

In September, landing pages for a previously unseen version of RIG started to appear in the wild. Security researchers at first informally referred to this version as "RIG-V," believing it was a variant of RIG 3; however, it eventually became clear this was the new 4.0 version of RIG once RIG operators phased out all-known instances of RIG 3 over a period of several months. Trustwave first noticed RIG 4 in mid-September after discovering pages the notorious Pseudo-Darkleech malware distribution campaign infected, redirecting visitors to the now malicious content. RIG 4 uses different URL patterns than RIG 3 and a more heavily obfuscated landing page with several non-printing control characters, though it closely resembles the RIG 3 landing page when de-obfuscated. Like the previous version, RIG 4 sports an improved user interface for customers and adds a whitelist for accessing the application program interface (API) that reveals the current address of the RIG landing page, probably to deter security researchers from using the API themselves to track the kit. The seven top campaigns, run by five different customers, were responsible for 82 percent of successful RIG 4 infections in 2016. The most common payloads were Cerber, a file-encrypting ransomware family; Chthonic, a variant of the decade-old Zeus Trojan; Tofsee, a spambot; and TrickLoader, another bot.



Login pages for RIG 4 (Top) and EmpireEK (bottom)

EMPIRE

Empire, also called RIG-E, is a private version of RIG that operators use to infect computers directly rather than rent out to customers. The interface is like RIG 4 but includes no customer-management features and focuses more on geolocation statistics and options for currently running campaigns — or “flows,” as the kit calls them.

As a private kit, Empire displays distinctly different traffic patterns than those of its public sibling. The kit’s customers control traffic to RIG 4 landing pages, which come from a wide range of sources. No single source comprises more than 2 percent of overall traffic. Empire gets less than a third of the RIG 4 traffic, and its traffic is significantly less diverse with more 30 percent originating from malvertisements placed with a single ad network. In total, Empire’s top 10 traffic sources account for about three-fourths of all traffic to the kit.

Empire’s focus on geolocation enables its operators to extensively customize their payloads based on visitor location. Trustwave observed Empire delivering the Smoke Loader bot to victims in Spain, while France received the GootKit password stealer, the United States received Chthonic and Korea received Locky ransomware. Although attackers privately operate Empire, researchers believe it may be selling infections, or loads, to other parties, which would explain the regional differences.

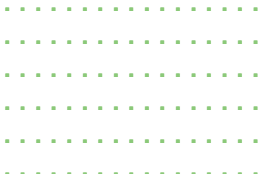
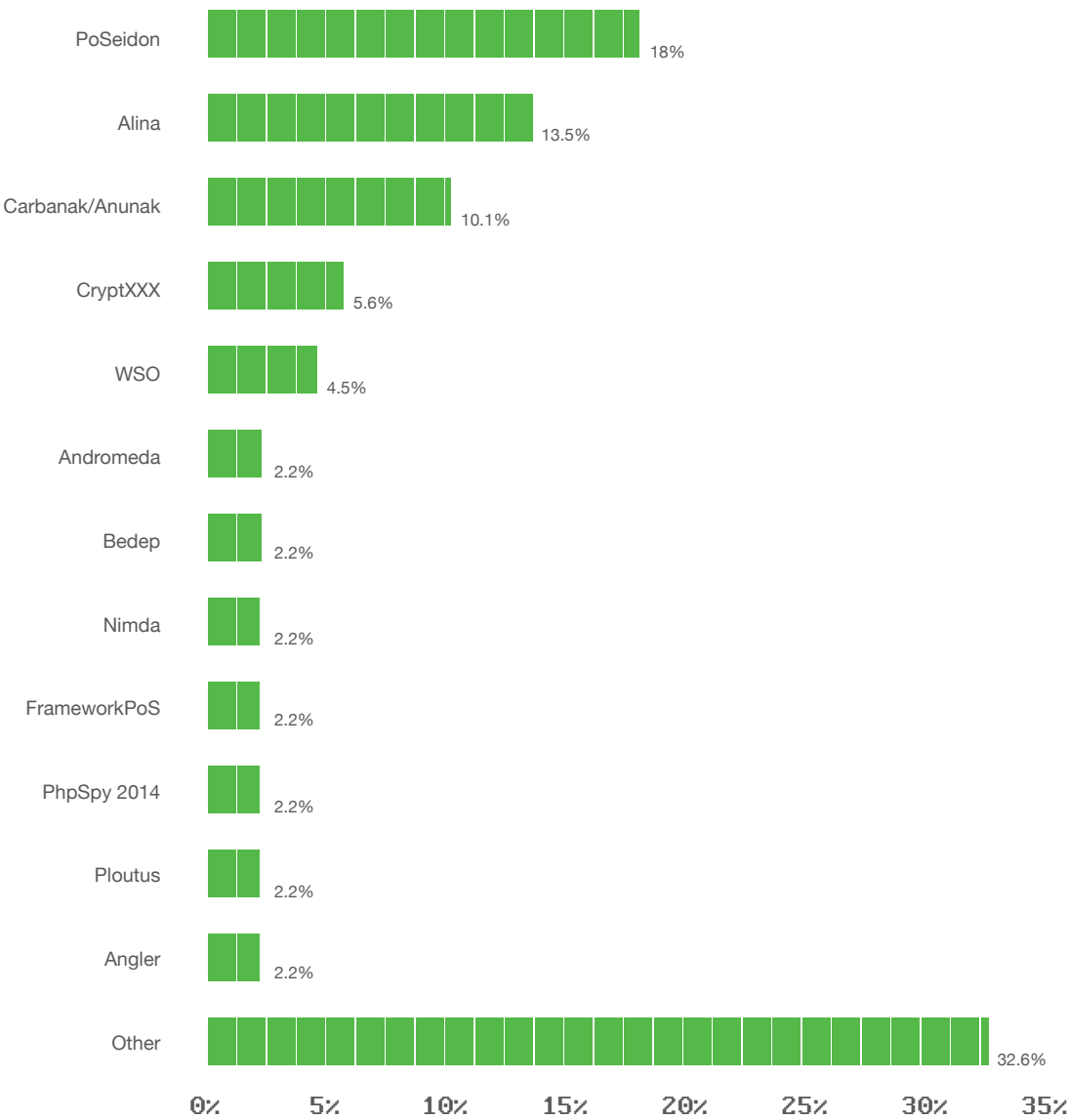
The screenshot shows the 'Country Stats' interface within the 'KING OF LOADS EMPIRE PACK'. The interface has a dark green header bar with the title and several menu items: Statistics, Country Stats, Files, Flows, VDS, Proxy, Options, Users, and Exit. Below the header, the main content area is titled 'Country Stats'. It features four main sections: 'Country', 'Flows', 'By flow/cc /selected', and 'Time'. The 'Country' section has a 'Select all' button and a list of countries (AT, AU, BE, BR, CA). The 'Flows' section has a 'Select all' button and a list of flows (15 | 1 gol, 17 | 1 tri, 18 | 1 inc, 19 | 1 ex0, 20 | 1.4.4.4). The 'By flow/cc /selected' section has three radio buttons: 'By Selected' (selected), 'By country', and 'By flow'. The 'Time' section has 'From' and 'To' date pickers (format: www-mm-dd) and a 'Not selected' dropdown menu.

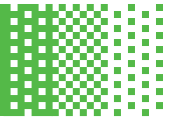
Geolocation features in Empire

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 2016 Trustwave investigations. Most of the information presented comes from compromise incidents affecting point-of-sale (POS) environments and the specialized equipment used to collect payment card data from customers. As a result, authors tailor most of the malware families discussed here specifically to steal and exfiltrate data from POS systems, although some malware samples also appeared in general purpose computers in those environments.

MALWARE FAMILIES ENCOUNTERED THROUGH DATA COMPROMISE INVESTIGATIONS





POSEIDON

Trustwave encountered malware family PoSeidon, which infects POS systems and exfiltrates card data, most often during data compromise investigations in 2016. PoSeidon is predominantly a memory scraper, a program that searches the computer's memory for data sequences that match patterns, such as a credit card number. POS terminals and other computers usually encrypt payment card data when storing and transmitting it, so attackers often use scrapers to locate card numbers in memory before encryption or after decryption for processing. PoSeidon's memory scraper component includes a keylogger capable of collecting operator credentials on the infected system. The component automatically transmits potentially valuable data to an attacker-controlled server via HTTP POST. PoSeidon has been around for several years, and its authors continually add new functionality. In 2016, they added two significant features: a privilege escalation exploit that attempts to give the malware more access on the target system and a monitor process that ensures PoSeidon remains installed and running on the infected system.

ALINA

One of the oldest POS-focused malware families still active, Alina made a resurgence in 2016 after largely fading from view the year before. Alina is also a memory scraper with command-and-control (C&C) features that exfiltrate data using HTTP POST and simple XOR encryption to deter casual monitoring. Alina is so popular many malware authors simply create variants of the family rather than re-invent the wheel. Spark, an Alina variant, installs itself via an Autoit script and has an expanded blacklist of processes to avoid when scraping memory for payment card data.

CARBANAK/ANUNAK

Also near the top of the 2016 list is a collection of related malware variants associated with Carbanak, a prolific crime group considered synonymous with the Anunak crime group that reportedly stole more than \$1 billion from banks in 2015. In 2016, Carbanak orchestrated an attack on a support website for a major POS vendor that put more than one million POS systems at risk. The Carbanak/Anunak malware often pops up during Trustwave investigations, and researchers increasingly see it targeting the hospitality industry. A memory scraper like PoSeidon and Alina, Carbanak/Anunak also includes features such as remote desktop functionality and the ability to steal passwords.

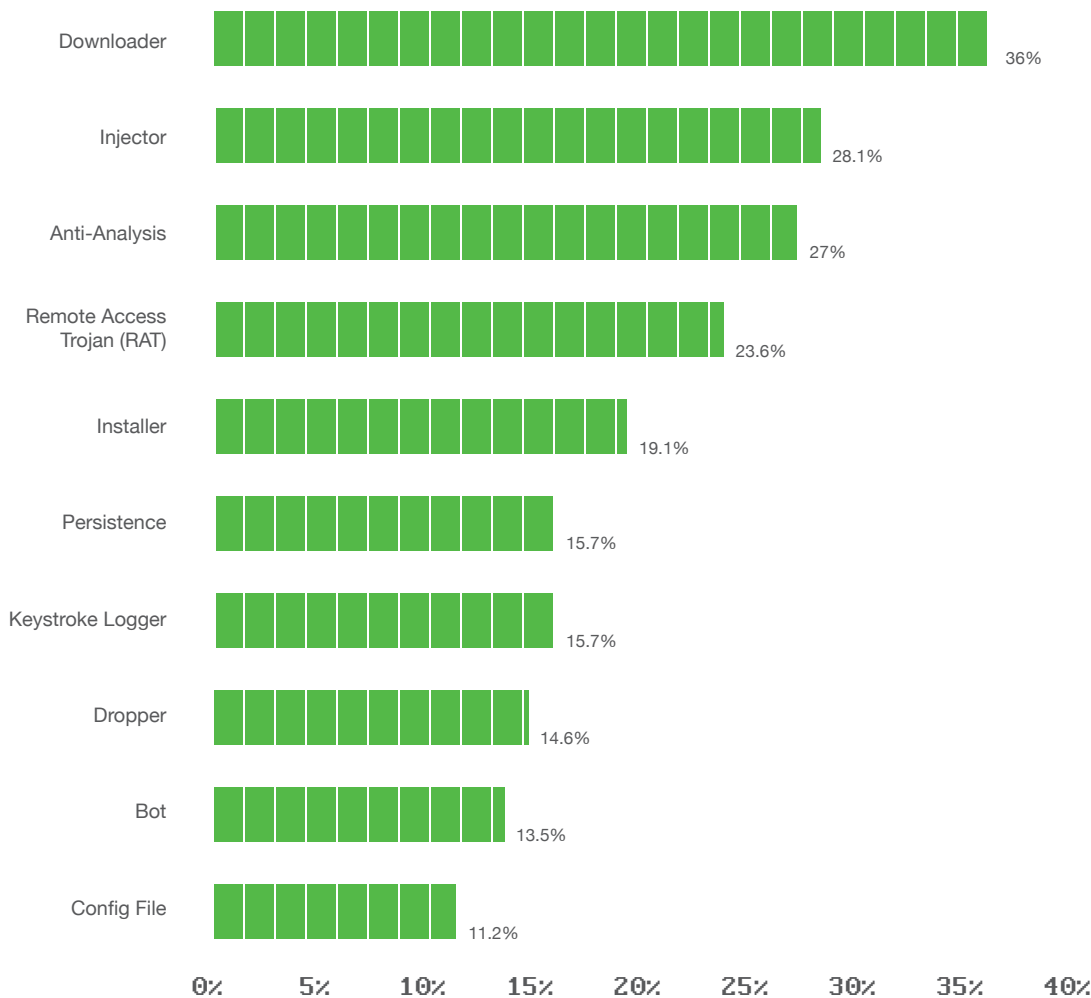
CRYPTXXX

Part of the ransomware family, CryptXXX is an example of a highly malignant new breed of malware that encrypts important files on the infected computer and demands the victim pay for the decryption key. Given the skyrocketing popularity of ransomware in the cybercriminal underground, it's not surprising to find it among the top malware families Trustwave encountered in 2016. Authors updated CryptXXX several times in recent months to correct flaws enabling security researchers to create decryption tools that allowed victims to recover their files without paying the ransom.



MALWARE FUNCTIONALITY

TOP FEATURES OF MALWARE ENCOUNTERED DURING INVESTIGATIONS



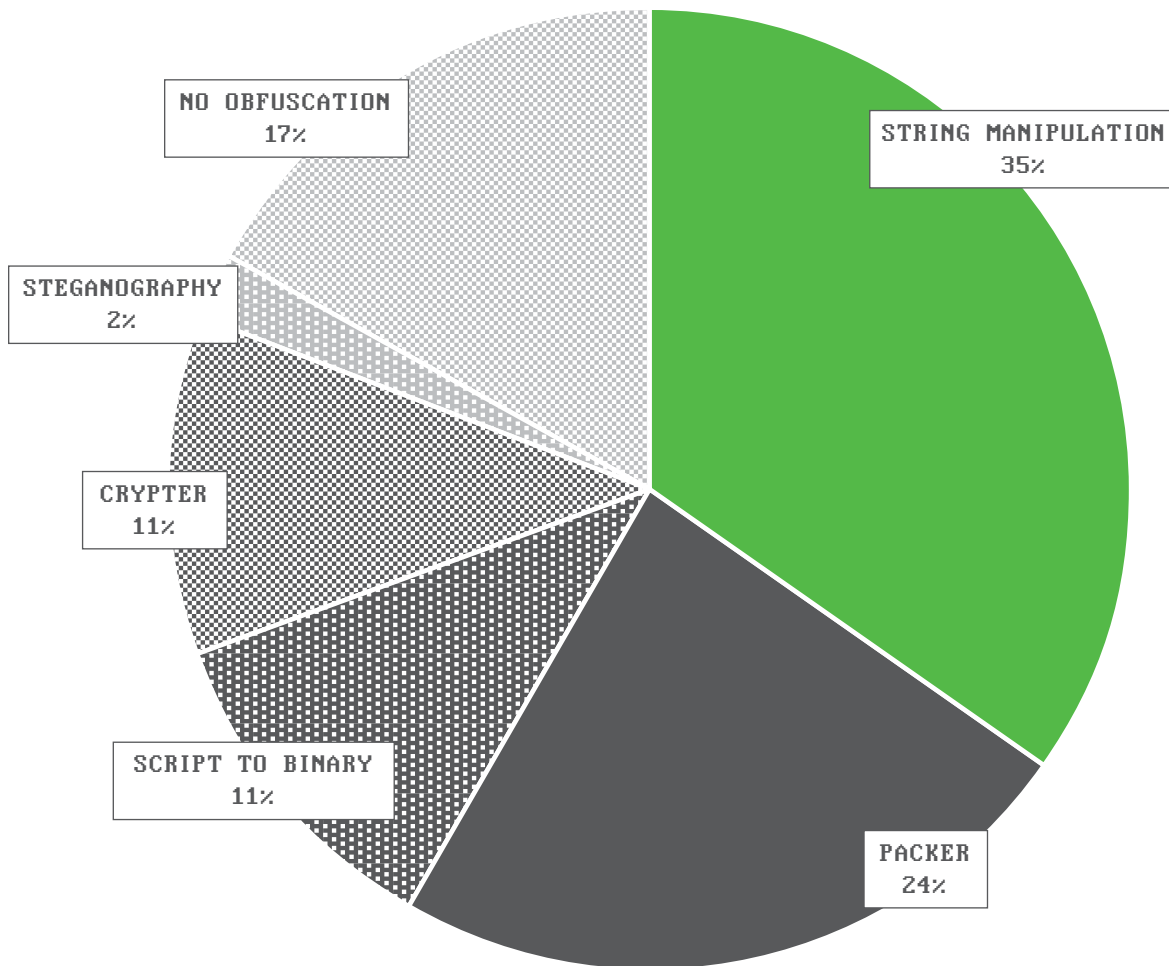
Many malware families have multiple features providing not only revenue-generating functionality, like memory scraping or ransomware, but also utility functions that help them install, spread, escape detection and others. About 36 percent of the malware Trustwave encountered included downloader functionality, allowing it to download additional malware or other files from a remote server under the attacker’s control. Significant percentages of the malware examined included various other anti-analysis features, including process injection functionality, which enables the malware to hide itself within another process running on the system, and/or remote administration (RAT) functionality giving the attacker a back door into the infected system.

MALWARE OBFUSCATION AND ENCRYPTION

Malware developers often use obfuscation and encryption techniques to avoid detection by security tools and personnel. In general, malware authors use obfuscation to attempt to hide the true nature of their code’s functionality from security tools. They use encryption to hide the data they save to disk and/or send outside the victim’s network so monitoring controls will not flag the data or related communications.

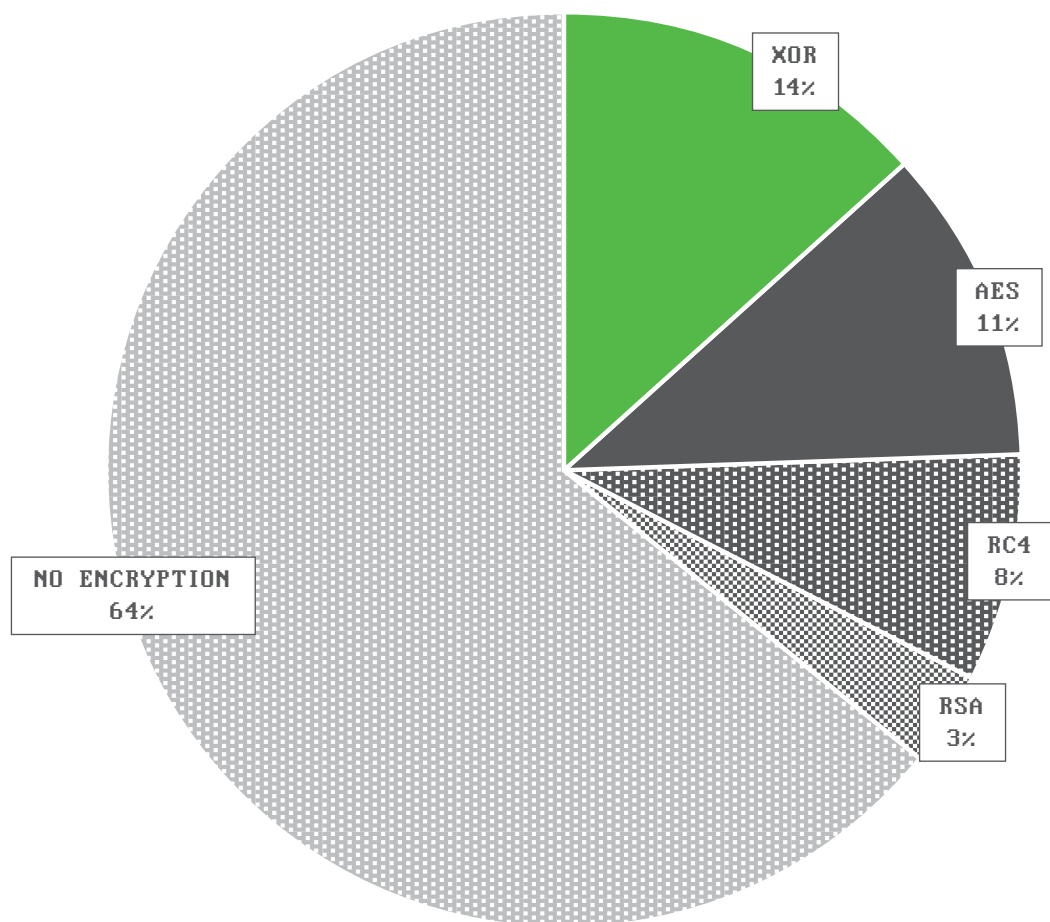


METHODS OF OBFUSCATION



More than 80 percent of the malware samples Trustwave obtained during 2016 investigations employed some form of obfuscation. The most common technique was string manipulation, which uses simple functions and escape sequences to render parts of the code unrecognizable until it is de-obfuscated. Next was packing, which involves an executable packing tool such as UPX that compresses or otherwise modifies a file for distribution. Malware obfuscated using crypters, which combine multiple encryption and obfuscation techniques, comprised about 11 percent of samples, as did scripts formatted as binary files to deter text scanners. A small percent of samples used steganographic techniques to hide information inside other media, such as an image file in which the least significant bits manipulated to contain a malicious script.

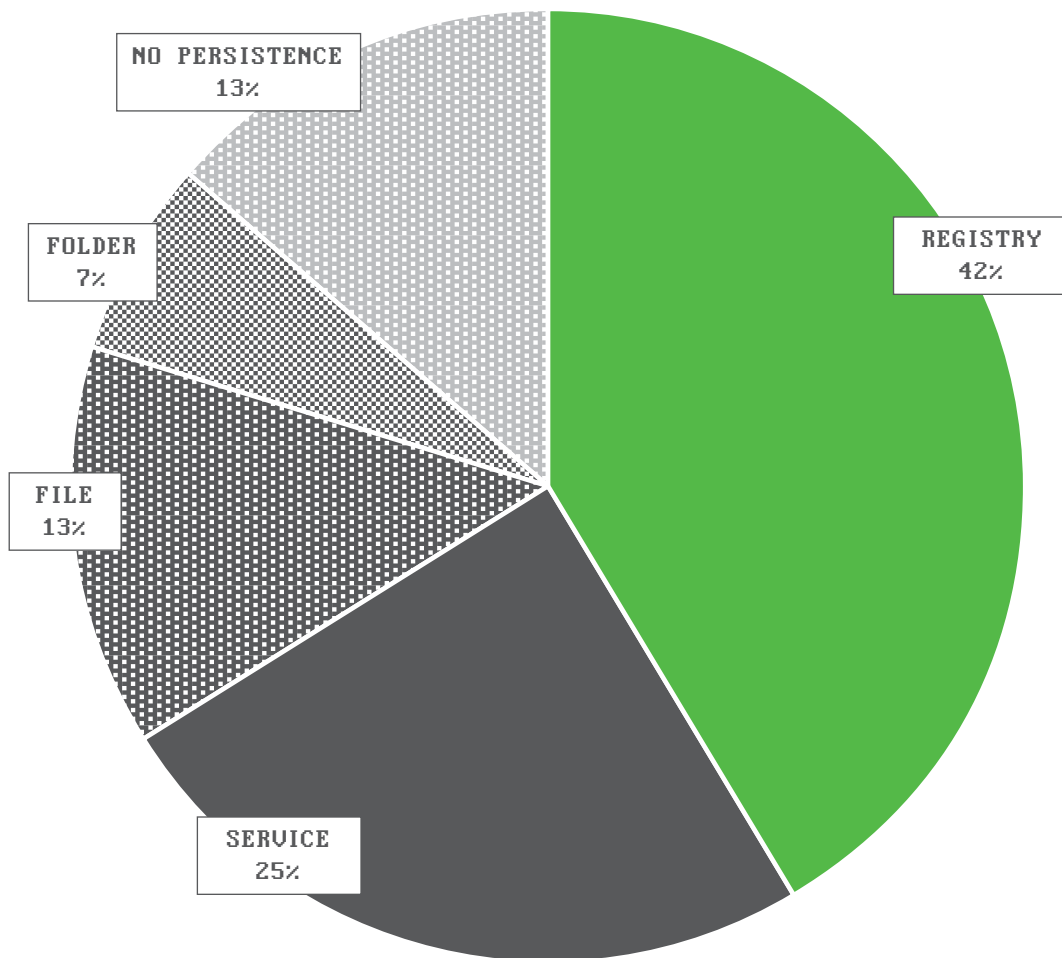
METHODS OF ENCRYPTION



By contrast, only 36 percent of the samples Trustwave investigated used encryption. The most common encryption method employed was XOR, which involves selectively manipulating the bits of a stream by comparing them to the bits of a repeating key. Reapplying the key to the encrypted stream decrypts it. Significant percentages of samples used AES and RC4, which are more advanced encryption methods.

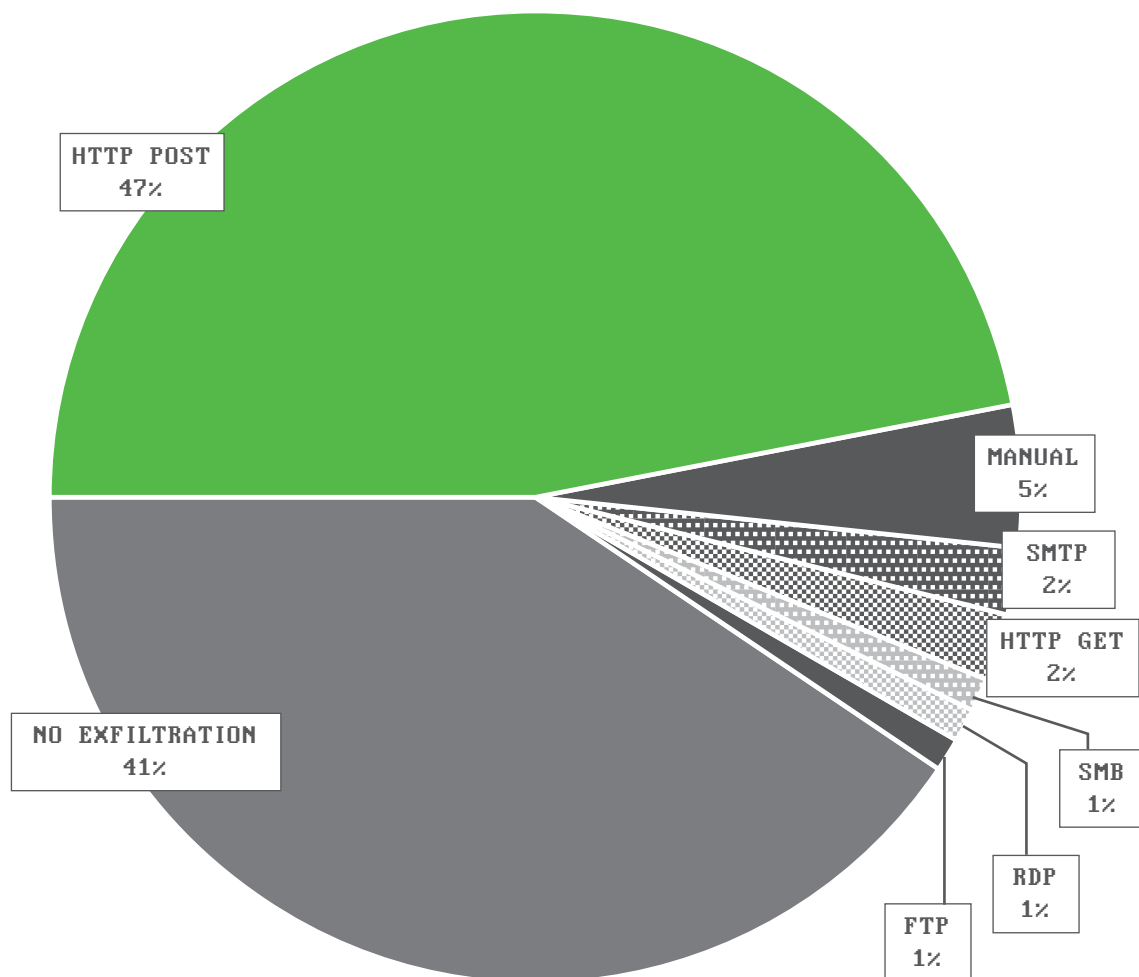
MALWARE PERSISTENCE

METHODS OF PERSISTENCE

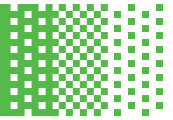


Eighty-seven percent of the samples Trustwave investigated used techniques to ensure malware execution every time the computer reboots. Nearly half of the samples that persisted did so by adding or changing entries in the Windows registry, such as the Run key that contains lists of programs that start automatically. The second most common technique was creating a service and setting its start type to “Automatic”.

MALWARE EXFILTRATION METHODS OF EXFILTRATION



Forty-one percent of the malware encountered did not use an exfiltration method because exfiltration can provide a trail that might help investigators identify the malware source. In these cases, the attacker typically connects to the computer remotely to exfiltrate the data. In other cases, another malware component handles exfiltration. Of the samples that did exfiltrate, most used HTTP POST to connect to an attacker-controlled remote server, the method used by the PoSeidon and Alina families of POS malware.



MEMORY RESIDENT MALWARE

Malware no longer resides on disk where an unknown binary sits in the %userprofile% of the local admin account. Neither can cyber security professionals simply search for a given SHA-1 (secure hash algorithm 1) across the environment. These methods locate old malware. Today's advanced malware generally does not reside on disk – it lives only in memory. If an attacker finds an infiltration vector and then drops malware, why not generate persistence by re-infiltrating and dropping again? Because persistence creates an artifact on disk. But re-exploiting a vulnerability overlooked the first go around could mean the victim will overlook it the second, third and fourth time and so on. Most likely, it will take advanced detection capabilities for the victim to discover the breach.

It is common for attackers to use pre-built malware purchased from the criminal underground. The attacker can then copy this malware and make a small change to inject it differently or exfiltrate data on a different port. This is one reason many variants of known malware are prevalent. Memory resident malware is very common to find now that it is out in the wild.

PoSeidon, which cybercriminals use to attack point-of-sale systems (POS), is a good example of the status of successful malware and of what's next. The PoSeidon binary is a simple injector into svchost.exe. The injector still resides on disk, but the credit card scraping malware only lives in memory. This will change as artifacts on disk disappear and criminals begin using a copy of the PoSeidon tactics. They will achieve persistence by re-infecting and injecting malware into another process' memory space all in one step.

Memory analysis is the only way to obtain a sample of this malware. The Trustwave SpiderLabs incident response team assists customers in memory acquisition, analysis and reporting so our malware experts can reverse engineer the malware and contain and remediate the infiltration vector.



SUSPICIOUS TRAFFIC AND ALERTS

Monitoring suspicious activity into, out of and within a network provides an important first line of defense against attack. The data in this section comes from Trustwave's sample of more than 10,000 firewall, network and host IDS alerts from customers in the Asia-Pacific region. Most of these alerts involved suspicious inbound or outbound traffic, while a small percentage involved suspicious behavior on a local computer.

RECONNAISSANCE

Most of the IDS alert data security researchers reviewed concerned network reconnaissance activity — typically scans or probes of public-facing systems from elsewhere on the internet using network discovery tools such as NMAP and MASSCAN. While reconnaissance alerts usually fill logs and filter out of security analyst's consoles, they can provide early warning of a targeted attack. Correlating the source or destination of reconnaissance with actual attacks should provide analysts insight and focus for when reconnaissance escalates to exploitation.

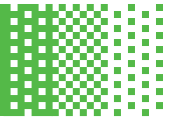
TOP FIVE RECONNAISSANCE ALERTS IN 2016

DESCRIPTION	PERCENT OF ALL ALERTS
Pass after Repetitive Blocks	22.57%
Attack from Source Having Reconnaissance History	0.50%
Malicious / VA Scanning	0.17%
Network Port Scan	0.04%
Blacklist: Known Scanning Tool	0.02%

The most common alert type Trustwave examined involved IP addresses that repeatedly failed to access systems behind a firewall before succeeding, commonly indicating automated scanners that probe multiple ports looking for potential avenues of attack. For example, a port scanner testing a web server might try connecting to common ports like 22 (SSH) and 25 (email) unsuccessfully before successfully connecting to port 80 (HTTP). Other reconnaissance alerts include scans from sources with a history of performing reconnaissance activity, scans for known vulnerabilities and network requests characteristic of known scanning tools.

AUDITING FOR UNUSUAL ACTIVITY

Many alerts show the benefits of security controls used for monitoring unusual activity. Such activity is not always malicious as repeated login failures for an administrative account may be a sign of a brute-force attack or indicate a forgotten password. However, such alerts do provide security analysts with information that can indicate a compromise is occurring or already occurred.



TOP FIVE UNUSUAL ACTIVITY ALERTS IN 2016

DESCRIPTION	PERCENT OF ALL ALERTS
File Modification Detected	2.50%
Potential Malicious Firewall Traffic (Outbound)	2.15%
Attempt to Execute Privileged Operation	1.62%
Failed Login Attempts Core Network Device	0.92%
Administrative User Failing Login Multiple Times in 5 Minutes	0.60%

The most common unauthorized activity alerts in 2016 involved suspicious file modifications and potentially malicious outbound traffic, which usually suggests a compromised system attempting to contact an attacker. Attempts to execute highly privileged operations from less-privileged accounts or security contexts also represented a significant portion of unusual activity alerts.

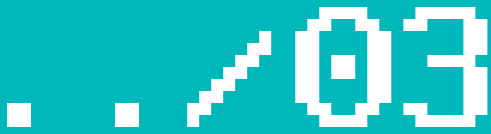
DATABASE ALERTS

Databases frequently contain the most valuable data on enterprise networks; so, organizations should take seriously alerts suggesting possible database intrusion attempts. This is especially true for databases behind web-based front ends, like e-commerce sites, which cybercriminals sometimes can access directly through a web page.

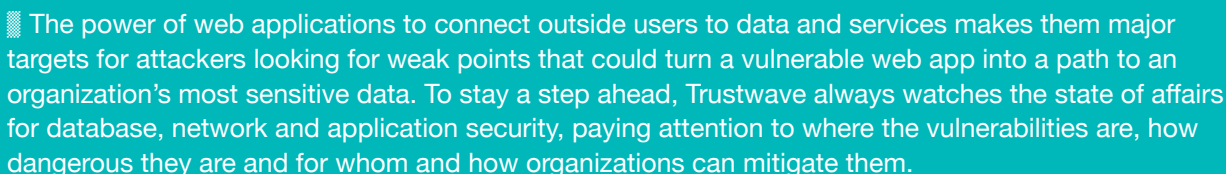
TOP FIVE DATABASE ALERTS IN 2016

DESCRIPTION	PERCENT OF ALL ALERTS
Database Large Query Response Size	1.39%
Excessive Attempts of Database Login	1.36%
Extremely Long SQL Request	0.97%
Unauthorized Database User	0.59%
SQL Injection	0.45%

Database queries that returned large responses comprised the biggest share of database alerts in 2016. While such queries can be legitimate, they may also denote an attempt to steal large amounts of data. Repeated unsuccessful attempts to log in to a database was the second most common class of database alerts followed by extremely long SQL requests, which can indicate a potential attempt at SQL injection.



THE STATE OF SECURITY



Trustwave's analysis of database security discovered a large increase in the number of security patches released for five of the most common database products. This is good in the sense that vendors remain vigilant about plugging holes where they arise; however, more known vulnerabilities mean more potential avenues for attack. In looking at network security, analysts found vulnerable SSL and TLS deployments remain too common, despite industry mandates, and that new proof-of-concept exploits published in 2016 make it essential that organizations secure their SSL infrastructures. In application security, Trustwave's application scanning and penetration testing services revealed all but a tiny fraction of the applications tested had at least one vulnerability. In addition, one expert looks at threat hunting; what it is, what it isn't and how organizations can use it to improve protections.

DATABASE SECURITY

Most common web applications use database management systems (DBMS) on the back end. Like the applications themselves, databases can have vulnerabilities that, under the right conditions, attackers can exploit to steal or damage sensitive information or gain control of the underlying operating systems. Databases hold a treasure trove of assets that is growing as digital information grows at record rates. Examining the patched vulnerabilities in several of the more frequently used database systems provides insight into the state of database security in 2016.

Some of the more common vulnerabilities found in databases fall into the following categories:

- **Privilege escalation flaws:** These vulnerabilities allow an unprivileged, or low-privileged, user to gain administrator-level read and/or write access to tables or configuration settings.
- **Buffer overflow vulnerabilities:** An attacker exploiting buffer overflow vulnerabilities can crash the database server and cause a denial-of-service (DoS) condition or, in some cases, even execute arbitrary code.
- **Advanced unused features:** Features, such as reporting services or third-party extensions can leave a database vulnerable even if the flaw is not in the core DBMS service or in other essential components.
- **Default credentials:** Allowing default credentials presents an opportunity for abuse by attackers. Trustwave penetration testing engagements often find default administrator-level accounts with default passwords.

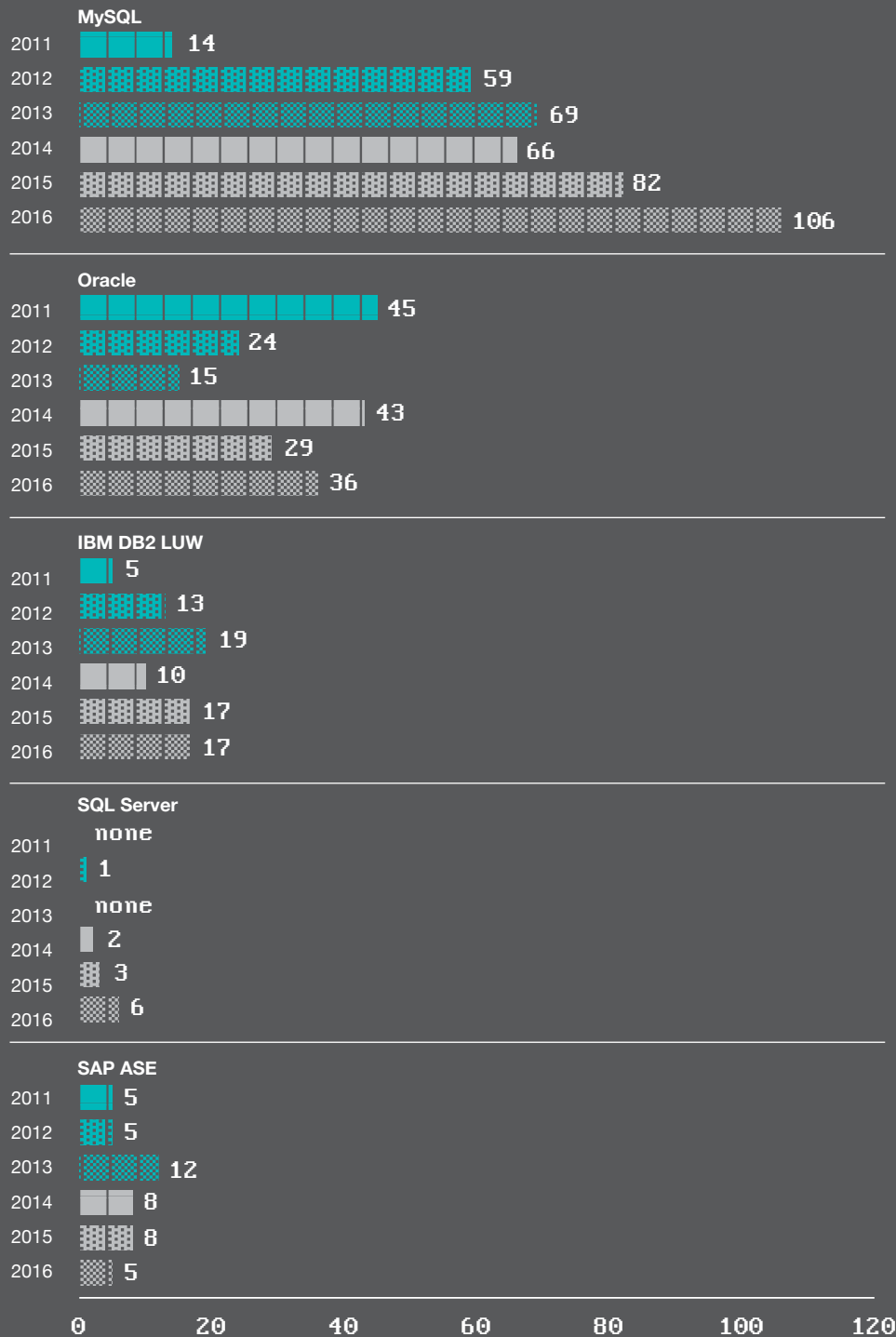
DATABASE PATCHING, 2011-2016

For the fifth consecutive year, MySQL patched the largest number of vulnerabilities (106) of any of the five database products Trustwave examined in 2016. That number exceeds those patched each year for all five database products in 2011 and 2012. Having numerous vulnerabilities disclosed and fixed does not necessarily mean a product is less secure than a comparable product with fewer known vulnerabilities. Usually the amount of time and effort researchers and other experts expend trying to find vulnerabilities in each product influences the number disclosed.

Of the five broadly used databases discussed in this section, MySQL is the only one with an open-source license. It also 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 attackers will find a given vulnerability. This not only provides more opportunity for exploitation but it also means the product becomes safer as researchers find and fix the vulnerabilities. By contrast, independent researchers must use techniques like fuzz testing to locate vulnerabilities in closed-source software, which makes them harder to find. Moreover, security professionals may never identify and disclose some security vulnerabilities in proprietary software because developers might take care of them as part of the normal testing process with the fix rolling out as part of a routine maintenance release.

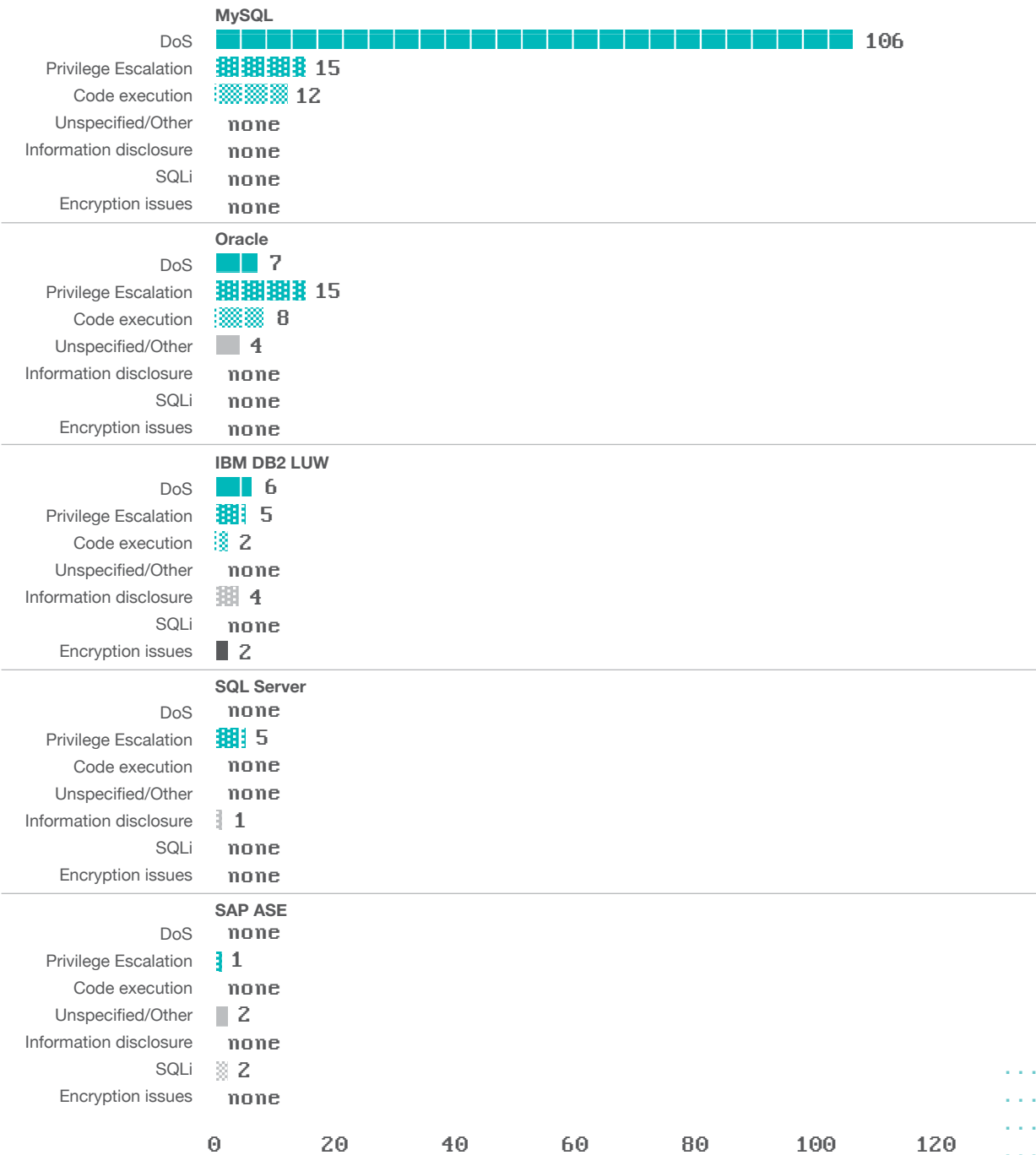
Oracle Database received the second largest number of patches in 2016 with 36, more than received in 2015 but less than in 2014. IBM DB2 and Microsoft SQL Server received 17 and 6 patches, respectively, with SAP's Adaptive Server Enterprise (ASE), also known as Sybase, bringing up the rear with five vulnerability patches in 2016.

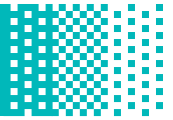
DATABASE VULNERABILITIES PATCHED, 2011-2016



DATABASE PATCHING BY VULNERABILITY TYPE

Trustwave analyzed the issues fixed in the five database products that received security patches in 2016 and categorized them into classes of vulnerabilities per product. In most cases, the totals for each database exceed the overall 2015 count because some vulnerabilities fall into more than one category; therefore, researchers count them multiple times.





DoS vulnerabilities represented the largest number of vulnerabilities patched, with MySQL responsible for most of them. 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 an attacker to read or alter the contents of the database. In part, the preponderance of DoS vulnerabilities in MySQL is due to modern compiler-level defense techniques that mitigate the effectiveness of exploit techniques such as buffer overflow attacks. So, many exploits that would otherwise allow code execution or information disclosure are instead limited to denial of service.

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 to which they're not entitled. Even if the user encrypts the data, an attacker may be able to execute functions not available to unprivileged users, which can include destroying data. Sometimes privilege escalation is the result of SQL injection targeting stored procedures or some other built-in database functionality. In one case uncovered by Trustwave researchers, a vulnerability in SAP ASE 16.0 enabled a malicious database owner to grant themselves system administrator status by altering a stored procedure via the syscomments table, thereby giving them access to all databases on the same server. Trustwave disclosed the vulnerability to SAP, which subsequently patched the vulnerability.

Vulnerabilities allowing an attacker to execute malicious code are quite serious. In the past, these vulnerabilities typically took the form of buffer overflows, wherein an attacker fed the system an input larger than the area of memory designated to hold it and thereby gained access to an adjacent area of memory designated for code execution. Newly disclosed buffer overflow vulnerabilities are less common today, but attackers are replacing them with vulnerabilities that take advantage of other memory corruption techniques, such as virtual function pointer abuse.

DATABASE CHANGES AND MILESTONES

Microsoft SQL Server: Microsoft released SQL Server 2016 on June 1, 2016. Security enhancements added to this latest version include row-level security, dynamic data masking, AES encryption for endpoints and more.

Extended support for SQL Server 2005 Service Pack 4, the final service pack for the platform, ended in April 2016. Mainstream support for SQL Server 2012 Enterprise Core and SQL Server 2012 Service Pack 3 ends on July 11, 2017; although, extended support will remain available.

IBM DB2: IBM released DB2 Version 11.1 for Linux, Unix and Windows (LUW) in June 2016. It includes several security enhancements in areas such as native encryption, key management and hardware encryption acceleration.

Since the end of 2015, IBM issued new fix packs for DB2 LUW 10.5 — Fix Pack 7 on December 30, 2015, and Fix Pack 8 on September 15, 2016.

Support for DB2 LUW 9.7 and 10.1 will end September 30, 2017.



NETWORK SECURITY

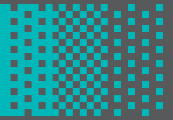
Trustwave’s internal and external network vulnerability scanning systems, which inspect servers for insecure configurations that could increase the risk of attack, provide insight into the most frequent network vulnerabilities. This year, analysts supplemented the data with exploit information gathered from external sources for some of our scan findings.

The figures listed in the tables below indicate the percentage of detections the Trustwave scanner attributed to that vulnerability. For example, 6.01 percent of the vulnerability detections recorded in 2016 are from the “TLSv1.0 Supported” vulnerability.

TOP FIVE SECURITY FINDINGS BY OCCURRENCE

Occurrence	Name
6.01%	TLSv1.0 Supported
2.59%	No X-FRAME-OPTIONS Header
2.53%	SSL/TLS Weak Encryption Algorithms
1.51%	SSLv3 Supported / SSL version 3 protocol padding-oracle attack (POODLE)
0.62%	SSL Certificate Public Key Too Small

As in 2015, four of the five vulnerabilities Trustwave’s network vulnerability scanning systems detected resulted from insecure server configurations for Secure Socket Layer (SSL) and Transport Layer Security (TLS), which underlie most of the secure client/server communication on the internet.



SSL/TLS SECURITY: AN INCOMPLETE JOURNEY

The Payment Card Industry Data Security Standard (PCI DSS) originally mandated that by 2016 companies and organizations that handle credit and debit cards could no longer support the insecure SSL 3.0 and TLS 1.0 protocols. In December 2015, however, the PCI Security Standards Council (PCI SSC) extended the deadline to June 30, 2018, giving processors more time to come into full compliance. When analyzing the top vulnerabilities by occurrence, Trustwave found that in 2016 support for TLS 1.0 topped the list, accounting for 6 percent of detected vulnerabilities. Support for SSL 3.0 was significantly lower but still comprised about 1.5 percent of detected vulnerabilities.

These protocols are vulnerable to an exploit, discovered in 2014, that researchers dubbed Padding Oracle on Downgraded Legacy Encryption, or POODLE. A successful exploit enables a man-in-the-middle attacker to capture a session cookie and hijack the encrypted session. The original POODLE exploit targeted SSL 3.0, an old and seldom-used protocol many browser vendors continued to support for backward compatibility reasons. A variant of the POODLE attack that affects TLS 1.0 and 1.1 came about a few months later. TLS 1.2 is not vulnerable to POODLE attacks.

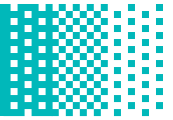
If secure protocols are available, some may wonder why servers still support the older, insecure protocols. Until recently, one stumbling block was a relative lack of support for TLS 1.2 by the major browsers, most of which did not provide support for TLS 1.2 until 2013 or 2014. The mobile space poses a particular problem. At the end of 2016, nearly 40 percent of Android devices continued running operating system versions that don't enable TLS 1.2 by default; although, many or most of those devices probably run web browsers and apps that do. In the era of quick, automatic software updates on desktop and mobile devices, however, the justification for maintaining TLS 1.0 as an option for negotiation in 2017 is weak.

The case for maintaining support for SSL 3.0 is weaker still. Browsers have been supporting TLS for more than a decade, and the major desktop and mobile web browsers currently disable support for SSL by default or have removed it entirely. Because a successful POODLE attack depends on the attacker's ability to force a server to downgrade to an insecure protocol during the handshake phase, maintaining support for such protocols introduces a significant vulnerability to a server even if few or no clients would ordinarily request them. While Trustwave certainly encourages payment card processors and everyone else to upgrade to TLS 1.2 as quickly as is feasible despite the extended grace period the PCI SSC offered, it's difficult to imagine why anyone would still be supporting SSL 3.0 and earlier protocols.

TOP VULNERABILITIES RELEASED IN 2016 BY OCCURRENCE

The list of the top vulnerabilities Trustwave encountered in 2016 includes a few named “celebrity” vulnerabilities, though fewer of them than in past years. For this section, researchers also analyzed exploit information available from external sources to review the number of detections with freely available exploits.

OCCURRENCE	CVE IDENTIFIER	DATE RELEASED	DESCRIPTION
0.39%	CVE-2016-2183	August 2016	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack, known as Sweet32
0.16%	CVE-2016-0800	March 2016	Cross-protocol attack on TLS using SSLv2: DROWN (Decrypting RSA using Obsolete and Weakened Encryption)
0.05%	CVE-2016-3115	March 2016	X11 forwarding data allows multiple CRLF injection in OpenSSH before 7.2p2
0.05%	CVE-2016-1907	January 2016	OpenSSH before 7.1p2 allows for Denial of Service via crafted network traffic
0.04%	CVE-2016-0777	January 2016	OpenSSH allows for the transmission of the entire buffer to remote servers before 7.1p2



DROWNING SWEETLY WITH BANANA AND BACON

The most common new vulnerability detected in 2016 involved servers supporting the use of block cipher algorithms with 64-bit block sizes in HTTPS or other security protocols, which are vulnerable to Sweet32, a proof-of-concept attack published in 2016. Sweet32 is a “birthday attack” that can enable a successful criminal to recover HTTPS cookies by monitoring traffic encrypted using algorithms that include the widely implemented Triple DES cipher. As its discoverers documented, Sweet32 is not a practical exploit. A successful attack requires monitoring and capturing hundreds of gigabytes of encrypted traffic in a single session, but the fact that the majority of HTTPS servers support Triple DES makes it worthy of note.

The SSL/TLS vulnerability dubbed DROWN (“Decrypting RSA with Obsolete and Weakened eNcryption”) was ranked second in occurrences in 2016. DROWN is a cross-protocol attack that abuses SSL 2.0 to attack TLS. The attack works against every known SSL/TLS implementation supporting SSL 2.0 and criminals can use it more efficiently against OpenSSL because of additional flaws discovered in the OpenSSL library.

By gathering exploit information from external sources, Trustwave analysts determined that almost 9 percent of CVEs added to the network scanner in 2015/2016 had publicly available exploits. The OpenSSH vulnerability (CVE-2016-3115), listed in the top five occurrences for 2016, was one of them.

Though they didn’t make the list, other notable detections added to the network scanner in 2016 were Cisco ASA signatures for the EPICBANANA (CVE-2016-6367) and EXTRABACON (CVE-2016-6366), exploits an attacker or group called the Shadow Brokers publicly disclosed in August 2016. Researchers rated the EXTRABACON vulnerability as high because it could allow RCE on affected devices and obtain full control.

The Dirty Cow vulnerability (CVE-2016-5195), discovered in October 2016, also attracted Trustwave’s attention. So named because it exploits a mechanism called copy-on-write, Dirty Cow is a serious privilege escalation bug in the Linux kernel that has existed since 2007 and is relatively easy to exploit. The vulnerability allows the attacker to bypass the normal file system protections and write to files the system owns. This opens numerous avenues for attack, resulting in the unprivileged user gaining root privileges and the ability to access system resources.



THREAT HUNTING

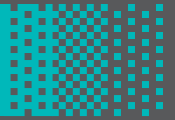
Threat hunting is not taking the latest and greatest threat feeds from as many vendors as possible and using those indicators to scan your network. It isn't about searching for metasploit or psexec or other tools attackers can use. That's scanning.

Threat hunting is about understanding your organization's environment and baselining continuously. In a way, it's the precursor to scanning. It's about creating the signatures for use in a scan.

To effectively threat hunt, it is important to understand how people and systems work by asking "why" and "how" about everything. For example, how does the HR department share resumés of potential employees? How does the IT team push updates to endpoints? What software does the support department need to manage the company's customers, and how does the organization use that software?

Once analysts understand the environment, they can start gathering data and using analytics to measure activity. The quality of the data gathered plays a big part in determining how successful the threat hunting will be. Collecting all data would be ideal, but the sheer volume of data produced makes it unwieldy. Data is not very useful unless it's storable, searchable and repeatable. So instead, IT professionals specialize. They get all the local admin accounts, domain admin accounts, type-10 events for 4624 logins, services created in the last hour and so on.

Once they have the data, they need people to interpret it and separate the wheat from the chaff. Most of the data will be noise. That's where the hunting starts. The security analyst sifts through the data to find the one 4624 type-10 that doesn't fit the rest. Those who know what they're doing will know an attacker is creating a service that shouldn't be in their environment though other environments might want this so-called service. One such example is psexec.



As more data comes in, people become more knowledgeable about their own environment, and that's how threat hunting grows. Start using open-source and cookie-cutter tools, then customize them to better narrow down the data and get the answers you're looking for. Eventually, your organization will reach a phase in which all your tools, managed or not, are customized for the environment.

Verbose data will help an inexperienced analyst and an experienced analyst who cannot do the job with little data. This is where Trustwave can be a major help in this field. The data collection capabilities and highly skilled people at Trustwave are already in place, all that's left is customizing the tooling for a customer environment.

Threat hunting
is about
understanding
your
organization's
environment
and baselining
continuously



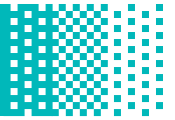
APPLICATION SECURITY

Trustwave's application scanning and testing services analyze thousands of applications each year for a wide range of vulnerabilities. Unfortunately, truly secure web applications are rare. For the last several years, security analysts uncovered vulnerabilities running the gamut from mostly harmless to potentially devastating in most of the applications tested. The situation in 2016 was no different. Higher than in the three previous years, 99.7 percent of tested applications displayed at least one vulnerability.

VULNERABLE APPLICATIONS



At the same time, the median number of vulnerabilities detected per application dropped to 11 in 2016 from 14 in 2015. The largest number of vulnerabilities found in a single application was 1,267.



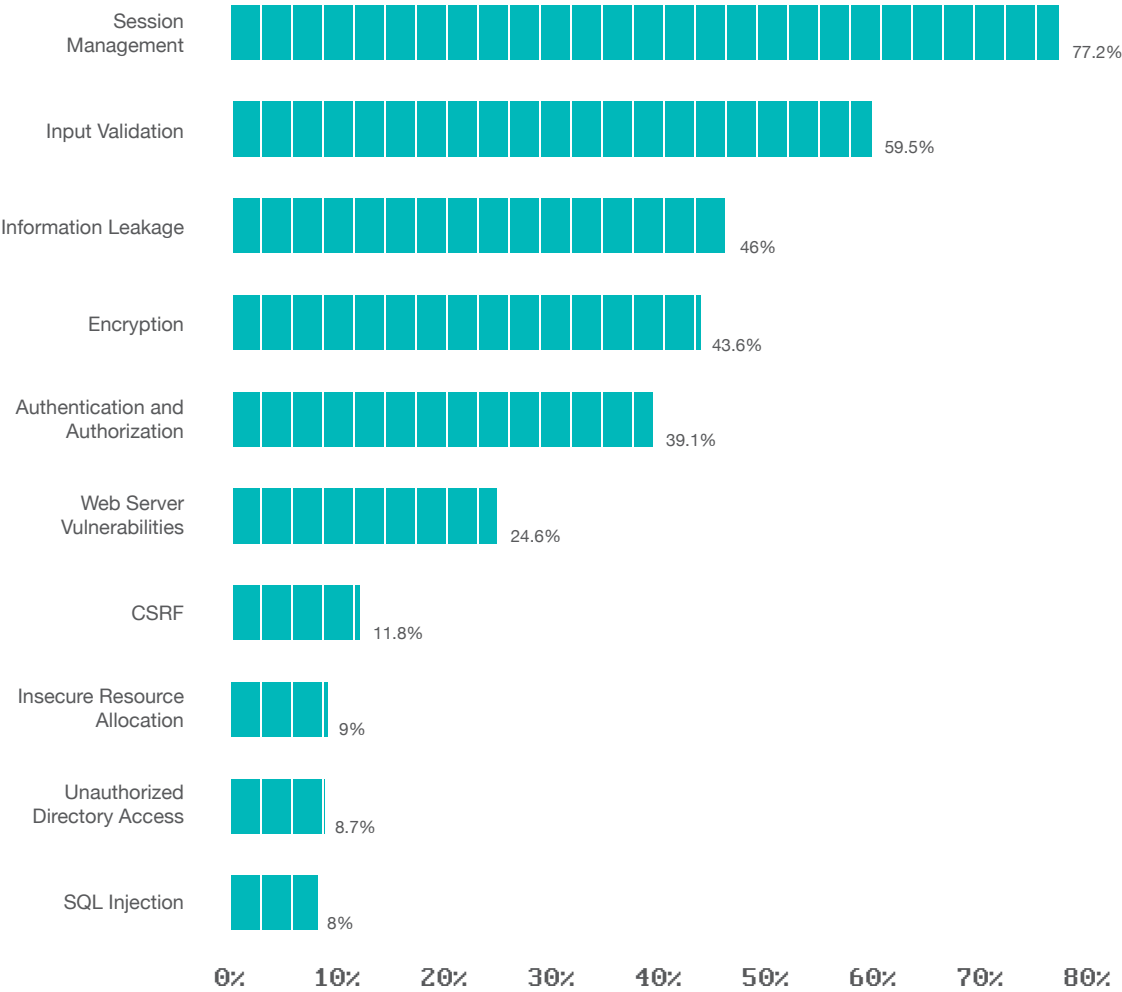
MEDIAN VULNERABILITIES PER APP

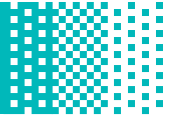


99.7%

of tested applications
displayed at least one
vulnerability

APPLICATION VULNERABILITY CATEGORIES





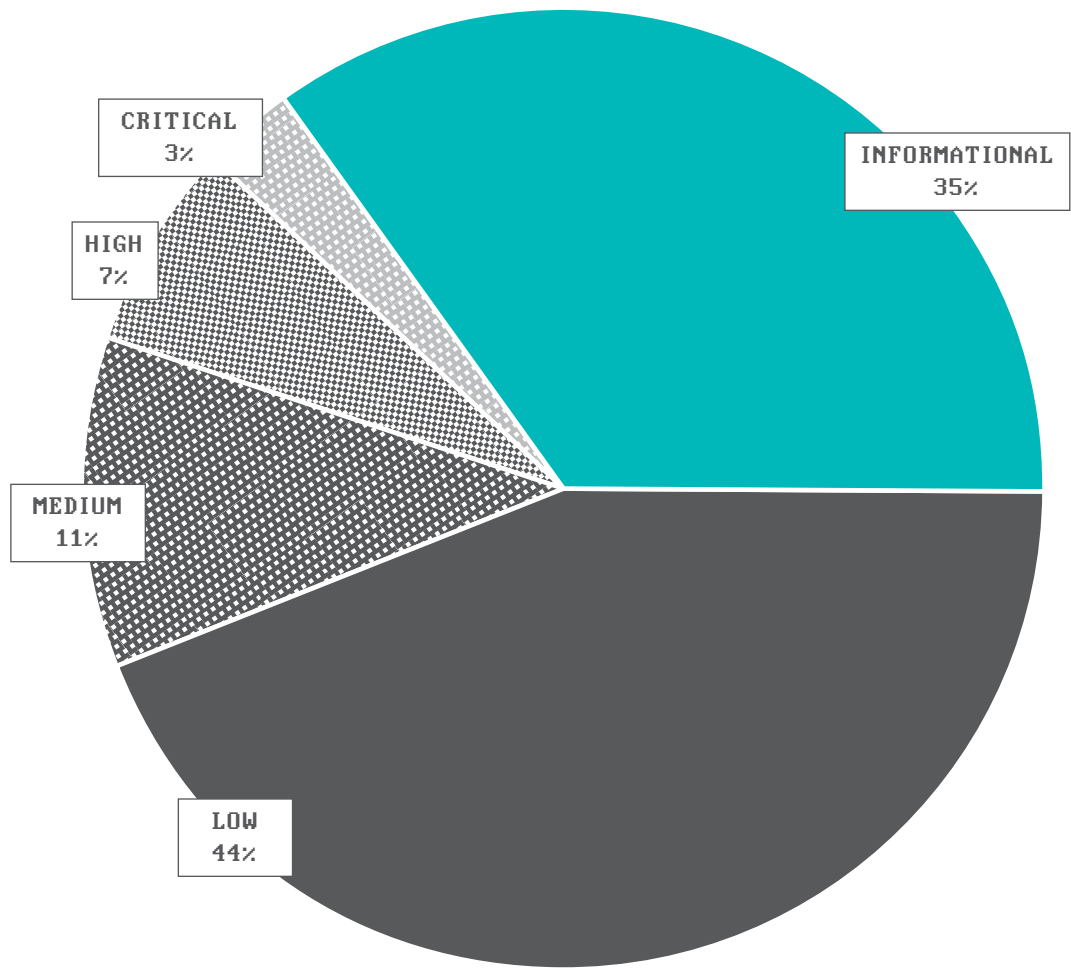
Trustwave found vulnerabilities related to session management in 77 percent of the applications analysts tested in 2016, making session management the most common category of vulnerabilities examined. This type of vulnerability can allow an attacker to take over or eavesdrop on a user session, placing sensitive information at risk. Most of the session management vulnerabilities identified involved improper handling of HTTP cookies, used to preserve state across inherently stateless web connections. Cookies are an integral part of almost all web applications, and Trustwave consistently finds cookie handling vulnerabilities. Sixty-nine percent of the applications examined in 2016 displayed one or more such vulnerabilities, which, in some cases, can expose session tokens, authentication information or other sensitive information that can facilitate session hijacking if compromised.

Vulnerabilities related to improper or inadequate validation and sanitization of user input affected 60 percent of the applications. Cross-site scripting (XSS) vulnerabilities comprised 27 percent of applications tested, the largest subset of the vulnerabilities. An XSS attack allows a cybercriminal to relay malicious scripts from an otherwise trusted URL to compromise information maintained within the victim's browser. Another significant subset of applications failed to encode browser output to safely filter entities like HTML tags, which can facilitate XSS and similar attacks.

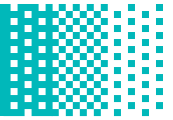
Information leakage vulnerabilities were present in 46 percent of applications tested. These vulnerabilities can directly expose sensitive data to unauthorized visitors, making them potentially treacherous. Application exceptions that disclose details about the web server, application or environment accounted for the largest single subset of these vulnerabilities. An attacker can sometimes take advantage of these vulnerabilities by deliberately creating an error condition that reveals details that may aid in further exploitation.



APPLICATION VULNERABILITY RISK LEVELS



Trustwave Managed Security Testing, Trustwave's on-demand penetration testing service, uncovered almost 30,000 vulnerabilities in web applications in 2016. Analysts classified 79 percent of them as informational or low-risk vulnerabilities, 11 percent as medium-risk, 7 percent as high-risk and 3 percent as critical, the most severe category.



TOP 10 CRITICAL VULNERABILITIES IDENTIFIED THROUGH PEN TESTING

VULNERABILITY	PERCENT OF CRITICAL VULNERABILITIES
Authentication Bypass	13.8%
JBoss Administrative Console Access	5.9%
NetBIOS Name Service Poisoning	5.9%
Heartbleed OpenSSL Memory Leakage	5.7%
Weak Administrator Password	5.6%
Phishing Site Captures Employee Usernames and Passwords	5.3%
Vertical Privilege Escalation	5.1%
Sensitive Data Stored Unencrypted	4.8%
SQL Injection	4.2%
Local Network Poisoning	2.7%

The most common critical vulnerability identified in 2016 involved web pages intended for authenticated users that nevertheless were accessible 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.

Improperly secured instances of the JMX administrative console for JBoss, a Java-based web application server platform, accounted for 5.9 percent of critical vulnerabilities Trustwave found in 2016. In most of the vulnerable instances, the penetration testing process accessed the JMX console without a password or with an easily guessed password. An attacker that can access the console gains the ability to upload malicious JSP packages containing arbitrary code that will execute in the context of the web service account. In most cases, organizations can address this vulnerability by adding or strengthening the password protection for the console.

Workstations vulnerable to NetBIOS name service poisoning represented another 5.9 percent of critical vulnerabilities. By default, when a domain name server (DNS) name lookup fails on a Windows computer and it cannot locate the name in the local hosts file, it makes a broadcast NetBIOS request to the local network that any other system can answer. A malicious or compromised device in the local network could respond to broadcast NetBIOS requests with the IP address of a system under the control of an attacker that then could capture login credentials or other sensitive information.

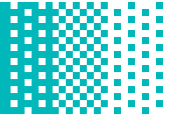
The Heartbleed vulnerability affecting the OpenSSL library remained a significant problem in 2016. First reported in 2014, Heartbleed is a serious flaw in the way OpenSSL implements the “heartbeat” function of transport layer security (TLS), which allows for longer sessions without renegotiating the encryption channel. Exploiting the vulnerability can allow an attacker to access up to 64KB of data dumped directly from memory, which can include sensitive information like usernames, passwords, payment card details and even the server’s private encryption key. Updating any servers relying on OpenSSL to the latest version of the library will patch this vulnerability.

Other critical vulnerabilities uncovered through penetration testing in 2016 included weak administrator passwords, employees responding to phishing attempts with usernames and passwords, sensitive unencrypted data and systems vulnerable to SQL injection.

TOP 10 HIGH RISK VULNERABILITIES IDENTIFIED THROUGH PEN TESTING

VULNERABILITY	PERCENT OF HIGH RISK VULNERABILITIES
Cross-Site Scripting (XSS), Persistent	29.6%
LLMNR Name Service Poisoning	23.8%
Vertical Privilege Escalation	16.3%
SQL Injection	14.2%
Sensitive Data Stored Unencrypted	13.8%
Horizontal Privilege Escalation	13.7%
Shared Password for Local Administrator with Remote Logon	11.7%
NetBIOS Name Service Poisoning	9.7%
Web Proxy Auto-discovery Protocol Man-in-the-Middle	9.4%
Default Credentials Identified	8.3%





In 2016, Trustwave penetration testing uncovered the two most high-risk vulnerabilities. Applications vulnerable to XSS comprised the largest share, at 29.6 percent. 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 that other users can then execute. Criminals use this method to steal information, such as usernames, passwords, and other sensitive material; remotely control or monitor the victim's browser; or impersonate a web page used to gather order information, including payment card numbers.

Link-local Multicast Name Resolution (LLMNR) implementations comprise the second largest percentage of high-risk vulnerabilities, at 23.8 percent. Like DNS, LLMNR is a name-resolution protocol Microsoft Windows machines use. When a DNS name lookup fails, the host making the request can use LLMNR to broadcast the request to other hosts on the network. As with NetBIOS, a malicious host on the network can respond with the IP address of a machine under the control of an attacker, which the attacker can then use to capture user credentials and other sensitive information.

Penetration testing also uncovered vertical and horizontal privilege escalation flaws, systems vulnerable to SQL injection, sensitive data stored unencrypted, administrator passwords shared between machines and NetBIOS name service poisoning.



CONTRIBUTERS

James Antonakos

Anat Davidi

Christophe De La Fuente

Sachin Deodhar

Thanassis Diogos

Dixie Fisher

Rob Foggia

Phil Hay

Brian Hussey

Eliran Itzhak

Dan Kaplan

Simon Kenin

Rami Kogan

Arseny Levin

Ziv Mador

Lawrence Munro

Prutha Parikh

Cas Purdy

Martin Rakhmanov

John Randall

Alex Rothacker

Karl Sigler

Todd Wilson

Aaron Wooten

Reno Zenere



WWW.TRUSTWAVE.COM