





THIS CLICKABLE REPORT WILL MAKE IT EASY TO NAVIGATE BETWEEN SECTIONS AND SUBSECTIONS. LOOK FOR CALLOUTS IN THE NEXT SEVERAL PAGES THAT WILL HELP YOU NAVIGATE, OR USE THE BAR AT THE TOP OF EACH PAGE TO CLICK TO EACH MAIN SECTION.

# DEAR READER

The past year brought another reality check to IT and security professionals. We thought we'd officially experienced the "year of the breach" in 2011. But in 2012, as we continued to transform our businesses—embracing mobility, moving to the cloud, expanding social collaboration and creating and sharing extraordinary volumes of data—cybercriminals likewise continued to transform and escalate.

Today's reality is this: No matter what business you are, no matter where in the world you are—if you've got data, then your business is at constant risk. From the outside in, to the inside out, threats are increasing as quickly as you can implement measures against them, and in spite of tremendous technology investment, many organizations are still ill-prepared for attacks.

This is why we're pleased to share the results of our 2013 Trustwave Global Security Report with you. In this report, we've analyzed the results of hundreds of incident response investigations, thousands of penetration tests, millions of website and Web application attacks and tens of billions of events. We've also included detailed contributions from law enforcement agencies and experts from around the world. All in an effort to provide you with perspectives on the latest threats and vulnerabilities facing organizations just like yours, along with actionable recommendations you can begin implementing immediately to strengthen your security program.

We hope you find the 2013 Trustwave Global Security Report to be a valuable resource for your business, helping you defend better, act faster and prepare for what's ahead in the upcoming year and beyond.

Best wishes,

**Robert J. McCullen**  
Chairman, CEO and President  
Trustwave

 Trustwave®





CLICK ON EACH ICON TO GO STRAIGHT TO THE DATA.

# EXECUTIVE SUMMARY

DURING 2012, NEARLY EVERY INDUSTRY, COUNTRY AND TYPE OF DATA WAS INVOLVED IN A BREACH OF SOME KIND.

Cybersecurity threats are increasing as quickly as businesses can implement measures against them. At the same time, businesses must embrace virtualization and cloud, user mobility and heterogeneous platforms and devices. They also have to find ways to handle and protect exploding volumes of sensitive data. The combination of business and IT transformation, compliance and governance demands and the onslaught of security threats continues to make the job of safeguarding data assets a serious challenge for organizations of all types—from multinational corporations to independent merchants to government entities.

Today, organizations need not only to understand current trends in security threats but also be able to identify inherent vulnerabilities within existing systems. In the 2013 Global Security Report, Trustwave tested, analyzed and discovered the top vulnerabilities and threats that have the most potential to negatively impact organizations. Read on for the key discoveries of 2012 and trends to watch in 2013 and beyond.

## KEY DISCOVERIES



Retail businesses and their sensitive data are back in the crosshairs. For the first time in three years, the retail industry made up the highest percentage of investigations at 45%.



Web applications have now emerged as the most popular attack vector. E-commerce sites were the No. 1 targeted asset, accounting for 48% of all investigations.



Mobile malware explodes by 400%. As organizations embrace mobility, mobile malware continues to be a problem for Android, with the number of samples in Trustwave's collection growing 400% in 2012.



Businesses are embracing an outsourced IT operations model. In 63% of incident response investigations, a major component of IT support was outsourced to a third party. Outsourcing can help businesses gain effective, cost-friendly IT services; however, businesses need to understand the risk their vendors may introduce and proactively work to decrease that risk.



Businesses are slow to “self-detect” breach activity. The average time from initial breach to detection was 210 days, more than 35 days longer than in 2011. Most victim organizations (64%) took over 90 days to detect the intrusion, while 5% took three or more years to identify the criminal activity.



More responsibility falls onto security staff to stay on top of zero-day attacks. Software developers vary greatly in their ability to respond and patch zero-day vulnerabilities. In this study, the Linux platform had the worst response time, with almost three years on average from initial vulnerability to patch.



Spam volume declines, but impact on the business doesn't. Spam volume shrank in 2012 to a level lower than it was in 2007 but spam still represents 75.2% of a typical organization's inbound email. Most importantly, new malware research conducted by Trustwave found nearly 10% of spam messages to be malicious.



Basic security measures are still not in place. “Password1” is still the most common password used by global businesses. Of three million user passwords analyzed, 50% of users are using the bare minimum.



CLICK ON EACH PERCENTAGE FIGURE TO GO STRAIGHT TO THE DATA.

# TACTICAL THREAT INTELLIGENCE

ENCRYPTION  
SOPHISTICATION

**25%**

The use of encryption by attackers during data exfiltration is on the rise; over 25% of all data was encrypted by cybercriminals.

MEMORY SCRAPING  
DOMINANT

**50%**

The most popular malware family was memory scraping; 20% of new case samples included memory scraping functionality, and such activity was detected in almost 50% of investigations where associated malware had identifiable data collection functionality.

PDF FILES  
AT RISK

**61%**

Of all client-side attacks observed, 61% targeted Adobe Reader users via malicious PDFs.

BLACKHOLE ON  
THE RISE

**70%**

Versions of the Blackhole exploit kit made up over 70% of all client-side attacks serving up zero-day exploits.

SQL & REMOTE  
STILL REIGN

**73%**

Always the two most noteworthy methods of intrusion, SQL injection and remote access made up 73% of the infiltration methods used by criminals in 2012.

## LOOKING AHEAD

Cybercriminals will never stop trying to compromise systems to obtain data. Organizations need to be aware of where they may be open to attacks, how attackers can enter their environment and what to do if (and when) an attack occurs. The 2013 Trustwave Global Security Report identifies the most serious and common vulnerabilities, how cybercriminals are breaking in and what they're mostly likely to steal. Based on research and analysis of hundreds of investigations and thousands of client engagements, the report further offers six key security pursuits for 2013, highlighting the tools organizations need to evaluate in order to build a comprehensive information security strategy that can reduce risk, protect data and safeguard their reputations.



CLICK ON EACH SECTION TITLE TO JUMP DIRECTLY TO EACH AREA OF STUDY.

## REPORT DESIGN

The 2013 Trustwave Global Security Report delivers information and analysis gathered from and presented in five distinct sections:



### INCIDENT INVESTIGATIONS

The report analyzes the results of more than 450 incident response investigations Trustwave performed due to suspected security breaches, identified by either the target organization or a third party (regulatory body, law enforcement or other group).

- Data from more than two million network and application vulnerability scans.
- Approximately 400 Web-based data breaches publicly disclosed in 2012.
- More than 20 billion emails collected and analyzed from 2007 to 2012.
- Mobile threats that impact the most popular mobile device platforms.
- Usage and weakness trends of more than three million real-world passwords used within corporate information systems.



### LAW ENFORCEMENT AGENCY UPDATES

Law enforcement agencies worldwide are committed to identifying and disrupting cybercriminals working against both businesses and governments. In this report, updates from agencies in Australia, Mexico, the United Kingdom and the United States showcase firsthand accounts of cybercriminal activity in those regions.



### INTERNATIONAL PERSPECTIVES

Trustwave security experts in regions around the world identify and apply macro trends and client experiences across international regions to provide a global view and implications of the threat landscape.



### THREAT INTELLIGENCE

In this report, Trustwave dives deep to correlate, dissect and analyze data gathered from:

- All vulnerabilities disclosed by the major server and client vendors to compare their average zero-day responsiveness.
- More than five million malicious websites to understand the most popular exploits and exploit kits used to infect victim visitors.
- More than nine million Web application attacks to determine top attack methods.
- More than 2,500 penetration tests performed against more than one million devices or websites.



### CONCLUSIONS & PURSUITS

Threats to sensitive data can occur at anytime, anywhere, originating from a cybercriminal group or from within a company. It's no longer a matter of "if" but "when." Highlighting the trends and discoveries outlined in the report, this section also suggests six key security pursuits for 2013.

Standardized tools were used to record data and other relevant details for each case or test. To protect the confidentiality of Trustwave clients, the information and the statistics within this report are presented in an aggregate form only.





USE THE TABLE OF CONTENTS TO CLICK TO THE SECTIONS YOU WANT TO VISIT. AND, THROUGHOUT THE REST OF THE REPORT, USE THE NAVIGATION BAR ON THE TOP TO JUMP FROM SECTION TO SECTION, AND BACK TO THE TABLE OF CONTENTS.

# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

KEY DISCOVERIES	02
TACTICAL THREAT INTELLIGENCE	03
REPORT DESIGN	04

## INCIDENT INVESTIGATIONS

UNIQUE DATA SOURCES, COUNTRIES & METHODOLOGIES	07
TYPES OF DATA TARGETED	08
TOP FIVE COMPROMISED INDUSTRIES	09
TARGET ASSETS	10
SYSTEM ADMINISTRATION RESPONSIBILITY	10
DETECTION	11
TIMELINE: INTRUSION TO CONTAINMENT	11
THE BREACH QUADRILATERAL	12
INFILTRATION	12
PROPAGATION	14
AGGREGATION	15
EXFILTRATION	16
MALWARE EVOLUTION	16

## LAW ENFORCEMENT AGENCY UPDATES

UNITED STATES SECRET SERVICE	22
SERIOUS ORGANISED CRIME AGENCY (UK)	23
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO	24
NEW SOUTH WALES POLICE FORCE CYBERCRIME SQUAD (AUSTRALIA)	25

## 02

## THREAT INTELLIGENCE

## 26

ATTACKER SOURCES	27
ATTACKER MOTIVATIONS	28
EMERGING TECHNIQUE: SOPHISTICATED EMBEDDED MALWARE	30
EMERGING TECHNIQUE: FAKE SSL CERTIFICATES	31
Critical Vulnerability Study: Tracking Zero-Day Response Times	32
Attack Trends	34
Web Client	34
Web Server	38
Mail-Based Attacks	41
Mobile	46
Defense Failures	48
Network	48
Applications	50
Mobile	52
Passwords	54
Physical	58

## INTERNATIONAL PERSPECTIVES

## 59

EUROPE, MIDDLE EAST & AFRICA (EMEA)	60
ASIA PACIFIC (APAC)	62
LATIN AMERICA & THE CARIBBEAN (LAC)	64

## CONCLUSIONS & PURSUITS

## 68

GLOSSARY	74
CONTRIBUTORS	76



THROUGHOUT THE REPORT, LOOK FOR THE LOCATOR ICON TO FIND INSTANT, ACTIONABLE, BUSINESS-RELEVANT IMPLICATIONS AND/OR ADVICE. CLICK ON THE ICON HERE TO GO TO THE FIRST ONE, THEN CLICK THAT ONE TO GO TO THE NEXT, AND SO ON.





# INCIDENT INVESTIGATIONS



## UNIQUE DATA SOURCES, COUNTRIES & METHODOLOGIES

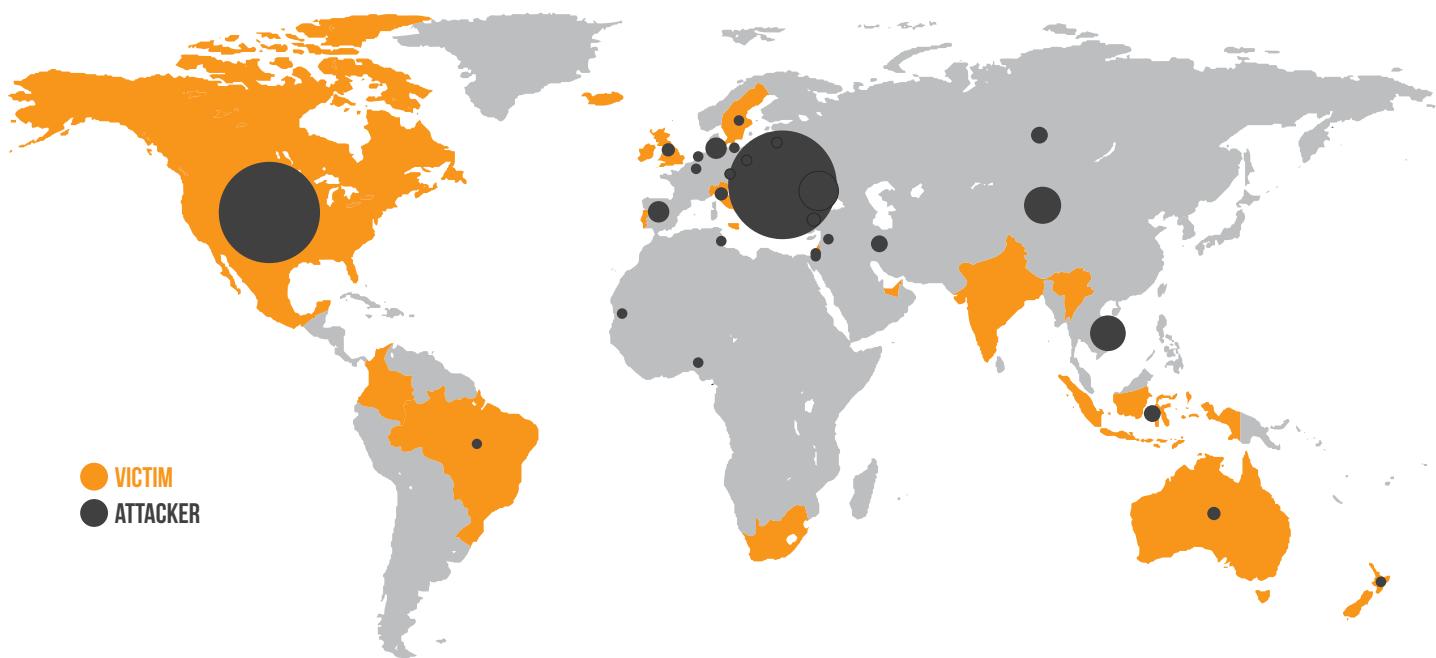
In 2012, Trustwave SpiderLabs performed more than 450 data breach investigations in 19 countries—an increase of 50% compared to investigations performed in 2011.

From these investigations, Trustwave determined that attacks in 2012 originated in 29 different countries, with the largest percentage originating in Romania—a country known as a hotbed of criminal activity, specifically for organized crime focused on obtaining cardholder data (CHD).<sup>1</sup>

Source IP addresses do not necessarily establish where attackers are physically located, and maintaining online anonymity is trivial for attackers today. Therefore, points of origin may represent either the actual attacker source or an anonymous service endpoint.

Based on the investigations and analysis of source IP addresses, attackers are using networks of compromised systems to mask their actual locations. For some regions, such as Asia-Pacific, the increase is likely to be a reflection of abundant and rising broadband coverage combined with a still-maturing information security industry.

## LOCATIONS: VICTIMS & ATTACKERS



> **450**  
DATA BREACHES  
**19**  
COUNTRIES

### TOP VICTIM LOCATIONS:

UNITED STATES	73.0%
AUSTRALIA	7.0%
CANADA	3.0%
UNITED KINGDOM	2.0%
BRAZIL	1.2%

### TOP ATTACKER LOCATIONS:

ROMANIA	33.4%
UNITED STATES	29.0%
UNKNOWN	14.8%
UKRAINE	4.4%
CHINA	3.9%

Trustwave incident response engagements are undertaken in response to security issues, identified either by the victim organization or a third party (law enforcement or regulatory body). In this report, data from these investigations are analyzed and findings are presented in an aggregated form. It is important to note that the data presented in this report are not survey data. All figures in this section are from actual Trustwave SpiderLabs investigations.

1. <http://www.afp.gov.au/media-centre/news/afp/2012/november/seven-arrested-in-australias-largest-credit-card-data-theft-investigation.aspx>



## TYPES OF DATA TARGETED

The primary data type targeted by attackers in 2012, as in 2011, was cardholder data. There is a well-established underground marketplace for stolen payment card data; it is bought and sold quickly for use in fraudulent transactions.

With such a vast number of merchants accepting payment cards (estimates from major credit card brands put the total in the United States between nine and 10 million merchants), and with so many available attack vectors, it is unlikely this market will change any time soon.

Criminals also sought personally identifiable information (PII), which has some monetary value, albeit not as much as cardholder data, since it requires additional work and risk (i.e., posing as someone else) without the same lucrative return on investment.

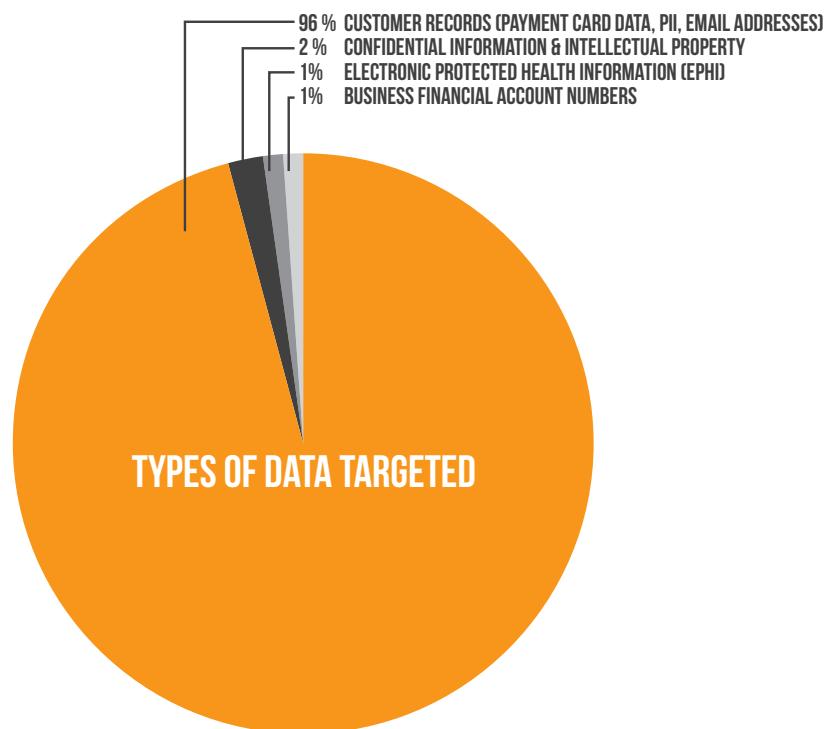
The primary targets of cybercriminals in 2012 were Retail (45%), Food & Beverage (24%) and Hospitality (9%). There are several contributing factors to this continuing trend:

- The sheer volume of payment cards used in these industries makes them obvious targets.
- The main focus of organizations operating in these spaces is customer service, not data security.
- There's a misconception that these organizations are not a target. In practically all of the 2012 investigations, this statement was made in just about every case: "Why me?" The answer can only be "Because, you have something worth taking that is not protected."



Trustwave witnessed the compromise of both physical and virtual businesses worldwide. By using the intelligence gathered from each of these breaches, a strong defense-in-depth strategy can be formulated to protect business-critical assets. Whether that asset is something physical or something digital, the strategy remains the same:

- 1 Identify the points of likely infiltration and defend them.**
- 2 Identify the likely target and defend it.**
- 3 Identify the likely exfiltration point and seal it off.**
- 4 Implement monitoring controls to detect compromise.**



## TOP 5 COMPROMISED INDUSTRIES

### 1 Retail and Food & Beverage

The retail space saw a 15% increase in 2012 compared to 2011, nearly equal to the 17% drop in Food & Beverage breaches. Over the past three years, these two have been almost interchangeable, with similar network layouts due to the payment systems and software vendors used. In these industries, security often becomes an afterthought until a breach is identified.

### 3 Hospitality

Three years ago, Hospitality was hardest hit by far. This industry has made significant strides to resolve data security issues. The majority of Hospitality breaches this year were actually at Food & Beverage locations within the building and not necessarily in the Hospitality Management System (HMS). The reason for this is twofold: The Food & Beverage systems are usually easier to compromise and more payment cards are used in these establishments (as the HMS is limited to the guests staying at that hotel).

This is not to say that an HMS is more secure than Food & Beverage systems. A successful HMS breach may include data from an "interface" server that combines the HMS with the hotel's Food & Beverage and Retail locations (e.g., gift shop), harvesting significantly more data.

### 4 Financial Services

A small increase for Financial Services highlights the fact that attackers are continuing to look at central aggregation points like payment processors and merchant banks as viable targets. The Payment Card Industry Data Security Standard (PCI DSS) has made comprehensive security controls more commonplace in larger organizations. Therefore, the organizations become more difficult to compromise. This by no means indicates that attackers have given up on these high-dollar targets, simply that they are better defended, presenting a bigger challenge to would-be intruders.

The logical progression for attackers will be to hit the next stop in the payment card industry (PCI) flow: the banks. If attackers are able to breach financial institutions such as payment gateways or merchant processors, the payoff would be huge.

### 5 Nonprofit

The increase in attacks on Nonprofit has several potential causes. Attacks could be based on beliefs (personal, religious or political), or they could simply be financial targets, considering that many of these organizations typically do not have the funds to spend on security.





## TOP TARGET ASSETS

- 1% ATM
- 4% DATA CENTERS/CORPORATE INFRASTRUCTURE
- 47% POINT OF SALE/PAYMENT PROCESSING
- 48% E-COMMERCE/WEBSITES

## TARGET ASSETS

Systems that store, process or transmit cardholder data remain primary targets. With the massive proliferation of systems that contain CHD, the number of targets for attackers is almost inexhaustible.

Also targeted in 2012 were systems housed within data centers. These systems provide attackers with a beachhead within the target environment that, once established, allows them to explore systems and network segments as they search for the data of value. Once attackers gain access, they identify and exfiltrate Microsoft Office documents from My Documents folders, finding data like client lists and PII.

Breaches of automated teller machines (ATMs) also appeared this year; while less frequent, when they are successful, they yield a payout many times larger than any other type of cardholder data breach.

Regardless of which assets are targeted, there are three security controls to consider: remote access, network access and employee education. Remote access should be tightly controlled with strong password requirements and properly configured firewalls. Network access control, network segregation and data access control provide another layer of defense. Finally, all the security controls in the world are useless if an attacker can manipulate an employee with system access.

The majority of Trustwave's investigations (63%) revealed that a third party responsible for system support, development and/or maintenance introduced the security deficiencies exploited by attackers. Small businesses/franchises within Food & Beverage and Retail were most often impacted, as they typically outsource IT support and are often unaware of security best practices or compliance mandates by which their partners were required to

abide. In some instances, victims were unaware that the third party was responsible only for a subset of security controls, leaving these systems open to attack.

## SYSTEM ADMINISTRATION RESPONSIBILITY

### TOP CHALLENGES FOR ORGANIZATIONS THAT SUFFERED THESE THIRD-PARTY BREACHES INCLUDE:

- 1. Remote administration:** Many third-party IT organizations have hundreds or even thousands of customers. Such a large client base can make remote administration a challenge; to make it easier, service providers choose a remote administration utility that remains always on—almost certainly not the most secure option.
- 2. Password weaknesses and reuse:** To further facilitate remote administration, providers frequently choose simple, default-like passwords that are then reused at multiple client locations.
- 3. Lack of a properly configured firewall:** When implemented properly—with sound ingress and egress—firewalls are great network security appliances. However, many IT providers either have very weak access controls or use ingress filters.
- 4. Lack of support:** Once an organization has been breached, third-party support tends to become a difficult conversation. The service provider will often try to ensure that it is not held responsible, thus leaving its customer hanging.
- 5. Software updates:** Trustwave investigations found that the majority of systems in this category do not have the latest operating system patches or business-critical software updates.

## SYSTEM ADMINISTRATION RESPONSIBILITY

SELF 37% | 63% THIRD PARTY

 Protecting critical applications requires more than technology products. Ensure holistic protection of applications by combining Web application firewalls with code development training, secure code review and application penetration testing services.



## METHOD OF DETECTION

- 
- 1% PUBLIC DETECTION
  - 2% THIRD PARTY
  - 24% SELF-DETECTION
  - 25% LAW ENFORCEMENT
  - 48% REGULATORY DETECTION

## DETECTION

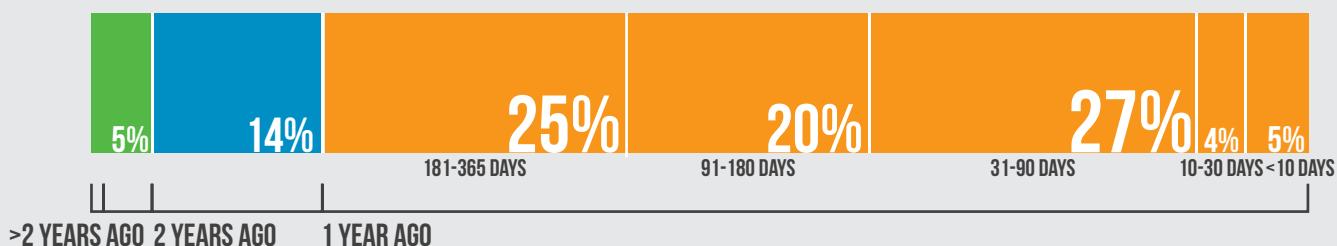
In the past two years, attacks have grown significantly in complexity, rendering the majority of “off the shelf” detection solutions, such as commercial antivirus programs, ineffective. In addition, due to advanced subterfuge techniques, malware often goes unnoticed by systems administrators despite being clearly visible to investigators.

During the course of every breach investigation, Trustwave investigators are invariably asked, “How could this have been prevented?” The best answer is to build a defense-in-depth strategy with multiple layers of security. As in sports, where there are several lines of defense against the opponent, these strategies put together multiple solutions—and can be built to cater to each unique business rather than simply combining point products that might not fit.



**Close the gap between detection and remediation.**  
Technologies that provide real-time, advanced anti-malware and deep inspection technologies, such as secure Web gateway, can help mitigate threats not captured by antivirus, firewalls or intrusion detection systems.

## TIMELINE: INTRUSION TO CONTAINMENT



Often compromises are detected at greatly varying intervals, and the time from initial breach date to containment may be six to 12 months or more. The Timeline: Intrusion to Containment graph represents investigations that took place in 2012, demonstrating that initial entry may have been up to four years before the investigation.

Unfortunately, it's not always possible to determine the specific date on which a compromise occurred, because victim organizations often do not maintain relevant forensic artifacts, like log files, and attackers sometimes cover their tracks.



# PROPAGATION

## THE BREACH QUADRILATERAL

In previous years, the “Breach Triad” was used to describe the basics of a data compromise, from Infiltration to Aggregation to Exfiltration. This year, a fourth component, Propagation, shows how the infection moves from one target system to another—important because attacks are now rarely restricted to a single system.



### INFILTRATION

Remote access remained the most widely used method of infiltration in 2012. Unfortunately for victim organizations, the front door is still open.

Organizations that use third-party support typically use remote access applications like Terminal Services (termserv) or Remote Desktop Protocol (RDP), pcAnywhere, Virtual Network Client (VNC), LogMeIn or Remote Administrator to access their customers' systems. If these utilities are left enabled, attackers can access them as though they are legitimate system administrators.

**How do attackers find remote access systems?** Would-be attackers simply scan blocks of IP addresses looking for hosts that respond to queries on one of these ports. Once they have a focused target list of IP addresses with open remote administration ports, they can move on to the next part of the attack, the No. 2 most exploited weakness: default/weak credentials.

Unfortunately, gaining access to systems is just as easy as it is for attackers to identify targets.

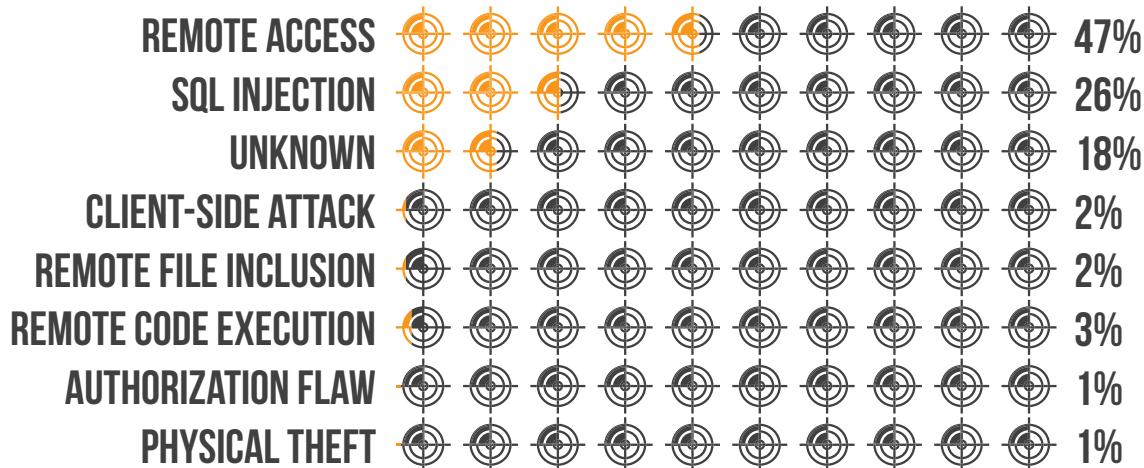
Most current Web pages are not made up of static content as they were years ago, but of fluid dynamic components and content. In addition, many pages ask for information—location, preferences, PII—with the goal of improved efficiency and user interaction.

This dynamic content is usually transferred to and from back-end databases that contain volumes of information—anything from cardholder data to which type of running shoes is most purchased. Pages will make Structured Query Language (SQL) queries to databases to send and receive information critical to making a positive user experience.

Poor coding practices have allowed the SQL injection attack vector to remain on the threat landscape for more than 15 years. Any application that fails to properly handle user-supplied input is at risk. The good news is that properly using parameterized statements (aka prepared statements) will prevent SQL injection. When programmers fail to validate input (either by incorrectly validating or not validating at all), attackers can send arbitrary SQL commands to the database server.



## METHOD OF ENTRY



The most common attack goal with SQL injection is bulk extraction of data. Attackers can dump database tables with hundreds of thousands of customer records that contain PII, CHD and anything else stored by the victim organization. In the wrong environment, SQL injection can also be exploited to modify or delete data, execute arbitrary operating system commands or launch denial of service (DoS) attacks.

The third most widely seen method of entry in Trustwave's investigations was "Unknown." However, an overwhelming number of these cases possessed a common indicator of compromise (IOC), specifically weak and/or default credentials.

In the majority of cases Trustwave investigated in 2012, username and password combinations were woefully simple. Combinations included administrator:password, guest:guest and admin:admin. In addition, many IT service providers had standard passwords that were used by administrators allowing them to access any customer at any time. This means that if one location is compromised, every customer with that same username:password combination could also be compromised.



"How did the attackers find me?" The answer is simple: "You had open remote access ports and a weak or vendor-supplied default password." Compare this to a neighborhood in which all the houses have the same lock: anyone can enter any house because everyone has the same key.





## PROPAGATION

In many of Trustwave's 2012 investigations, the initial point of entry was not the ultimate target; additional reconnaissance and movement were needed to identify the location of valuable data (commonly called "establishing a beachhead"). Once a beachhead was formed, attackers conducted network scanning to determine what other systems were either on the same network segment or communicating with the compromised host. This information was then used to penetrate deeper into the target's infrastructure and find valuable data.

While propagation method varied by case, compromising additional systems used the same weaknesses that allowed the initial compromise, usually weak and/or vendor-supplied passwords. The top three methods of internal propagation methods were:

- 1 Open default administrative shares.**
- 2 Use of legitimate administrative remote access utilities.**
- 3 Use of remote command utilities.**

By default, versions of Microsoft Windows up to (but not including) XP Service Pack 3 contain administrative shares. These permit access to all logical drives as well as to the %SYSTEMROOT% directory for anyone who can authenticate with proper credentials. Since the user credentials compromised in most of Trustwave's investigations were administrator credentials, and the majority of operating systems were variants of Windows prior to SP3, this propagation method was popular.

Using default shares, an attacker simply needs to know the IP address of the target system and assumes the target was the same operating system with the same patch level as the beachhead. Then they can enter the Windows Universal Naming Convention (UNC) path into the Run prompt or browser window (or use the "NET USE" command from a DOS prompt). They can then transfer files to and from the target with ease.

Theoretically, the discovery of this propagation method could be attributed to the identification of event ID 5145 (a network share object was checked to see whether a client can be granted desired access) and 5140 (a network share object was accessed) in Windows Security Event logs. However, security event logging was disabled in most cases, making it impossible to discover through these methods. The method of discovery was either from an ntuser.dat file or from Web browser history.

The second-most popular method of propagation is the use of existing legitimate remote access utilities. In environments where administration can be handled remotely, utilities exist to facilitate remote access to Windows-based systems within the environment by a system administrator.

Internally-facing remote administration utilities are frequently set up even less securely than externally-facing versions (since it is assumed that if a user is accessing the system with one of these tools, he is already "inside," and therefore trusted). Many have abysmally weak username:password combinations—and sometimes require no credentials at all. Some even retain historical data. All an attacker has to do is initiate the program to see the number of systems available and their status. Once access is gained, they can quickly transfer files to and from the target.

Finally, command line remote administration utilities is a third method of propagation. Once an attacker has established a beachhead, he will often bring a number of tools with him to perform various stages of the hack.

Among the most popular of these tools are psexec<sup>2</sup> and winexe.<sup>3</sup> These command line tools do not require installation and provide the attacker with the ability to transfer files to and from the target and remotely execute commands. Attackers can then automate propagation and execution of additional components of the breach (such as malware).

## DATA EXPOSURE VOLUMES



Data exposure volumes are extraordinarily difficult to track and estimate due to the data harvesting methods used in the majority of breaches—predominantly memory dumpers, keyloggers and network sniffers.

In cases where memory dumpers and/or keyloggers are used, there is normally a period of approximately 18 months in which the malware operates undetected and the files used by attackers to store the stolen data are truncated multiple times. Since deleting the output file to a running process would cause it to crash, truncating the file removes the contents of a file without actually having to delete and recreate it. This means the forensic investigation yields only the most recent iteration of harvested data, resulting in being able to retrieve only a fragment of the data that attackers harvested.

Many modern variants of network sniffers use automatic exfiltration mechanisms that send harvested data to the attacker's drop site immediately upon identification. This means that unlike memory dumpers and keyloggers, no output file with the stolen data is ever created. Without real-time network packet captures starting with the initial infection data, a comprehensive accounting of the targeted data is not possible.

2. <http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>

3. <http://sourceforge.net/projects/winexe>

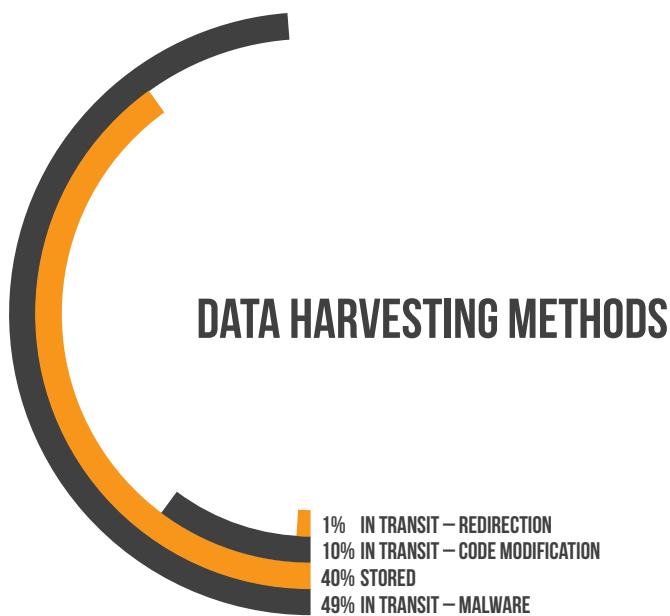


## AGGREGATION

When Trustwave investigated cases in which vast quantities of stored data were compromised, it was usually the result of weak administrative credentials, SQL injection or remote file inclusion (RFI).

In many such cases, attackers used RFI (and sometimes SQL injection) to upload Web shells to the target Web server, which ran under the same user account as the Web instance. Once in place, an attacker can navigate to the Web shell location to access the newly uploaded tool. These Web shells provide attackers with a user interface that allows them to dump hashes, upload/download files, create/remove user accounts and remove the utility altogether.

Attackers were more successful at maintaining persistence and harvesting data in transit than they were at attacking stored data. They became much more adept at hiding their malware in plain sight, known as malware subterfuge—the use of legitimate process names or injection of malware into legitimate Windows binaries. This means that an attacker's malware could live on a target system undetected for as long as four years, and all data processed during that timeframe may be compromised.



## FRANCHISES

Over the past year, Trustwave has investigated multiple breaches involving hundreds of franchise locations. Franchise investigations are unique in that the location initially investigated is not necessarily the first location to be compromised. In fact, in 2012, only about a third of the franchise locations were the original point of compromise.

In several of these cases, the original entry point was never identified because the corporate entity had little control over the actions of individual franchisees. This makes franchise breaches extremely difficult to manage, since the investigation has to involve all franchise owners, who often have incomplete data.

What's more, the infiltration method may not be immediately apparent from the investigation of a single/small subset of locations. This is especially true if there is interconnectivity between locations or from franchises to headquarters. However, once the first few investigations have been completed and the IOCs have been identified, other franchise locations can be quickly checked.

Like single location breach investigations, franchise breaches have the same basic components of the Breach Quadrilateral. Once these components are identified, the investigations are no different, provided IOCs remain consistent. If IOCs are not consistent, and the attackers either change their attack method, or a second breach is identified, then the process simply repeats itself with the newly identified IOCs.

One aspect that is consistent in franchise breach investigations is that the attack is normally launched by the same attacker(s). This can at least add some consistency to the investigation.



## EXFILTRATION METHOD

1%	PHYSICAL HARVESTING
1%	SOURCE CODE MODIFICATION
17%	NATIVE UTILITIES/SERVICES
21%	BUILT-IN MALWARE FUNCTIONALITY
60%	SAME AS ENTRY METHOD

## EXFILTRATION CHANNEL

11%	SMB
13%	SMTP
18%	HTTPS
25%	RDP
33%	HTTP

## DATA ENCODED/ENCRYPTED FOR EXFILTRATION

YES 26%	74% NO
---------	--------

### EXFILTRATION

Exfiltration is often referred to as “the getaway.” In 2012, as in previous years, the primary data exfiltration enabler was either the lack of a firewall or a firewall without egress filters.

Ingress filtering monitors and inspects traffic as it enters the protected network. Egress filtering is the opposite; it examines and restricts network traffic as it flows from the protected segment to make sure that data is headed for the proper location, over the proper port, using an authorized protocol.

In 2012, the majority of breach cases and penetration tests revealed that the victim organization did not have proper egress filtering. During interviews conducted throughout the engagements, organizations indicated that this is because the internal network is “trusted.”

This line of thinking would be accurate only if a breach were never possible. Since a breach is always possible, measures need to be taken to ensure that the attacker will have to circumvent an additional layer of technical safeguards to complete the breach.

### MALWARE EVOLUTION

Each year, malware research brings new data regarding spreading, multiplying and evading detection. Malware’s history arguably coincides with the first computers; there are stories about resource-stealing programs dating back to systems that ran on punch cards. Often they were the creations of enthusiastic computer scientists trying to flex their muscles or discover flaws in the system.

Unfortunately, the academic pursuits of security researchers do not account for the malware listed in this report. The samples collected and analyzed for this report come from a number of sources like honeypots, forensic investigations, customer submissions and shared security resources.

These samples demonstrate that malware authors are taking advantage of both well-known and new vulnerabilities, evolving their attacks as business systems have evolved to meet demand.

Fortunately, malware research has evolved as well.

Thanks to a process known as “fuzzy hashing,” first developed by Jesse Kornblum,<sup>4</sup> researchers can more easily determine malware “families.” Most of the malware files analyzed belong to one of several families, each file used by an exploit kit to weaponize and distribute malware. These kits allow attackers to create and deploy customized malware instances quickly. Depending on the target, they may use different vectors: malicious documents, payloads destined for vulnerable servers, malicious browser plug-ins.

4. <http://www.sciencedirect.com/science/article/pii/S1742287606000764>



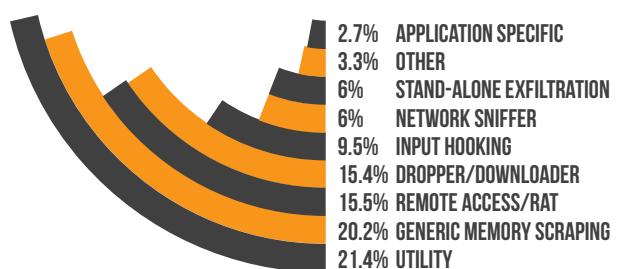
The exploit kits revealed that there is a mature malware economy comprising those who supply malware (the “arms dealers”) and those who spread it. Understanding this relationship brings the security community as a whole much closer to understanding how and why malware is created and how it proliferates. It also encourages continued efforts to create software solidly founded on security.

The malware cases Trustwave analyzes are often part of highly targeted attacks that differ from what is commonly covered in public malware discussions. Samples may be part of ongoing criminal investigations, limiting the data that can be disclosed.

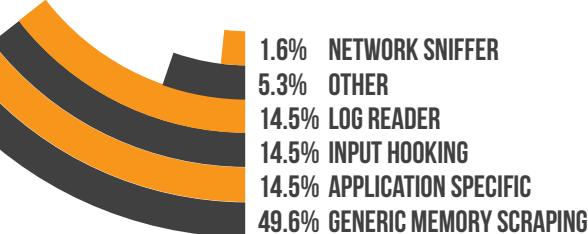
In this section:

- Incident response cases:** Individual cases as they apply to a particular victim and event. A single case may involve many systems and malware samples. Attackers do not limit themselves to a single target, and the same criminal groups may repurpose their attack tool kits for many victims.
- Malware analysis cases:** Kits or combinations of malware used together in one or more incident response cases. Trustwave researchers view the data through this lens to understand how the cases relate and to develop a sense of the attacker’s abilities and growth.
- Individual malware samples:** Analysis of samples that make up the cases to identify how attackers handle the functions required to successfully run a data theft campaign.

## UNIQUE SAMPLES BY CLASSIFICATION



## PERCENTAGE OF INCIDENT RESPONSE CASES WITH IDENTIFIED DATA-TARGETING METHODS



## MEMORY SCRAPERS

Attacks using memory scrapers can target any application that processes credit card numbers; they're often multistaged, including separate discovery and capture tools. In the past, memory scraping often required the attacker to have a small amount of target environment knowledge to configure the capture tool.

The trend in 2012 was toward generic discovery tools that could identify the desired information in a list of preconfigured processes or all running processes on the affected system. This generic data targeting technique is simple but very effective.

The quality and accuracy of a tool's discovery and capture mechanisms can assist in linking cases. Simplistic searches for cardholder data can yield a lot of results, but can also result in false positives, forcing the attacker to waste time collecting useless data.

Alternatively, the attacker can use a pattern that targets data more accurately at the expense of computational power and adherence to expected format. In addition to tools, automation scripts can reveal a wealth of information about the attacker and their sophistication.



**Memory scrapers are used to target very specific data. Combined with the growth in software-agnostic techniques for extracting that data, they have become popular in targeted attacks. New samples that included memory-scraping functionality accounted for 32% of cases, and such activity was detected in 49% of all incident response cases for which the associated malware had identifiable data collection functionality.**

## REMOTE ACCESS

Remote access can range from full-on remote desktop to simple botlike command and control (C&C) channels. Poorly configured remote administration is a leading infection vector, and maintaining that access is often vital to exfiltration.

Sometimes remote access attacks are as simple as the attacker adding itself as a user and ensuring that the firewall permits traffic to a remote desktop. Other times, third-party remote administration tools are abused when attackers find flaws or misconfigurations. Custom remote access tools are more closely related to common Trojans and malware kits. Attackers hide C&C through techniques such as proxying through translation services, hiding messages in container files and using encrypted communications. Through their C&C, an attacker may issue commands that result in direct terminal access.



**Similar to trends in common malware, custom-targeted remote access tools increased in 2012. Their indirect administrative controls added yet another layer of obfuscation from regular users and did not require any visible interaction with the system terminal. The skills to develop completely custom remote access tools limits this technology to the higher tiers of attackers. Although the complexity and behavior of these tools introduce additional challenges in antivirus evasion, their limited distribution appears highly effective in preventing detection.**

## INPUT HOOKING

Input hooking is a method of acquiring user-supplied inputs to systems by intercepting the OS-level functions associated with the input. This is popular in payment system malware, as users need to input credit cards, either through a card-swipe device or keypad. These devices often emulate keyboard activity, making them vulnerable to keyloggers, both physical and software-based.

Generic input hooking, on the other hand, requires some understanding of Windows. The human interface device (HID) protocol is a mechanism for bridging different input sources into a common application programming interface (API) for ease of use in application development. The HID protocol works out communication between devices and the host. To the system, the protocol presents a unified mechanism for reading input from any device using HID.

This unified mechanism makes it relatively straightforward to insert hooks into the HID library. Card readers, check scanners, fingerprint readers and proximity card readers usually work with the HID on Windows, and all are likely malware targets.



**Historically, keyloggers have been common in incident response cases. While 2012 cases still showed keylogger-based attack campaigns, not as many new versions appeared to be in use. Only 9% of our new case samples included keylogging and other input interception components, but 15% of cases with identifiable data targeting functionality acquired said data via input hooking techniques. It appears attackers are largely using the same cracked software as they have for some time. What did increase in 2012 is the instance of custom-crafted input interception malware, many targeting keystrokes but several that expanded into USB, serial and other vulnerable HID inputs.**



## MALWARE: EXFILTRATION

The methods and tools an attacker uses for exfiltration can be used to link cases and roughly estimate their sophistication. In fully automated attacks, the end result is usually a capture-store-exfiltrate loop, wherein malware saves logs of captured data until a triggering event causes the log to be transferred and deleted and a new round of logging begins. Triggering events are usually time- or size-based. Less sophisticated samples may skip the storage step, ensuring quick turnaround on data collection but producing a consistent stream of outbound connections that may result in detection.



## MALWARE BY EXFILTRATION METHOD

The network communications involved in exfiltration are also varied. FTP is falling out of favor, with HTTP, SMTP and Web services picking up the slack. "Other" accounts for things like free webmail, online-storage accounts and custom HTTP services.

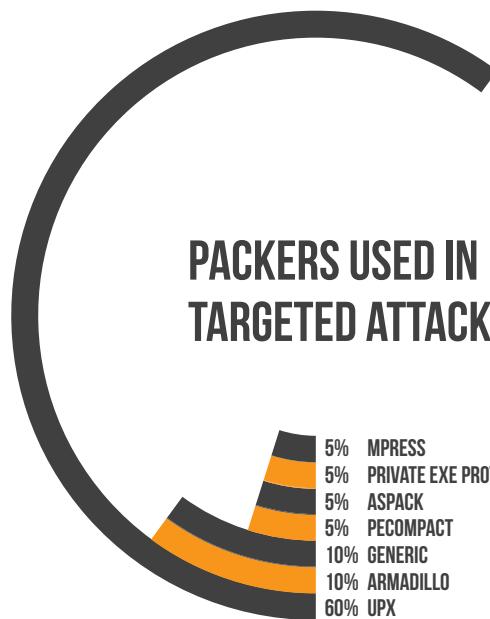
These are often obfuscated using simple ciphers and encrypted using strong cryptography. Strong cryptography was detected in only 21% of Trustwave's malware cases. An additional 31% of malware cases included components using more common obfuscation techniques. Obfuscation methods ranged from simple Base64 and nonstandard ASCII encoding, XOR encoding and bit swapping; there were even examples of the polygraphic Vigenère cipher.

## SCRIPTS AND BITS

As with managing any diverse, globally distributed network, automation is an important component of an attack campaign. Scripts are used to automate all parts: **reconnaissance**, **infection**, **data discovery/configuration** and **exfiltration**.

Sometimes the malicious malware is itself a script. Because scripts are plain text, it is easier to see their evolution as malware is developed. They often contain configuration data including encryption keys, exfiltration targets, and other information that can link cases to each other and, one hopes, back to the attacker that created them.

While only 4% of unique, executable samples processed by Trustwave's malware analysis team fall into this category, 17% of incident response cases for 2012 included such functionality. This is indicative of a growing trend. Along with additional evidence, many of these cases have been identified as related due to the similarities of the script-based components (along with additional evidence).



## PACKERS USED IN TARGETED ATTACKS

Packers are utilities used to shrink executable files and are an example of dual-use software (malicious and non-malicious). In addition to compressing files, packers can often obfuscate or encrypt payloads, aiding in anti-malware bypass. While par for the course when dealing with common malware, packers are seen less in targeted malware. Only 44% of Trustwave's malware cases included samples with identifiable packers, and even then only a sample or two out of each of those cases were packed.

Many packers are easily identifiable and used primarily by malware. Their use increases the chances of detecting specially crafted targeted malware because anti-malware software can trigger on the packer's signature. UPX is a popular multiuse packer, accounting for 60% of Trustwave's detected packers in targeted attacks.



## MALWARE INVESTIGATION

Targeted malware has become a norm in Trustwave's forensic investigations, especially in credit card breaches. Point-of-sale (POS) software continues to get better security architecture and encryption, meaning attackers can no longer rely on simply exporting databases and reading plain text credit card data. In 2012, almost all POS breach investigations involved targeted malware.

From the time the first memory scraper was witnessed by Trustwave in 2008, this targeted malware space has been on the watch list. To that end, Trustwave collects and tracks malware fingerprints, including infection vector, data aggregation mechanisms, regular expressions, exfiltration IPs, exfiltration channels, encryption techniques, compilers, packing mechanisms, SMTP servers used, destination email addresses and more.

Out of the 450 cases investigated in 2012, about 40 variations of malware were found. The discrepancy in the ratio of cases vs. malware samples is due to the commonality between the victims investigated where one malware was deployed to multiple environments all with the same target systems. Analyzing each of the 40 samples led to the discovery of banking Trojans, document Trojans (MS Office and Adobe), rootkits, keyloggers, sniffers, memory scrapers and various remote access Trojans (RATs).

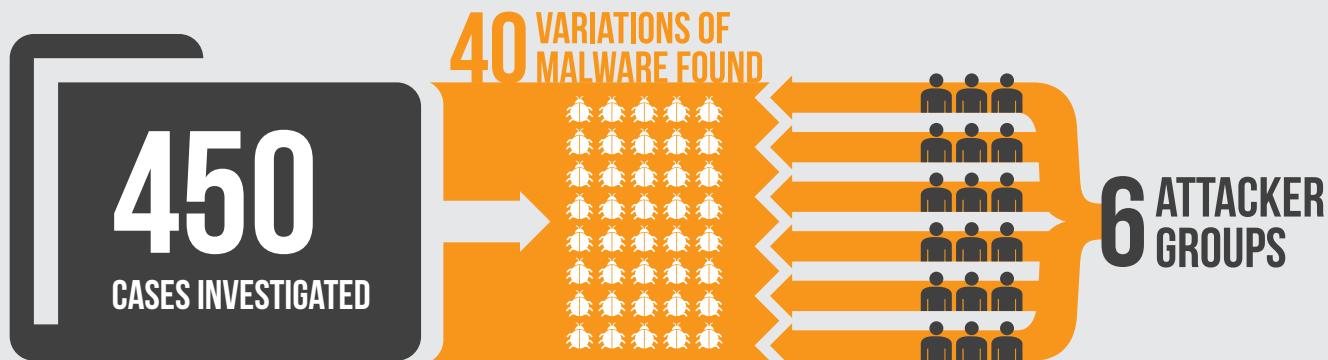
Attackers combine these tools in different ways for any given victim, using reconnaissance to determine which type will offer the best results. Each criminal group also uses different malware types for infiltration, aggregation and exfiltration. From the 40 unique types of malware, Trustwave can attribute them to six distinct criminal groups. This is after filtering the outlier script kiddies using off-the-shelf tools and some advanced malware used to target critical government agencies.

After a deeper comparison of the malware attributed to the six groups, additional similarities were found, seemingly indicating there are only three criminal teams that cause the majority of the POS credit card breaches in the United States, Canada, APAC and EMEA.

As far as geographical disbursement of attackers goes, Russia and the Ukraine were dump sites for one group and Romania for a second. The third group doesn't have set exfiltration sites and appears to be a distributed network of attackers and tools.

Again, the malware fingerprints mentioned above played a role in connecting the dots.

Trustwave's constant coordination with law enforcement agencies worldwide through shared intelligence and evidence serves to help those agencies identify and arrest criminal groups such as those described above.





# LAW ENFORCEMENT AGENCY UPDATES





## U.S. SECRET SERVICE

### SEATTLE ELECTRONIC CRIMES TASK FORCE

**Robert Kierstead, Assistant Special Agent in Charge,  
Seattle Field Office**

In its continuing effort to combat cybercrimes, the U.S. Secret Service has an effective weapon with its successful Electronic Crimes Task Force (ECTF), created in New York in 1995. In 2001, the USA PATRIOT Act mandated that the Secret Service establish a nationwide network of task forces to “prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructures and financial payment systems.”

To this end, the Secret Service today has 31 ECTFs—located throughout the United States as well as London and Rome—that leverage the combined resources of academia, the private sector, and local, state and federal law enforcement in a coordinated effort. The partnerships allow ECTFs to identify and address potential cyber vulnerabilities before the criminal element exploits them. This proactive approach has successfully prevented cyber attacks that otherwise would have resulted in large-scale financial losses to U.S.-based companies or disruptions of critical infrastructure.

A recent case, investigated by the Secret Service’s Seattle ECTF, demonstrates how established partnerships employ both proactive and responsive investigative tactics targeting vulnerabilities utilized in the cybercrime underworld.

In the summer of 2011, the owner of a restaurant in Seattle contacted the Seattle Police Department when several customers complained fraudulent charges appeared on their credit card accounts shortly after they dined at the restaurant. Customers believed an employee had compromised their credit card information. However, many of the fraudulent transactions occurred in locations more than 1,000 miles from Seattle just minutes after victims made their purchases at the local eatery.

Seattle Police Department notified the Seattle ECTF investigators, who interviewed the restaurant’s employees and

Through Trustwave’s global reach in performing investigations into data breaches, partnerships with various law enforcement and Computer Emergency Response Teams (CERTs) around the world have formed. Each agency in this section has provided firsthand insight into the cybercrime problems facing its particular jurisdiction.





conducted a forensic examination of the restaurant's computer servers. The agents determined unknown suspects used malicious software and remotely hacked the establishment's payment system and stole voluminous amounts of credit card data.

Agents conducted additional forensic analysis of the restaurant servers and determined the perpetrators transmitted the compromised account information to a computer server located in Kansas. Working with the Secret Service office in Kansas City, agents discovered the server was linked to the debit card account of a potential suspect in Keedysville, Maryland. A task force investigator discovered information linking this suspect and other co-conspirators with network intrusions at numerous restaurant and retail businesses in over 20 states.

Seattle ECTF agents discovered a significant number of U.S.-based businesses experienced payment system intrusions similar to the restaurant's. Shortly after many of these incidents, suspects posted customers' credit card information for sale on illegal Internet carding sites. Online brokers purchased the stolen account numbers and distributed the data to smaller, loosely organized fraud rings nationwide. Members of these criminal networks re-encoded the stolen card numbers onto counterfeit credit cards and distributed the bogus cards to accomplices before issuing banks shut down the accounts.

In October 2011, agents from the Secret Service's Baltimore field office executed a search warrant on the suspect's residence and seized a laptop computer and other electronic storage media, which were sent to the Seattle field office for forensic examination. The forensic examiners discovered more than 86,000 stolen credit card numbers on the laptop.

The suspect and his co-conspirators were subsequently identified and charged with conspiracy, bank fraud, access device fraud and aggravated identity theft.

The suspect confessed his role in numerous network intrusions, including the Seattle restaurant. He told agents he worked in collusion with a European suspect to exchange information regarding techniques and methods in computer hacking. The two individuals created online carding websites for criminals to purchase stolen credit card information in large quantities and to exchange hacking procedures.

A total of 180,000 credit card numbers were stolen in this case, exposing the banking and credit card industry to a potential loss of \$90 million. The actual loss in this case is still being compiled and is believed to be approximately \$20 million.

This investigation exemplifies the Secret Service's ECTF model, which seeks to cultivate and leverage working relationships across transnational boundaries to relentlessly pursue cybercriminals in partnership with the private sector, law enforcement and prosecutors' offices.

In October 2012, U.S. Attorney Jenny A. Durkan of the Western District of Washington hosted a cybercrime conference in Seattle. This event focused on security, privacy and cooperation between law enforcement, the private sector and academia in combating cybercrimes. "Cyber threats are rapidly

evolving. They impact our daily lives, our economy, and our personal and national security. We will use every means to detect, disrupt and defend against this growing problem," explained Ms. Durkan, who serves as the chair of the Department of Justice Committee on Cybercrime and Intellectual Property Enforcement. "Fortunately, we are bringing the right people with better tools to the fight. To confront cyber threats we need to ensure that law enforcement, private industry and our international partners are sharing information, working together and coordinating responses," added Ms. Durkan.

Since its inception in 1865, the Secret Service has taken a lead role in mitigating the threat of financial crimes. As technology has evolved, the scope of the agency's mission has expanded from its original counterfeit currency investigations to also include emerging financial crimes. As a component agency within the U.S. Department of Homeland Security, the Secret Service has established successful partnerships in both the law enforcement and business communities—across the country and around the world—to effectively combat financial crimes.



## SERIOUS ORGANISED CRIME AGENCY (SOCA)

The Cyber department within the U.K.'s Serious Organised Crime Agency has a strong history of bringing online criminals to justice globally through direct prosecution and innovating new intervention solutions.

The fight to contain organized crime is rightly recognized as one of the threats to national security. The U.K. government has invested in providing SOCA with the skills and resources necessary to respond to the unique threats that include an explicit acknowledgement of the challenges now presented to law enforcement by cybercrime.

This support will extend through to 2013 and beyond when SOCA becomes part of the new National Crime Agency. The NCA will incorporate the National Cybercrime Unit, which will be dedicated to tackling the national and international complexities of this facet of criminality. As technology becomes more





accessible it will also address the increasing use of cyber-enabled crime by other criminals, whether they are using the Internet to commit fraud, cover financial trails, or attempt to conceal activity such as drug or human trafficking.

The chair of SOCA, Sir Ian Andrews, noted during a presentation to industry that: "...law enforcement can never expect to arrest its way to a cybercrime solution."

Not only are there the issue of international jurisdiction and the problems of transnational boundaries, but there is also a simple one of even prosecuting and jailing every individual who might be guilty of an offense online. Even if both criminal and victim are located within the U.K., the advent of cloud computing makes the legal and technical identification of responsibility for data complex and involved. Where traditional techniques of investigation and detection used to be obvious, the global paper chase of linking online crime to online criminal is increasingly involved and labor intensive.

As a result, SOCA manages a robust process of investigation, arrest and prosecution. Where this isn't feasible, the extensive international network SOCA has established supports our efforts to shut down criminal websites, facilities and accounts, denying them access at the source. Partner agencies and law enforcement globally support the intelligence gathering function and ensure that where arrests can't be made by U.K. officers, they can be made by local police instead. The effectiveness of this approach has already been demonstrated in joint activity with the FBI, European partners and other global agencies in coordinated activity made against automatic vending cart sites (AVC) catering to the online criminal community.

By shutting down criminal domains, using the intelligence gathered to generate further activity and identifying users within the U.K. who can be cautioned or arrested, depending on the severity of the abuse of the criminal site, a comprehensive approach to tackling a global issue can be generated.

It's not enough to simply shut down a site; those users who believe they have anonymity due to the nature of the Internet need to be identified and warned they are not able to escape legal action, even when online. Where SOCA has conducted visits or made arrests, word has spread quickly that we have the capacity to identify and contain threats to U.K. citizens.

This approach is both cost-effective and resource-light, allowing the heavy work of identifying key criminals that actually create and manage hacking tools to be freed up.

This approach—when applied in conjunction with specialists from the private sector, encouraging simple steps to increase security, reduce risks and expand awareness of the threat of cybercrime—provides an extensive solution to the varied problems it presents.

While law enforcement cannot sit in isolation in addressing such a complex and involved issue, it's important that organizations such as SOCA take a lead in managing the response. It's also crucial that government bodies demonstrate to the public that

they are protected by an efficient and well-trained group of officers who both understand and can respond to the many threats posed by online criminality.



## UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO CERT (UNAM-CERT)

UNAM-CERT is a team of information security professionals whose primary responsibility is to provide incident detection and response capabilities at the Universidad Nacional Autónoma de México (National Autonomous University of Mexico), better known as "UNAM" in México and Latin America. The initiative started in 1993 when the Computer Security Team was created as part of UNAM's Supercomputing Department.

In 1999 a formal Computer Security Department was created due to the rising need for highly specialized personnel and professional services to protect the university's IT assets. In 2001 UNAM-CERT was established, thenceforth being internationally recognized as a member of FIRST (Forum of Incident Response and Security Teams) and the only member in Mexico until 2010.

Since 2010, UNAM-CERT had their incident response process certified under the ISO/IEC 27001:2005 – Information Security Management System (ISMS) Standard as part of their continual improvement process. UNAM-CERT also provides other information security services, including penetration tests, security audits, implementation of best practices, specialized training, and content generation promoting both awareness and a culture for "online safety" in general. These services are primarily aimed at UNAM's schools, colleges, institutes and administrative areas, composed of 361,163 students and academic and administrative personnel.





UNAM-CERT keeps track of nearly 66,000 computers physically distributed on different campuses and facilities across the whole of Mexico. UNAM's primary network is composed of two Class-B networks on the Internet, connecting specialized academic and private networks in addition to providing Internet access to the entire infrastructure. UNAM's network is essentially open and highly diverse in terms of the type of services provided, existing applications and their use. Perimeter restrictions are minimal; therefore, it is essential to detect incidents based on alerts, enabling timely response and appropriate actions.

### INCIDENT DETECTION AND RESPONSE

The framework for threat, pattern and trend detection has been improved in the last 12 months by analyzing potentially malicious network traffic captured from a recently implemented "Darknet" composed of more than 20,000 unassigned IP addresses. In the same period, close to 1,060 low-interaction honeypots were deployed to identify new threats and obtain malware samples.

UNAM-CERT devised an initiative called "Sensors for Malicious Traffic" (or PSTM in Spanish) that involves the implementation of collaborating sensors composed of intrusion detection systems, traffic flow analysis and honeypots distributed throughout UNAM's network and other colleges and universities in Mexico.

### MALWARE ANALYSIS

A specialized team within UNAM-CERT focuses on research and analysis of malware behavior. Each week, almost 2,500 malware samples are captured from honeypots, or by propagation of new threat vectors through the network or obtained from user reports. An average of 15 new samples are recorded weekly.

Dynamic and static analyses of malware are performed to determine the potential impact and risk, and test results are published on the [www.malware.unam.mx](http://www.malware.unam.mx) website.

### CONTRIBUTION TO THE LAC REGION AND BEYOND

Since 2007, UNAM-CERT has participated as "UNAM-Chapter" within the International Honeynet Project in an effort to stay at the cutting edge in monitoring attacks and threats against Mexico's national infrastructure. The creation of incident response teams is highly encouraged by working on projects like AMPARO, sponsored by LACNIC, which aims to strengthen regional capacity attention to security incidents in Latin America and the Caribbean.

To promote prevention and information security awareness to the general public, UNAM-CERT in collaboration with the SANS Institute actively translates and distributes the monthly newsletter OUCH! Also, UNAM-CERT works nationwide with banks, ISPs, universities and other organizations by sharing relevant information about security incidents targeting their networks or their customers.



## NEW SOUTH WALES (NSW) POLICE FORCE CYBERCRIME SQUAD

The New South Wales Police Force Cybercrime Squad launched in November 2011 to protect Australia's most populous state. Since its inception, it has worked aggressively to identify and apprehend individuals participating in organized crime, cybercrime and technology-enabled crime.

Technology-enabled crime is fast-moving and complex. There are many challenges facing investigators, including cross-jurisdictional issues as well as the relentless pace of innovation shown by perpetrators.

Carding forums continue to be a major facilitator of credit card fraud in Australia. In these forums, data from compromised websites, in particular those of e-commerce merchants, are used by local criminals to go on shopping sprees and generate substantial profits.

In 2012, a member of several of these carding forums was identified by the NSW Police Force Cybercrime Squad's ongoing Strike Force Werewolf. Using the stolen credit card data purchased on the forums, he arranged for expensive items, in particular iPhones and other electronics, to be delivered to a network of addresses occupied temporarily by his accomplices and to virtual offices.

His carding activity also included flights and holiday rentals, Black Label scotch and somewhat less than gallantly, flowers for a girlfriend.

A search warrant was executed on his temporary accommodation, and substantial evidence of his crimes was recovered, including cash and electronic goods.

A financial analysis of his family showed unexplained deposits to the family home mortgage, and confiscation proceedings were commenced to recover around 900,000 Australian dollars.

He was charged with 58 offenses, including recruiting children to carry out these profitable crimes, and is currently awaiting sentence.





# THREAT INTELLIGENCE





Presented in this section is data from Trustwave client engagements and security telemetry from Trustwave products and services.

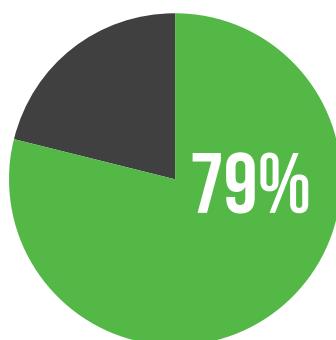
## ATTACKER SOURCES

Over the past 12 months, a large data set pertaining to global attacker origins has been acquired and built. These attackers are responsible for a number of malicious activities including (but not limited to) malware hosting, brute force and exploit attempts.

Through the use of geographically diverse network-based honeypots as well as Trustwave's worldwide security operation centers (SOCs), a picture of the threat landscape as it relates to source IP addresses of attackers emerges. In addition, Trustwave logged and analyzed more than 100 million attacks in the wild. While source IP addresses do not always establish the attacker's true location, they do help pinpoint the general location of a specific attack.

Attackers may also proxy, adding another layer of abstraction between the perceived location and the true origin. Trustwave has also been constantly aggregating a large number of malicious binaries from various Internet sources. As such, geographic data has been acquired as it relates to the location of malicious files. Using this information can help determine—with a fair amount of certainty—where attacks and malware originate.

**THE TOP 10 COUNTRIES  
ACCOUNT FOR ROUGHLY 79%  
OF NETWORK-BASED ATTACKS**



### NETWORK ATTACKS

A network attack is any connection that is used to perform an attack on a network-based protocol. Such examples include but are not limited to brute force attacks (against FTP, SSH, Telnet, etc.), exploit attempts on network-based services (SMB, FTP, RDP, etc.) and Web-based attacks (SQL injection, XSS, CSRF, etc.).

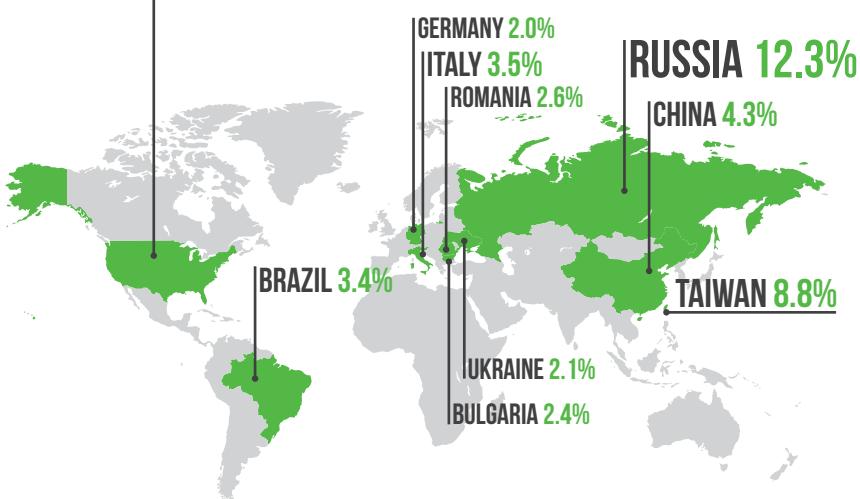
As in previous years, the two most active countries with respect to origin were the United States and Russia, at 37.8% and 12.3% of attacks, respectively. This is likely due to network infrastructure speeds and reliability, high resource availability and current legislation.

### MALWARE HOSTING

In this particular context, malware is defined as some malicious binary file being served on a Web server. Some examples include PE executables, PDF documents, ZIP files and Microsoft Word documents.

Russia and the United States are still the largest contributors when it comes to malicious activity, making up 39.4% and 19.7% of hosted malware, respectively. Notably, while the top 10 countries account for roughly 79% of network-based attacks, this statistic rises to more than 90% when looking at malware origin.

### UNITED STATES 37.8%





There are a number of reasons an attacker chooses a specific geographic location to launch a network-based attack or host malware:

1. **Availability:** Compromised machines and cheap hosted devices are very easy to acquire in countries that rank high on Trustwave's list of hosted malware.
2. **Access control lists:** More and more system and network administrators are placing restrictions against entire blocks of IP addresses for one or more countries or geographic regions. In order to thwart these restrictions, attackers are originating attacks from countries that are not blocked.
3. **Target environments:** A majority of online services are provided in a relatively small number of countries around the world. Therefore, attackers are often launching attacks in those same countries to avoid suspicion by the targeted entity.
4. **Legislation and law enforcement:** A country's extradition laws (or lack thereof) may entice an attacker to originate his or her attacks from a specific geographic location.

## ATTACKER MOTIVATIONS

### FINANCIALLY MOTIVATED ATTACKS

Cybercriminals can monetize activity using traditional credit card fraud and advertising banner click fraud or newer techniques such as fake electronic funds transfers (EFTs) and secret premium-rate SMS messages on smartphones. Criminal gangs in Eastern Europe have traditionally dominated these activities, turning them into million-dollar enterprises.

Credit card fraud usually involves compromising a card processing vendor or transaction clearing center to get access to the card data. Once card data is acquired, it's usually sold in bulk on underground forums for pennies per card. Buyers can then monetize the card data by creating counterfeit cards or processing online transactions.

**Advertising banner click fraud** is now completely automated by malware and botnets. The returns are low, as rates for clicks have dropped significantly in recent years, but the volume of clicks that can be generated and the relatively low overhead make this an attractive option for otherwise idle botnets.

**EFTs** are slightly more complicated than traditional click fraud, but the rewards can be much higher. The entire process can take just a few hours or even minutes, after which the money is gone and cannot be recovered. Often thefts like this are not covered by a bank's insurance, leaving the victims to suffer the financial consequences.

**Premium-rate SMS messages** are currently the most prolific on Android devices. These attacks start as malware (such as Loozfoon or FinFisher) that can send SMS messages to premium-rate SMS services. Users have no idea anything has happened until they get their bills.

Of course, these activities rely on various bits of infrastructure: botnets, drive-by malware installs, DoS attack services, anonymous money laundering, and even hosting criminal websites are all part of the underground economy that allows larger crimes to happen.

### ESPIONAGE

Espionage cases are often conducted by government-sponsored groups; currently, the most commonly accused is China, though Iran and Russia have had serious allegations levied against them as well.

In espionage cases, the initial attack vector is often a direct phishing attempt in which a PDF or Word document is emailed to a known contact within an organization. When opened, it triggers a previously unknown or zero-day exploit to compromise the machine. The attacker can then use this foothold to get deeper into the network and complete the breach.

This year, Trustwave discovered espionage malware including Flame, Mahdi and Gauss, which are closely related to Stuxnet and Duqu found in previous years—there really is no way to contain them.

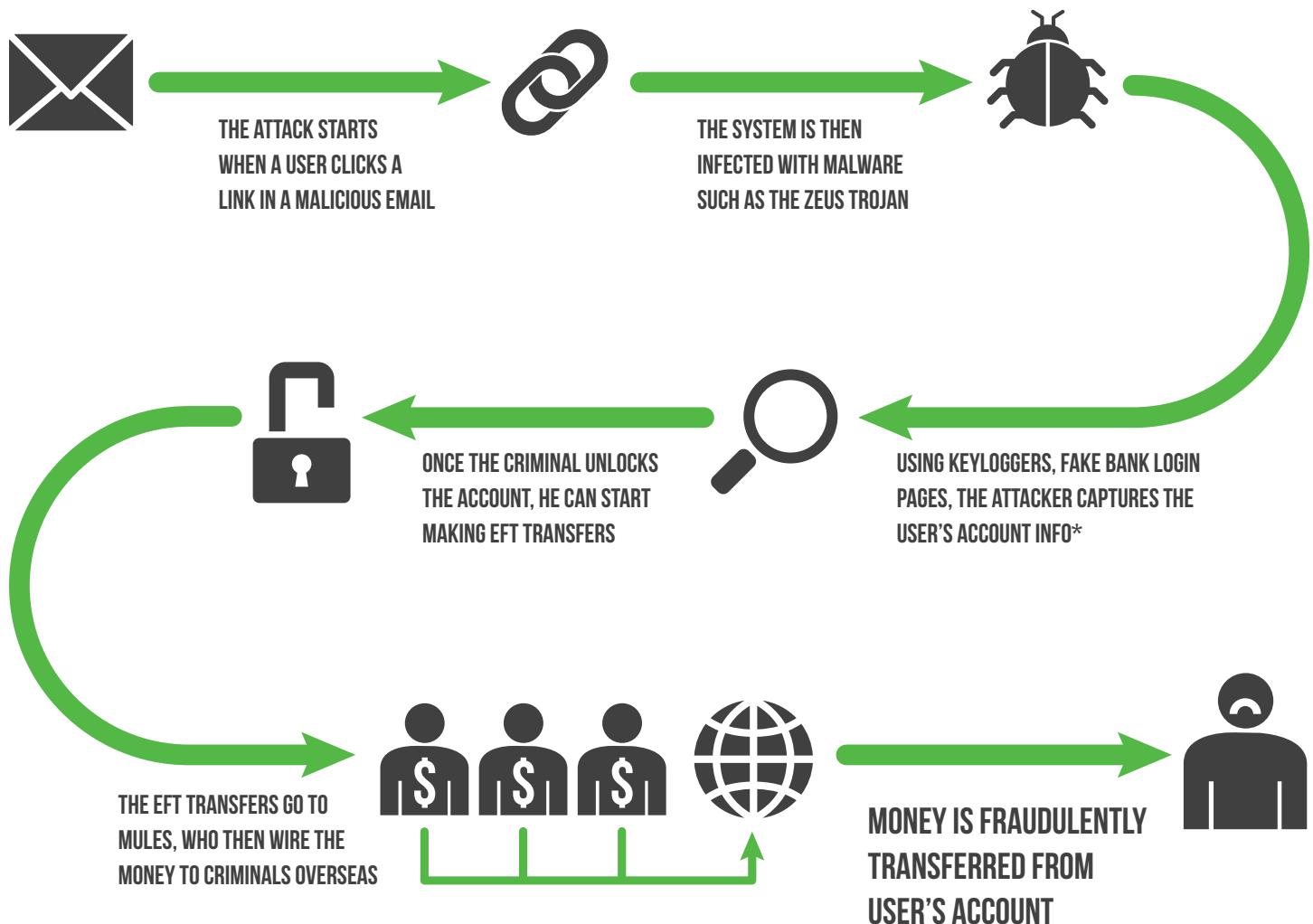
### HACKTIVISM

The most effective tool in the hacktivist toolbox is the DoS attack. Since many sites are hosted along with hundreds or thousands of other sites, a single DoS attack can have wide-reaching effects to disable other sites that just happen to be hosted on the same server.

Hacktivists have more specific targets than financially motivated attackers (who can target virtually anyone), and are therefore willing to exhaust other methods to make their presence known. Anonymous, arguably the largest and most well-known hacktivist group, has become increasingly fragmented, with factions sometimes take opposing viewpoints on the same topic.



## MALWARE-ENABLING EFT TRANSFERS



\* ADVANCED BANKING MALWARE CAN EVEN DEFEAT SECURITY FEATURES SUCH AS IP CHECKING BY THE BANK OR TWO-FACTOR AUTHENTICATION MECHANISMS USED TO DETECT FRAUDULENT LOGINS.



## EMERGING TECHNIQUE: SOPHISTICATED, EMBEDDED MALWARE

Embedded malware is not a new concept. Malware authors have been embedding files within one another for a couple of years now. But the technique has grown more complex. Now, analyzing Web-based attacks feels a lot like opening Russian nesting dolls: every time you open an attachment, there's another one hiding inside ... it's quite exhausting. In looking at a recent attack known as CVE-2012-4969, this complexity is clearly evident.

For instance, CVE-2012-4969 dealt with a zero-day vulnerability in Internet Explorer. Attackers chose to use an SWF file as part of the attack, encrypting it using a commercial tool called "doSWF." The tool essentially embeds the desired SWF as data within another SWF file and dynamically loads this inner SWF file during execution. Unwrapping the bundle reveals JIT spraying code and writes an iFrame back to the original HTML page from which the first SWF file was loaded.

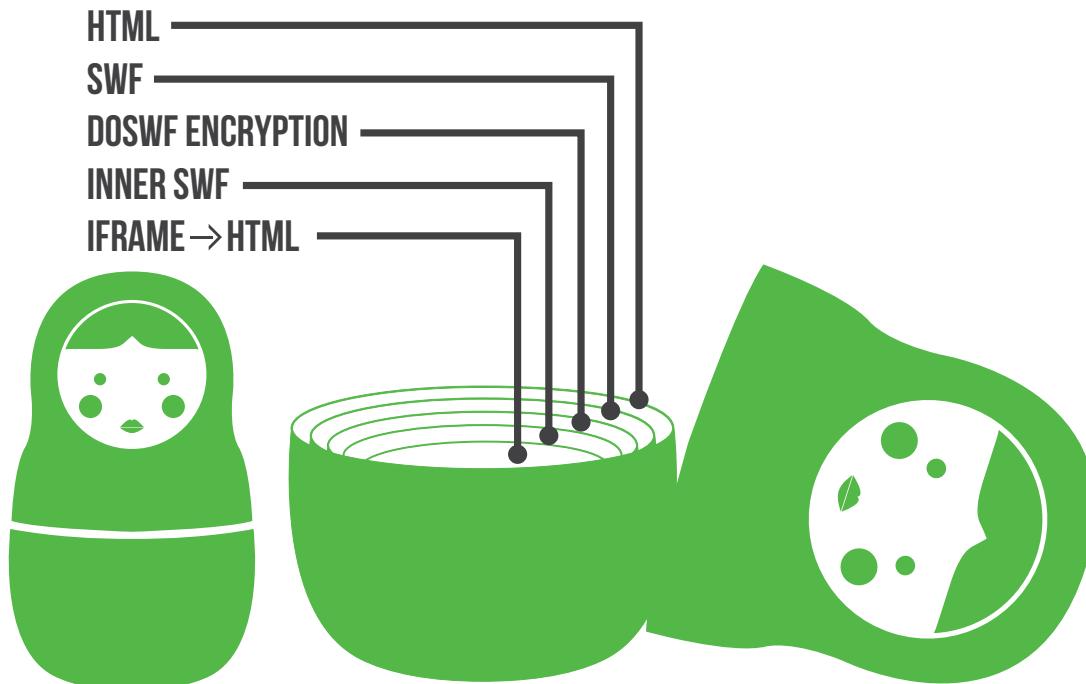
In another example, attackers used embedded malware to exploit the vulnerability CVE-2012-0754. The vulnerability was related to the way in which Adobe Flash Player parses MP4 files—this requires a SWF file that will load an MP4 file. The attackers embedded both a SWF and an MP4 file within a single PDF.

By abusing the way embedded files are managed within Adobe's Acrobat Reader, they referenced the embedded MP4 file directly and locally from within the embedded SWF file (which was loaded by the wrapper PDF).



The use of embedded files not only makes it extremely difficult for security products to detect malicious files but also exploits the functionality of each file format. It's becoming difficult for system administrators to control what can and cannot be executed. Flash Player does not need to be installed for a Flash file to be loaded within a PDF, MP4s can be loaded directly from within Flash Player, and most PDF readers will execute JavaScript code out of the box. Attackers make good use of these facts.

## EMBEDDED MALWARE IS LIKE NESTING DOLLS: FILES INSIDE FILES INSIDE FILES INSIDE FILES





## EMERGING TECHNIQUE: FAKE SSL CERTIFICATES

Digital certificates are core to the trust between users and software companies—as well as between clients who surf the Web and sites that deal with sensitive data. Code signed with a trusted digital certificate is treated by the OS as legitimate and is installed, bypassing protective barriers and alerts. The same goes for sites connected securely over SSL: if the site is using a trusted digital certificate, the browsers connect without alerting the client.



Some companies have taken steps to lower the risk of falling for fraudulent certificates; for example, Microsoft recently updated Windows to ban the use of digital certificates signed with RSA keys lower than 1024 bits, since they are relatively easy to brute force by attackers.

## NOTABLE FAKE SSL CERTIFICATES IN 2012

MARCH	APRIL	JUNE	SEPTEMBER
A Trojan called Mediyes was discovered on more than 5,000 computers, mainly in Western Europe. It was signed with a fake Symantec VeriSign digital certificate issued to Compavi AG, which is known to work with Swiss government agencies.	Evidences of a malware campaign against NGOs and human rights activists began to spread among the security community. A Chinese gang was allegedly installing digitally signed RAT malware using the CVE-2012-0158 exploit, including a digitally signed certificate issued by Quanzhou Xiegao Microwave Electronic Co. Ltd.	Microsoft released an urgent security advisory dealing with the revocation of two intermediate certificates. The malware, famously known as Flame (aka Flamer or sKyWIper), signed code with a fraudulent Microsoft digital certificate and took advantage of a design flaw in Microsoft's Terminal Services Licensing service that allowed them to sign their malware as if it originated from Microsoft and thus was recognized by the OS vendors as legitimate software.*	One of Adobe's servers used for signing Adobe software was attacked and then used for signing malware. While Adobe responded with the revocation of the misused certificate a few days later, the attackers still had time to distribute the signed malware until the certificates were revoked.

\*Microsoft Security Advisory 2718704:  
<http://technet.microsoft.com/en-us/security/advisory/2718704>





## DISCLOSURE TIMELINES

### TIMELINE | RESPONSIBLE DISCLOSURE

#### THREAT LEVEL



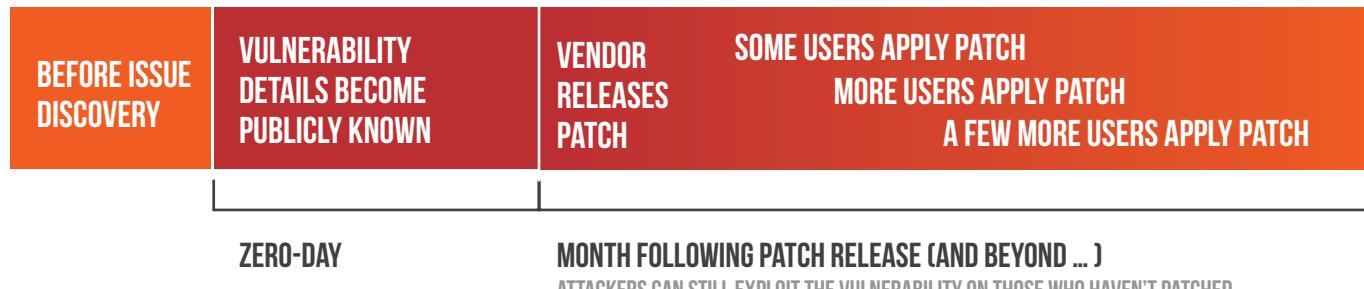
HIGH

NORMAL

0



### TIMELINE | ZERO-DAY



## CRITICAL VULNERABILITY STUDY: TRACKING ZERO-DAY RESPONSE TIMES

Malware is usually successful because of programming flaws in popular applications. Vendors have a crucial role in protecting systems from attack. A vendor-supplied patch is the only response that can truly fix vulnerability and help bridge the gap between a discovered attack and a vendor-supplied patch.

### ZERO-DAY, DEFINED

The gap between attack observation (or proof-of-concept code release) and patch availability is commonly referred to as “zero-day” (though it usually lasts more than a single day). Zero-day vulnerabilities represent a limited period of opportunity (lapse in protection) during which hackers can hastily put together campaigns. Discovery of zero-day periods can vary, but the first one to disclose the issue usually receives credit (and sometimes public notoriety).

Not all flaws are publicly disclosed in this way. Many security researchers, Trustwave included, believe in responsible disclosure: understanding and fixing certain flaws before publicizing them. During this time, the vulnerability is technically the same as a zero-day, but only the vendor and security researcher are aware—it is not being abused in the wild. In the end, the vendor and researcher release details consistently and simultaneously.

### TRACKING VULNERABILITIES

In the United States, these paths result in the creation of a common vulnerabilities and exposures (CVE) identifier. Each CVE assigned is catalogued in detail in the National Vulnerability Database (NVD),<sup>5</sup> which the nonprofit research organization MITRE references and uses as the de facto source of CVE data. Each CVE also contains a score that represents the vulnerability's severity, a product of the Common Vulnerability Scoring System (CVSS). The current version of this standard, CVSSv2, includes contextual information such as time and environment considerations.

5. nvd.nist.gov





This permanent record helps highlight turnaround times associated with the patching process. Using the platforms most frequently encountered by Trustwave's scanning and client security platforms as a baseline, this report offers an interesting look at how different vendors prioritize and fix vulnerabilities once they are discovered.

## DETAILS OF THE STUDY

This study focuses on determining time from discovery to patch release across a number of major vendors. It is non-exhaustive due to the sheer number of vendors and vulnerabilities, but it attempts to detect trends and uncover a better understanding than is currently available.

The report identifies these platforms through several methods:

- Trustwave TrustKeeper vulnerability scanner was used to assess the security posture of each network, using fingerprinting logic to see which type of platform is utilized on each server.

- Fingerprinting results were reviewed to find top platforms seen in the wild, based on one million Trustwave TrustKeeper users.
- Similarly, Trustwave Secure Web Gateway technology was used to obtain a list of the most prominent client platforms encountered.
- For each server platform, CVE information was filtered for vulnerabilities that posed a significant threat, denoted as a CVSSv2 score of 7.0 or higher.
- Client platforms were also chosen based on size of installed base and vulnerabilities observed.

For each platform in the list with vulnerabilities that met the severity criteria, corresponding vulnerabilities and research were scrutinized to determine:

- Whether the vulnerability was zero-day.
- Whether the vulnerability was discovered in-house or by a third party.
- The delta between the date the vulnerability disclosure and the patch release.

Product Name	Critical CVEs	Third-Party Reported	Number of Zero-Days	Average CVSS Score	Average Zero-Day Response
<b>2012 Server Vulnerabilities</b>					
Linux Kernel	9	4	2	7.68	857 DAYS
Microsoft Windows	34	34	2	8.41	375 DAYS
Cisco IOS	77	21	1	8.15	113 DAYS
PHP	8	6	5	8.13	90 DAYS
Wordpress	3	3	1	9.17	39 DAYS
OpenSSL	3	3	1	8.10	5 DAYS
ISC BIND	4	2	1	7.98	4 DAYS
phpMyAdmin	1	1	1	7.50	3 DAYS
Oracle MySQL	3	2	0	8.33	N/A
Microsoft .NET	6	5	0	9.30	N/A
Joomla CMS	1	1	0	7.50	N/A
<b>2012 Client Vulnerabilities</b>					
Microsoft IE	31	31	2	9.25	16 DAYS
Adobe Flash	58	56	2	9.92	9 DAYS
Oracle Java JRE	32	32	1	9.44	4 DAYS

Note: Time delta information is difficult to obtain due to the fact that Trustwave can discover only the date the information is received by the security community. While these dates cannot be 100% accurate, they are more reliable on the server side than on the client side, where there is less reliable instrumentation for the detection of threats. Threats such as Stuxnet, for example, have the potential to remain undetected for a long period of time.





## PHPMYADMIN

While most zero-day flaws stem from a programming error on the part of the developer, in this case phpMyAdmin code was compromised outside the organization. A server belonging to Sourceforge was compromised in September, affecting phpMyAdmin, whose code was modified to include a backdoor into infected systems after installation.

The first indication of this situation was discovered on Sept. 25, at which time phpMyAdmin published an advisory. Forensic records indicate that the breach occurred on Sept. 22, three days earlier, and was isolated to a single server. This is disturbing considering the number of phpMyAdmin downloads that occur daily, but the situation could have been much worse. This serves as a reminder that code contamination is a real threat. While open source mirrors are a likely target, Trustwave also witnessed this activity in the commercial software world when malicious insiders add their own backdoors to production code. Unlike those situations, however, there is nothing phpMyAdmin could do to prevent this; the mirroring system placed this issue completely out of their hands.

The items above are not recorded consistently by NVD (or any other database), so each CVE was researched in depth. Several cases were found to have missing details. Using search engines and security mailing lists such as Bugtraq<sup>6</sup> and Full Disclosure,<sup>7</sup> each of these advisories was fact-checked to ensure accuracy.

These numbers paint an interesting picture of the security landscape. Open source projects usually uphold constant code scrutiny, but some issues can fall through the cracks until someone digs them up years later. Commercial vendors, despite their secrecy, deal with this in their own way, encouraging proper disclosure but sometimes missing a public exploit until a researcher calls attention to it.

Also interesting is the difference between server and client-side zero-day response times. In the server space, there are a number of examples where a public exploit is not addressed for months—or even more than a year. Client zero-day vulnerabilities are patched quickly, usually within days, and garner a large amount of media coverage. The 49-day delay between the CVE-2012-0507 Java advisory and Apple's distribution of the fix was an unusual exception and caused

outrage from information security journalists. Compare this to CVE-2012-2386, a 403-day open flaw in a PHP core module that received almost no attention.

The ratio of released patches to reported vulnerabilities suggests that there could be a zero-day likelihood associated with a certain platform. In other words, the data suggests that researchers are more likely to publicly disclose findings on some platforms than on others.

Take, for example, PHP, which would certainly be among the platforms most likely to disclose findings, possibly because of the importance the PHP team places on these vulnerabilities. PHP is also open source, making it easier for independent researchers to find and test flaws. That being said, a majority of platforms in the study are open source; code availability does not necessarily equate with disclosure of vulnerabilities.

Even though Trustwave makes distinctions between “social” and “technical” penetration tests, most penetration testers will agree that every test is ultimately focused on people—those who create the code, configure the firewalls, disclose vulnerabilities and patch the systems. This study also shows that businesses and open-source projects have adopted very different ways of analyzing and responding to vulnerabilities.

## ATTACK TRENDS

### WEB CLIENT

A Web client is much more than a browser; it's a full-blown platform, with infrastructure, utilities and extensibility via plug-ins. This extensibility is what poses the most vulnerability, as malware authors disguise exploit kits as browser plug-ins. Since cybercriminals aim to exploit as many client machines as possible, they put a lot of effort into updating and improving exploit kits. For years, malware authors have been obfuscating their code to avoid AV signature detection, and this process is now automated (polymorphic JavaScript obfuscators are common in exploit kits, for example).

With the shift from HTML/JavaScript-centric browser attacks to browser plug-in attacks, it was only a matter of time before malware authors would adopt the same techniques. This means Java and ActionScript (the programming language used in Flash) now use automated obfuscation tools. And with these two languages, it seems malware authors have gone a step further, choosing to use commercial obfuscation tools.

The same exploit kit developers recognized a new opportunity this year and began distributing OS X malware as well. It was an expected move, since exploit kits are a proven malware delivery method. In other words, since the browser is the platform, malware authors couldn't care less about the underlying OS; they can achieve higher exploitation rates while reducing their R&D costs.

6. <http://seclists.org/bugtraq/>  
7. <http://seclists.org/fulldisclosure/>





## Most Observed Web Exploits Used

CVE	Name	Percentage of CVE-Based Detections	Month Disclosed	Used in a Zero-Day Attack?
CVE-2009-0927	Adobe Reader GetIcon JavaScript Method Buffer Overflow Vulnerability	<div style="width: 32.4%; background-color: #2e6b2e; height: 10px;"></div> 32.4%	MAR-09	YES
CVE-2010-0188	Adobe Acrobat and Reader CVE-2010-0188 Remote Code Execution Vulnerability (libTiff)	<div style="width: 21.4%; background-color: #2e6b2e; height: 10px;"></div> 21.4%	FEB-10	YES
CVE-2012-1889	Microsoft MSXML ActiveX Remote Code Execution Vulnerability	<div style="width: 16.1%; background-color: #2e6b2e; height: 10px;"></div> 16.1%	JUN-12	YES
CVE-2004-0549	Microsoft Internet Explorer Self-Executing HTML Arbitrary Code Execution Vulnerability	<div style="width: 13.4%; background-color: #2e6b2e; height: 10px;"></div> 13.4%	JUN-04	YES
CVE-2007-5659	Adobe Acrobat and Adobe Reader CollectEmailInfo JavaScript Method Buffer Overflow Vulnerability	<div style="width: 3.6%; background-color: #2e6b2e; height: 10px;"></div> 3.6%	OCT-07	YES
CVE-2010-1885	Microsoft Windows Help and Support Center Protocol Handler Vulnerability	<div style="width: 3.6%; background-color: #2e6b2e; height: 10px;"></div> 3.6%	JUN-10	YES
CVE-2009-0075	Microsoft Internet Explorer Cloned DOM Object Malformed Reference Vulnerability	<div style="width: 2.7%; background-color: #2e6b2e; height: 10px;"></div> 2.7%	JAN-09	NO
CVE-2008-2992	Adobe Reader util.printf() JavaScript Function Stack Overflow Exploit	<div style="width: 1.7%; background-color: #2e6b2e; height: 10px;"></div> 1.7%	JAN-08	NO
CVE-2006-0003	Microsoft Internet Explorer RDS ActiveX Vulnerability	<div style="width: 1.1%; background-color: #2e6b2e; height: 10px;"></div> 1.1%	APR-06	NO
CVE-2012-0507	Oracle Java Applet java.util.concurrent Type Confusion Remote Code Execution Vulnerability	<div style="width: 1.1%; background-color: #2e6b2e; height: 10px;"></div> 1.1%	FEB-12	NO
CVE-2011-0611	Adobe Flash Player CVE-2011-0611 SWF File Remote Memory Corruption Vulnerability	<div style="width: 1.1%; background-color: #2e6b2e; height: 10px;"></div> 1.1%	APR-11	YES

Analyzing more than 5 million malicious URLs passing through Trustwave Secure Web Gateway, Trustwave found that the popular exploits targeted products like Internet Explorer (IE), Adobe Acrobat Reader, Adobe Flash Player, Oracle Java and Microsoft Office. While some exploits were new in 2012, others were patched years ago. This issue repeats itself year after year; users and organizations alike often use unpatched software or patch their software late.

Interestingly, there was a significant increase in zero-day vulnerabilities detected in Java in 2012, particularly those exploited via the browser plug-in. These vulnerabilities were quickly adopted by malware authors such as in the Blackhole exploit kit. Java is successfully exploited because:

- Its browser plug-in is widespread, even though most users don't need it.
- Java is cross-platform, making it a great research target for malware authors.

- Some vendors, such as Apple, are usually late in rewrapping Java patches, making the zero-day last longer.

The most prevalent exploits targeted Adobe products, mostly Acrobat. Adobe recently added an auto-updating mechanism (which initially requires user approval), with the aim of helping reduce such widespread vulnerability.

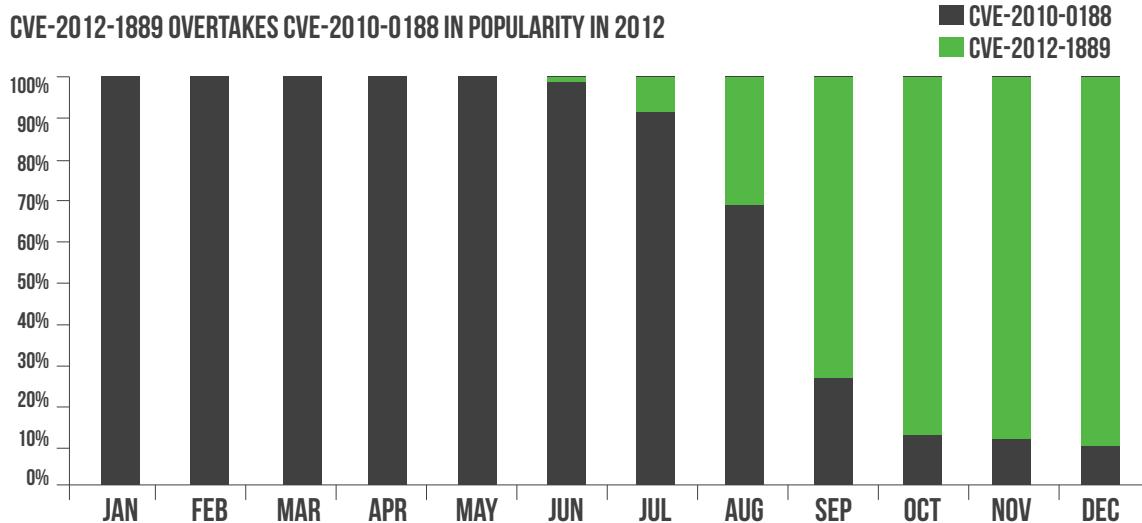
Two IE zero-day vulnerabilities were actively exploited in 2012, causing Microsoft to release out-of-band security updates. One of those, CVE-2012-1889 (Remote Code Execution Vulnerability in Microsoft XML Core Services), became so popular that it was the third-most prevalent exploit in 2012, quickly replacing the aging CVE-2010-0188 (Remote Code Execution Vulnerability in Adobe Acrobat Reader). ([See graph on next page.](#))

Last, old vulnerabilities are still popular. Most exploit kits keep fallback exploitation code for target organizations still using older software.





### CVE-2012-1889 OVERTAKES CVE-2010-0188 IN POPULARITY IN 2012



### Exploit Kits

Exploit kits are well-established in the cybercrime market. The exploits generated by the latest kits are heavily obfuscated in order to avoid antivirus detection, and some even abuse differences in browser behavior to mislead automatic deobfuscators, such as JSunpack and Wepawet, which usually emulate behavior of only one browser.

Low-sophistication evasion techniques to avoid automatic exploit kit scanners and security engine detection include randomizing exploit page file names, hiding the malicious content inside comments and use of legitimate packers for malicious purposes.

Rather than quantity over quality, attackers are now looking for reliability in their exploits. They want packs with a few reliable exploits in them, which helps ensure that the target machine is vulnerable to the specific exploit before executing it.

### Commercial Obfuscators

Attackers are using commercial obfuscators—but whether they actually buy licenses or simply crack legitimate software is not confirmed. The fact remains: Anti-malware products and security researchers alike are increasingly combating malicious code hidden with commercial products.

Java malware makes use of commercial obfuscators like Allatori and DoSWF. The most advanced obfuscators don't need to change the Java source at all; instead, they obfuscate bytecode (the compilation result of Java code). Obfuscation at the bytecode level greatly increases the difficulty of analyzing malicious Java; such modification can make it impossible to accurately decompile the code for research purposes.

ActionScript has also seen its fair share of obfuscation advances. Simple obfuscation means changing variable names and making modifications to the code flow. Sophisticated obfuscation involves compressing the Flash file and wrapping it in a second file that

performs the decompression. This means that there's a new Flash file, with new ActionScript code, that has to unpack the original file before it can be executed. Multilevel obfuscation like this raises the bar for researchers and automated analysis tools.

### MOST OBSERVED COMMERCIAL OBFUSCATORS USED IN 2012

OBFUSCATOR TYPE	OBFUSCATOR NAME
	Allatori
	KlassMaster
	Kindi SecureSWF
	DoSWF

### Malware for Mac

This year was a roller coaster of uncertainty for Mac users, most notably from the unexpected Flashback virus. Surprisingly, the infection method relied mostly on unpatched Java vulnerabilities, where the exploit payload will execute regardless of underlying OS (i.e., if the payload is "download and execute," it will in fact download and execute no matter what the OS).

Flashback distributors relied on three different Java vulnerabilities: the trusted JList chaining vulnerability (CVE-2010-0840), the infamous Rhino (CVE-2011-3544) and the AtomicReferenceArray (CVE-2012-0507).





Flashback's permeation was a direct result of Java being enabled by default. At the time, Apple updated Java on the OS X platform about one to two months behind schedule. At this time, Apple has disabled the Java plug-in by default. Disabling or removing unused software can effectively minimize the attack surface.

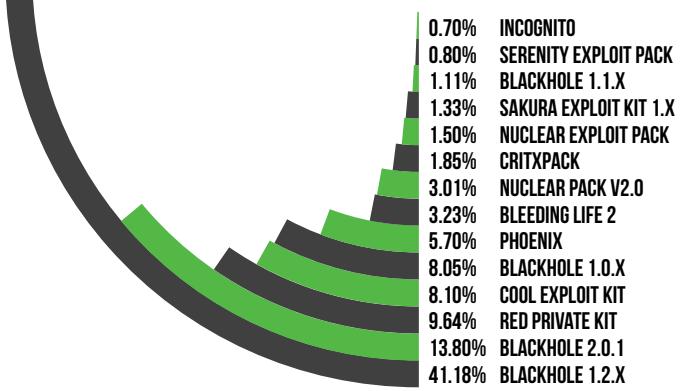
### Most Prevalent Exploit Kits Seen in 2012

Several new tool kits were found this year, while others were "updated." Blackhole remained the most prevalent by far.

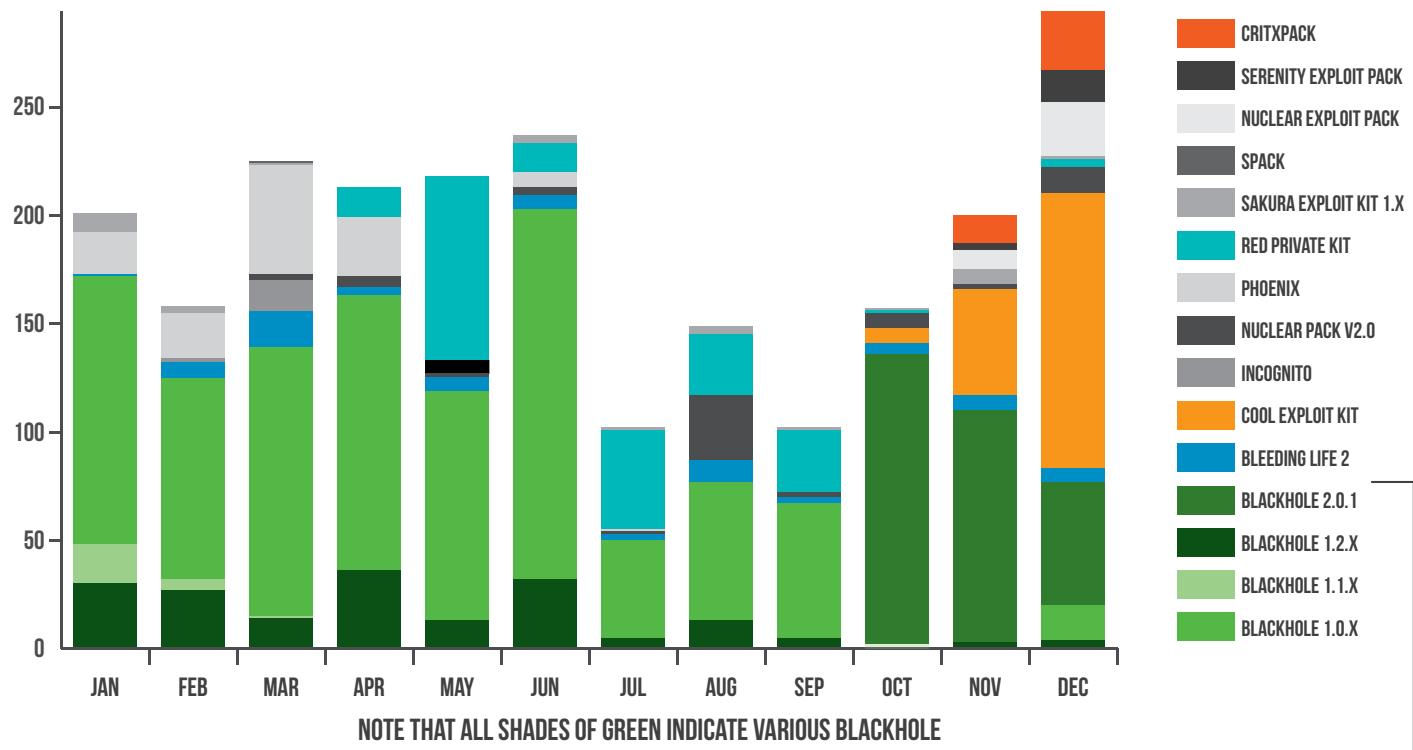
Several kits that were popular in 2011, such as Eleonore and Spack, have gone off the charts. And exploit kits like Phoenix have been deprecated (i.e., no versions were released recently).

Exploit kits continue to draw industry attention time and again. Financially motivated developers keep creating new and better versions, building a marketplace for exploit kits. Development of deobfuscator tools may also be on the rise for 2013.

## MOST PREVALENT EXPLOIT KITS SEEN IN 2012



### 2012 EXPLOIT KIT INSTANCES BY MONTH





## WEB SERVER

Websites are a valuable target for cybercriminals. Target selection falls into two categories:

- **Targeted attacks:** Chosen specifically for monetary gain, hacktivist or political motivations. Once the target is selected, attackers must identify some type of vulnerability to exploit in order to achieve their goals.
- **Random opportunistic attacks:** Specific known vulnerabilities are chosen rather than specific target organizations. These types of attacks are largely automated, and success is measured by the quantity of compromised sites.

### Targeted Attacks

Here the focus is on real-world Web application breaches in which victim sites are targeted for financial gain or political or hacktivist reasons. Data is sourced from the the Web Application Security Consortium (WASC) Web Hacking Incident Database (WHID) project.<sup>8</sup> WHID is dedicated to maintaining a list of publicly disclosed Web application-related security incidents, to raise awareness and rate risk level, as well as focus on the attack's impact.

To be included in the WHID, an incident must be publicly reported, be associated with Web application vulnerabilities and have an identified outcome.

The number of incidents reported in 2012 is approximately 400, compared to 289 in 2011. Since this sample includes only publicly disclosed compromises, analysis is based on relative percentage.

Hacktivists narrowed in on disrupting normal business operations; downtime (32%) and defacement (24%) were two goals toward that end. During 2012, political and activist groups,

such as Anonymous, primarily used DoS attacks to knock target websites offline for extended periods of time.

**Monetary loss**, occurring in 5% of incidents, is largely the result of criminals utilizing various methods to fraudulently transfer funds from online bank accounts using client-side banking Trojans like Zeus and SpyEye. Banking Trojans pose a major problem not just for the end users that become infected but also for financial Web applications. Better fraud detection capabilities are needed to identify abnormal behaviors when malicious programs attempt to transfer funds out of the victim's accounts.

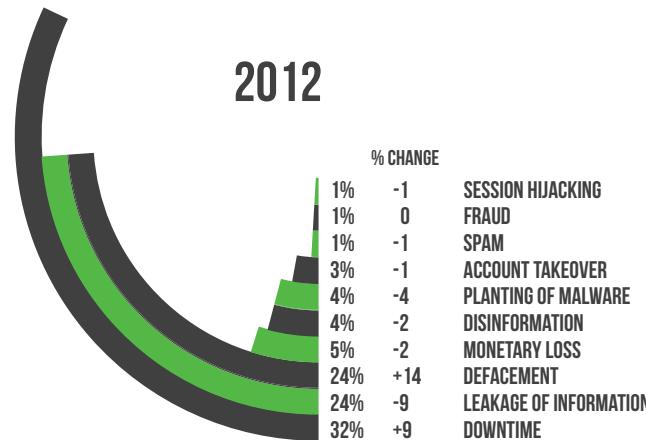
### Attack Methods

The top attack category is Unknown, meaning 46% of the incidents reported did not specify a specific attack method. This is likely attributable to:

1. **Insufficient/nonexistent logging:** Organizations have not properly configured their Web application infrastructure to provide adequate monitoring and logging mechanisms, sometimes a simple logic flaw. If proper monitoring mechanisms are not in place, attacks and successful compromises may go unnoticed for extended periods of time. The longer the intrusion lasts, the more severe the aftermath. Visibility into HTTP traffic is one of the major reasons why organizations often deploy a Web application firewall (WAF).
2. **Public disclosure resistance:** Most organizations are reluctant to publicly disclose compromise details for fear of public perception and possible impact on customer confidence or competitive advantage.

After Unknown, DoS is the No. 1 attack method because it results in downtime. Attackers constantly create tools to facilitate DoS attacks—such as WHID 2012-372, in which Chase and the NYSE were targeted, or WHID 2012-368, in which GoDaddy was stopped by a massive DoS attack.

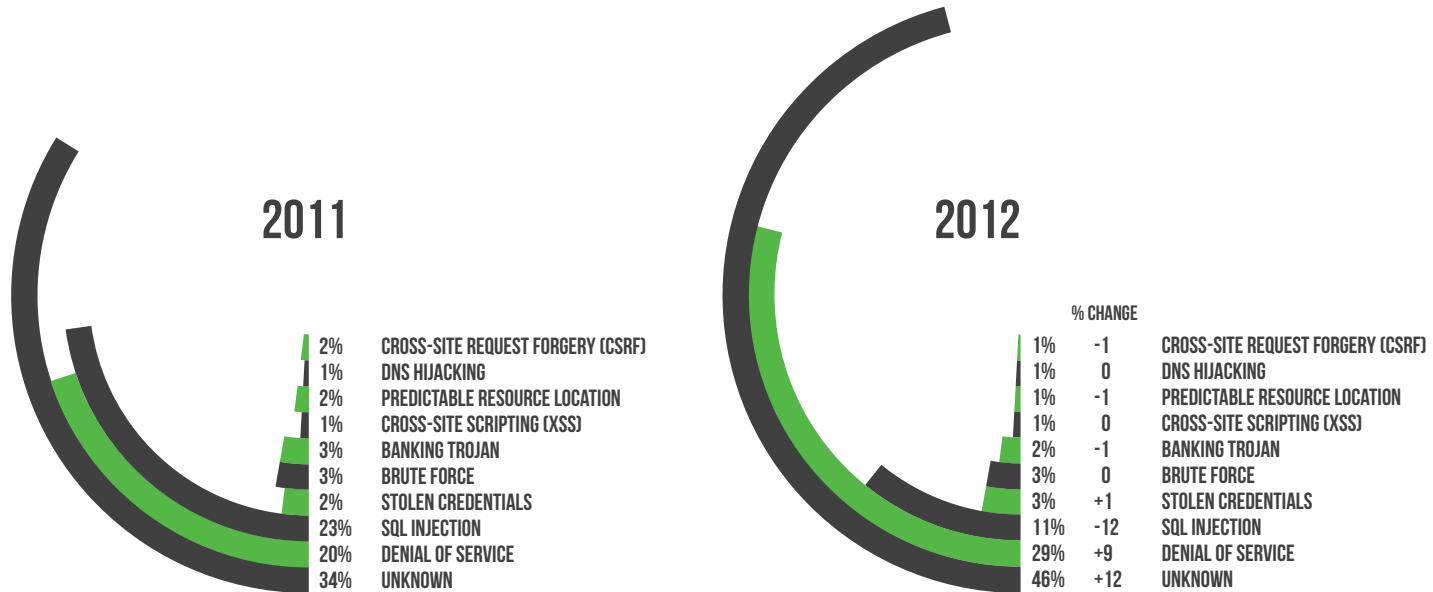
## TOP 10 WHID OUTCOMES



8. Trustwave SpiderLabs is the WHID project sponsor. For further information about the WHID, refer to <http://projects.webappsec.org/Web-Hacking-Incident-Database>. For a list of all active projects, visit Trustwave's website at <https://www.trustwave.com/spiderLabs-projects.php>.

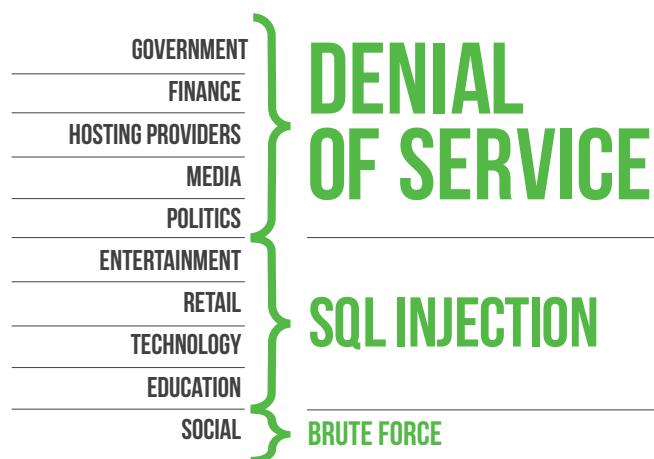


## TOP 10 WHID ATTACK METHODS



## TOP WEB ATTACK METHOD BY VERTICAL MARKET

2012



## Random Opportunistic Attacks

To gain insight into opportunistic attacks, Trustwave analyzed more than 9 million Web application attacks during 2012 from:

- **Web honeypot sensors:** Roughly 100 Web servers distributed in Austria, Canada, France, Germany, Hungary, Italy, Japan, Korea, Macedonia, Netherlands, Poland, Russia, Turkey, the U.K. and the U.S.
- **Web application firewall (WAF) alerts from hosting providers:** Through a strategic opt-in partnership with some commercial hosting providers using the open source.

Using Trustwave WAF technology, Trustwave identified 205,660 unique Web domains that were attacked.

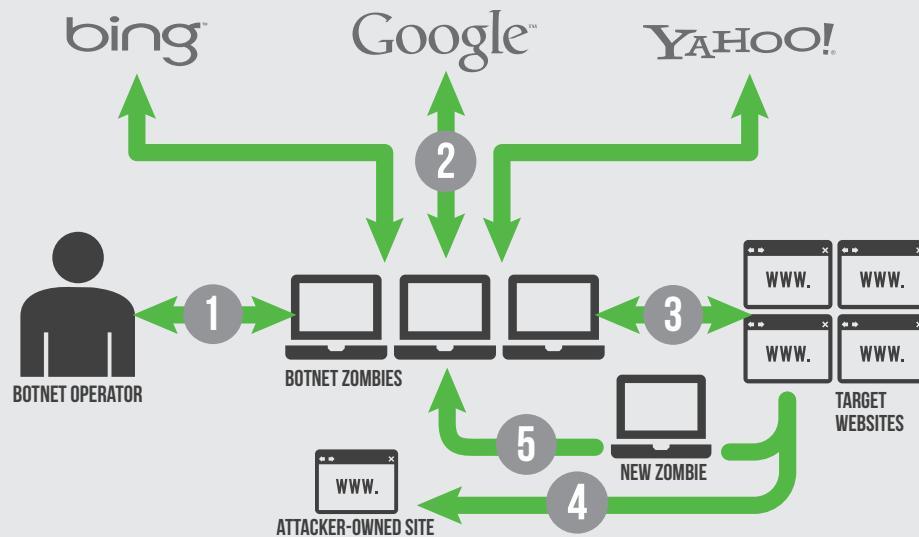
Two main threat agents were identified in 2012:

- Botnet owners looking to recruit sites into their control.
- Malware proprietors whose goal is to infect the clients with exploit kits such as Blackhole.

In both cases, threat agents want to control as many websites as possible through whatever means necessary. This is typically achieved by executing RFI or similar attacks that trick the Web application into downloading malicious code from an attack-controlled website.



## THE LIFE CYCLE OF WEB SERVER BOTNET RECRUITMENT



### The Life Cycle of Web Server Botnet Recruitment

Trustwave was able to capture vast amounts of data within Web honeypots to accurately illustrate how botnet owners compromise websites and make them part of their army. The data in this section shows examples of code snippets and log file entries from real captured attacks.

#### Step 1: IRC botnet instructs zombies to search for targets

First, attackers identify potential target sites. While it is possible to methodically scan network ranges looking for targets, it is more efficient to use data already collected by legitimate search sites (e.g., Google, Bing, Yahoo). By using their built-in search capabilities, botnet operators can instruct zombies (previously compromised websites or home computer systems) to send custom search queries.

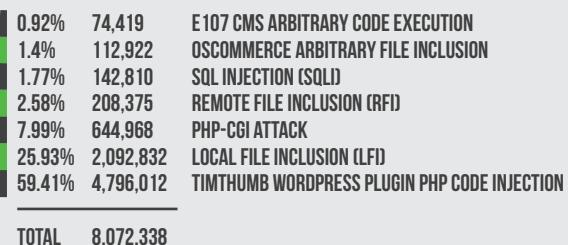
#### Step 2: IRC botnet zombies conduct search engine queries

Zombie clients receive their search commands from the operator and use code to send requests to the various search engines. The results are then parsed to identify target websites that match the vulnerability search data.

#### Step 3: IRC botnet instructs zombie to scan targets for vulnerabilities

Next, zombies verify the existence of the vulnerabilities in the target websites.

### TOP WEB VULNERABILITIES TARGETED BY BOTNET OWNERS





#### Step 4: IRC botnet instructs zombie to exploit vulnerability & install botnet client code

These malicious requests attempt to trick the Web application into downloading the code (hosted on a remote, attacker-owned site). If the Web application is vulnerable, it attempts to download the code. In most cases, simply downloading the code is enough, since the attacker can access the file by Web browser.

During 2012, Trustwave identified 2,546 attacker-controlled websites that were being used as RFI payload distribution points. Trustwave also captured 3,788 malicious RFI code samples, grouped into the following categories:

## MALICIOUS RFI CODE SAMPLES



3,788

- BASIC FILE UPLOADER 1,033**
- R57SHELL BACKDOOR WEBSHELL 889**
- IRC BOTNET CLIENT SCRIPTS 597**
- C99SHELL BACKDOOR WEBSHELL 284**
- CUSTOM WEBSHELL 285**
- BASIC RFI VULNERABILITY TESTING 241**

#### Step 5: Compromised site joins the IRC botnet army

The final step is for the compromised website to join the botnet as a zombie client. The exploit files installed have all the proper IRC channel and authentication credentials. Once logged in, the botnet operator can then control the website and use it as part of ongoing exploitation. Once the server has been compromised, the botnet owner can use it to:

- Search, scan and exploit other Web servers.
- Modify site content to conduct drive-by downloads for browser exploit kits.
- Participate in DoS attack campaigns.

## MAIL-BASED ATTACKS

According to a recent report by The Radicati Group Inc., there were more than 2 billion email users worldwide and more than 140 billion emails sent daily in 2012.<sup>9</sup> Not surprisingly, email remains an extremely popular conduit for cybercriminals to distribute attacks, whether through mass spam attacks or targeted attacks.

## MAIL-BASED TRENDS FROM 2012

LARGE REDUCTION IN SPAM VOLUME TO A LEVEL  
**LOWER THAN IN 2007**

BUT SPAM STILL REPRESENTS **75.2%** OF  
A TYPICAL ORGANIZATION'S INBOUND EMAIL

**10%** OF SPAM MESSAGES ARE MALICIOUS

NEARLY **7%** OF SPAM CONTAINS A  
LINK TO A MALICIOUS WEBSITE



**OVER 80%** OF MALICIOUS SPAM ORIGINATED  
FROM ONE BOTNET, CUTWAIL

PHISHING REMAINED LOW AT **0.17%** OF SPAM

9. <http://www.radicati.com/wp/wp-content/uploads/2012/10>Email-Market-2012-2016-Executive-Summary.pdf>





## Spam Volume Declines

Trustwave measures spam output through a proxy, called Spam Volume Index (SVI), which tracks changes in the weekly volume of spam received by a representative bundle of domains. The index is linear, so a 50% drop in the index reflects a 50% drop in spam volumes.

In 2012, the average SVI value was just 755, less than half of what it was in 2011 and even less than when Trustwave started the index in 2007.

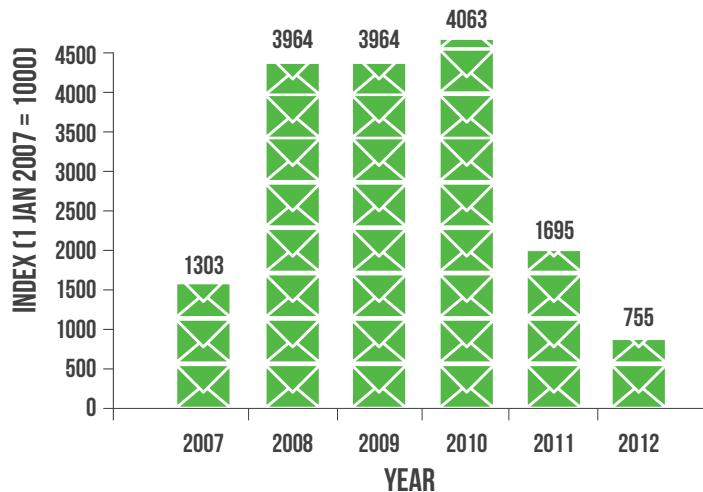
The boom years for spammers occurred between 2008 and 2010, with several large botnets and programs operating largely unhindered during that time.

The decline, from 2010 to present, reflects a number of complex, interrelated factors:

- Disruption of major spamming botnets (Rustock, Mega-D, Cutwail, Festi, Lethic and Grum) by law enforcement or researchers. In some cases, the effects have been temporary as operators have simply shifted control servers and built botnets again.
- Closure of spam affiliate programs, notably Spamit.com in late 2010, and the police apprehension of other program operators.

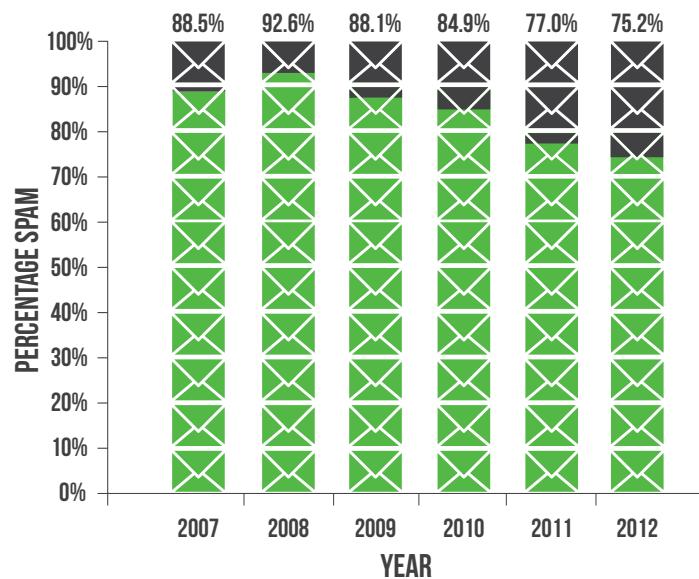
## TRUSTWAVE SPAM VOLUME INDEX

AVERAGE INDEX VALUE BY YEAR  
EACH EMAIL ICON = 500



The decline in spam means email systems and administrators no longer have to struggle with unmanageable volumes of spam from large and out-of-control botnets. However, the spam that's left is still enough to constitute 65% to 75% of a typical organization's inbound email.

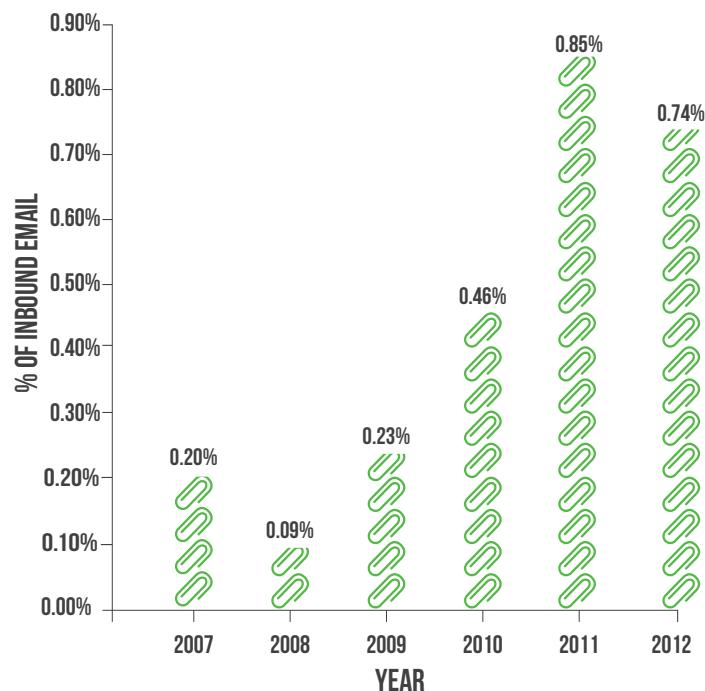
## SPAM AS A PERCENTAGE OF INBOUND EMAIL



Though volume has dropped, malicious spam has increased, demonstrated by the inbound messages with executable attachments—.85% of spam in 2011 and .74% in 2012.

## PERCENTAGE OF EXECUTABLE ATTACHMENTS

EACH ATTACHMENT ICON = 0.50%





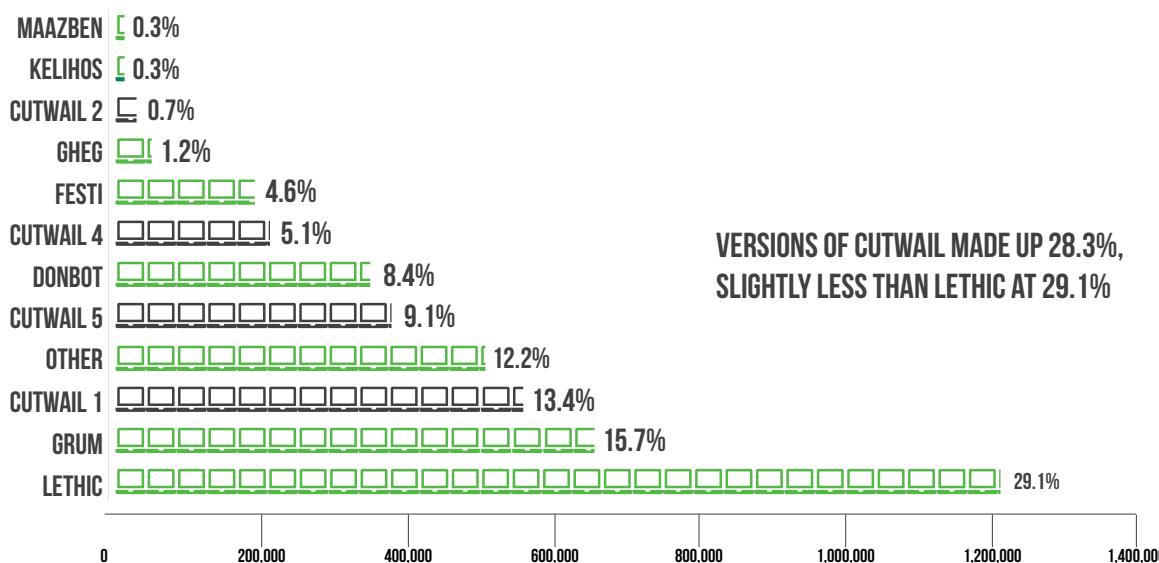
## Spam Botnets: Under Pressure

The most active spamming botnets are measured by filtering spam arriving at Trustwave's spam traps according to bot traits. Most prevalent in 2012 were Lethic, Grum and several Cutwail variants. The top seven botnets were responsible for more than 85% of all spam, consistent with findings from previous years. The chart Top Spam Botnets 2012 should be considered a snapshot in time because, in practice, spamming botnets are constantly in flux; they morph, become obsolete, are replaced or are upgraded in response to market forces, competition and law enforcement.<sup>10</sup>

### TOP SPAM BOTNETS 2012

AS A % OF TOTAL SPAM

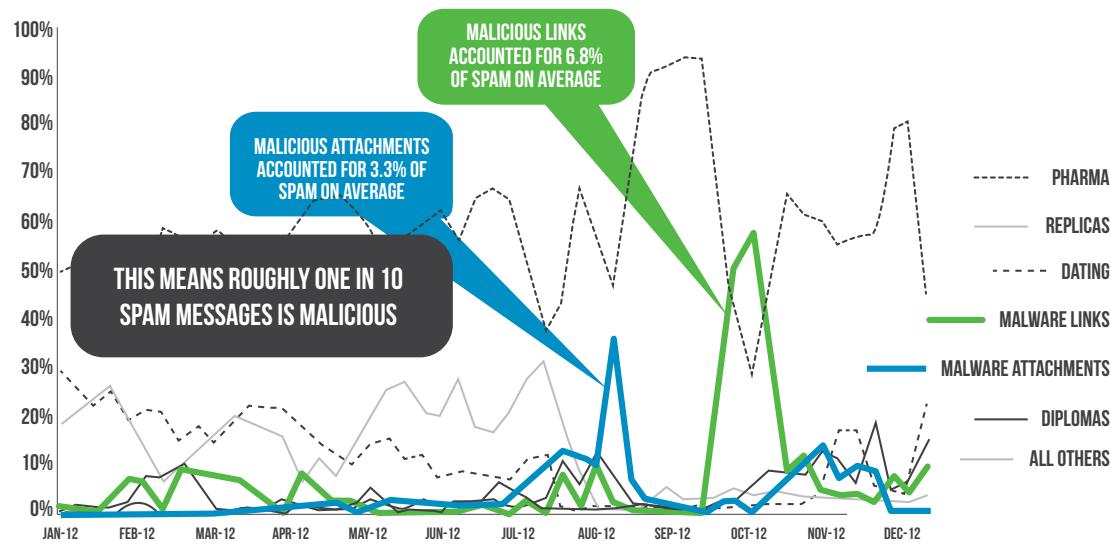
- = VERSIONS OF CUTWAIL
- = OTHER



## Spam Categories: Mass Malicious Campaigns a Big Threat

This year, for the first time, Trustwave separated messages with malicious attachments and those with links leading to malicious sites. Malicious links were found in an average of 6.8% of spam, while malicious attachments made up an average of 3.3%. In other words, roughly one in 10 spam messages was found to be malicious.

### SPAM BY CATEGORY 2012



10. For an up-to-date view of spam statistics, visit [https://www.trustwave.com/support/labs/spam\\_statistics.asp](https://www.trustwave.com/support/labs/spam_statistics.asp).





## Mass-Spammed Links to Blackhole

Spam packaged in realistic-looking templates and often mimicking major brands was a major issue in 2012. This spam mostly originated from Cutwail bots, with links leading to installations of the Blackhole exploit kit, which then seeks to install malware. Such spam campaigns are ongoing, widespread and change templates daily, and the list of impersonated brands includes most major companies in business today.

These campaigns work. One Blackhole server had a 10% exploit rate after people clicked the link in the spam message.<sup>11</sup> The messages are carefully crafted to be convincing, so much so that Trustwave receives daily feedback from end users seeking to recategorize malicious links that are blacklisted as a result of these campaigns.



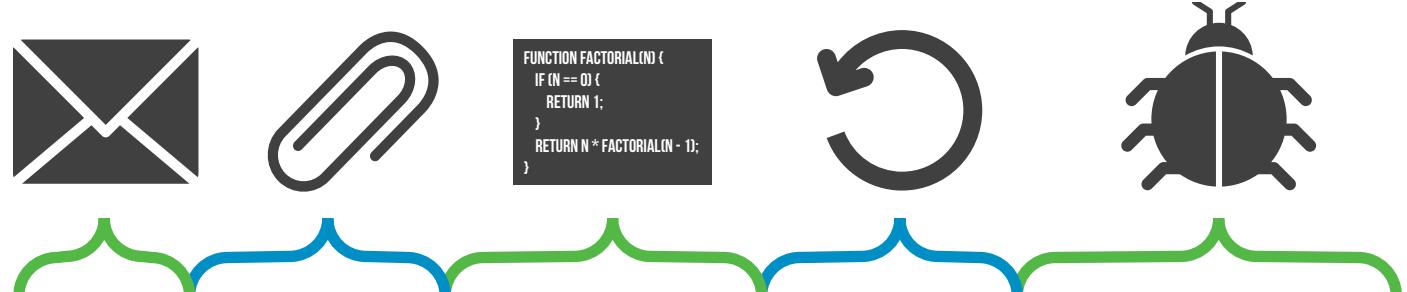
Treat every message with suspicion and carefully check URLs by hovering over links. Virtually all the exploits targeted by Blackhole are public and patches are available, and ensuring that software is up to date can further provide protection. Mail filtering to reduce inbound spam and a secure Web gateway to prevent users from accessing bad links may also be necessary.



**MALICIOUS SPAM MIMICKING LEGITIMATE COMPANY EMAIL WITH BOGUS LINKS LEADS TO BLACKHOLE EXPLOIT KIT**

## Spammed Malware Attachments With a Twist

Spam with malicious attachments is still a time-honored tradition among cybercriminals. As noted, 3.3% of spam in 2012 carried a malicious attachment. Most of these were standard win32 executable files, but a significant number were HTML files that when opened directed to Blackhole. And, like the messages with malicious links, these attachments also originated from Cutwail bots. In fact, Cutwail operators simply alternate between executables—HTML file attachments and malicious links—from day to day.



**HTML EMAIL ATTACHMENT WITH MALICIOUS JAVASCRIPT WILL REDIRECT TO THE BLACKHOLE EXPLOIT KIT**

11. Visit The Trustwave SpiderLabs blog for message examples: <http://blog.spiderlabs.com/2012/07/wham-bam-the-cutwailblackhole-combo.html>.





## Phishing Remained Constant

Levels of traditional phishing, in which users are lured to websites and asked to enter personal data, are relatively low. In 2012, around 0.17% of spam was phishing, the same as in 2011. Like malicious spam, there has also been a trend to using HTML attachments, where users are encouraged to enter data into an attached form.

## Targeted Attacks Often Start With Email

Concern over targeted attacks is increasing. In previous years and in 2012, the initial attack is frequently carried out by email, and this situation showed no sign of abating during 2012.

Targeted attacks are often thought to be ultrasophisticated and cutting-edge, using clever zero-days and custom malware. In fact, they are usually mundane, with messages taking advantage of:

- **Social engineering:** Common email themes are conferences, internal communications, employee reviews, surveys, meeting invitations and security updates.
- **Context:** The email makes sense to an employee of that organization.
- **Homework:** Attackers do their research, collect employee email addresses, and the “From” field is changed so it appears to come from someone known to the organization.
- **Attachments/links:** There is typically a malicious attachment (.doc, .xls, .pdf) that contains exploit code. Executable file attachments and links are also used.

### A few public examples from the last year:

- About 20 individuals from a defense industry firm were subject to an attack that featured a loaded PDF file that purported to be an Employee Satisfaction Survey.<sup>12</sup> The PDF file exploited a zero-day flaw (CVE-2011-2462), which installed Sykipot, known malware associated with targeted attacks for the past two years.
- Another defense contractor was targeted by an email attack involving a malicious Word file, which exploited a vulnerability in Windows Common Controls (CVE-2012-0158). The installed malware was a backdoor Trojan known as “PittyTiger.”<sup>13</sup>
- A journalist at a press freedom organization was targeted by an email that was carefully crafted to appear to be from a colleague at a sister organization, with a subject of “Fw: Journalists arrested in Gambia.” The email contained a password-protected zip file with an executable file disguised as an image.<sup>14</sup>
- Attacks using malicious Word documents were used against a range of organizations with the PlugX Remote Access Tool (RAT). PlugX and its cousin Poison Ivy are examples of malware that appear to be custom-made for such targeted attacks.<sup>15</sup>

Email is an easy way for cybercriminals to distribute malware. With the rise of mobile computing and email on-the-go, email will continue to be important to individuals and businesses alike.



To protect against the impact of email attacks, organizations should consider multiple protective layers, including:

- Email gateways with good spam filters, antivirus and content filtering capability.
- Filtering or flagging suspicious attachments, including executables, HTML files and password-protected archives.
- Keeping client machines fully patched.
- Web security gateways for checking clicked links and landing pages.
- Antivirus software on client machines.
- User education on the nature of email attacks.

12. For more about this, check: [https://threatpost.com/en\\_us/blogs/adobe-reader-zero-day-attacks-reused-code-2009-extremely-targeted-attacks-011112](https://threatpost.com/en_us/blogs/adobe-reader-zero-day-attacks-reused-code-2009-extremely-targeted-attacks-011112). 13. <http://nakedsecurity.sophos.com/2012/08/03/poisoned-doc-targeted-malware-attack> 14. <https://www.cpj.org/internet/2012/08/dear-cpj-some-malware-from-your-friend.php> 15. <http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-new-tool-for-a-not-so-new-campaign>





## MOBILE

The improvements made to mobile devices, while exciting for users, have created security headaches for individuals and businesses alike. The endpoint of a network can be anywhere, as these devices routinely connect to unknown networks every day. Mobile devices not only connect back to corporate networks but also contain valuable personal information, making them attractive targets for cybercriminals.

Date	Platform	Threat	Details
<b>2012.02.01</b>	Android/HTC	WiFi Credential Theft	Applications with certain permissions send usernames and passwords to a remote server
<b>2012.02.03</b>	Android	Premium-rate SMS	First malware known to use polymorphism to evade detection
<b>2012.03.15</b>	Android	Banking Trojans	First known use of a token generator masquerading as an official bank-issued app
<b>2012.03.21</b>	iOS 5.1	Address Spoofing	An address-spoofing vulnerability in iOS's Safari that allows an attacker to manipulate the address bar in the browser
<b>2012.04.04</b>	Android 2.3.4 and earlier	Trojan/Auto Root	LeNa Trojan can hide inside a JPEG and comes with its own copy of GingerBreak to auto root devices
<b>2012.04.12</b>	Android	Malware via SMS	UpdtBot spreads via SMS by advertising a fake system update
<b>2012.04.16</b>	Android	Malware on Boot	DroidKungFu adds itself to the boot sequence to bypass possible security protections
<b>2012.05.18</b>	iOS	Access to iCloud Backup	Attacker can access iCloud backups
<b>2012.05.21</b>	ZTE Score M Android Phone	Backdoor	The Score M shipped via MetroPCS contains a backdoor
<b>2012.05.30</b>	iOS 5.1.1	DOS	A DOS vulnerability exists in Safari on iOS 5.1.1
<b>2012.06.06</b>	LinkedIn App on iOS	Information Leakage	User calendar information leaked to LinkedIn servers via mobile app
<b>2012.06.20</b>	Cisco Anyconnect on iOS, Android + Win Mobile	Remote Code Execution	Several vulnerabilities in the Cisco AnyConnect Secure Mobility Client could result in RCE
<b>2012.06.21</b>	Android	Information Leakage	An Android App can read data from NFC cards
<b>2012.07.05</b>	iOS + Android	Information Leakage	App can upload contact lists to remote server for later spam via SMS
<b>2012.07.16</b>	iOS	Fraudulent Purchases	Custom DNS server could intercept In-App purchase authorizations
<b>2012.07.24</b>	iOS	Windows Malware	Apps in iTunes store found to contain Windows malware
<b>2012.08.08</b>	BlackBerry	Malware	Variants of Zeus banking malware found to target BlackBerry devices
<b>2012.08.17</b>	iOS	SMS Spoofing	Improper handling of the User Data Handler could allow SMS spoofing
<b>2012.09.19</b>	Android/Samsung	Factory Reset	A bug in Samsung handsets could allow remote factory resets, wiping all info
<b>2012.11.13</b>	Android/Samsung	Cleartext Passwords	Samsung S-Memo app store Google Drive password in the clear
<b>2012.11.19</b>	Android	Fake Apps	Fake versions of Apple apps found on official Google play store



## Insecure Applications

Several recent research projects have pointed out the common issue of incorrectly implementing SSL and TLS encryption. Certificates used in applications often fail verification and use self-signed or expired certificates, leaving the device and the user unable to trust the application. These issues have plagued desktop applications for years, but given the number of external networks a mobile device can contact, these issues are even more important in today's environment.

## Malware

The Android platform continues to be the focus of malware. In 2012, Trustwave's malware collection for Android grew 400%, from 50,000 to over 200,000 samples.

In an effort to combat the exponentially growing problem of Android malware, Google introduced Bouncer in the first quarter of 2012. Bouncer automatically scans applications in the Google Play store (formerly Android Marketplace) for the presence of malware or malicious behavior. Shortly after its release, however, Trustwave's researchers discovered ways applications might be able to bypass Bouncer and get listed anyway.

Bouncer also has no effect on third-party app stores, which is where a majority of malware is distributed.

In addition, SMS is quickly evolving into a primary attack tool on Android. One method of attack is through the use of premium-rate SMS messages or SMS reverse billing. Another uses hidden SMS messages as the command and control function of malware already on a device. An increase in mobile banking malware is also apparent as attackers start to use SpyEye and Tatanga, traditional desktop banking malware, in the mobile space.

## TWO COMMON MOBILE MALWARE SCENARIOS





Android malware leverages numerous new techniques for distribution and monetization. Some examples include:

- The LeNa Trojan no longer requires a device to be rooted and can hide itself in a .jpeg image.
- Two pieces of malware recently posed as System Updates Malware dubbed as 'UpdtBot.' The first used an SMS message to disguise itself as a system update, and the second used a Wordpress-infected iFrame to automatically initiate the download of a fake system update to infect a device.
- A new variant of the DroidKungFu family piggybacks onto a legitimate app that is likely to be granted root access; the malware uses this root access to add itself as part of the boot sequence.
- DDSpy poses as a Gmail application and uses secret SMS messages to communicate with its command and control server. This malware has the ability to email recordings of all telephone conversations, SMSs and call logs. These new features show an ever-increasing level of sophistication on the part of malware authors.

While most malware takes advantage of Android, some malware appeared in the Apple iTunes Store this year. All the malware discovered there was quickly removed, the most notable being Find and Call. This malware would upload a copy of the user's address book and send SMS spam to all contacts.

iOS suffered from other security concerns, such as address bar spoofing in Safari. While Apple quickly patches issues, users with older phones running earlier versions of iOS will need to remain vigilant for threats against their devices.

It's a common misconception that BlackBerry is immune to malware. Several new variants of the Zeus family target BlackBerry devices, primarily in Germany, Italy and Spain. Most mobile Zeus variants tend to masquerade as security applications in an effort to circumvent out-of-band authentication systems. RIM has a very large installed base, which is attractive to any malware author.

Windows 8 for mobile was released in late October 2012, and, so far, not much has been seen in the way of malware or exploits directed specifically at this mobile operating system. This may change quickly as the operating system gains market acceptance.

## Outdated Operating Systems

All major vendors routinely issue OS updates, but device manufacturers are often not motivated to roll out those updates to users. This leaves users vulnerable to exploits that may have patches—but those patches are useful only if the OS is up to date.

This issue is most prevalent with Android; device carriers are reluctant to make new versions of the OS available to users of older devices. Some estimates indicate that at least 90% of Android owners are vulnerable to known flaws because they can't update their OS.

With the release of the Google Phone and Android 4.2 (Key Lime Pie), Google is hoping to be able to issue OS updates directly without needing to wait for a carrier. If Google is successful with this plan, it will be of great benefit to users of future Android phones but will do nothing to help the millions with the phones already in existence.

As Apple is the sole device manufacturer for iPhone, they have a bit more control over leaving users orphaned on older OSs, but it is still an issue. For example, iPhone 3G users are limited to running iOS 4.2.1, making them vulnerable to anything patched in version 5 or 6.

Despite being the sole manufacturer for BlackBerry, RIM has a similar issue. Its latest OS is often available only for the latest devices and dependent on the carrier to roll them out.

## DEFENSE FAILURES

Defending every remove attack vector available today is no easy task for security professionals. As in previous years, there were some truly innovative attack techniques.

But the most effective vectors that led to successful compromises were not necessarily the newest or most innovative techniques. Many times, successful attacks took advantage of the oldest, most proven methods. Year after year, legacy issues appear to be causing the most problems. Rather than the distractions of new techniques, new patches and products, and news reports, the security industry needs to support and promote sound, in-depth security strategy.

## NETWORK

### 2012 Network Vulnerability Trends

Trends in 2012 skewed toward legacy issues such as password security, ineffectual security controls, and legacy devices, protocols and attacks.

### Man-in-the-Middle Attacks Are Alive, Well and Quite Dangerous

One new, much-talked-about technique for 2012 is weaponization of man-in-the-middle (MitM) techniques. Across all our penetration tests, MitM is the most popular and common exploit vector.

The methods for traffic interception are many, including simple Address Resolution Protocol (ARP) cache poisoning, name resolution poisoning, wireless attacks (like Karma), DHCP attacks and more. The subsequent attack methods include snooping, injection of browser-hijacking frameworks, false authentication services and others.





## Passwords Can Still Hurt You

Analysis still shows a pervasive, well-documented issue of devices (routers, network switches, firewalls, etc.) and services (including administrative interfaces for those services) configured with weak or easily guessable default passwords.

While the impact of this category varies, devices like routers or databases often give attackers a very easy path to escalate their privileges or access data.

Placing the emphasis on password complexity over length may not be enough. Accordingly, secure password guides are starting to be rewritten to encourage longer, easier-to-remember passphrases over special characters and mixed cases.

## Legacy Attacks

Many networks and systems fell victim to legacy attack vectors (some more than 10 years old) in 2012. The most abundant were:

- **Layer 2:** Attacks like ARP spoofing/ARP cache poisoning and other vectors at lower layers that allow for passive and active

MitM attacks remain high impact because they enable everything from credential theft to session theft to direct data theft.

- **Unencrypted protocols:** Protocols that transmit sensitive information in the clear remain an issue even though more secure replacements exist. These protocols are known to be vulnerable to passive and active attacks from simple eavesdropping to session theft.
- **Legacy protocols:** Surprisingly, protocols such as Unix “r” services are still found in abundance in multiple environments. These protocols have been well-documented for years to be rife with authentication bypass and other attack vectors.
- **Misconfigured network access rules:** Network access control devices like packet filtering routers and firewalls are often implemented and configured incorrectly. Trustwave's analysis showed an overwhelming number of cases in which organizations implemented the wrong type of device for cost savings, opening themselves up to easy DoS attacks. They also implemented devices in ways contrary to best practices.

## Top 10 Network Vulnerabilities

RANK*	Name	CVSS v2 Score	Percentage of Networks Containing Vulnerability
1	Weak or Blank System Admin Password	6.7	89%
2	Sensitive Information Transmitted Unencrypted	6.7	88%
3	Weak or Blank Database Password	4.7	86%
4	ARP Chase Poisoning	10	83%
5	NetBIOS Name Service Poisoning	6.5	79%
6	Wireless WEP in Use	8	43%
7	LM Response for NTML Authentication	4.7	67%
8	Misconfigured Firewall Allows Internal Access	4.7	22%
9	Accessible Sensitive Data Stores/Systems	3.3	80%
10	Bluetooth for Sensitive Data Transmission	4.5	16%





## APPLICATIONS

### 2012 Application Security Trends

Cloud-based application deployments continue to grow in popularity but introduce no fundamentally new application challenges. Rather, the security difficulties are policy- and procedure-driven, not technical. In a traditional application architecture, security roles and responsibilities are typically well-understood, but many organizations fail to document those responsibilities when transitioning to a cloud environment. As a result, internal stakeholders may incorrectly assume that security roles are covered. This is even more pronounced when the cloud is managed by an external provider.

### Top 10 Application Vulnerabilities

The top 10 application vulnerabilities were determined by combining vulnerability risk with frequency of observation. In addition to ranking top vulnerabilities, percentages of applications that contain at least one instance of the vulnerability are also documented. In the end, an application needs to have only a single instance of a significant flaw to result in a full compromise.

These results are based on a sample of applications that underwent penetration tests conducted by Trustwave SpiderLabs.

### Top 10 Application Vulnerabilities

RANK*	Finding	Percentage of Applications Containing Vulnerability
1	SQL Injection	15%
2	Miscellaneous Logic Flaws	14%
3	Insecure Direct Object Reference	28%
4	Cross-Site Scripting (XSS)	82%
5	Failure to Restrict URL Access	16%
6	Cross-Site Request Forgery	72%
7	Other Injection	7%
8	Insecure File Uploads	10%
9	Insecure Redirects	24%
10	Various Denial of Service	11%

### Attack Scenarios

Two general approaches to exploiting weak application security are attack the server directly (SQL injection, logic flaws, IDOR, etc.) or send attacks through the user (XSS, CSRF, etc.). Attacking the application server directly is by far the most common scenario because it allows for bulk data extraction and simultaneous compromise of many accounts.

Some user-oriented vulnerabilities, chiefly persistent XSS, can allow for a single attack to be launched simultaneously against many users. If the users have access to sufficiently valuable data, this can also be a viable scenario.

New technologies (or new ways of using old technologies) are always likely to bring in a new wave of vulnerabilities, though. For example, various NoSQL solutions have been increasing in popularity as more applications start to handle massive amounts of data.

Also, HTML5 has potential to impact application security, both on the client and server sides. Web applications have historically been modeled on thin clients with data/logic on the server and superficial presentation performed in the browser. That began to change when rich Internet applications (RIAs) introduced more complex presentation logic to the browser. HTML5 applications that use local storage APIs must contend with a variety of security issues far more complex than those presented by the comparatively simple browser cache directives.





## ATTACK SCENARIOS

### SCENARIO 1

A Fortune 1000 retailer makes national headlines after a lost laptop results in employee data being potentially stolen. State disclosure laws make it obvious the retailer didn't have great internal security controls in place. After reading the news, Attacker X decides to take a look at the retailer's online security.

Visiting their corporate site, the attacker discovers their online affiliate program. The affiliate website was last updated four years ago, but he signs up. Once he has a login to the affiliate site, he finds a SQL injection vulnerability and pulls down the entire database overnight. The user credentials are stored securely, so he can't get direct access to other accounts, but he deduces the affiliate link tracking mechanism from a table named Affiliate\_Keys.

Attacker X is clever, so he doesn't want to blow his position right away by doing anything that will make affiliates complain and alert the company. He searches and finds another SQL injection vulnerability that allows him to issue update commands. He then writes a tool that will cycle through other affiliates and swap keys with top referrers for short periods of time. The script starts stealing affiliate revenue slowly, increasing pace over the next several months. By the end of the year, he is the retailer's top affiliate.

### SCENARIO 2

Attacker Y decides to target the Bank of the United States (not a real bank since 1930). Its online banking website is reasonably secure: Application penetration tests are performed annually, developers are well-trained, and it's even behind a well-configured firewall. Attacker Y is unlikely to successfully launch direct attacks against it.

Attacker Y is persistent, so he looks within the bank's domain. After some reconnaissance, he notices the bank's

trust services division website, which is not considered a critical system, is built on a popular (and famously insecure) application framework.

After downloading and installing a local evaluation copy of the framework, Attacker Y sees several extra default files, a few of which are vulnerable to reflected XSS. He checks back on the bank's website and, sure enough, the vulnerable files are there, too. No vulnerability scanner would have found these files, so the bank has no idea they're vulnerable.

Because the vulnerable site's hostname begins with "trust" (trust services division), Attacker Y realizes this could be perfect for a phishing attack. He signs up for a simple checking account and now has internal access to the online banking application, so he starts crafting an email template using the same language and format as the bank. He then finds an XSS vulnerability that allows for a relatively short payload in the URL, further reducing suspicion. The payload points at an Attacker Y-controlled server and will run JavaScript that reformats an error page into the bank's full login page.

The only hard part is identifying targets. Fortunately, the bank recently started a social media push, so he writes several scripts to grab names and emails of social media followers. He also creates dummy accounts to send automated connection requests to bank customers.

Once he has a sizeable email list, Attacker Y starts phishing. Bank customers who have posted negative comments, for instance, are sent fake apology emails and are asked to click the link for resolution purposes. Attacker Y sits back north of the border and waits for requests to start flowing to his server. Out of more than 50,000 phishing emails, 300 actually click on the link. Of those, 150 actually log in (Attacker Y has set up attack scripts to generate errors and redirect to the real login page so they aren't suspicious). Once he has someone's credentials, he immediately logs in and initiates online transfers to accounts he has created. Within two weeks, he nets \$80,000.



## MOBILE

In this section, findings from mobile application penetration tests are analyzed, with the methodology and findings closely tracked to the new OWASP Mobile Top 10.<sup>16</sup> Trustwave conducted two related but slightly different kinds of tests:

1. **Application tests:** Testing individual applications, whether installed on a mobile device or in an emulator/simulator.
2. **Platform tests:** Testing resiliency of various platforms and Mobile Device Manager (MDM) solutions used to protect data on devices.

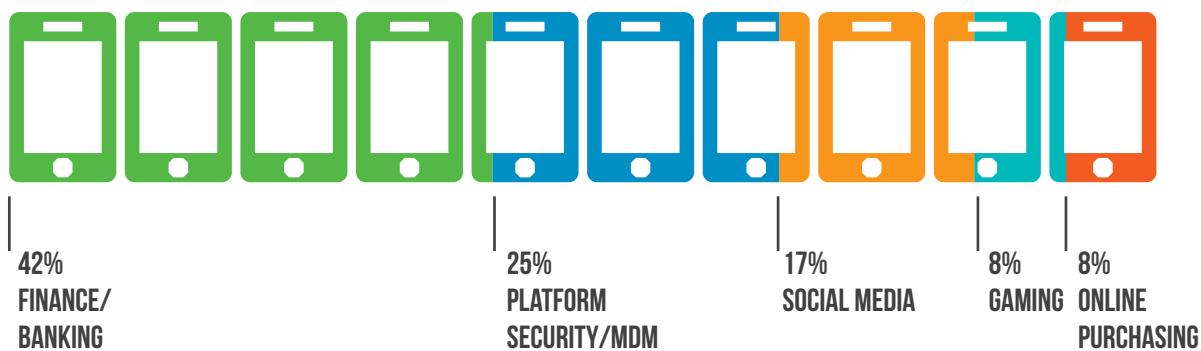
Most tests were conducted on either iOS or Android platforms and included parallel testing of these platforms; that is, most tests were of an Android and iOS version of the same application. In the case of platform and MDM testing, this also meant testing both platform security and MDM effectiveness in parallel.

Most findings were related to some kind of information disclosure, and 87.5% of applications tested had one or more flaws. This includes caching sensitive data on the device or transmitting sensitive data, often unbeknownst to the developer due to default caching by an included library or framework. Replay attacks, where attackers repeatedly send transactions to the backend, allowing access to sensitive server-side data or the integrity of that data, accounted for 29% of all tests.

Nearly all the individual mobile applications tested in 2012 were created on top of WebKit- or webview-based frameworks (like Phonegap or Kony) or a customized screen-scraping code. As a result, 90% of vulnerabilities common in desktop Web application tests were also present in mobile tests for both Android and iOS. Applications are still susceptible to code or content injection attacks because they do not do proper input validation or output encoding on the client.

## MOBILE SECURITY TYPES OF APPS TESTED

EACH PHONE = 10%



16. [https://www.owasp.org/index.php/OWASP\\_Mobile\\_Security\\_Project](https://www.owasp.org/index.php/OWASP_Mobile_Security_Project)





## Top 10 Mobile Vulnerabilities

RANK*	Finding	Percentage of Mobile Applications Containing Vulnerability
1	Insufficient Cache Controls	21%
2	Replay Attack on Sensitive Transactions	21%
3	XSS and Code/Content Injection	8%
4	MDM/Platform Security Bypass	8%
5	Sensitive Information in a Server Response	17%
6	Insecure Password Policy	8%
7	Username Enumeration	8%
8	Sensitive Data in Application Cache	8%
9	Secure Cookie Options Not Used	8%
10	Verbose Error Messages	8%

## Possible Attacks

Attacks perpetrated against mobile applications are not very different from those launched against the Web. Attacks can vary depending on platform and application purpose ([see Mobile Malware](#)). With Web-based applications, client applications and the server endpoint are the usual targets.

Typical attack vectors in mobile are:

- 1. Insufficient cache controls:** Attackers get temporary, physical access to a device. They jailbreak or root the device and use a terminal emulation program to log in to the file system as the root user. They use this access to obtain sensitive information from application caches. Further, attackers can surreptitiously plant malware and spyware to be used when the device is returned to the owner. It should be noted that this kind of attack can be conducted remotely on Android.
- 2. Replay attack:** In this case, attackers are able to get MitM position during a transaction (either through social engineering or misconfigured SSL/TLS in the app) and intercept a transaction. They can then replay this transaction or alter its logic without having to go through the initial steps of authentication and authorization.

**3. Code injection:** Similar to a cross-site scripting vulnerability, this attack is based on applications that use thinly wrapped webviews for data displays. Again, an attacker with MitM position can inject JavaScript code in a server response. Because the client application does not do input validation, the JavaScript will fire. This can be used to steal sessions or, in an extreme example, inject and exploit via a heap spray in the WebKit component and install malware on a device.

With the integration of social media and other external applications for data sharing or authentication on the rise, it is likely, especially in Android, that tokens and credentials will become attack targets. More may need to be done at the developer level to help ensure the security of the underlying platforms and frameworks. Most information leakage vulnerabilities encountered in the past year are the result of developers using cut-and-paste sample code or failing to realize that some frameworks cache by default.

As more Web endpoints for mobile applications become protected by WAFs, it is likely that mobile device attacks will shift to malware-driven attacks, physical attacks and logic flaw exploitation, particularly for applications with widespread use.





## PASSWORDS

Encrypted passwords were obtained from thousands of network penetration tests performed throughout 2012, mainly from Active Directory servers. The most exciting part of statistical analysis this year begins with the sheer number of samples: Trustwave's sample size contained nearly 3.1 million passwords. Of those, there was a marked improvement of recovery; over 95.52% were recovered in this rigorous testing regimen, and approximately 1 million (just over 33%) were unique.

### Top 25 Passwords by Count

In this year's study, it's important to take into account not only the most common passwords but also their presence across samples. By sheer count, the most common password for 2012 was "Welcome1."



BY COUNT

<b>Welcome1</b>	<b>30,465</b>
<b>STORE123</b>	<b>21,362</b>
<b>Password1</b>	<b>15,383</b>
<b>password</b>	<b>9,466</b>
<b>Hello123</b>	<b>9,400</b>
<b>12345678</b>	<b>7,008</b>
<b>training</b>	<b>5,281</b>
<b>Welcome2</b>	<b>4,181</b>
<b>holiday</b>	<b>3,063</b>
<b>Happy123</b>	<b>2,987</b>

<b>123456</b>	<b>2,972</b>
<b>summer11</b>	<b>2,610</b>
<b>Welcome01</b>	<b>2,512</b>
<b>Welcome123</b>	<b>2,438</b>
<b>Changeme1</b>	<b>2,336</b>
<b>job12345</b>	<b>2,317</b>
<b>Welcome4</b>	<b>2,183</b>
<b>Password2</b>	<b>2,056</b>
<b>password1</b>	<b>2,053</b>
<b>Welcome3</b>	<b>2,047</b>
<b>Welcome22</b>	<b>2,029</b>
<b>Spring10</b>	<b>1,907</b>
<b>abcd1234</b>	<b>1,849</b>
<b>Password123</b>	<b>1,714</b>
<b>Summer11</b>	<b>1,473</b>

### Percentage of Unique Active Directory Samples Containing Password

However, Password1 is still widely used. By reviewing the number of samples (unique files of a single Active Directory environment) in which a particular password is found, Password1 is being used in more environments than Welcome1.



BY PERCENT

<b>Password1</b>	<b>38.7%</b>
<b>password</b>	<b>34.5%</b>
<b>Welcome1</b>	<b>16.0%</b>
<b>123456</b>	<b>12.6%</b>
<b>P@ssw0rd</b>	<b>11.8%</b>
<b>Passw0rd</b>	<b>10.9%</b>
<b>Password123</b>	<b>10.9%</b>
<b>Password2</b>	<b>10.1%</b>
<b>Summer12</b>	<b>10.1%</b>
<b>password1</b>	<b>10.1%</b>

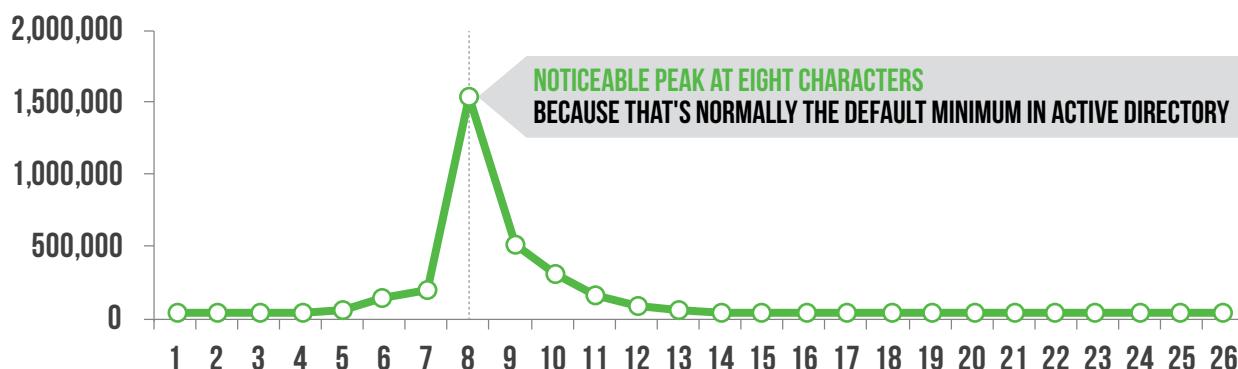
<b>12345678</b>	<b>9.2%</b>
<b>Welcome2</b>	<b>7.6%</b>
<b>Spring2012</b>	<b>6.7%</b>
<b>Summer2012</b>	<b>6.7%</b>
<b>Password3</b>	<b>6.7%</b>
<b>Hello123</b>	<b>5.9%</b>
<b>Welcome3</b>	<b>5.9%</b>
<b>Fall2012</b>	<b>5.9%</b>
<b>Spring12</b>	<b>5.9%</b>
<b>pa\$\$w0rd</b>	<b>5.9%</b>
<b>p@ssw0rd</b>	<b>5.9%</b>
<b>p@ssword</b>	<b>5.0%</b>
<b>p@ssword1</b>	<b>5.0%</b>
<b>Summer11</b>	<b>5.0%</b>
<b>password9</b>	<b>5.0%</b>



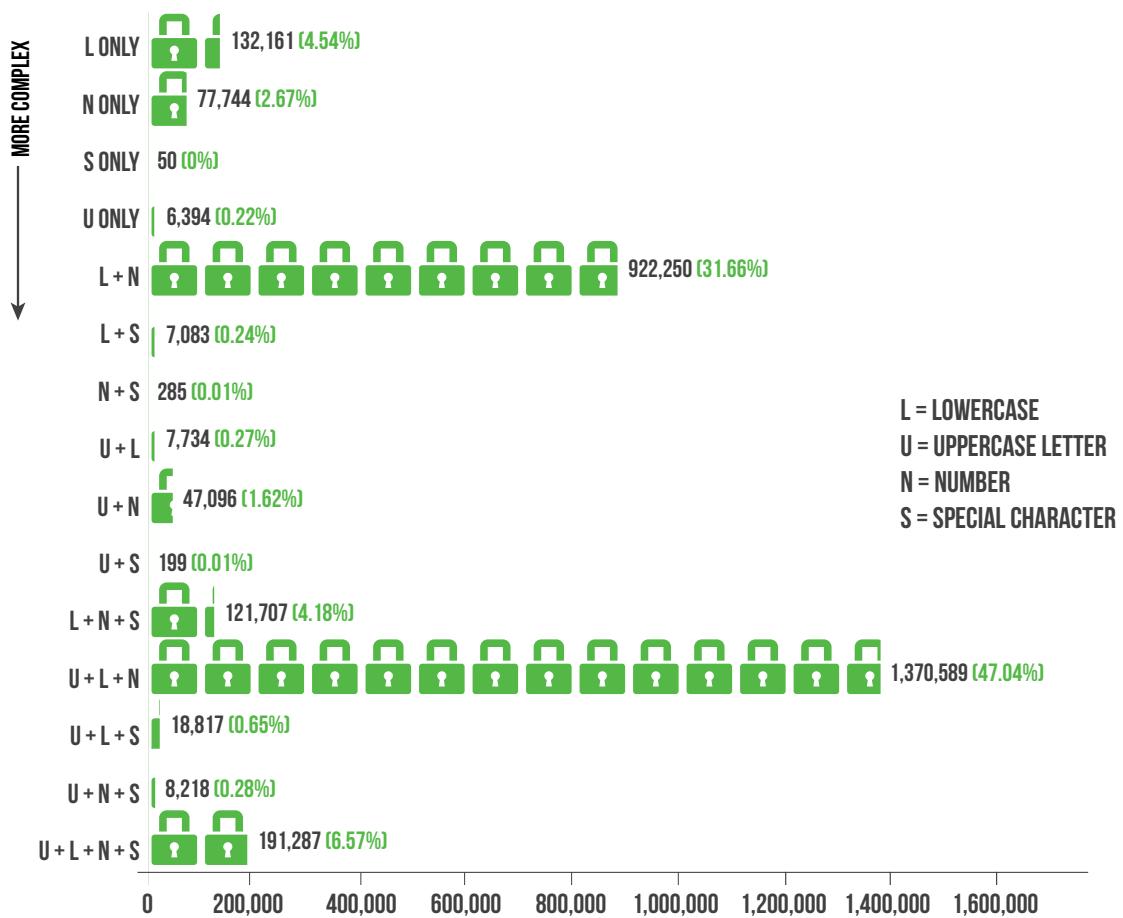


## Password Length

Most samples from 2012 are from an environment where eight-character passwords are typically mandated by policy. Eight-character passwords are the most popular, however, as users continue abiding by this minimum.



Passwords continue to consist of upper/lower/number combinations, as these may be easier for users to remember. Over 88% of passwords did NOT contain a special character.

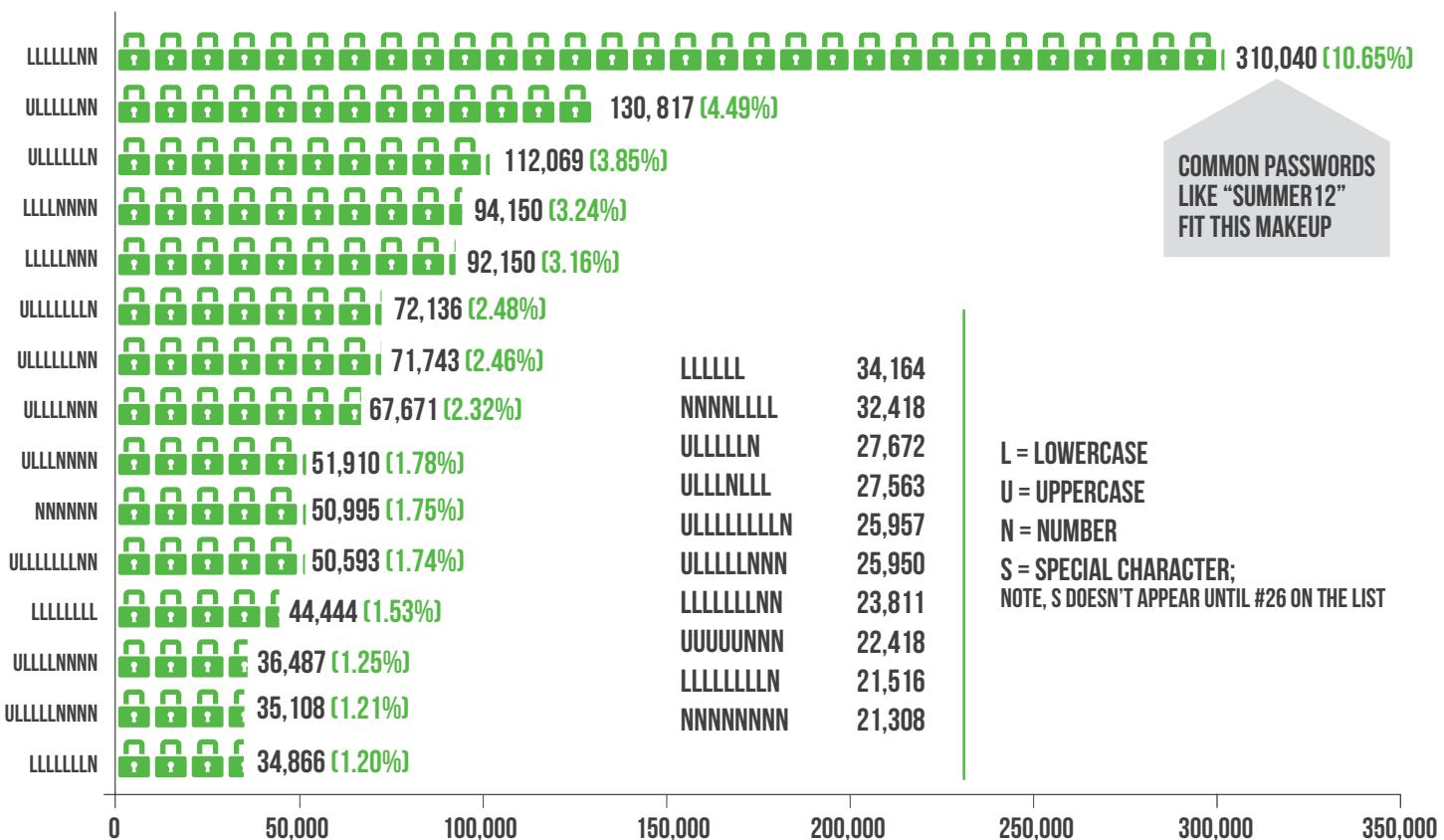




## PASSWORD MAKEUP

1 LOCK = 10,000 PASSWORDS

XX.XX% = PERCENTAGE OF PASSWORDS ANALYZED



COMMON PASSWORDS  
LIKE "SUMMER12"  
FIT THIS MAKEUP

L = LOWERCASE

U = UPPERCASE

N = NUMBER

S = SPECIAL CHARACTER;  
NOTE, S DOESN'T APPEAR UNTIL #26 ON THE LIST

## Implications for Passwords

Users often conform only to the absolute minimum requirements of complexity policies enforced by IT administrators. The default “use complexity” policy in Active Directory outlines the following requirements:

- The password is a minimum of six characters long (although it can be altered to increase or decrease character count).
- The password contains characters from at least three of the following five categories:
  - English lowercase characters (a-z).
  - English uppercase characters (A-Z).
  - Numeric characters (0-9).
  - Special non-alphanumeric characters (For example, !, @, \$, # or %).
  - Unicode characters (For example, ½, © or ±).
- The password cannot contain three or more characters from the user's account name.

An easily guessable password such as “Welcome1” or “Password1,” based on the requirements of Active Directory, is no different than the password “J\*1jaw2” even though one password is obviously far harder to guess than the other. This is the result of Active Directory only examining the password as a whole to determine whether it follows the rules instead of comparing it to dictionary words or slight variations like Linux does.

Passwords once thought to be complex enough to make cracking improbable are now able to be reversed in hours or days. This requires users and administrators to rethink how they create passwords and how users are educated about password security.

Unfortunately, there is still no easy way for administrators to combat password incrementing or similar password choices within Active Directory. Measures can be instituted to prevent identical passwords from being used if administrators enable password histories, but this does not keep users from incrementing their passwords numerically or utilizing character substitution. Thus, Password2 or P@ssword1 will be accepted as a valid password to replace the original Password1.

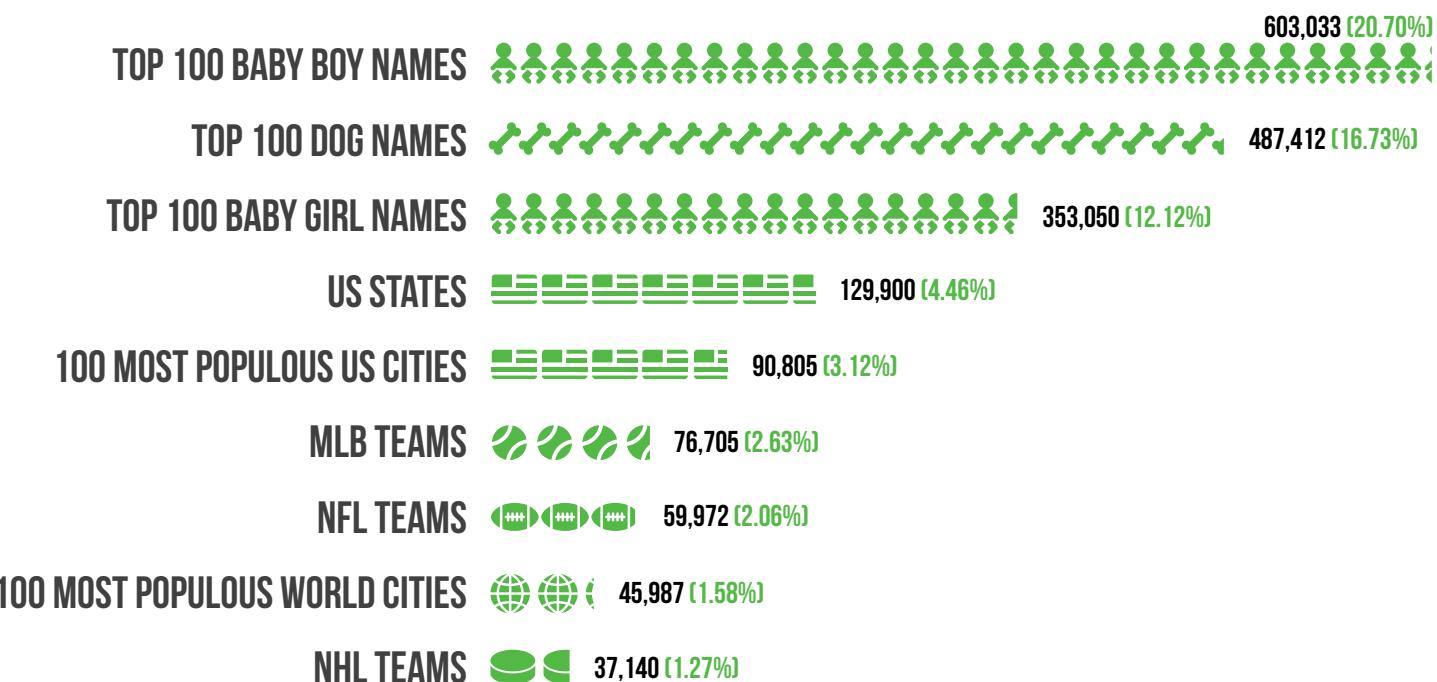




## KEYWORD USAGE IN PASSWORDS

1 ICON = 20,000 PASSWORDS

XX.XX% = PERCENTAGE OF PASSWORDS ANALYZED



### Password Recommendations

The days of passwords are gone. Even a completely random eight-character password that utilizes all four character types, such as J\*1jaw)2, is far easier to crack than a 25-character passphrase with upper and lower case letters, such as HereIsMyPassphraseGuessIt.

A passphrase is also easier to remember and doesn't need to be written down. Not only do long passphrases make brute force attacks impractical for an attacker, they also combat rainbow table-based attacks given their large disk space requirements.

Implementing a policy like this requires a significant amount of user education (mostly by giving examples). Employees may become more receptive when they discover the personal and corporate benefits of complying with new policies.

Eliminating weaker, legacy and insecure encryption methods for storing passwords is absolutely necessary as well. Within Windows environments, especially where Active Directory is in use, LAN Manager password storage needs to end. While companies are slowly migrating to Windows Vista/Server 2008 or higher, organizations still hanging onto their Windows XP/Server 2003 based environments still see this problem persisting.

Techniques to slow down or eliminate password-cracking techniques would also be beneficial. Utilizing a random salt for each password like in Unix-based systems eliminates the possibility of using rainbow tables and significantly slows down dictionary-based attacks. This can become an important countermeasure, especially in Web applications.





## PHYSICAL



### Exposure of Security Information via Social Media

Employees, through social media, expose data in ways that might not appear to be insecure.

Posting one's place of work on Facebook might not seem dangerous, but when combined with co-worker connections on LinkedIn, pictures of office parties from Flickr and check-ins on Foursquare, an attacker can create a very detailed picture of the internal workings of a company without ever setting foot inside. From social media, he now knows what ID badges look like, what names to drop if questioned while on-site and what restaurants or bars to go to eavesdrop or steal laptops.

Third parties also share seemingly harmless client information via social media; legal, architecture and server room design firms are excellent sources of photographic information and other details. In one case, a client was particularly difficult to research, but their architecture firm, found through a simple Google search, had recently redesigned the client's headquarters and posted case studies, including blueprints, online. The consultant then knew where security details would be and the types of servers he would encounter, since the firm also posted photos of the newly designed server room.

Physical attacks that leverage social media are the most common to occur, the most difficult to correct and the most likely to continue to grow. Businesses must build and uphold strong policies when it comes to social media usage by employees and third parties.



### Insecure Configuration of Security Management Systems

Over the last several years, the idea of security convergence has taken hold across a growing number of companies. This term refers to physical security and information security merging into one

coherent program. While this may be an easier, better way to manage physical security devices, policies and procedures, it can also create a large security gap if not properly configured.

Rarely, though, are management systems properly secured out of the box, and documentation is not provided to instruct administrators on how to harden the system. In fact, the Trustwave SpiderLabs team found some management system documentation in 2012 that almost seemed to encourage improper and insecure usage. For instance, one organization discouraged changing default passwords and insisted that no patching ever needed to occur.

Security convergence needs proper planning. Thorough evaluation, including documentation and penetration testing, should occur before purchase and installation of systems supporting a security convergence program.



### Incorrect Physical Security Device Usage

Cameras, locking doors and motion sensors, while commonplace in most business facilities, are frequently too weak, installed improperly or too numerous to properly monitor.

Cameras are usually installed correctly when initially put in place. Over time, though, everyday things can alter effectiveness—mostly bumps and vibrations from traffic, weather, air conditioning and other factors—moving the camera enough so it no longer sees what it needs to see.

Using an unwieldy number of cameras is also just as common. Cameras covering every conceivable angle may seem necessary, but they aren't practical. During client engagements, Trustwave SpiderLabs testers noticed that even though they had crossed coverage of multiple cameras during the course of a test, no security guard was alerted to their presence. With the large number of cameras in use, it took too much time for security guards to view all the cameras as they rotated across the screen or screens. Trustwave's testers spent hours undetected after closing time in office buildings, gathering sensitive information and important corporate assets.

Cheap locks are another problem; they're generally installed during the construction of a building or room and not replaced later. Cheap locks may be good enough when an area in a building is used as a break room or a noncritical storage room. But with changes in floor plans or when a new company moves in, that same area may become a server room. Increasing the risk here is the growing popularity of lock picking—and demonstrations online and at security conferences have made lock picking easy to learn.

Regular reviews of camera coverage, motion detector software on cameras and evaluating security whenever a room's purpose changes are just some recommendations to help remediate these problems. Regular physical security assessments are another way for companies to ensure that adequate measures are in place throughout a facility.



No matter where a corporate asset, physical or logical, exists, appropriate protection measures must be implemented to protect it according to its value to the business. Only through proper assessments and testing can a company be truly aware of how its security policies, procedures and devices will perform during an attack.





# INTERNATIONAL PERSPECTIVES





## EUROPE, MIDDLE EAST & AFRICA (EMEA)



Payment card compromises account for a large number of EMEA investigations. Most of these compromises target “card not present” transactions processed through websites largely due to the successful rollouts of Europay, MasterCard, Visa (EMV) or “chip and PIN” for “card present” environments within Europe. Europe’s regulatory framework strongly encourages merchants to use EMV; if a merchant elects to process a magstripe transaction and it turns out to be fraudulent, the merchant will be liable.

EMV has vastly reduced the value of data available to attackers compromising POS systems. For almost all cards issued in the region, it is not possible to produce a valid magstripe using EMV data. The net effect is that the small number of POS compromises in EMEA are heavily concentrated on merchants who process more magstripe transactions, typically hotels and premium retailers that attract international cardholders with non-EMV cards.

### DATA COMPROMISE TRENDS IN EMEA

Attackers that target businesses in EMEA are more likely to go after card-not-present transactions and small e-commerce merchants because these merchants have little security awareness. Attackers will scan large numbers of merchants looking for well-known vulnerabilities in the e-commerce site or in the software components used—such as off-the-shelf shopping cart software. Typical vulnerabilities exploited here are SQL injections or vulnerabilities in file-upload functionality.

On finding a vulnerability, attackers typically run prepackaged exploits to gain access to the backend database (where a business may be storing sensitive card data) or modify the payment page to siphon off a copy of credit card data on a per-transaction basis.

Within EMEA, specifically outside Western Europe, it's worth noting that there were a handful of large compromises of financial

institutions (banks and service providers). These compromises did not differ greatly in terms of vulnerabilities exploited, but attackers were required to perform more detailed reconnaissance post-compromise in order to access data because of the increased size and complexity of the compromised entity's IT environment. In these organizations, the impact was far greater given the volume of data records compromised.

A small number of incident response cases in EMEA were the result of employee misuse of systems rather than external attackers. Data compromised in these cases typically included customer records or intellectual property.

Of course, when an incident investigation is required, either independently or by a third party, it should be thorough. In one of several cases Trustwave witnessed over the years, a website was compromised via SQL injection. System administrators noted that weak passwords were the problem and wrongly concluded that strengthening them would solve the problem. This clearly had no effect on the SQL injection actually used to perpetrate the attack. As unauthorized data access continued, the company then decided to call in outside assistance. Unfortunately, the delay unnecessarily exacerbated the overall impact of the incident.

### DEFENSIVE STRATEGIES FOR EMEA

#### Large Enterprises, Looking Inward

Defensive strategies observed within larger enterprises, specifically financial institutions, trend toward the correlation of activities and events taking place within the IT environment. In part, this is in response to the “low and slow” attacks that such organizations are not always able to prevent. The focus for these organizations is on improving detective and monitoring controls in order to increase the likelihood of detection.

Most organizations, however, are typically still dependent upon third parties, customers, law enforcement or a regulatory body to notify the victim organization a breach has occurred, which is a worldwide security problem.

Another significant issue is that the payment card industry designed a process in which cardholder data is secured but the merchant website is not. Merchant websites are not necessarily any more secure after the projects than before. Therefore, an attacker may still have access to perform malicious acts. Merchants should manage information security risk across their entire business and not solely for cardholder data.

#### Application Security Programs No Longer Unique to Financial Institutions

Strategic application security programs are often used by large financial institutions, particularly banks with more than 100 Web applications. These programs vary but consist of assurance activities based on the risk each Web application presents to the business and may include a combination of automated





application scanning, application penetration testing, source code review and Web application firewall technology.

Over the course of 2012, a number of medium-sized, non-banking organizations in EMEA sought to develop and implement these types of programs, albeit on a smaller scale.

This demonstrates a growing awareness of the risks insecure Web applications pose, much of which is a result of the industry repeatedly highlighting breaches that were a result of an insecure Web application. Expect this trend to continue as businesses look to protect more than just their flagship websites.

## NOTABLE EVENTS FROM 2012

### Data Breach Disclosure

Globally, there is a trend toward data breach disclosure laws. In Europe, the General Data Protection Regulation is a key piece of regulation that has been proposed. Its current draft, if adopted, will require organizations that process personal data to notify the relevant authorities without delay following a breach.

Noncompliant organizations will face fines of up to 2% of global turnover. A large development from this legislation is an increasing interest in cybersecurity insurance products; currently, interest is primarily supply-side with demand yet to follow.

If the public and the regulators are aware of information security breaches, there will be a greater pressure for specialists in the form of independent investigation, reactive security remediation, public relations and legal assistance. As publicity around data compromises increases, specialist cyber insurance may become the norm even for businesses with a modest Web presence.

CESG, the U.K. government's national technical authority for information assurance, as part of the U.K.'s wider cybersecurity strategy, has made a push to improve high-level awareness of security issues in order to encourage improved security governance within U.K. industry. This involved an executive briefing paper aimed at U.K. enterprises, encouraging focus on:

- Home and mobile working.
- User education and awareness.
- Incident management.
- Information risk management regime.
- Managing user privileges.
- Removable media controls.
- Monitoring.
- Secure configuration.
- Malware protection.
- Network security.



Although the U.K. government's overall cybersecurity strategy has drawn criticism for being complex and bureaucratic, businesses should still welcome activity aimed at raising awareness of key information security risks at the C-level and board level. Their message to U.K. businesses was unusually direct:

**VALUE, REVENUE AND CREDIBILITY ARE AT STAKE. DON'T LET CYBERSECURITY BECOME THE AGENDA—PUT IT ON THE AGENDA.<sup>17</sup>**

17. <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive>





## ASIA PACIFIC (APAC)



Most of Trustwave's incident response work still focuses on payment card data compromises primarily in Australia and New Zealand. Media reports and industry networking demonstrate that compromises outside the payment card space are occurring, but it is Trustwave's experience within APAC that few organizations are seeking outside expertise. For most organizations, the first imperative is ensuring that compromise details are kept confidential, usually for public image reasons.

APAC has a wide range of information security maturity levels. Australia, Hong Kong, Japan, Korea, New Zealand and Singapore tend to have more maturity with respect to information security. Large organizations in these countries usually have internal teams dedicated to proactive information security and incident response. In China, India and parts of Southeast Asia, organizations are generally still in the infancy of information security evolution.

In non-payment card data cases in APAC, Trustwave works with organizations that have started but not finished their information security evolution. They have the capability to detect potential compromises but no in-house expertise to adequately contain and respond to them. As organizations throughout APAC evolve their security programs, enlisting security providers such as Trustwave will become increasingly relevant.

### DATA COMPROMISE TRENDS IN APAC

Trustwave APAC conducted roughly 50 investigations in 2012, most related to payment card fraud. In 2011, POS systems in Australia and New Zealand had been the primary target, surprising in a region where attackers traditionally focused on e-commerce merchants.

This year, that trend reversed to again favor e-commerce sites. This is primarily due to hard work on the part of financial institutions; these organizations are helping merchants improve

system security and ensure that even if a merchant's system is compromised, payment card data is not put at risk. How? By using hardware point-to-point encryption.

In this model, tamper-resilient payment card terminals encrypt sensitive information prior to sending it over the network to the acquiring bank; only the terminal and the bank possess the encryption/decryption keys. Most banks in Australia and New Zealand now use this model though other parts of APAC have not yet adopted it. Without point-to-point encryption, payment card data security is dependent on the merchant's network security (which is frequently substandard). If the merchant allows its IT service provider to remotely access its systems, attackers can also gain access.

It is easy to be complacent and assume that these attacks will not occur. But if the experience in Australia and New Zealand teaches anything, it is that acquirers should assume these attacks will at some point occur and that they should plan accordingly.

### Economics of Compromise

Most compromised e-commerce merchants investigated this year share several characteristics: They processed a relatively low number of transactions (< 5,000), relied on third-party service providers to run their sites, used an open-source (low-cost, off-the-shelf) e-commerce package to run the online store and invested few resources into the upkeep of said store.

Most of these merchants figured they were unattractive targets, asking, for instance, "Why would a hacker bother to break into my site?" or even "My customers struggle to find my site; how did a hacker find it?!"

These questions are based on a common misunderstanding of how financially motivated cybercriminals operate. The merchant believes attackers identify an interesting target and then use all available methods to compromise it; he also believes criminals wouldn't waste time and effort attacking a small e-commerce merchant. These assumptions are fundamentally flawed because:

1. Due to automation, the time it takes for an attacker to compromise a site and identify sensitive data within it is a lot shorter than assumed.
2. Attackers rarely test a particular site to exhaustion. Instead, they focus on a small number of security flaws they understand, check each site for these flaws, and simply give up and move on if they are unsuccessful.
3. The value of the data contained within the merchant's system is actually very high, as each card number or email address can be monetized on the black market.

### Attacker Motives

While financially motivated attackers are a threat, attacks initiated under ideological or strategic factors are also a problem for organizations. In APAC, less is known about the prevalence of these nonfinancial motivations.





However, knowledge sharing with large private and government organizations in APAC yields more insight into these attacks. The methods are largely the same, but the potential victim base is smaller. As a result, these attackers are more likely to use the full range of available attack methods. Increasingly, these methods include email and social media targeting, and the attacks focus on browser/browser plug-in vulnerabilities and gaining a foothold in an environment the attacker can then use as he pleases.

## DEFENSIVE STRATEGIES USED IN APAC

### Keep It Simple

For APAC organizations just beginning to mature their information security controls, it is tempting to react to media coverage about new, blended and advanced threats. It is critical that they first focus on security fundamentals before focusing on new and specific threats.

For most APAC-based private organizations, the main threat is the financially motivated attacker. Trustwave data has continually shown that none of the methods being used by these attackers were advanced or complex. In most cases, attackers relied on easy-to-guess passwords or missing patches.

### Trust, but Verify

The majority of merchants Trustwave worked with this year relied heavily on third parties because they did not have the knowledge required to set up and operate their own systems.

In most cases, these merchants completely trusted those service providers to maintain security. Unfortunately, the service providers were either naïve about security requirements and attack methods or they were willfully ignoring them due to cost or inconvenience.

Small e-commerce merchants should of course choose a service provider they are comfortable working with, but they should also be looking for third-party verification that these service providers are both trustworthy and knowledgeable about security measures. In the payment card space, all service providers should be asked to provide assurance of PCI DSS compliance from a Qualified Security Assessor (QSA).

### Mind the Browser

Of the nonfinancially motivated compromises in APAC, vulnerabilities in Web browsers or in Web browser plugins were the primary cause of compromise. These attacks were more sophisticated and sometimes included the use of zero-day vulnerabilities.

Browsers are notoriously difficult to manage. There are many of them, they are updated frequently, users often expand their functionality through plug-ins and they are used for a variety of tasks. APAC-based organizations that believe they might become targets of nonfinancially motivated attackers and have already addressed security fundamentals should review how to best secure Web browsers and plug-ins.

This strategy would likely include an element of patch management and antivirus, but other layers must be included to assist with mitigating zero-day vulnerability and targeted malware risk. In this respect, secure Web gateway technologies can be effective in providing a consistent level of protection for employees when browsing the Web.

## NOTABLE EVENTS FROM 2012

### Compromises of Cloud-Based Services

In 2012, Trustwave saw the first APAC instances of merchants compromised by using cloud-based services. Investigating these compromises proved difficult, due to service provider's terms of service. Merchants had to rely on internal investigations performed by the service provider on their own infrastructure. In one example, Trustwave worked with a merchant who was convinced they had suffered from a credit card-related compromise. The service provider insisted otherwise, leading to a stalemate.

For this merchant, shifting to an alternate platform would have been complex and costly. If the service provider had been able to confirm a compromise and resolve it, the merchant would have been able to confidently continue operations. Instead, there was a loss of trust.

Compromises of cloud-based services will become more common as organizations continue to rely on them. Organizations need to ensure that they are satisfied with the service provider's information security approach and their contractual terms regarding incident response.

### Compromises of "Out of Scope" Environments

Traditionally, small e-commerce merchants know to protect themselves from cardholder data theft by taking the data flow outside their environments. This is usually achieved through the use of a third-party-hosted, PCI DSS-compliant payment page. In practice, though, attackers have started capturing payment card data in other ways. And this year, Trustwave investigated compromises of merchants who were using third-party-hosted payment pages.

In these cases, attackers modified the merchants' sites to send cardholder data not to the third-party payment gateway but to an attacker-controlled site. Attackers harvested the data and redirected the customer silently onto the third-party gateway to ensure that the legitimate purchase completed successfully.

Merchants and acquiring banks should watch this space; more attackers will revert to this methodology as more merchants opt to use third-party-hosted payment pages.

Mitigating these attacks will be difficult and may require merchants to perform security testing in order to show their sites are not susceptible to attacks that result in the modification of payment gateway configurations.





## LATIN AMERICA & THE CARIBBEAN (LAC)



In LAC, 2012 brought a focus on defensive initiatives from large enterprises in the private sector and some government agencies in the public sector. This is likely the result of increased information security awareness following many publicized attacks in 2011 and 2012.

These same organizations are proactively looking to defend themselves, not only with technology but also with user awareness programs driven by cybercriminals' new focus on attacking individual employees through client-side attacks.

Another observation was an improved understanding of security requirements from the buying community. Specifically, Trustwave has seen increased inclusion of information security-related requirements within RFP-type invitations to vendors.

Not surprisingly, hot topics like bring your own device (BYOD) and cloud computing are also high on the agenda, not only for security implications but also for "tropicalization" for the realities of LAC markets. Some of this involves jailbroken devices; as mobile devices in LAC are very expensive, individuals will buy cheaper phones from outside the region, jailbreaking the phone in order to use it with their local carrier. However, jailbreaking may compromise the security mechanisms of the device and consequently expose the corporate information stored on the device.

From an application security standpoint, organizations with in-house development teams for financial data applications are investing in secure development training to solve recurring vulnerabilities like XSS and SQL injection often identified in Web application penetration tests.

### DATA COMPROMISE TRENDS IN LAC

The common attack techniques used in LAC to expose sensitive/confidential data are similar to all regions and most often are:

- Man-in-the-middle (MitM) attacks (primarily through ARP poisoning).
- Sensitive data/credentials passed in plaintext through internal Web apps or telnet.
- Passwords stored insecurely in files with names such as "password" (or its Portuguese and Spanish translations, "senha" and "credenciales").
- Exploiting the use of weak and default passwords within an environment.

### Targeting the Individual

Typically, targeting the individual is a means of gaining indirect unauthorized access to an organization's data. Since defensive strategies have been effective in improving perimeter network security, cybercriminals have shifted focus to easier routes to initial intrusion, specifically by targeting employees. Although some organizations in LAC have security education and awareness programs in place, it remains challenging for a user to differentiate a legitimate email from a well-crafted fake (malicious) email.

Most organizations in LAC understand client-side attacks to be synonymous with malicious/phishing emails, but there has been growth in "baiting attacks" in which a malicious USB stick or CD/DVD received by mail is used by an unwitting employee; this is successful, especially if the CD is labeled with something like "salary data."

### The Insider

Internal networks are still quite vulnerable, especially when the attacker is an employee—disgruntled employees hired by outsiders to provide confidential information, recently terminated employees whose access has not been removed quickly enough or employees who simply do not know they have been compromised.

### Phishing and Fake Websites

Criminals take over vulnerable Web systems and, through prepackaged scripts, quickly deploy fake websites for services like banks or airlines in order to harvest personal data.

Although some banks have implemented two-step authentication for ATM or online transactions, some phishing websites use sophisticated techniques to obtain one-time passwords from electronic tokens for (almost) real-time attacks. Trustwave has also seen instances that harvest passwords in the password cards provided by banks. The ultimate goal is to produce fake cards and use them along with password card data to obtain cash.





## Defensive Strategies Used in LAC

On the defensive side, two primary improvements were observed:

1. **Improved perimeter security:** In general, external infrastructures are significantly more resilient to attack than in the past. This has largely come about as a reaction to the many attacks in 2011, mostly distributed denial of service (DDoS).
2. **Usage of incident response teams:** As information security incidents became more of a certainty than a possibility, a few organizations realized the importance of having a prepared incident response team. They understood the payoff of not having their names on the evening news for having a security breach or leakage.

and reach into the network than it should. ATMs should reside on dedicated network segments with security controls in place to allow communication only with the authorization switches.

- **Physical security flaws:** Of course, newer ATM models (usually deployed in bigger cities) may have better physical security protections—but legacy models (complete with legacy physical security flaws) are sometimes moved to smaller cities or less secure locations. For example, an ATM that was originally used inside a shopping mall with staff supervision may now sit in an unsupervised gas station parking lot, an open opportunity for attackers.

In addition, it is not uncommon for ATMs to be running end-of-support or -life operating systems that no longer get patched and/or systems that cannot be upgraded due to hardware limitations.

## NOTABLE EVENTS FROM 2012

### Developing and Enforcing Laws

Argentina, Brazil, Colombia, Mexico and Peru are leading efforts on developing and enforcing specific laws to deal with personal data-related cybercrime. Protecting personal data is important to all individuals, but there is a major concern within the security community on how these laws may impact security research. But since cybercrime is often a division of each well-established criminal organization in the region, defining laws is essential.

### Financial Motivation Versus Hacktivism

Cybercrime associated with hacktivism remains relatively prevalent. Protests happen worldwide, and their motivations usually focus on personal privacy. In LAC, these usually take the form of denial of service (DoS) attacks—attacks that temporarily cripple websites of well-known businesses or government organizations dealing with financial or personal records (though in some cases, targets are news sites, celebrity pages, etc.). While financially motivated criminals and hacktivists use the same methods, there is one key difference: The financially motivated shy from the spotlight, while hacktivists want to make headlines.

### ATM-Specific Attacks

ATM network operators (usually banks) are engaging security providers to help address the issue of ATM fraud. ATM fraud is not new, and it has several tried-and-true methods, such as skimmers and cameras. However, ATM threats have gone beyond card cloning to include physical theft and explosives.

Attacks have focused on ATM networks and maintenance software. Usually, criminals gain physical access to a single ATM and then compromise others within its network. In some LAC countries, the problem grew to necessitate detailed investigations. The top problems observed were:

- **Lack of network segmentation:** In some investigations, one ATM in a network will be found to have more access to data





## INTERNATIONAL BREACH REPORTING LAWS

As demonstrated by the global proliferation of data breaches in 2012, the current environment knows no boundaries when it comes to cybercrime. Attackers can come from anywhere, attack at any time and wreak havoc on organizations of all sizes. When law enforcement is able to successfully apprehend criminals, jurisdiction normally falls under the laws of the country from which the attack originated. There are some exceptions, but they normally involve cooperation between the victim nation and the originating nation.

Countries that currently have data breach legislation break down targeted data elements into three categories:

- **Personal data:** Typically PII.
- **Sensitive data:** Includes more politically-relevant information like ethnicity, gender, religious affiliation, political opinions, physical or mental health state, sexual orientation.
- **Judicial data:** Information pertaining to criminal activity.

Countries lacking specific legislation to govern unauthorized access, misuse or exfiltration of data do not necessarily require that incidents be reported to law enforcement. While violation of laws may carry penalties, there is no impetus for the breached party to report the crimes. And even in countries where reporting is required, not everyone conforms.

Legislation between countries often proves to be the largest barrier for law enforcement officials when attempting to apprehend criminals. When a computer or device is part of a computer crime located abroad, a mutual legal assistance treaty (MLAT) is often required before any progress is made. An MLAT is a temporary treaty between two countries with the intent of gathering or exchanging information regarding criminal offenses—and one must be obtained for every proxy an attacker goes through.

This step often causes delays or even completely halts investigations, especially because MLATs may be denied for political or legal reasons (e.g., the laws of the two countries don't coincide, so the party is guilty by one country's standards but not by the other's). Language barriers and translation issues also cause delays in properly creating MLATs, as do misunderstandings by parties who simply do not know enough about technology to understand the MLAT's purpose. The latter issue is being corrected as technical proficiency is improving or legislative bodies are utilizing third-party experts to assist on these cases.

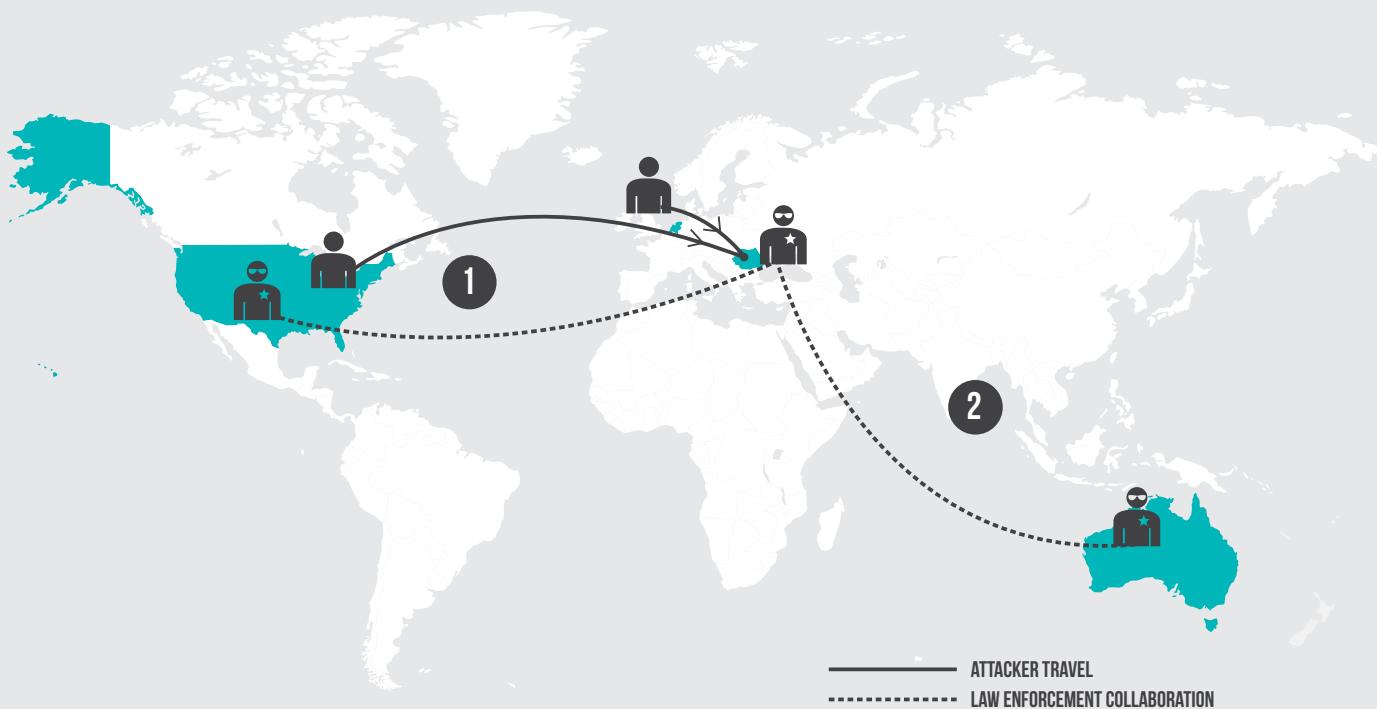
BONJOUR

HOLA





## INTERNATIONAL BREACH REPORTING LAWS



### CASE STUDIES

**1**

Even with so many difficulties, there are success stories. In July 2012, David Benjamin Schrooten (aka Fortezza) and Christopher A. Schroebel were arrested<sup>18</sup> for the theft of at least 44,000 credit card numbers. While Schrooten is Dutch and Schroebel is American, Schrooten was visiting Romania to commit crimes, thus prompting cooperation between the governments of the United States and Romania to make the arrest.

**2**

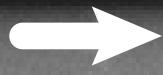
During 2011, Trustwave investigated a number of POS compromises at small retailers in Australia. Trustwave's analysis indicated that the same Romanian attackers perpetrated many of them. In November 2012, the Australian Federal Police announced that in conjunction with the Romanian National Police they had apprehended 16 gang members in Romania. Trustwave is proud to be a part of the all-of-industry initiative to provide the Australian Federal Police with the intelligence and evidence they needed to bring these criminals to justice.

18. [http://www.msnbc.msn.com/id/47785726/ns/technology\\_and\\_science-security/t/feds-arrest-alleged-credit-card-fraud-kingpin/#.UP9UuCdWyuI](http://www.msnbc.msn.com/id/47785726/ns/technology_and_science-security/t/feds-arrest-alleged-credit-card-fraud-kingpin/#.UP9UuCdWyuI)





# CONCLUSIONS & PURSUITS





## CONCLUSIONS

For 2013 and beyond, several key predictions and recommendations can be made based on the trends of the past year. While new malware hit the scene and more devices were affected, major trends were consistent with previous years:

1. Cyber attacks are increasing with little sign of abatement. As evidenced by media reports and Trustwave's growing queue of investigations, especially concerning mobile devices, cybercriminals continue to have ample opportunity to locate and steal data.
2. Valuable data makes businesses a target. Data is a viable commodity for cybercriminals—credit card data, Social Security numbers and intellectual property all have a price on the black market. And the risk is even greater for consumer-facing businesses and brand-name chains.
3. Outsourcing IT and business systems saves money only if there's no attack. Many third-party vendors leave the door open for attack, as they don't necessarily keep client security interests top of mind.
4. Client-side attacks—both targeted and en masse—are on the rise. These are perpetrated by both Web-based systems and email, two vectors that are most used but in many cases least protected.
5. Weak and default passwords continue to be a notable risk. The combination of a properly designed password storage method and a properly designed methodology/policy for a user password choice is absolutely critical. If this first line of defense fails, it leaves an organization vulnerable to a complete compromise.
6. Moreover, employees leave the door open to further attacks. Whether due to lack of education or policy enforcement, employees pick weak passwords, click on phishing links, and share company information on social and public platforms.

Organizations that remain committed to their security initiatives, integrating them into the entire business, will be most resilient to attack. By reducing risk through education, identification, homogenization, registration, unification and visualization, organizations will not only protect sensitive data and their employees, but they'll also safeguard their reputation.

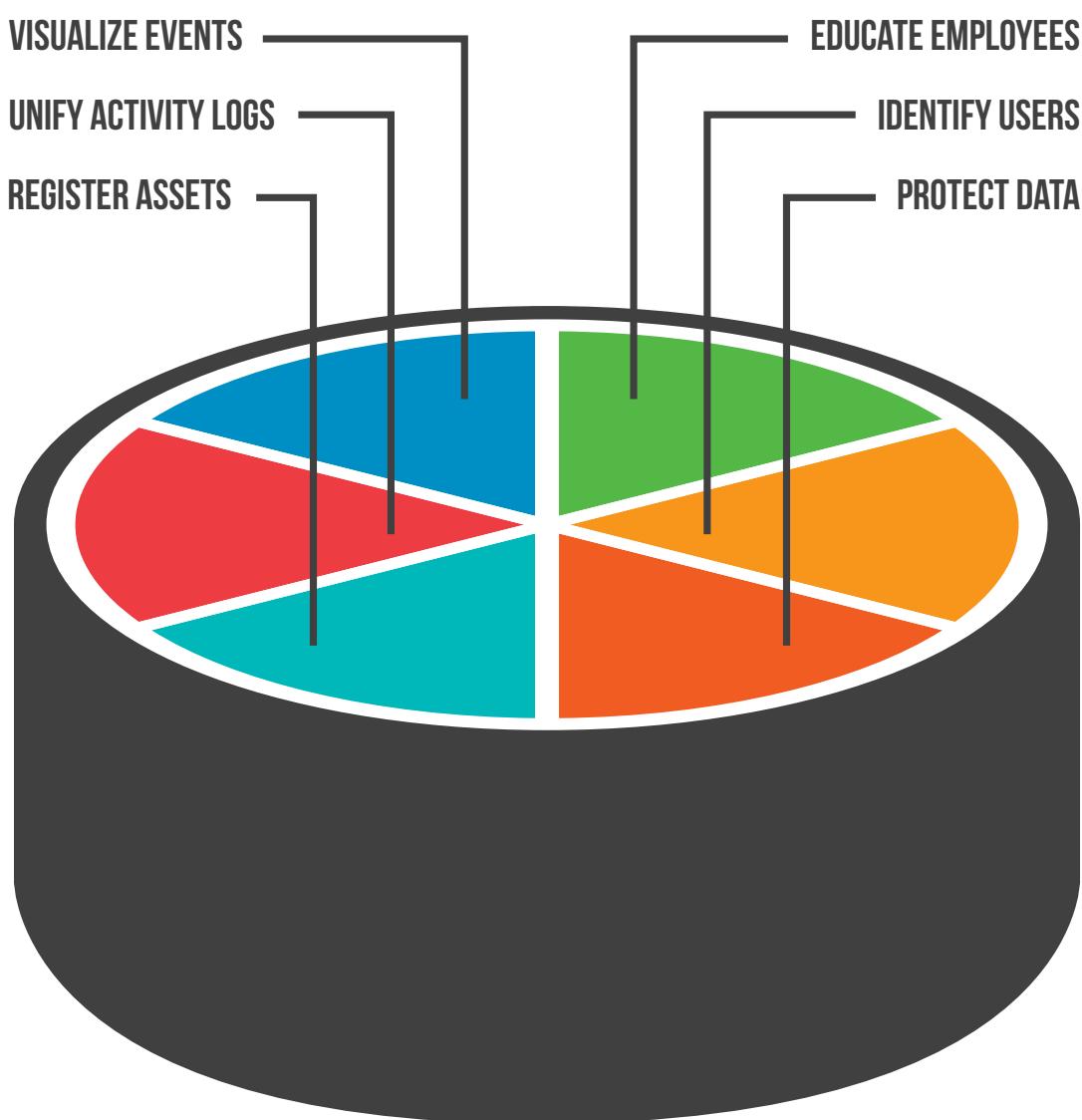


## SIX SECURITY PURSUITS FOR 2013

The best way to approach security initiatives for 2013 is to realize one simple truth: There is no **if** an attack will happen, only when.

Based on the trends outlined here, the 2013 Trustwave Global Security Report identifies six key pursuits businesses can undertake to improve their overall security posture.

Building and running an informed, comprehensive security strategy is not easy; acting on a general area like security education takes time and thought—but the effort will pay off with fewer attacks, more efficient processes and reduced data loss. The following six pursuits highlight the pieces organizations everywhere can adopt, in part or in whole, to achieve a complete security strategy.



WORK TO EXPAND SECURITY STRATEGY INTO THE AREAS THAT ARE NEW TO YOUR BUSINESS, AND KEEP IN MIND THAT SECURITY IS CONTINUOUS AND ONGOING.



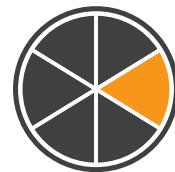


### EDUCATE EMPLOYEES

Employees are the first line of defense against physical and digital attack vectors. A lack of proper training and awareness can turn employees from assets into liabilities.

Untrained employees may click malicious links and open malicious emails—but they also might commit other mistakes, ones that seem completely harmless (like posting telling photos or info on social media and maintaining easily guessable passwords).

These actions can result in loss of intellectual property and exposure of customer data, leading to incident response investigations, costly fines and loss of reputation. But no policy enacted will have much impact if employees aren't on board (especially if they don't truly understand the consequences of their actions).



### IDENTIFY USERS

Every user-initiated action should be tagged to a specific person, whether in the physical or digital environment. This may seem a lofty goal, but it is achievable in most environments.

Every year, a significant number of data breaches occur as the result of an attacker obtaining a user account for a system. More often than not, it's the result of a shared vendor or default account that should have been changed before the application was placed into production—one that cannot be attributed to one individual.

This level of security is important at the office or facility level as well. Employees may wear badges for access control and movement within a facility, but as soon as they forget that badge, they only need to request a temporary keycard for the day, leaving the door open (almost literally) for criminals to fraudulently gain access.

### Next Steps

1. **Conduct security awareness training:** Regular staff training on both core security techniques and topical issues is important to build a successful security foundation. This awareness training must include case studies highlighting both obvious pitfalls (clicking on suspicious links) and not-so-obvious ones (posting company photos online in which staff members are wearing their security badges).
2. **Run security awareness campaigns:** Repetition is key; regularly featured security topics will help maintain staff awareness levels and employee vigilance. Reward staff for identifying incidents, which will encourage them to be observant.
3. **Perform attack simulation exercises:** Like a fire drill, attack simulations can help staff understand how a security event may appear and what they should do in response.

### Next Steps

1. **Eliminate generic, shared, vendor and default accounts:** These types of accounts allow criminals to get into systems.
2. **Review access management:** Periodic analysis of all user and group roles will improve security around access levels and may even identify obsolete accounts.
3. **Enact password-complexity policies:** Set password policies of high complexity and educate staff on best-practice password techniques, such as using passphrases.
4. **Employ two-factor authentication:** This requires users to authenticate using both what they know (password) and what they have (device/certificate). This should also be applied in the physical world (e.g., combining a keycard with an access PIN).
5. **Utilize biometrics:** These tactics—like fingerprint or voice readers—may be necessary for more sensitive areas, such as data centers and R&D environments.

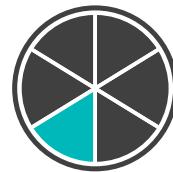




### PROTECT DATA

Regulatory and competitive pressures are driving the need to understand and protect data across the organization. Understanding the life cycle of data is paramount to protecting it. How data is created, categorized, accessed and stored, how it relates to business processes and even who can remediate are all important aspects in effectively managing data.

Attacks are more sophisticated than ever, and keeping cybercriminals out requires a multifaceted approach. Controls must be set that govern who can send data, where and by what means (such as social media and instant messaging). Careful consideration must also be given to securing e-commerce applications; these applications are critical to business yet have become the most attacked asset in the company.



### REGISTER ASSETS

Networked devices are widespread in organizations today. And with the increase of BYOD, it is more important than ever to have a complete inventory or registry of valid devices.

Businesses that adopt a BYOD policy without a registration process are opening the door to malicious threats. Take, for example, the announcement of malware embedded on the motherboard of a specific laptop model. Users can be asked to check their laptop type, but some won't report accurately, making a survey of devices unreliable—businesses can never be sure they've ridded the network of vulnerable devices.

From desktops to laptops, servers to mobile devices, anything that can connect to an organization's systems is capable of providing a unique identifier. A unique identifier aids in access control and can provide an accurate record of what devices have access to the environment and when that access is initiated.

Security controls also play a strong role here. A device should never be allowed access to a controlled environment unless it is registered and known. In addition, the patch levels and vulnerabilities should be assessed on a regular basis not only to work to improve the security of those in the environment but also to understand what risks exist when issues can't be resolved in the short term.

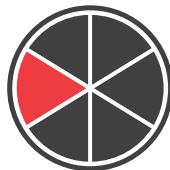
#### Next Steps

- Create a methodology:** Institute a "more than technology" approach to security. For e-commerce Web applications, include team training and education, secure code review and periodic penetration and vulnerability testing. For data, create a data life cycle methodology that governs data from creation to destruction.
- Layer technologies:** Create resiliency in systems by layering proven technologies. A powerful secure Web gateway provides deep content inspection for real-time anti-malware protection and complements existing firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS). A Web application firewall can be deployed to improve protection and performance of business-critical applications with virtual patching capabilities that combat threats in real-time.

#### Next Steps

- Manage assets:** Institute a system to track devices, applications and other assets.
- Implement network access control (NAC):** NAC can control access to various network environments based on defined rules. It can also be used to remove devices from the network if and when security issues are identified.
- Manage patches:** When there is an active threat, understanding patch levels of systems and applications is critical.
- Scan for vulnerabilities:** Even with the above solutions in place, there will still be instances in which configurations or combinations of various services will introduce vulnerability. Regular scanning of both internal and external systems should be performed.



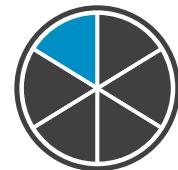


### UNIFY ACTIVITY LOGS

Most businesses today treat physical and information security controls separately. Badge systems, HR records and even loss prevention are not typically tied to the same team that monitors firewalls, intrusion detection and other security technology.

Attacks are becoming more sophisticated, and criminals are finding out how lax security controls are in most organizations. Attackers also know that certain activities may not be flagged as suspicious. An attacker may log in and access email remotely as a user currently “checked in” at the corporate office, but because that user travels extensively and badge swipes are not connected to logins, no red flags appear.

Combining these two sides of security can also help reduce consoles. Instead of viewing multiple consoles and attempting to correlate data, you can feed logs of each point solution into a single console. Too often systems are tuned down to reduce the “noise.” Instead, use a tool like security information and event management (SIEM) technology to take over the processing of these logs.



### VISUALIZE EVENTS

Security event visualization is still rare in most enterprises today. Many security professionals conduct manual log reviews or perform “spreadsheet” analysis, and for some, implementation of basic SIEM technology is where the path ends. But the ultimate goal should be to develop an environment in which security events are discovered innately—by both responsible security professionals or others in the organization. Data aggregation or correlation as seen in a SIEM is a precursor to real-time security event visualization and notification.

Security event visualization allows businesses to identify patterns, emerging vulnerabilities and attacks and to respond quickly and decisively across the organization when an attack does occur. Using the right data sources, advanced SIEM analytics and data modeling, security event visualization prepares businesses to effectively mitigate current and future threats.

Not everything can be automated—or monitored by computers—but when security event visualization is combined with employees trained to recognize attacks, from phishing emails to malware, businesses are better equipped to defend against and respond to security attacks.

### Next Steps

- Employ SIEM technology:** Whether managed by you or a third party, SIEM helps achieve log normalization, correlation and rules to be applied to trigger security events.
- Analyze and tune:** Analyze systems to identify which systems need to be correlated to maximize the events captured. Regularly review and tune systems to ensure that proper data capture and review are taking place.

### Next Steps

- Interactive and sensory controls:** Build or adopt tools that visualize abstract data, helping identify patterns and improve monitoring efficiency.
- Threat intelligence:** Understanding what the emerging threat landscape looks like and continuously tuning systems and processes will help organizations stay on top of and even ahead of attacks.
- Incident readiness program:** Much like a fire drill, an incident readiness program should include training for key staff, an incident response plan and an attack simulation exercise.



By learning from the good and bad experiences of others and beginning to apply both tactical and strategic changes outlined in this report, organizations worldwide can build stronger and more proactive security programs in order to protect their businesses, users and customers.





# GLOSSARY

<b>ACTIONSCRIPT</b>	The programming language used for Flash
<b>APAC</b>	Asia Pacific
<b>API</b>	Application programming interface
<b>ARP</b>	Address resolution protocol
<b>ARP POISONING/SPOOFING</b>	A technique in which an attacker sends fake ARP messages onto a LAN
<b>ATM</b>	Automated teller machine
<b>BLACKHOLE EXPLOIT KIT</b>	Currently the most common Web threat
<b>BOTNET</b>	A collection of Internet-connected computers whose security defenses have been breached and control ceded to a third party
<b>BYOD</b>	Bring your own device
<b>C&amp;C CHANNELS</b>	Command & control
<b>CERT</b>	Computer emergency response team
<b>CESG</b>	Communication-Electronics Security Group, the U.K. government's national technical authority for information assurance
<b>CHD</b>	Cardholder data
<b>CSRF</b>	Cross-site request forgery ("sea surf" or XSRF), a type of malicious exploit whereby unauthorized commands are transmitted from a user the website trusts
<b>CVE IDENTIFIER</b>	Common vulnerabilities and exposure identifier, a reference tool by which all vulnerability cases, whether zero-day or responsible disclosure, are recorded

<b>CVSS</b>	Common Vulnerability Scoring System, a ranking protocol for CVE cases; now in its second iteration, CVSSv2
<b>DOS ATTACK</b>	Denial of service attack, an attempt to make a machine or network resource unavailable to its intended users; distributed denial of service (DDoS) attacks occur when multiple systems flood the bandwidth or resources of a targeted system; sometimes used interchangeably with DoS
<b>ECTF</b>	Electronic Crimes Task Force, a faction of the USSS
<b>EFT</b>	Electronic funds transfer
<b>EMEA</b>	Europe, Middle East and Africa
<b>EMV</b>	Europay, MasterCard, Visa
<b>EXPLOIT KIT</b>	Apart from the exploits themselves, the exploit kit contains a control panel that helps the administrator operate the attack
<b>FTP</b>	File transfer protocol
<b>FUZZY HASHING</b>	A process through which researchers can more easily determine malware "families"
<b>HACKTIVISM</b>	When the motivation for an attack is political or ideological; accordingly, the term is a portmanteau of "hack" and "activism"
<b>HID</b>	Human interface device
<b>HMS</b>	Hospitality management system
<b>HONEYBOT</b>	A trap to help fight unauthorized computer access





<b>IDS</b>	Intrusion detection systems	<b>RIA</b>	Rich Internet application
<b>IE</b>	Internet Explorer, Microsoft's default Web browser	<b>SOCa</b>	Serious Organised Crime Agency, a national police unit in the United Kingdom
<b>IOC</b>	Indicator of compromise	<b>SOCs</b>	Security operation centers, global locations out of which Trustwave operates
<b>iOS</b>	Apple's mobile operating system	<b>SQL</b>	Structured Query Language
<b>IPS</b>	Intrusion prevention systems	<b>SQLI</b>	SQL injection
<b>LAC</b>	Latin America & the Caribbean	<b>SSL CERTIFICATE</b>	An electronic document that uses a digital signature to bind a public key with an identity
<b>LM</b>	LAN manager	<b>SVI</b>	Trustwave's Spam Volume Index
<b>MAGSTRIPE</b>	Magnetic stripe (on a credit card)	<b>TERMSERV</b>	Terminal services, a remote access application
<b>MDM</b>	Mobile device manager	<b>TROJANS</b>	A kind of malware
<b>MITM</b>	Man-in-the-middle attack, a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them	<b>TROPICALIZATION</b>	Adjusting devices for the realities of LAC markets
<b>MLAT</b>	Mutual legal assistance treaty, a document required in order for countries to collaborate on prosecuting international crimes	<b>UNAM-CERT</b>	A CERT from the Universidad Nacional Autónoma de México
<b>NSW</b>	New South Wales; in this context, the NSW Police Force Cybercrime Squad	<b>UNC</b>	Uniform naming convention
<b>NTLM</b>	NT LAN manager	<b>USSS</b>	United States Secret Service
<b>NVD</b>	National Vulnerability Database, where all CVE data are stored	<b>VIGENÈRE CIPHER</b>	A method of encrypting alphabetic text
<b>OS</b>	Operating system	<b>VNC</b>	Virtual network client
<b>OS X</b>	Apple's desktop operating system; "X" = 10	<b>WAF</b>	Web application firewall
<b>PCI</b>	Payment card industry	<b>WASC WHID</b>	Web Application Security Consortium Web Hacking Incident Database, dedicated to maintaining a list of publicly disclosed Web application-related security incidents
<b>PCI DSS</b>	Payment Card Industry Data Security Standard	<b>WEBKIT</b>	A layout engine software designed to allow Web browsers to render Web pages; used by Apple Safari and Google Chrome
<b>PFI</b>	PCI forensic investigator	<b>XOR</b>	Shorthand for "exclusive or," a method used in encryption
<b>PFI LITE</b>	A truncated version of PFI, becoming popular for smaller vendors in EMEA	<b>XSS</b>	Cross-site scripting, a vulnerability in Web applications that attackers may exploit to steal users' information
<b>PII</b>	Personally identifiable information	<b>ZERO-DAY</b>	The gap between attack observation (or proof-of-concept code release) and patch availability
<b>PIN</b>	Personal identification number	<b>ZOMBIE</b>	A computer accessed by a hacker without the owner's knowledge and used for purposes such as sending spam
<b>POS</b>	Point of sale		
<b>QSA</b>	Qualified security assessor		
<b>RAT</b>	Remote-access Trojan		
<b>RDP</b>	Remote desktop protocol, a remote access application developed by Microsoft		
<b>RFI</b>	Remote file inclusion		





# CONTRIBUTORS

## LEAD AUTHOR

Nicholas J. Percoco

## AUTHORS

Ryan Barnett  
Moshe Basanchig  
Joshua Brashars  
David Byrne  
Daniel Chechik  
Marc Bown  
Anat Davidi  
Josh Grunzweig  
Charles Henderson  
Jibran Ilyas  
Phil Hay  
Rob Havelt  
Ryan Jones  
Mike Kelly  
Rami Kogan  
Arseny Levin  
Ziv Mador  
John Miller  
Ryan Merritt  
Steve Ocepek  
Mike Park  
Garrett Picchioni  
Chris Pogue  
Luiz Eduardo Dos Santos  
Cris Thomas  
Barrett Weisshaar  
John Yeo

## MANAGING EDITOR

Sarah B. Brown

## ORGANIZATION CONTRIBUTORS

United States Secret Service  
Serious Organised Crime Agency  
Universidad Nacional Autónoma de México  
New South Wales Police Force Cybercrime Squad





FOCUSING ON RESEARCH & DEVELOPMENT, ANALYSIS &  
TESTING AND INCIDENT RESPONSE, TEAMS  
AT TRUSTWAVE AND TRUSTWAVE SPIDERLABS DELIVER THREAT  
INTELLIGENCE, COMPLIANCE MANAGEMENT AND  
INTEGRATED SECURITY TECHNOLOGIES, AVAILABLE ON  
DEMAND, AROUND THE WORLD AND IN THE CLOUD.

FOR MORE INFORMATION VISIT [WWW.TRUSTWAVE.COM](http://WWW.TRUSTWAVE.COM)



**CORPORATE HEADQUARTERS**

70 West Madison St.  
Suite 1050  
Chicago, IL 60602  
P: 312 873 7500  
F: 312 443 8028

**EMEA HEADQUARTERS**

Westminster Tower  
3 Albert Embankment  
London SE1 7SP  
P: +44 (0) 845 456 9611  
F: +44 (0) 845 456 9612

**APAC HEADQUARTERS**

Suite 3, Level 7 100 Walker St.  
North Sydney NSW 2060  
Australia  
P: +61 0 2 9466 5800  
F: +61 0 2 9466 5899

**LAC HEADQUARTERS**

Rua Cincinato Braga, 340 nº 71  
Edificio Delta Plaza  
Bairro Bela Vista - São Paulo - SP  
CEP: 01333-010 - BRASIL  
P: +55 (11) 4064-6101

Copyright © 2013 Trustwave Holdings Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written consent of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. Trustwave and Trustwave's SpiderLabs names and logos are trademarks of Trustwave. Such trademarks may not be used, copied or disseminated in any manner without the prior written permission of Trustwave.

