Trustwave®

2012 Global Security Report

Dear Reader,

Organizations, regardless of industry and size, continue to face similar information security risks. Old systems with known flaws can take time to decommission and new systems are implemented with little or no thought to security. In its third year, the Trustwave 2012 Global Security Report will help you understand today's information security threat landscape, as well as how to better protect your organization from cyber attacks in the years ahead.

The Trustwave 2012 Global Security Report is a reflection and analysis of investigations, research and other client engagements conducted throughout 2011. During the past year, Trustwave SpiderLabs investigated more than 300 breaches and performed more than 2,000 penetration tests around the world.

Research featured in the report is collected from the many data sources maintained by Trustwave, such as our managed security service and SSL offerings, allowing us to bring new perspectives to the global state of information security.

We're excited to share the Trustwave 2012 Global Security Report with our customers and the industry at large. By understanding how breaches happen, and sharing that knowledge with you, we work to eliminate information security threats for all businesses.

Regards,

Nicholas J. Percoco
Senior Vice President & Head of SpiderLabs

Trustwave® Trustwave® SpiderLabs®

Contributors

Authors

Ryan Barnett
Sol Bhala
Marc Bown
Jonathan Claudius
Josh Grunzweig
Rob Havelt
Charles Henderson
Jibran Ilyas
Ryan Jones (UK)
Ryan Jones (U.S.)
Paul Kehrer
Mike Kelly
Ryan Merritt
John Miller
Steve Ocepek
Nicholas J. Percoco (lead)
Garret Picchioni
Christopher E. Pogue
Michael Ryan
Luiz Eduardo Dos Santos
Sean Schulte
Colin Sheppard
Barrett Weisshaar
Chris Woodbury
John Yeo

Editor

Sarah B. Brown

Art Direction and Design

Nathan Glick

Organization Contributors

CERT.br
United States Secret Service

Contact Us

For comments or questions regarding this report, please contact Trustwave SpiderLabs at the information listed below.

To request information about our services for environments or applications, we at Trustwave SpiderLabs are available to discuss any organization's needs.

+1 312 873-7500

info@trustwave.com

https://www.trustwave.com/spiderlabs

Twitter: @SpiderLabs / @Trustwave

Table of Contents

Executive Summary

Nearly every week in 2011 brought reports of data breaches in the media, ranging from the theft of personally identifiable information to sensitive government documents to credit card data. Cyber criminals targeted many diverse organizations. Those most affected represent a broad spectrum of organizations that have one thing in common: valuable data.

2012 Key Findings

Each year we strive to issue an informative and educational report on the latest security issues and trends, as well as provide insight into unaddressed legacy issues.

- Customer records remained a valuable target for attackers, making up 89% of breached data investigated.
- For the second year, the food and beverage industry made up the highest percentage of investigations at nearly 44%.
- Industries with franchise models are the new cyber targets: more than a third of 2011 investigations occurred in a franchise business.
- In 76% of incident response investigations, a third party responsible for system support, development and/or maintenance of business environments introduced the security deficiencies.
- Law enforcement detected more breaches in 2011 – up from 7% in 2010 to 33% in 2011.
- Data harvesting techniques continued to target data "in-transit" within victim environments showing up in 62.5% of 2011 investigations.
- Anti-virus detected less than 12% of the targeted malware samples collected during 2011 investigations.
- For Web-based attacks, SQL injection remains the number one attack method for the fourth year in a row.
- The most common password used by global businesses is "Password1" because it satisfies the default Microsoft Active Directory complexity setting.

The Trustwave 2012 Global Security Report highlights these risk areas and more, offering predictions on future targets based on our analysis and perceived trends.

Real-World Data, Expert Analysis

The Trustwave 2012 Global Security Report is founded on data from real-world investigations and research performed by Trustwave SpiderLabs in 2011. Standardized tools were used to record data and other relevant details for each case or test. Trustwave is strongly committed to protecting the privacy of our clients, and the statistics within this report are presented in an aggregate form only.

The report follows four distinct sections:

2011 Incident Response Investigations

This section analyzes the results of more than 300 incident response investigations performed due to a suspected security breach identified by either the target organization or a third party, such as a regulatory body, law enforcement or other group.

Security Weaknesses under the Microscope

This section features data correlation and analysis from many sources, including:

- Analysis of more than 2,000 penetration tests performed on 300,000 devices.
- Review of 25 different anti-virus vendors against the various malicious files Trustwave SpiderLabs encountered in 2011.
- Data from more than 2 million network and application vulnerability scans.
- Analysis and trends from 16 billion emails collected from 2008 to 2011.
- Review of approximately 300 Web-based breaches publicly disclosed by organizations in 2011.
- Usage and weakness trends of more than 2 million real-world passwords used within corporate information systems.
- Analysis of almost 300,000 unique digital certificates (SSL) from scans of more than 17 million Internet-facing devices, including Online Certificate Status Protocol (OCSP) usage data from Trustwave.
- A review of 250,000 public devices from 132 different countries for Broken Network Address Translation (BNAT) instances that could expose internal services to external attackers.

Information Security Strategy Pyramid for 2012

To improve any organization’s security posture, Trustwave SpiderLabs recommends six areas to focus on in 2012:

- Education of Employees — The best intrusion detection systems are neither security experts nor expensive technology, but employees. Security awareness education for employees can often be the first line of defense.
- Identification of Users — Focus on achieving a state where every user-initiated action in your environment is identifiable and tagged to a specific person.
- Homogenization of Hardware and Software — Fragmentation of enterprises computing platforms is an enemy to security. Reducing fragmentation through standardization of hardware and software, and decommissioning old systems, will create a more homogenous environment that is easier to manage, maintain and secure.
- Registration of Assets — A complete inventory or registry of valid assets can provide the insight needed to identify malware or a malicious attack.
- Unification of Activity Logs — Combining the physical world with the digital affords organization new ways to combine activities and logs to identify security events more quickly.
- Visualization of Events — Log reviews alone are no longer sufficient. Visualizing methods to identify security events within the organization better narrow security gaps.

Global Conclusions

Any business can be a target; those most susceptible will be businesses that maintain customer records or that consumers frequent most, such as restaurants, retail stores and hotels. The risk is even greater for brand name chains. Areas of focus for 2012 include employee security awareness, anti-virus software and legacy firewalls.

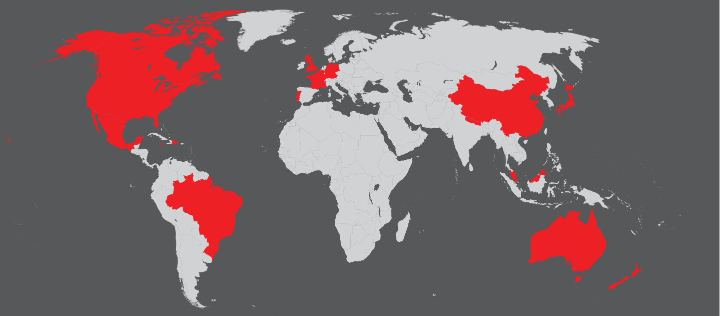
By learning from others’ misfortunes or vulnerabilities, and applying tactical and strategic change outlined in this report, any organization will be better able to reduce the likelihood of incidents and resultant data loss.

2011 Incident Response Investigations

Trustwave incident response engagements are undertaken in response to a security issue, either identified by the victim organization or a third party, such as law enforcement or a regulatory body. Data from these investigations are analyzed and findings and trends are presented in an aggregated form. It is important to note that the data presented in this report are not survey data — all data within this section are from actual Trustwave SpiderLabs investigations.

Unique Data Sources, Countries and Methodologies

In 2011, Trustwave SpiderLabs performed more than 300 data breach investigations in 18 countries. More investigations were conducted in the Asia-Pacific (APAC) region than in the previous year, primarily the result of maturing data disclosure laws and compliance mandates. For example, more countries in the APAC region are adopting and adhering to the Payment Card Industry Data Security Standard (PCI DSS). With this adoption more organizations are made aware of their obligation to report data breaches when they occur. Similarly, the Latin America–Caribbean (LAC) region had increased data breach disclosure procedures and adoption of compliance mandates, such as PCI DSS.



>300 Data Breaches

18 Countries

Types of Data Targeted

Continuing the trend of previous years, 89% of investigations involved the theft of customer records, including payment card data, personally identifiable information and other records, such as email addresses. Active email addresses of consumers are valuable to attackers as they can lead to further attacks like traditional phishing or sophisticated, targeted attacks. Cyber criminals continue to focus their efforts in this area due to the large number of available targets and well-established black markets where criminals are quickly able to turn items such as payment card data into cash with minimal effort.

Trustwave SpiderLabs is one of a few firms authorized to conduct investigations on behalf of all five major card brands and, as a result, payment card data breach investigations remain prevalent within the data set.

Several engagements in 2011 found that criminals explicitly targeted business financial account numbers (e.g., account routing codes, merchant identification numbers) to perpetrate payment card fraud. When merchant identification numbers from legitimate businesses are obtained, criminals utilize this information to configure their own fraudulent payment systems and perform card testing with stolen payment card accounts. These fraudulent transactions then appear to originate from a legitimate business.

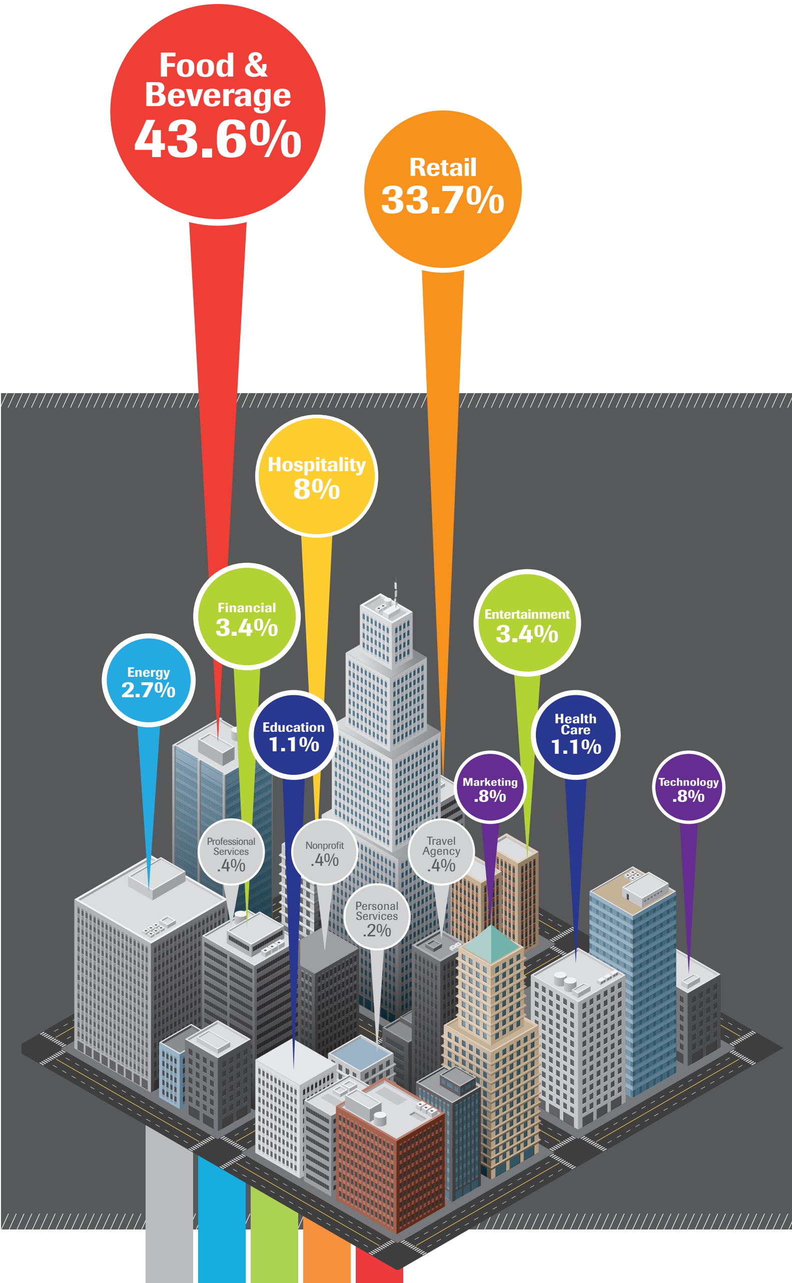
This process is also used to launder money through an unsuspecting merchant. For instance, an attacker can use a batch of payment cards to make purchases and then perform credits (or charge-backs) to a small set of payment cards. The result is the consolidation of value from stolen cards to payment cards that are in the control of the attacker. The business unknowingly facilitating the transactions does not lose or gain anything except a small transaction processing fee during the process, as the money received is equal to the amount transferred out of their accounts.

By far, the theft of trade secrets were the most advanced breaches in terms of attacker technical skill level and persistence. Trade secrets are unique to a given entity and, unlike payment card data, an attacker cannot simply move on to another target organization to obtain this information. Therefore, efforts to gain trade secret data are far more focused.

Industry Breakdown and Data Targeted

New this year, electronic protected health information (ePHI) theft investigations accounted for 3% of the caseload. We attribute this addition to the continued adoption of breach notification laws, and a maturing of information security policies within the health care industry.

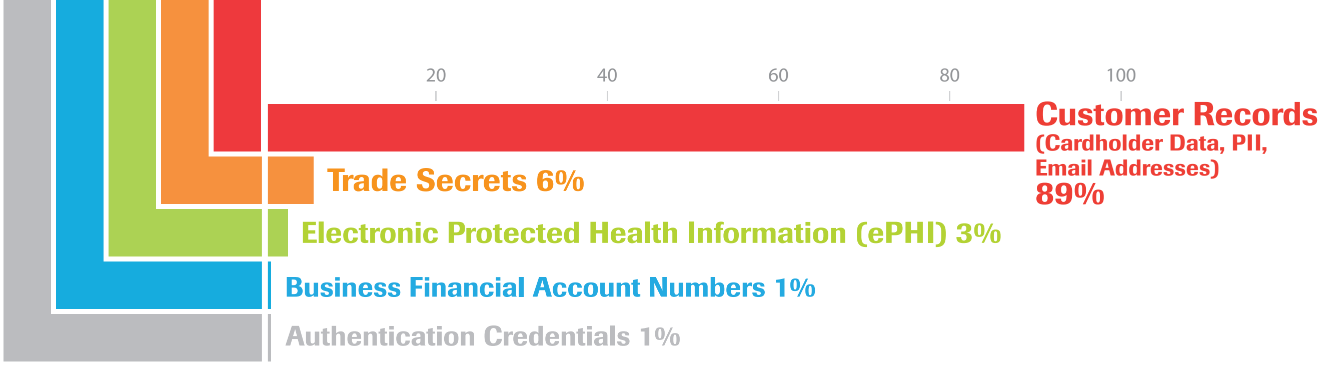
For the theft of authentication credentials, the motive is not one of immediate financial gain, but information gathering for a subsequent attack. In many cases such data, particularly from a consumer-focused organization, can be utilized in a targeted attack against a commercial or government organization.



Industries

Consistent from the prior year, the food and beverage, retail and hospitality industries accounted for about 85% of data breach investigations. In these industries, the primary target was payment card data. While such businesses typically represented a smaller reward for attackers in comparison to large banks or payment processors, they continue to be a target due to well-known payment system vulnerabilities and poor security practices on behalf of those responsible for the upkeep of these systems. Organized crime groups in particular continued to focus on these industries.

More than one-third of breached entities in food and beverage, retail, and hospitality represented franchised businesses. Standardization of computer systems among the franchise models is common and, in the event a security deficiency exists within a specific system, deficiencies will be duplicated among the entire franchise base. Cyber criminals took full advantage of this vulnerability, targeting specific franchised businesses and exploiting common points of failure across franchisee properties.



Target Assets

Information systems involved with payment processing continue to be the Achilles' heel of the payment industry and represent the easiest way for criminals to obtain payment card magnetic stripe data *en masse*. Once magnetic stripe data is obtained, attackers are able to perform fraud by encoding stolen data onto legitimate or counterfeit cards, subsequently purchasing goods and services.

Point-to-point encryption (P2PE) solutions, while not bulletproof, have the potential to lower the risk of POS system breaches. When properly configured to protect data in transit, P2PE technology can dramatically reduce the currently broad attack surface of payment systems, whether data is sent between merchants and their payment processing banks, or via the merchant's own internal systems.

E-commerce targets increased from 9% to 20% over the previous year, largely due to additional engagements in the APAC region, where e-commerce compromises are more common than software POS system compromise.

ATMs were infrequently targeted. However, if payment card magnetic stripe data and PIN are successfully obtained by an attacker this results in direct access to cash. The most common method to obtain this information is hardware tampering (i.e., keyboard overlays, cameras and skimming devices). But in a trend consistent with our investigations over the last two years, cyber criminals obtained this information via system intrusions and the subsequent installation of ATM-specific malware instead.[1]

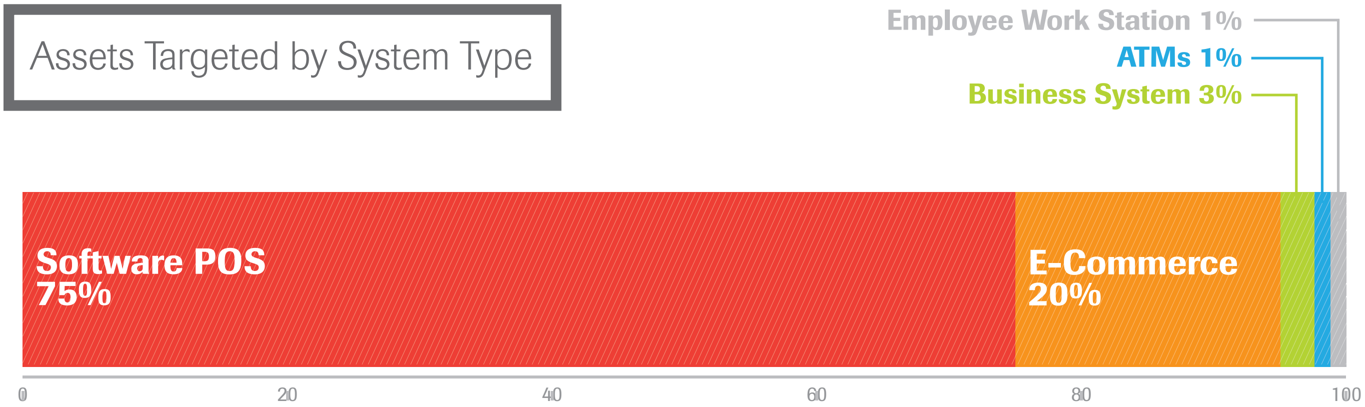
Employee workstations and servers were the primary targets for the theft of trade secrets and credentials. In these cases, email with malicious intent was sent to targeted and specific employees. This email contained an attachment, such as a PDF, an executable file or a URL. Users accessed the file or link and malware was then deployed to their systems. Once installed, it established an initial foothold that ultimately allowed additional propagation within the internal network by establishing a tunnel for the attackers for further attacks.

Investigation Basics

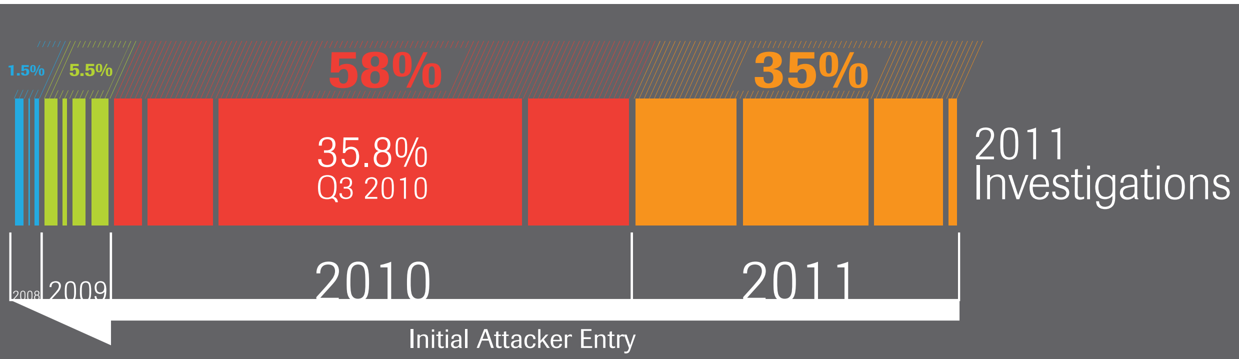
When a security event occurs, incident response investigations are undertaken to identify if and what sensitive information was extracted from the target organization. In the event that sensitive information has been exposed, Trustwave SpiderLabs performs a thorough analysis to quantify the specific information at risk. Various public breach disclosure laws and compliance mandates typically require timely reporting of this information. To meet the demands of accuracy and timeliness, we employ a robust methodology called "sniper forensics" that allows us to quickly focus on the most important aspects of an investigation by understanding and following the data flows.

Once an in-depth understanding of the incident is reached, containment and remediation plans are implemented to remove the threat and reduce the risk of re-occurrence. As other prominent leaders in the industry have stated, an understanding of the threat factors responsible for the breach is of upmost importance, given that this intelligence can determine the response. Involvement of law enforcement in these investigations often plays a critical role in augmenting our own intelligence in this respect.

Assets Targeted by System Type



[1] ATM Malware Analysis https://www.trustwave.com/downloads/spiderlabs/Trustwave-Security-Alert-ATM-Malware-Analysis-Briefing.pdf

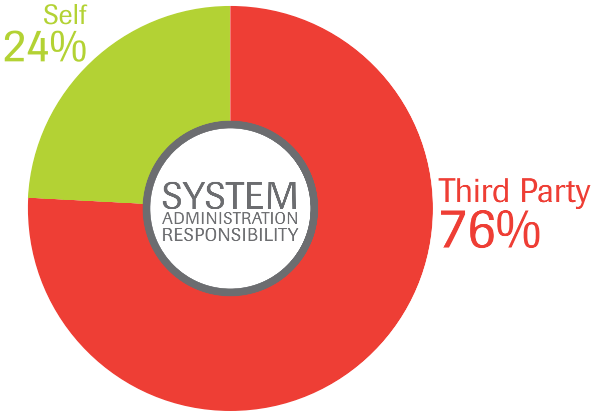


Attack Timeline

Many times compromises are detected at greatly varying intervals and the time from initial breach date to incident investigation may be six to 12 months or more. The graph above represents investigations that took place in 2011, but demonstrates that initial entry by the attacker could have taken place up to three years before detection and investigation.

System Administration Responsibility

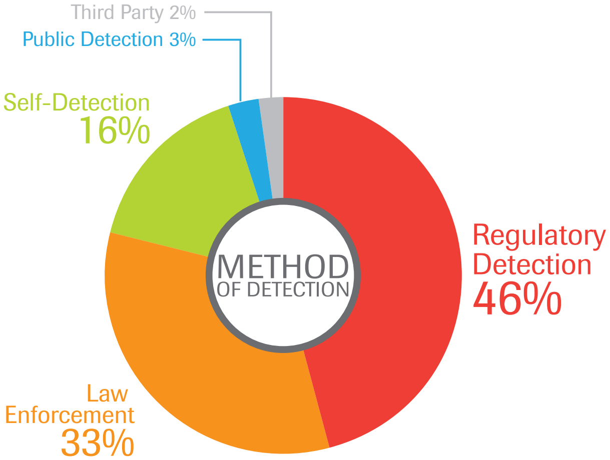
The majority of our analysis of data breach investigations – 76% – revealed that the third party responsible for system support, development and/or maintenance introduced the security deficiencies exploited by attackers. Small businesses within the food and beverage and retail industries were most often impacted by these attacks, as they typically outsource all development and support of their systems. Anecdotally, merchants were unaware of the security best practices or compliance mandates by which their partners were required to abide. In other instances, victims were unaware that this third party was only responsible for a subset of security controls – thus still leaving these systems open to attack.



Detection

The number of self-detected compromises decreased in 2011; only 16% self-detected compared to 20% in 2010. This may indicate a decline in resources for properly detecting incidents. The remaining 84% of organizations relied on information reported to them by an external entity: regulatory, law enforcement, third party or public. This reliance has serious drawbacks; in those cases in which an external entity was necessary for detection, analysis found that attackers had an average of 173.5 days within the victim's environment before detection occurred. Conversely, organizations that relied on self-detection were able to identify attackers within their systems an average of 43 days after initial compromise.

The most common method of identification was regulatory detection. It should be noted though, that law enforcement notifications increased almost five-fold to 33%. This increase can be attributed to work performed by the United States Secret Service and Electronic Crime Task Force members. Due to the efforts by these and other law enforcement agencies worldwide, the number of our investigations that resulted from law enforcement detection increased from 7% in 2010 to 33% in 2011. The involvement of law enforcement can minimize the damage inflicted upon compromised organizations. Law enforcement is often privy to additional intelligence, which can result in victim notification prior to actual fraud.



The Breach Triad

At its most basic form, a data breach consists of three elements: infiltration, aggregation and exfiltration.

BREACH Infiltration
Aggregation
Exfiltration

Infiltration

Remote access solutions are still the most widely used method of infiltration into target networks. Organizations without dedicated information technology (IT) staff often hire third-party vendors to maintain their systems and networks. These vendors use remote access applications or a virtual private network (VPN) to access the customer systems. When these services are left enabled, an attacker can access them as easily as an approved administrator.

With the number of IP addresses in the world, how are attackers able to identify remote access applications open to attack? To illustrate, picture an international airport, with many airlines and planes arriving from locations around the world. Each plane is sent to a predetermined "port" based on a variety of factors, such as airline or arrival and departure information. A plane from "Airline A" will always dock in the terminal designated for Airline A.

Computers communicate similarly; there are 65,535 ports and each is used for different types of communication. Ports used by remote access applications, unless altered from their default configuration, will always be the same.

An attacker can scan the Internet for hosts that respond to queries on one of these ports. The results of the scan will produce a list of hosts (along with system information suggesting the host's function) that are potential targets. Once they have a focused target list of IP addresses that have open remote access or VPN ports, they move to the next part of the attack: weak credentials.

Sharing credentials from one location to another potentially puts every customer using the same username:password combination in a position to be compromised.

Although method of entry was unknown in 19.9% of cases, many possessed a common indicator of compromise (IOC), specifically weak and/or default administrative credentials.

System logins require a username and a password, and often these combinations are pitifully simple: administrator:password, guest:guest, and admin:admin were commonly found in our investigations. Many third-party IT service providers use standard passwords across their client base. In one 2011 case, more than 90 locations were compromised due to shared authentication credentials.

Another IOC is often client-side attacks, which are difficult to detect as the date of the initial compromise may occur months before an investigation when log files needed to identify the attack are no longer available. During a client-side attack, attackers implant malicious code on victim systems via a file, Web page or other document viewed in a client application such as a Web browser or document viewer. Systems administrators utilized production environments for personal use (frequently accessing personal email accounts, social networking sites and even online Flash or Java-based gaming sites) in about 60% of these cases, demonstrating the effectiveness of these types of attacks. In many cases, the breach was also extraordinarily difficult to detect.

Structured Query Language (SQL) injection continues to be a common infiltration mechanism for a wide variety of applications, most often for Web pages. Web pages today consist of dynamic components to improve the user experience, and many pages ask for additional information, ranging from bank account numbers to geographical location to shopping preferences, to improve speed and efficiency. Such pages make SQL queries to a database where user information is stored, sending and receiving information that impacts performance and drive business functionality to Web applications. In a SQL injection attack, the Web pages that use this dynamic content are not doing proper input validation.

Attackers used SQL injection to infiltrate environments 6.9% of the time. Attackers use SQL injection to execute code on the target systems, which often results in a compromise of the system running the database.

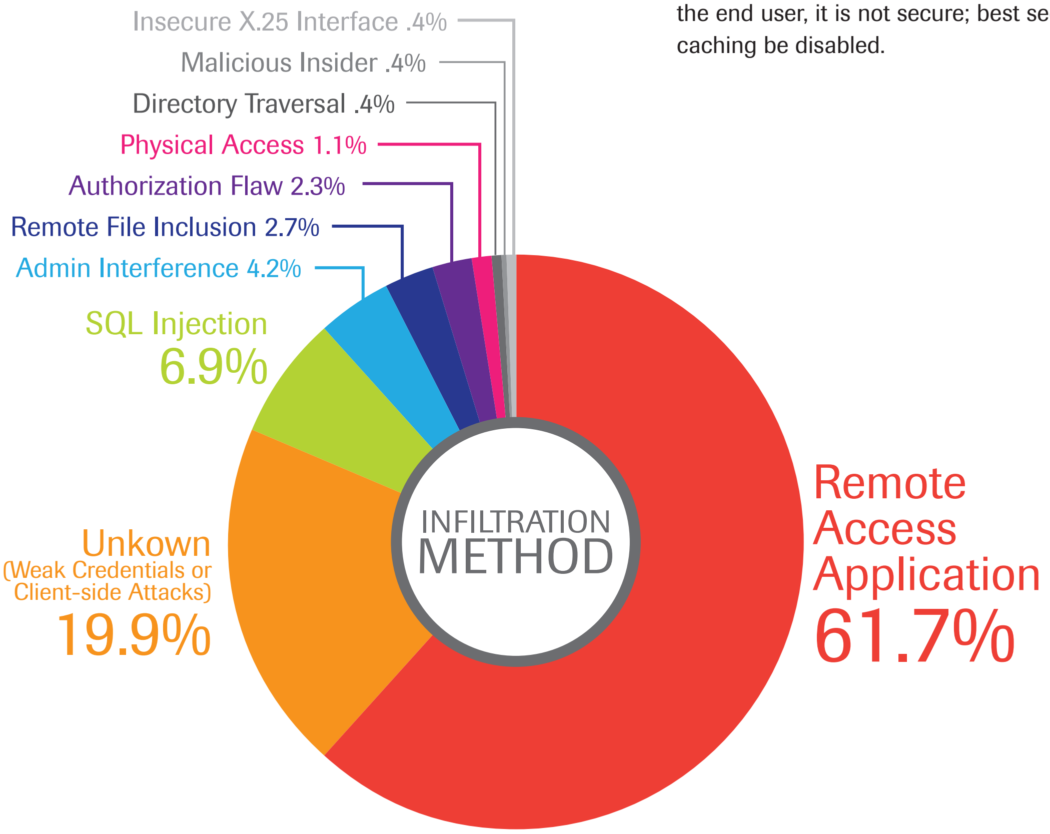
After achieving an initial point of compromise, commonly referred to as a "foothold" or a "beachhead," attackers work to identify additional targets on the compromised network, and propagate the intrusion.

In 2011 the top three methods of propagation were:

80% Use of weak administrative credentials

15% Default hidden administrative shares

5% Remote access solution credential caching



The use of weak and/or default credentials continues to be one of the primary weaknesses exploited by attackers for internal propagation. This is true for both large and small organizations, and largely due to poor administration. In one instance, attackers were able to compromise as many as 250 unique critical systems at a single target location by exploiting duplicate credentials.

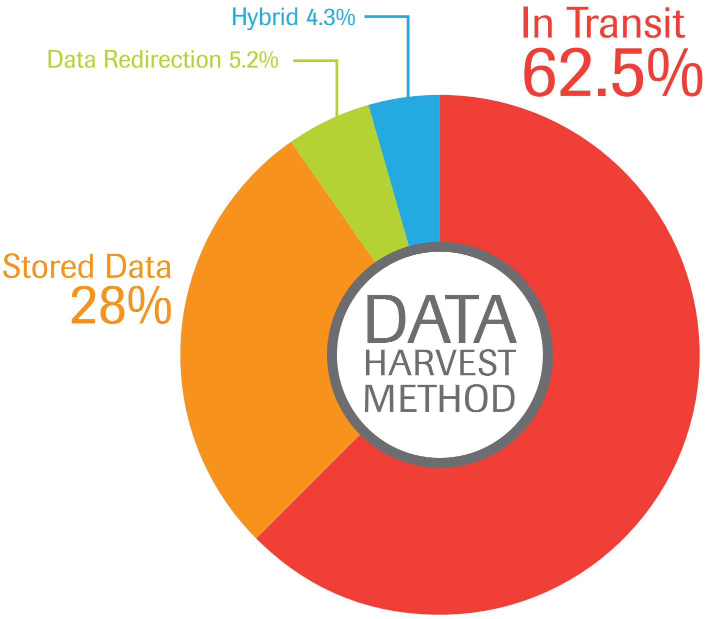
Overall, the propagation methods most commonly used in 2011 were similar to those being used last year and several years prior. Most target networks are Windows-based and use the NetBIOS protocol for file and print sharing. Attackers need only scan the network from the foothold for devices sharing file and print services to identify additional targets (specifically for ports 135, 137, 139 and 445). They can also use a technique called Address Resolution Protocol (ARP) cache poisoning, a complicated attack that allows an attacker to view network traffic and intercept clear text credentials and other sensitive data in real time.

Attacks such as these, however, were not needed in many of the networks investigated in 2011. Instead, systems using shared administrative username and password combinations, as well as mapped drives and open-by-default Windows hidden shares, enabled attackers to quickly identify additional targets, gain credentials and administrative access and then subsequently deploy their malware. These types of attacks can propagate across an entire small network (between one and 20 devices) in less than 10 minutes.

The third most used method of propagation is remote access caching. Many remote access programs have the option to "cache" or remember login credentials. While convenient for the end user, it is not secure; best security practices dictate that caching be disabled.

Aggregation

Like 2010, attackers in 2011 were more successful at harvesting data in transit than they were attacking stored data. Further, these attackers were more adept at hiding malware (e.g., memory dumpers, keystroke loggers and network sniffers) in plain sight, with processes appearing as subtle variants of legitimate process names, or as legitimate process names running from non-standard directories. Data exposure volumes are difficult to track and/or estimate, primarily due to the data harvesting methods used, but in cases where memory dumpers and/or key loggers were used, malware lived on a target system undetected for an average of six months before discovery.

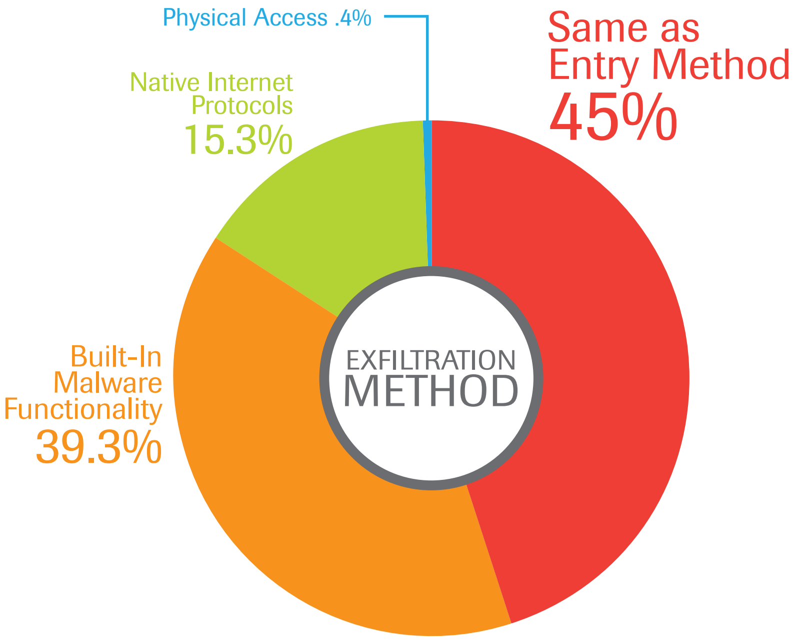


Exfiltration

Exfiltration, the third component of the Breach Triad, is the act of actually removing the data from the targeted systems. For 2011, the number one method is the removal of data via the same method in which the system was entered. Because the majority of breaches go unnoticed for long periods of time, attackers often do not need to establish an alternative method of data exfiltration.

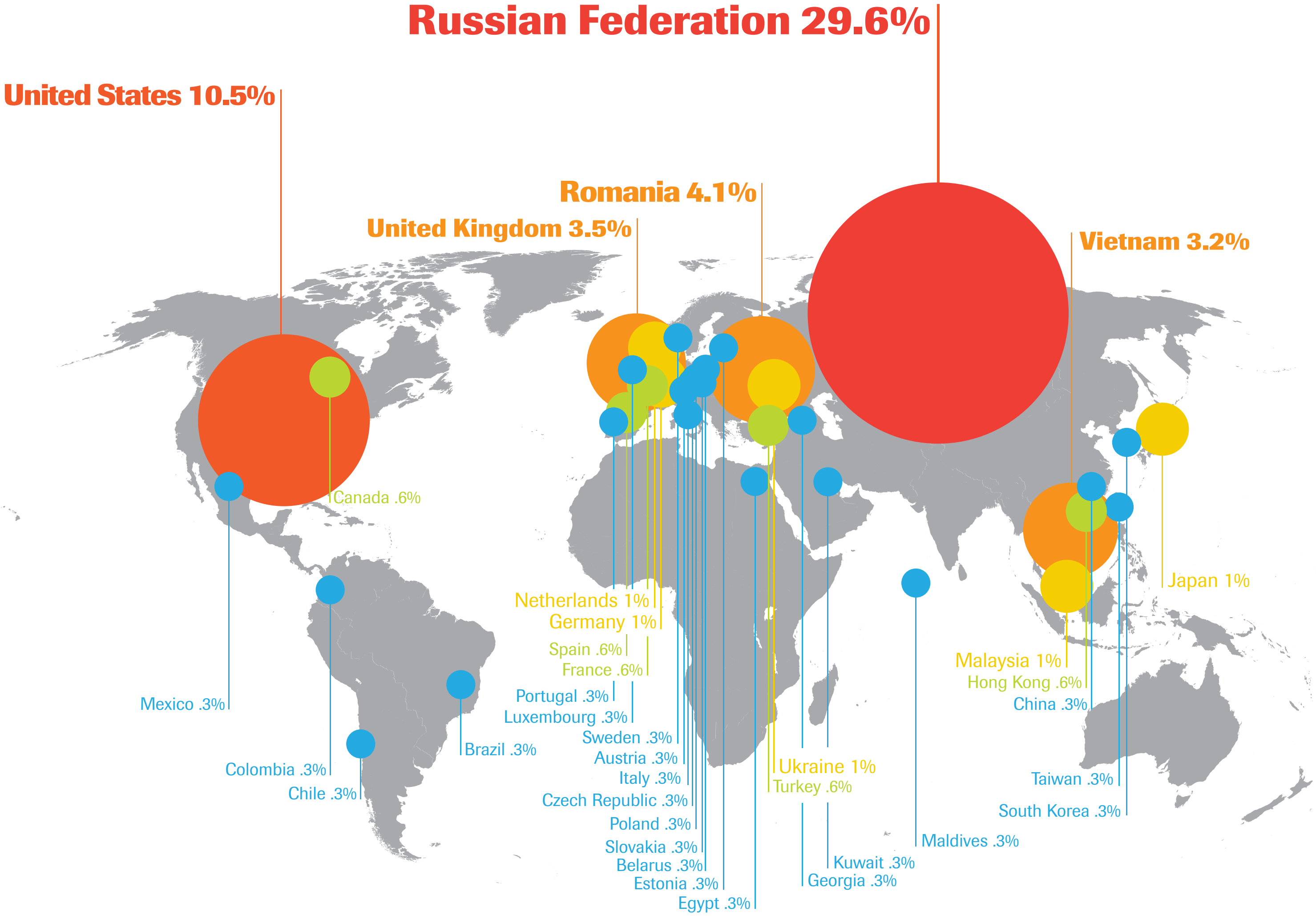
In cases where SQL injection is used as an infiltration method, it can also be used as a method of exfiltration. By this method, attackers can dump database tables with hundreds of thousands of customer records containing names, addresses, phone numbers and credit card numbers.

Attackers continue to exploit the lack of a firewall, or firewalls without egress filters to enable data exfiltration; 88.4% of cases involved firewall deficiencies, with 78% of organizations lacking firewalls completely.



Of the breach investigations involving firewall misconfigurations, 99% of the organizations' firewalls did not include proper egress filtering. Egress filtering employs rules to ensure data is being sent to the proper location, over the proper port, using an authorized protocol. In interviews conducted during investigations, the pervasive rationale behind the lack of egress filters is the belief that the internal network is "trusted" and any traffic originating from the trusted network must likewise be trusted. This rationale would only be accurate if a breach were not possible. Assuming a breach is not possible is an unrealistic view; data breaches are affecting organizations daily and globally. Practical, preemptive measures should be taken to ensure that, if a compromise occurs, the attacker has to circumvent an additional layer of technical controls to successfully extract data from a compromised environment.

Origin of Attack



✱ 32.5% Unknown Origin

International Perspectives

Attacker Source Geography

Based on our investigations, attacks in 2011 originated from 40 different countries, although the largest percentage shows origin to be unknown. Source IP addresses do not necessarily establish where attackers are physically located and maintaining online anonymity is very easy for attackers today. Therefore, the unknown points of origin simply represent anonymous service endpoints.

Both public anonymity services, such as Tor, and private alternatives available for small fees exist for dedicated criminals. Even when the point of origin is anonymous, this information can frequently assist law enforcement. Therefore, sharing intelligence among victim organizations, law enforcement and private security companies, such as Trustwave, is essential in combating cyber crime.

Based on our investigations and analysis of the 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.

Europe, Middle East and Africa

In contrast to data compromise trends in the Americas, very few data compromises occurred in POS networks in Europe, the Middle East and Africa (EMEA). Rather, as a result of higher adoption of "chip & pin" (EMV) and deprecation of magnetic stripe (mag-stripe) transactions within Europe, fewer opportunities exist in EMEA for the theft of track data used in mag-stripe transactions.

However, across the region many mag-stripe enabled POS systems remain in use to support mag-stripe only cards or transactions that fall back to mag-stripe when EMV fails. As such, card-present compromises do still occur in small numbers.

Overwhelmingly, e-commerce merchants in EMEA were the targets for cyber criminals. E-commerce businesses allow attackers to be geographically indiscriminate and concerned only with identifying targets that pose little technical complexity in compromising.

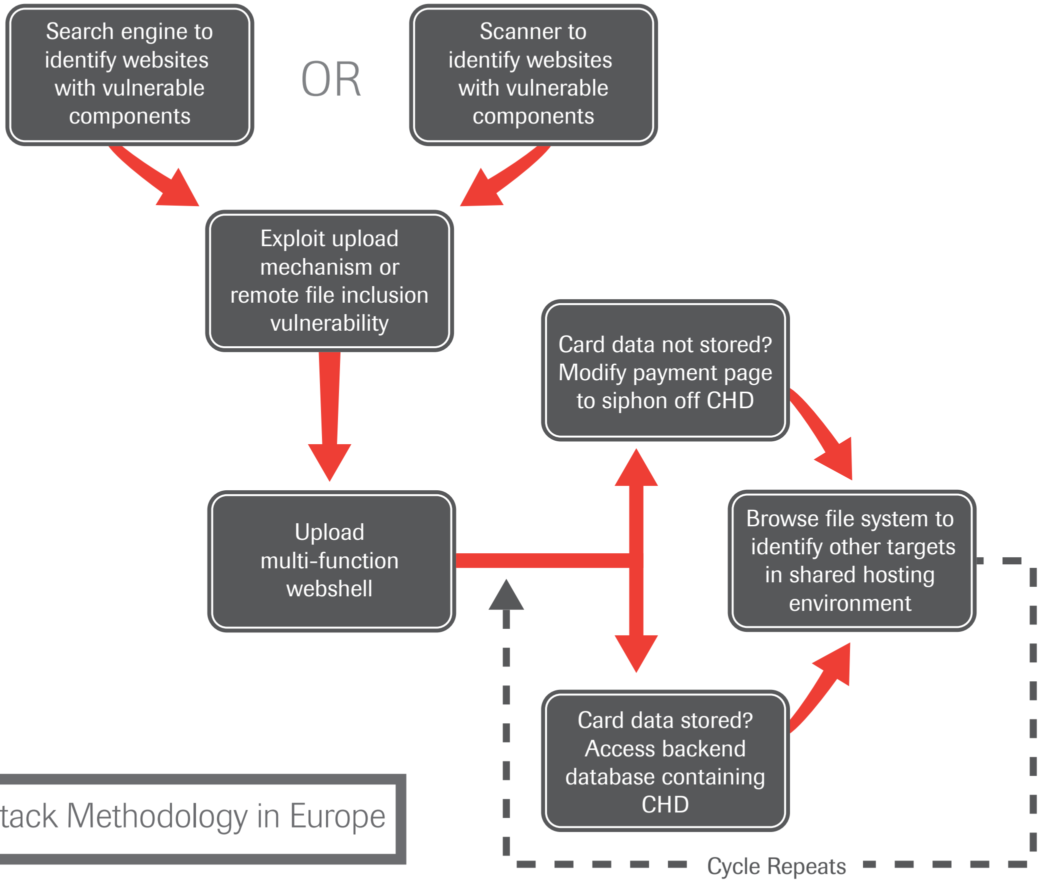
The typical vulnerabilities exploited in EMEA investigations were insecure, but legitimate file upload mechanisms or exploitable remote file inclusion vectors.

Very few SQL injection-based data compromises were investigated over the last year in EMEA. This may in part have been due to a regulatory change introduced by Visa Europe in 2010. The change stated that investigations only proceed when a minimum of 10,000 Visa cards are suspected to be at risk, and it was often these smaller merchants who had been associated with SQL injection-based data compromises.

Visa Europe introduced the PFI[2] Lite program in November 2011 to establish guidelines for performing investigations for merchants with less than 10,000 Visa cards at risk. Next year may see an increased number of investigations of smaller compromised entities as a result.

A pervasive problem with e-commerce compromises is highly inadequate logging and monitoring. Small and medium-sized e-commerce merchants typically do not have logging configured to identify possible security events. Further exacerbating investigations, merchants will sometimes erase everything as part of the containment process, including logs, following a compromise.

Unlike previous years, investigators from Trustwave SpiderLabs found no cases in EMEA where compromised resources were re-used for activities outside of data theft. In other words, attackers did not utilize the compromised infrastructure for file-sharing, hosting illegal content, hacking tools or other activities. The attackers appeared to be solely focused on obtaining data from target systems.


Search engine to identify websites with vulnerable components
OR
Scanner to identify websites with vulnerable components
Exploit upload mechanism or remote file inclusion vulnerability
Upload multi-function webshell
Card data not stored? Modify payment page to siphon off CHD
Browse file system to identify other targets in shared hosting environment
Card data stored? Access backend database containing CHD
Cycle Repeats

Typical Attack Methodology in Europe

[2] The PCI Security Standards Council's PCI Forensic Investigator (PFI) Program https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php

Notable Events: EMEA 2011

In one of the most significant EMEA compromises of 2011, in which a payment service provider was hacked, multiple servers and a wide area network with more than a thousand hosts were attacked. Trustwave SpiderLabs identified the single point of weakness as a legacy X.25 node. X.25 is a protocol suite which was widely used in the 1980s to build Wide Area Networks. Today it remains commonly utilized by financial institutions for inter-bank data exchange.

Unlike the relatively low-skilled e-commerce compromises, the attacker in this case demonstrated persistence and novelty in the technical aspects of the compromise. Having gained initial access to the environment via the X.25 node, the attacker identified an internal development system and proceeded to re-rewrite a well-known rootkit to function on the HP-UX operating system. The rootkit was then installed across a number of cardholder data processing servers to mask the presence of other malicious programs introduced by the attacker.

During the operation, the malicious scripts harvested cardholder data by terminating the legitimate instances of payment-processing software and then restarting the software with a Trojanized-debugger attached. The debugger captured all inter-process communications including unencrypted payment card data from within the system memory, which was otherwise encrypted when at rest on the disk and in transit on the network.

The attacker went unidentified within the environment for almost 18 months. Of note, the attacker was only identified when a subtle flaw within their own customized malware alerted the payment service provider's operational staff to suspicious activity.

It is worth noting that the payment service provider's environment was not PCI DSS compliant. Without mandates that strictly regulate payment processors, individual merchants that take steps towards PCI compliance still remain at risk of compromise on third-party systems that store and process their data. Appreciation that such a breach necessarily affects many merchants at once highlights the risk of partnering with small hosting/service providers with limited security expertise.

Finally there is continued traction toward data privacy legislation across the European Union. Proposals have been drafted, but still need to be approved by national governments. This effort signals a movement towards mandatory data breach disclosure laws across the region, as well as potential fines for organizations that do not adequately safeguard customer data. As such we expect to see continued growth in demand for proactive security.

Asia-Pacific

In 2011, APAC investigations made up 19% of investigations overall. A significant vulnerability was discovered in Australian "integrated point of sale" products (i.e., point of sale software that communicates with payment card terminals). Attackers remotely collected card details from these systems for use in counterfeit cards operations around the world.

In APAC, as witnessed in other parts of the world, attackers are increasingly automating the process of finding victims and extracting valuable data. This lowers the cost of performing attacks, which in turn lowers the minimum yield for a victim to be of interest.

Approximately 90% of APAC investigations were undertaken as a result of payment card data compromises.

In addition to payment card compromises, Trustwave investigated cases in APAC involving denial of service, loss of intellectual property, internal fraud, computer misuse and a variety of other computer-based incidents. Prior to 2011, all investigations related to payment card data compromise in APAC involved e-commerce breaches. While attackers are now migrating to POS systems, e-commerce attacks are still common.

A relatively small number of publicly disclosed vulnerabilities accounted for the majority of e-commerce compromises. These vulnerabilities appeared in popular shopping cart software. In most cases, patches had been released to resolve the issues, but had not been applied. Attackers used pre-packaged toolsets to exploit these vulnerabilities to dump data, gain access to an administrative interface or to upload malicious software to the Web server.

As in EMEA, remote e-commerce attacks designed to capture payment card data in real time increased in 2011, however, approximately two-thirds of e-commerce attacks continued to rely upon stored data, indicating these merchants continue to store payment card data on their systems. Many of these compromised entities reported that a third-party was responsible for the administration of their systems. They often did not know that payment card data was being stored, and that their service provider had not been applying software patches in a timely manner.

Similarly, most merchants did not believe their site was a target for cyber attackers. Some merchants believed, wrongly, that attackers leveraged sophisticated techniques that would be difficult to protect against or that victims were chosen carefully by a cost/benefit equation.

Attackers are not concerned with the victim's nature of business, and indiscriminately choose targets that offer little resistance to attack.

The reality is that the cost of finding vulnerable sites is close to zero, and attackers increasingly use software that constantly searches the Internet for potential victims. As a result an attacker stands to profit from a site accepting just a handful of payment cards per year. As with the EMEA e-commerce compromises it is a volume game for the attackers; given the relatively low overhead costs, a conveyor-belt-like process for finding and exploiting targets provides a satisfactory yield for the criminals.

Many of our investigations—55%—took place due to compromises in cardholder-present, or brick-and-mortar, environments. Almost all of the cardholder-present cases occurred in Australia and involved integrated point of sales environments.

In almost every brick and mortar case in APAC, attackers gained access to the victim environment via remote access software intended for use by a legitimate third-party provider. Alarmingly, many of these support vendors were using the same or similar passwords for all of their clients. Worse still, passwords were often the name of the vendor that provided remote support.

Preventing these attacks again relies on the implementation of security fundamentals. Ensuring that appropriate password security controls are in place for internal staff and that external service providers are subjected to the same level of adherence is key. Similarly, ensuring that cardholder data is truncated, tokenized or properly encrypted as soon as possible in the transaction flow minimizes the chance of compromise.

Following security basics like strong passwords, secure remote access, least privilege and patch management would have prevented almost all of the compromises investigated in APAC in 2011. In particular, organizations should ensure that their third-party service providers leverage appropriate information security controls when dealing with their data.

POS Attacks in Australia

In a common integrated point of sale (POS) environment, a PIN entry device, connected to the POS device, is used to read cards and collect PINs. The PIN entry device conducts the financial transaction and informs the point of sale device whether the transaction was a success or not. By design, the point of sale device should not be able to access cardholder account details. In fact, this is one of the key reasons a separate PIN entry device is used, as it reduces the risk of a compromise affecting cardholder data should a merchant's system be breached.

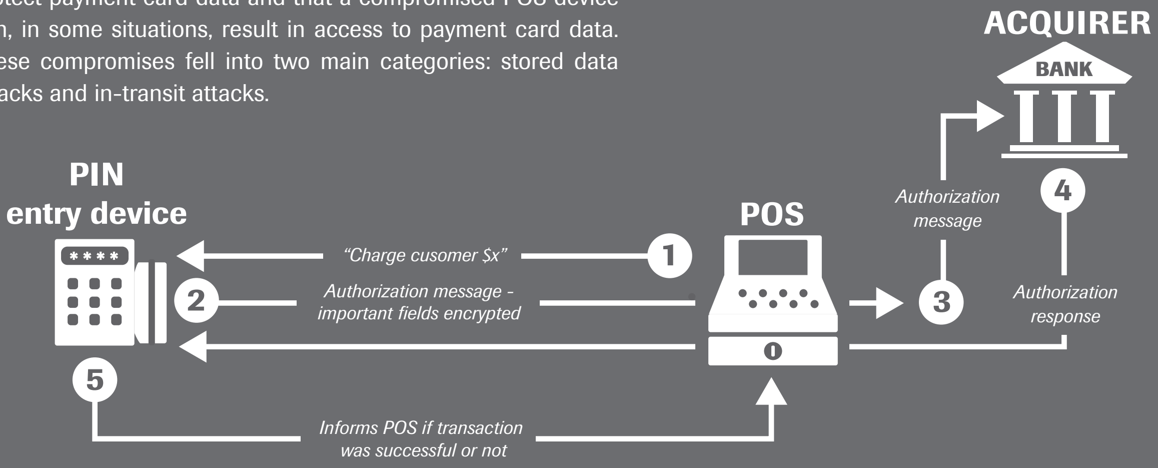
Attackers discovered that some PIN entry devices do not properly protect payment card data and that a compromised POS device can, in some situations, result in access to payment card data. These compromises fell into two main categories: stored data attacks and in-transit attacks.

In the majority of the stored data attacks, a PIN entry device that routinely shared payment card data with the POS device was in use or had been used in the past. Additionally, a piece of software used to interface the POS device with the PIN entry device was misconfigured to log this cardholder data onto the hard disk of the POS system. As a result, all payment card details processed by that POS system would also be stored in log files on the disk of the POS system. In several cases Trustwave SpiderLabs investigated, this amounted to more than three years of transactions.

In-transit attacks were first seen in Australian-based investigations towards the end of 2011 and are thought to be an evolution of the stored data attacks. The in-transit attack relies on the presence of a PIN entry device that shares clear-text cardholder data with the POS. Attackers then place memory-dumping malware on the POS, and collect this data in real time as it is processed.

This memory dumping malware is no different from the malware samples observed in the U.S. and EMEA. The malware succeeds if any device transmits clear-text payment card data through the POS regardless of the version and type of software being used on the POS. This type of attack is not unique to Australia and similar compromises have occurred in other countries in the APAC region.

Most of the newly deployed PIN entry devices used by Australian integrated point of sale merchants today are no longer vulnerable to either of these attacks. As with e-commerce, though, the cost of performing an attack is relatively low and attackers will continue to have a viable business even if a small proportion of the entire integrated POS merchant base still has vulnerable PIN entry devices.



Latin America and Caribbean

Companies in LAC have been targets for cyber criminals for many years, especially those companies in countries that have implemented online banking services. Economic growth, particularly in places such as Brazil, has been driving more people and business online, opening up avenues of attack for cyber criminals.

New for 2011 in LAC was the use of information technology, social networks and other methods to publicize confidential documents and recruit people with the intent to disrupt services through denial of service and other types of attacks. Some attackers also used denial of service attacks to distract the target while performing additional attacks to steal confidential information.

CERT.br Observations: Incident Response and Cyber Security Efforts in Brazil

Brazil, like many other countries, has observed a significant increase in computer security incidents and online crimes in the past few years. As criminals develop new techniques and evolve their skills, there is a growing need for cooperation, coordination and awareness to deal with the threats. With that in mind, several initiatives have been put in place in order to raise awareness and prepare the country to manage incidents accordingly.

Early Days

The birth of commercial Internet in Brazil comes from the establishment of the Brazilian Internet Steering Committee (CGI.br) in May 31, 1995. CGI.br is a multi-stakeholder organization, composed of members from government, private sector, non-governmental organizations and the academic community, and was created with the purpose of coordinating and integrating all Internet service initiatives in Brazil, as well as promoting technical quality, innovation and the dissemination of the available services.

One of the CGI.br attributions is promoting studies and technical standards for network and service security in the country. The development of incident response capabilities in Brazil originated from discussions inside the CGI.br Security Working Committee and culminated with the creation of the Brazilian National Computer Emergency Response Team - CERT.br (initially called NIC BR Security Office - NBSO) in June of 1997. Since 2006 CERT.br has been maintained by NIC.br, which is the executive branch of the Brazilian Internet Steering Committee.

Activities and Initiatives

CERT.br is responsible for handling any incidents that involve Brazilian networks connected to the Internet, providing coordination and support to organizations involved in incidents, establishing collaborative relationships with other entities, such as other CSIRTs, Universities, ISPs and telecommunication companies, and maintaining public statistics of incidents handled and spam complaints received.

As a Software Engineering Institute Partner, CERT.br delivers the CERTÆ Program Incident Handling courses in Brazil, helping new Computer Security Incident Response Teams (CSIRTs) to establish their activities and prepare their staff. Currently there are more than 35 CSIRT's in Brazil.

In the awareness field, CERT.br produces videos, guidelines and other literature targeting different audiences. For end-users there are educational videos and an Internet Security best practices guide, covering basic security concepts, information about virus, worms, fraud, and vulnerabilities. For network administrators there are guidelines with best practices on network security and technical white papers about specific threats.

Aiming for the improvement of network monitoring and the proactive detection of incidents in the country, CERT.br coordinates the "honeyTARG Honeynet Project," a chapter of the Global Honeynet Project, which uses low-interaction honeypots to gather information about the Internet infrastructure abuse by attackers and spammers. The initiative encompasses two sub-projects:

The Distributed Honeypots Project- a network of distributed honeypots hosted at partner organizations with the goal of increasing the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet space. For the international community, publicly available statistics and anonymized data is donated to other National CERTs and research organizations that provide information about detected network security incidents to affected parties. For the Brazilian community, there is a service that notifies CSIRTs and network administrators about the attacks originated from their networks, along with the relevant information for detection and recovery.

The SpamPots Project- comprised of 10 sensors deployed in nine countries to measure the abuse of network infrastructure for sending spam. It also helps to develop better ways of identifying phishing and malware, as well as botnets abusing open proxies and relays.

CERT.br is also part of the CGI.br Anti-Spam Working Group (CT-Spam), which developed several national initiatives against spam, including an awareness campaign for end-users, the evaluation and proposal of anti-spam legislation and the definition of a Code of Practice for Email Marketing.

However, the most significant initiative to reduce the abuse of the Brazilian broadband networks by spammers is the adoption of "Port 25 Management" in all domestic broadband networks. Because of the regulatory environment in Brazil, the adoption of this best practice required coordination among the Internet Industry, regulatory authorities and consumer rights organizations. Finally, on November 23, 2011, an agreement defining the steps for implementation was signed by CGI.br, NIC.br, the Brazilian National Telecommunication Agency (ANATEL), the Associations of Telecommunication Providers and the Associations of ISPs. The expected benefits include reducing the abuse of Brazilian networks by spammers, including the abuse performed by spambots.

Current Statistics and Trends

From January to September 2011, CERT.br handled about 318,000 incident notifications. This number represents a growth of 215% when compared to the same period during 2010, and 123% when these nine months are compared with the whole year of 2010. These incidents are split in categories such as fraud, worms (which includes bots spreading), and attacks to Web servers, scans, DoS, intrusions and "others."

Some trends observed since 2010 are the rise in attacks to Web servers and fraud attempts. The Web server attacks are, for the most part, to host phishing, Trojans, malicious scripts and tools to attack other Web servers. Regarding fraud attempts, notifications related to phishing are now greater in number than Trojan notifications.

We have also noticed an increase in reports of scans for SIP service (5060/UDP - used for VoIP connections). Although scans for SIP have been seen on the Internet for quite some time – and in the CERT.br honeypots top scanned ports for about two years – it was only by the third quarter of 2011 that it made the list of top 10 scanned ports. Further information about statistics on incident notifications is available at http://www.cert.br/stats/.

Sources

- About CGI.br. http://www.cgi.br/english/
- About CERT.br. http://www.cert.br/en/
- Antispam. http://antispam.br/
- honeyTARG Honeynet Project. http://honeytarg.cert.br/
- Cartilha de Segurança para Internet 3.1. http://cartilha.cert.br/
- Estatísticas Mantidas pelo CERT.br. http://www.cert.br/stats/

Malware Statistics

Malware comes in all shapes and sizes, and is often purposefully designed to capture and exfiltrate data, provide remote access, or automate compromised systems into a botnet — or to just cause general mayhem. Historically, Trustwave SpiderLabs analyzed malware specific to incident response investigations, yielding interesting samples not previously publicly available. In 2011, Trustwave SpiderLabs began building a database of malware samples, gathering samples from a SpiderLabs-maintained honeypot network and from underground malware repositories.

The database is used to identify trends in malware development, and to see how advancements in mass-deployed malware and targeted malware influence each other. By establishing a broad collection, specific malware capabilities can be correlated not just between malware variants, but also across families and categories. The collection is based on publicly identifiable malware samples.

Common versus Targeted Malware

Common, mass-distributed malware usually seeks to self-replicate through security vulnerabilities. Targeted malware doesn't self-replicate and may not exploit common vulnerabilities. Without these traits, it is more difficult for anti-virus software to detect targeted malware as malicious. While anti-virus products detected at least 60% of all malware samples in our database, when we focused only on samples found during our compromise investigations, anti-virus detected less than 12% as malicious.

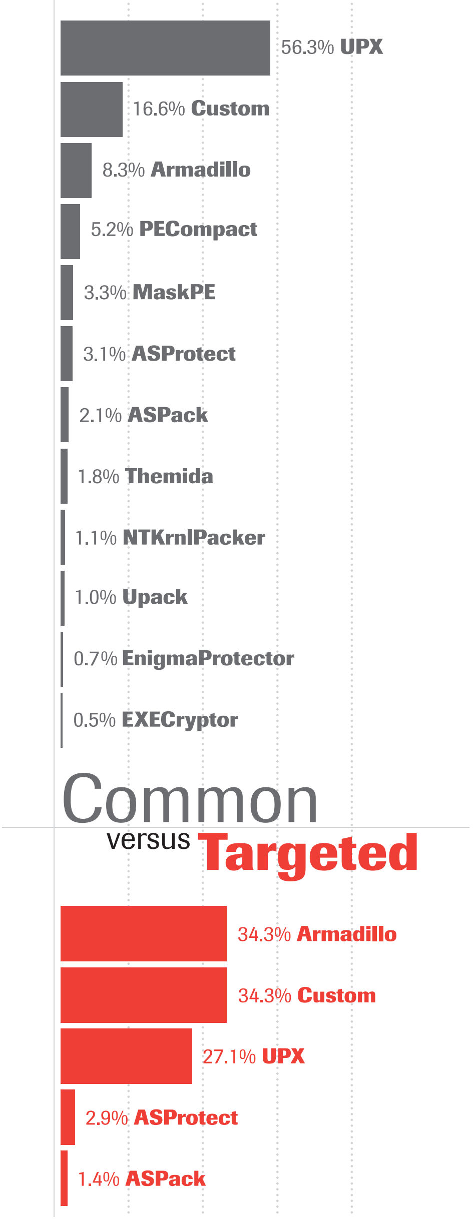
Common malware usually contains components for infection, privilege escalation, and command and control. While these components can be switched out, doing so requires packaging a new variant of the malware. Trustwave SpiderLabs found targeted malware to be much more modular, allowing for a per-attack workflow to be established. In approximately 89% of these database samples, malware had direct exfiltration mechanisms built-in, sending the stolen data automatically to the attacker.

Scheduling a system-wide service is a fairly common technique for both mass-distributed and targeted malware. Running as a service allows malware to recover from removal attempts, maintain a high level of access and read the memory of other processes. Both common and targeted malware use this technique, especially in the case of memory scrapers, accounting for approximately 42% of our database of public samples.

Targeted malware is becoming more advanced; approximately 13% of our database samples used inside knowledge or an in-depth understanding of how the target business application worked to directly hook into the target applications. Techniques such as DLL registration, the AppInit_DLLs registry setting[3], and DLL Hijacking[4] were all observed in Trustwave SpiderLabs engagements during 2011. DLL hooking is an example of legitimate code techniques that can be used by malware authors to perform malicious actions.

Packers

Packers are utility applications that can reduce the size of an executable and often include encryption or reverse engineering protections. Packers can be used by legitimate applications to reduce their memory footprint and protect intellectual property and trade secrets present in the application code. Malware authors have long used packers to obfuscate their malicious binaries in order to avoid detection by anti-virus and confound researchers attempting to understand their code.



[3] Working with the AppInit_DLLs registry value. http://support.microsoft.com/kb/197571

[4] Dynamic-link library. https://en.wikipedia.org/wiki/Dynamic-link_library#DLL_hijacking

Packers are much more common in public malware samples, appearing in more than 36% of our database samples, than in Trustwave SpiderLabs' case-specific malware samples, which at approximately 16%, likely due to the different needs of the malware authors. Targeted malware, lacking self-propagation functionality, generally flies under the radar of anti-virus software. For such malware, using an identifiable packer can actually increase the chance of detection. Malware destined for widespread distribution must work harder to disguise itself, and its authors need to protect sensitive information, such as domains for command and control, in each variant to avoid detection by law enforcement and other Internet security organizations.

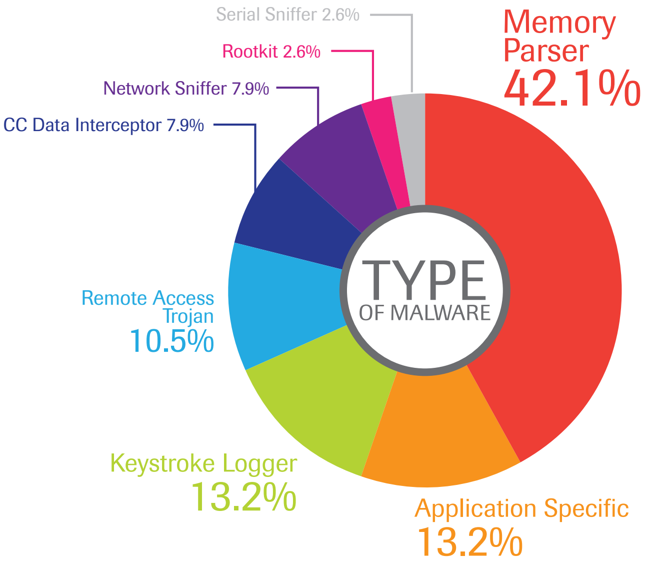
Known packers, like UPX, are being used by more than 56% of packed common malware. Armadillo and PECompact were used about 8.5% and 5.2%, respectively. For targeted samples, however, Armadillo was used 34.3% of the time and UPX only 27.1%.

Samples from both the database and customer engagements contained malware packed with custom packers. While the purpose and functionality of custom packers is essentially the same as out-of-the-box versions, the malware methods and resulting samples did not match any of the known packer utilities on the marketplace.

Malware Types

Memory-parsing malware accounted for 42.1% of investigations. Keystroke loggers[5] and application-specific malware tied for second place at 13.2% each.

Application-specific malware is an emerging trend, it requires a detailed knowledge of the targeted platform, for instance, in the case of POS, ATM or other bespoke business system. Application-specific malware directly targets sensitive data in memory, storage or by tricking the application to pass the data directly to the malware during processing. Investigations in 2011 revealed attackers returning to upgrade their malware as new versions of the affected application software were released, confirming the sophistication and dedication of the organizations developing and deploying this malware.

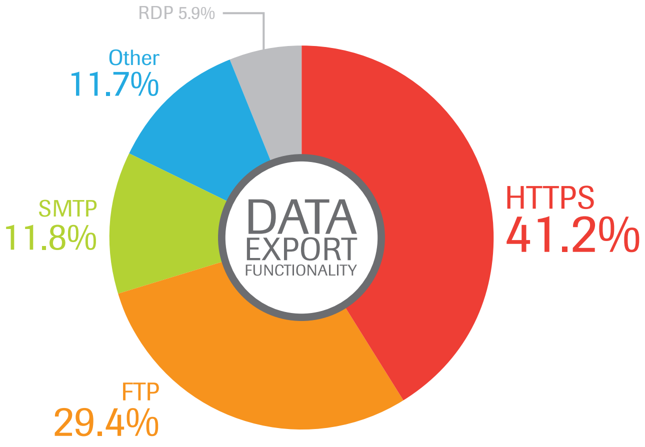


Classic, high-level languages such as C++, Delphi, Perl, and .NET have remained the favorite for malware authors. Old build dates for the compilers continue to be observed, suggesting high degrees of code reuse and minimal modification.

Reverse engineering of malware samples often uncovers plagiarism from online examples or re-purposing of existing open source code. A noticeable trend in samples collected during 2011 is an increase in the use of Perl2Exe in order to embed a portable Perl environment with the malware. Because of its ability to parse large batches of language for text, Perl is attractive to malware developers needing to parse through data in search of credit card or other personally identifiable information.

Data Export

An emerging trend in 2010, HTTP is now the most likely protocol to be used for data exfiltration in 2011. In analyzed samples, 41.2% of malware used HTTP, or TCP traffic over ports 80 and 443, to exfiltrate data. HTTP and HTTPS are regularly chosen for data exfiltration and control as Web traffic filtering is not as widespread as other egress filtering protections. The growth of malware using HTTP(S) should motivate enterprises to improve filtering for this common protocol.



File Transfer Protocol (FTP), historically a favorite exfiltration method, was utilized by only 29.4% of malware. And only 11.8% used Simple Mail Transfer Protocol (SMTP, the standard email protocol) to export data.

Malware samples that did not include any type of direct exfiltration, requiring an attacker to return to compromised hosts to recover captured data, was also observed in 2011. Some attackers may be moving away from automation, which can indicate a pattern of activity and trigger alerts, to increase the duration between compromise and detection. By staying "quiet" in an environment, the attacker will likely have more time to achieve their objectives.

[5] A keystroke logger intercepts data as it is being entered at a computer terminal via the keyboard, touch screen or external data entry device (e.g., card reader).

United States Secret Service: Protecting the Nation’s Leaders and Financial Infrastructure

Hugh Dunleavy
Special Agent in Charge, Criminal Investigative Division

In the spring of 2010, undercover agents of the United States Secret Service New York Field Office discovered some postings on an Internet forum from a member using the online nickname “f1ex.” In these messages, “f1ex” proudly boasted of his ability to compromise the networks of financial institutions and discussed his global network for the distribution of stolen financial data. In the early stages of the investigation, these agents, assigned to the New York Electronic Crimes Task Force, learned that “f1ex” had been a fixture in the criminal underground since 2003, with associations to cyber criminal organizations such as Shadowcrew, dismantled by the U.S. Secret Service in 2004. Agents classified “f1ex” as an overseas hacker involved in selling illegally obtained credit card account numbers through online forums and various other means.

Why is the Secret Service, an agency renowned for protecting the President of the United States, investigating an Internet hacker? The answer goes back to April 14, 1865, and the creation of the U.S. Secret Service. As the nation’s Civil War neared its end, President Abraham Lincoln and his Treasury Secretary, Hugh McCulloch, discussed the creation of the Secret Service to combat the counterfeiting of U.S. currency. At the time, nearly one-third to one-half of all U.S. currency in circulation was counterfeit, which threatened to destroy an already fragile wartime economy. Ironically, that evening after meeting with McCulloch, Abraham Lincoln was shot at Ford’s Theatre and died the next morning. Today, the Secret Service has a dual mission: to safeguard the nation’s financial infrastructure and to protect national leaders.

Over the years, the Secret Service has maintained a long history of protecting American consumers, industries and financial institutions from fraud. With the evolution of payment systems and modernization of commerce, the Secret Service has also evolved to ensure the protection of the economy. The passage of new legislation in the 1980s gave the Secret Service authority for investigating credit card and debit card fraud and parallel authority with other federal law enforcement agencies in identity theft cases. In 1984, Congress gave the Secret Service concurrent jurisdiction to investigate financial crimes as they relate to computers.

The Secret Service has long recognized that partnerships and cooperation act as force multipliers in conducting investigative and protection operations. In 2001, Congress recognized the value of the Secret Service Electronic Crimes Task Force (ECTF) model established in the New York Field Office, where law-enforcement, the private sector and academia collaborated in detecting and suppressing computer-based crime. Through 2001's USA PATRIOT Act, Congress directed the Secret Service to establish a network of ECTFs to combat the rise of cybercrime. Currently there are 31 ECTFs: 29 domestic task forces and two located overseas in London and Rome. These ECTFs and their associated partnerships allow the Secret Service to employ both proactive and responsive investigative tactics centered on exploiting vulnerabilities identified in the cybercrime underworld. Agents and ECTF partners have achieved success investigating financial and cybercrimes that range from bank and wire fraud to network intrusions, from botnets to credit card offenses and many cybercrimes in between. This explains why Secret Service undercover agents were looking into cybercrimes when they identified "f1ex" as an investigative target of interest.

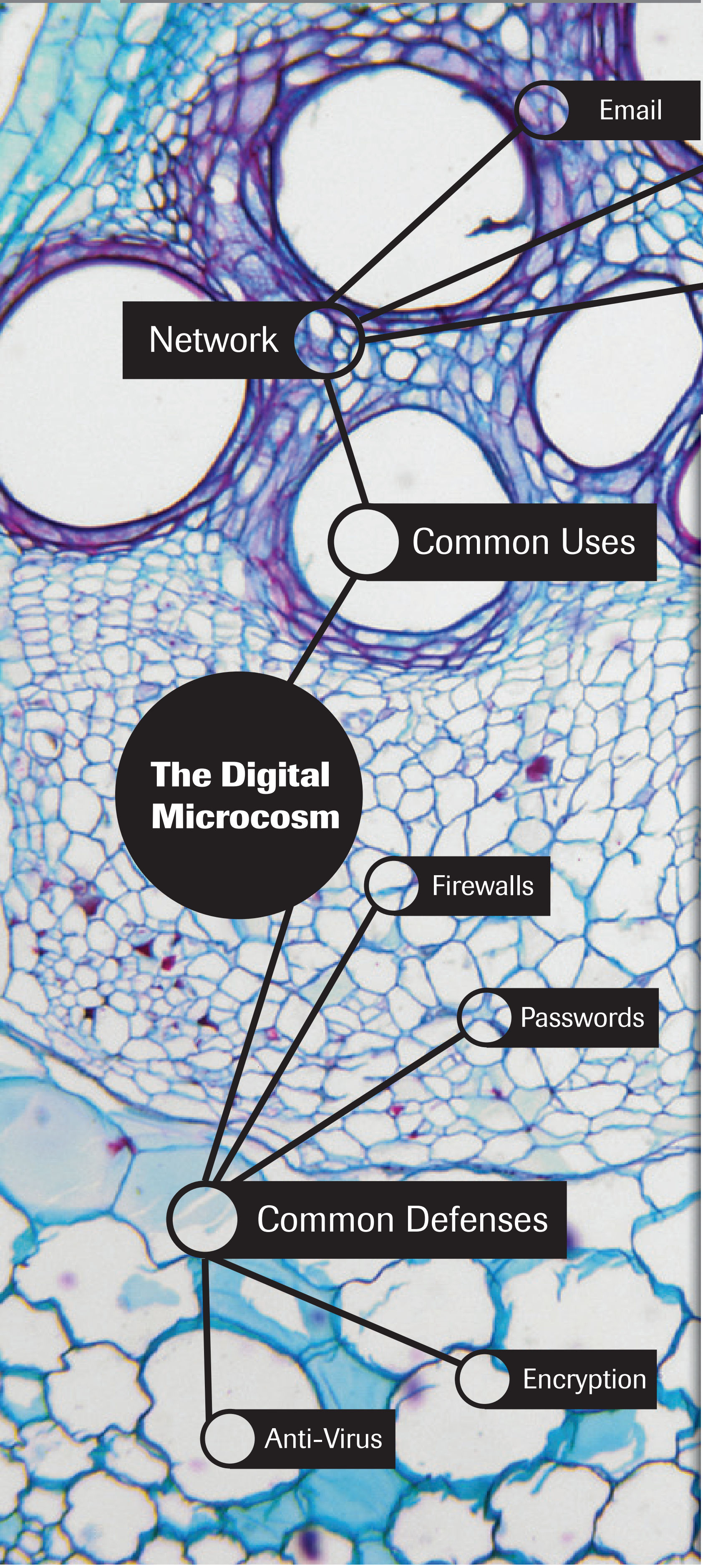
Through the spring and into the summer of 2010, undercover Secret Service ECTF agents monitored and engaged "f1ex" attempting to identify the hacker who now had been traced back to Malaysia. As this investigation progressed, Secret Service agents learned that "f1ex" was planning on traveling to the United States. Agents arranged to meet "f1ex" in New York City to purchase stolen credit card account numbers. During the course of the investigation, agents identified "f1ex" was Lin Mun Poo, a Malaysian citizen. On October 21, 2010, an undercover agent met with Poo at a Queens, New York, diner and purchased $1,000 worth of compromised credit card numbers. The New York ECTF later identified the account numbers were issued from a bank in Nepal.

In a second meeting with undercover agents, arrangements were discussed for a continued long term relationship for the distribution of compromised data, further illustrating Poo's access to stolen data. Agents set up in a hotel room in Brooklyn, New York waited for the deal to be finalized. Poo arrived with other associates and negotiations began to purchase thousands of stolen credit cards. During the meeting, Poo was taken into custody. A subsequent analysis of Poo's laptop computer revealed more than 100 GB of data, including approximately 413,000 credit card account numbers with an estimated value of $206 million. This analysis also revealed evidence of multiple network intrusions into government and banking sector systems.

On April 13, 2011, in the Eastern District of New York, Lin Mun Poo plead guilty to violating Title 18, United States Code, Section 1029 (Access Device Fraud). On November 4, 2011, Poo was sentenced to serve 10 years in a federal prison.

The investigative mission of the Secret Service has evolved to keep pace with the information revolution and rapid globalization of commerce. The combination of advanced technology with the worldwide Internet has created the venue for transnational cyber criminals to operate with nearly complete anonymity. The Secret Service and their law enforcement partners are committed to disrupting and dismantling these criminal networks. The arrest and successful prosecution of Lin Mun Poo is just one instance that demonstrates the proactive approach and cooperation that exemplifies the collaborative efforts of the Secret Service's ECTFs. The Secret Service will aggressively continue its mission to safeguard U.S. financial infrastructure and payment systems and preserve the integrity of the U.S. economy. The Secret Service is proud to partner with law enforcement, the private sector and academia to accomplish this mission.

Please visit the Secret Service website at http://www.secretservice.gov for more details and a complete list of resources.



Security Weaknesses under the Microscope

Businesses are continually looking to protect their assets, from employees to customer records to intellectual property and beyond. This section reviews client trends to identify four fundamental resources that are vital to business operations. We also identified four defenses that may require significant budget, whether as capital expenditures or operating costs, due to its iterative process.

Time and time again Trustwave clients ask: “Are the attackers getting better or are we getting weaker?” The answer isn’t simple, but the following sections aim to put weaknesses under the microscope to find ways to solve security problems.

In the Workplace: Four Vulnerable Resources

Every single day, employees access networks, send and receive email, access the Web, and use mobile devices. Some employees also manage such services for their companies. A cyber criminal sees the workplace as an opportunity, and they use these same services, in part or combined, to execute a targeted attack.

Trustwave SpiderLabs performed more than 2,000 tests on targeted attack vectors in 2011. While tests were conducted on areas of physical, social, wireless and devices like ATMs and kiosks, this section will analyze the four most vulnerable: network, email, the Web and mobile devices. The security community continues to focus on new attack vectors, while older threats are often overlooked, ineffectual security controls are implemented, and problems that have existed for years persist.

The Network – Legacy Issues Still At Large

Issues that have been pervasive for years include password security, legacy devices, protocols and attacks, and ineffectual security controls, continue to affect the security of networks.

Network Authentication

One of the most pervasive vulnerabilities of 2011 is network authentication. This vulnerability generally fits into one of four broad categories:

Network/Domain Issues

This category generally refers to issues within a Microsoft Active Directory (AD) domain, Netware Domain, or any other centralized network file or print-sharing authentication. Vulnerabilities may be lack of password policy enacted at the domain or, more often, exceptions to domain password policy, such as weak passwords for service accounts. Others include temporary administrative accounts that are never revoked or administrators exempting their accounts from policy enforcement. This allows an attacker or a malicious insider, once they gain entry to the network environment, the ability to access moderately privileged accounts. This can often lead to a compromise of the entire domain. Since domain authentication is used as a central authority for many different purposes, accessing sensitive data becomes a trivial exercise when an attacker can operate as a domain administrator.

Device/Service Issues

This category refers to a well-documented yet still pervasive issue of devices and services configured with default and blank passwords, or weak and easily guessable passwords such as “password.” Device and service examples include:

- Routers, network switches, firewalls and security devices with blank, weak, or default passwords
- Database services such as Oracle or Microsoft SQL administrative accounts
- Web application framework administrative accounts
- Administrative interfaces for VoIP and other PBX/telcom systems

The impact of this category varies by device type and, with certain devices such as routers or databases, there is often an easy path for an attacker to escalate their privileges or access data directly.

Workstation / Remote Access Issues

Blank or easily guessable local system accounts for end-user workstations or workstations with ad-hoc services such as VNC, PCAnywhere, or other remote access software can be a weak point for many organizations. Like the previous issue, the impact of this category varies by device type and content, and vulnerabilities here can allow for an escalation of privileges, especially if 1) the system in question stores cached domain credentials, 2) there is password reuse between local and domain accounts, or 3) the same password is used for local accounts across multiple systems.

Network/Transmission Issues

Authentication credentials transmitted over the network in clear text or weak or legacy authentication schemes are another issue of which to be aware. These vulnerabilities can be exploited by passive or active man-in-the-middle techniques to harvest passwords as they are transmitted over the network, either directly or by gathering data that can easily be cracked (such as the legacy Microsoft LM Half Challenge[6]).

Legacy Attacks

An abundance of networks and systems were still found vulnerable to legacy attack vectors; many of these vectors date back 10 years or more. Organizations are implementing new technology without decommissioning older, flawed infrastructure. Attack vectors found include:

Layer 2

Attacks that allow for passive and active man in the middle, such as ARP spoofing / ARP cache poisoning and other vectors at the lower layers, remain high impact for many organizations, allowing everything from credential and session theft, to direct data theft.

[6] How to disable LM authentication on Windows NT. http://support.microsoft.com/kb/147706

Unencrypted Protocols

Protocols that transmit sensitive information in the clear remain an issue for many organizations even though more secure replacements exist. Such protocols are widely known to be vulnerable to passive and active attacks from simple eavesdropping to session theft.

Legacy Protocols

Almost unbelievably, protocols such as Unix "r" services are still found in abundance in many environments. Documentation of authentication bypass and other attack vectors for these protocols have existed for years. They are often overlooked, however, as the systems were implemented before the risks associated with these protocols were widely known. Organizations running these systems work on maintaining functionality, but never assess the system security.

Misconfigured Network Access Rules

Network access control devices such as packet filtering routers and firewalls are often implemented and configured incorrectly. Organizations are not only implementing the wrong type of device as a cost savings (opening themselves up to straightforward denial of service attacks) they also often implement these devices without using best practices that have been established for 15 or more years. Pervasive issues such as access control rules that essentially render the device useless were common, as well as things like the non-implementation of egress filtering, which can allow for virus or worm propagation, and provide an attacker with an easy method of creating an exfiltration channel.

Paper Tigers

Organizations frequently implemented security controls with little or no efficacy against the threat it was intended to mitigate. The generic term for this is a "paper tiger," or "security theater" to use a term coined by security strategist Bruce Schneier.

Many paper tigers were found in 2011; one example was the use of host-based firewalls in place of actual network segmentation. Many organizations architect large flat networks. While not good network architecture, it was implemented at one point, likely because it was simple and inexpensive at the time and today re-architecting would be a large undertaking. Organizations addressed segmentation by simply adding host-based firewalls to their otherwise flat network rather than undergoing a re-architecting exercise. This solution does not provide the same level of security as proper segmentation and, for a malicious insider, it is barely a speed bump for layer 2 and man-in-the-middle attacks.

Vulnerability Scan Statistics

The next section analyzes more than two million scan results from 2011.[7]

Default Credentials

Many applications and devices are shipped or installed with default usernames and passwords, often with full access rights. These default passwords are frequently not changed, which can allow an attacker to use them to gain access.[8] Leaving default passwords unchanged is particularly dangerous for applications accessible from the Internet.

28% of Apache Tomcat installations with an accessible administrative interface have default credentials

10% of JBoss installations with an accessible administrative interface have default credentials

9% of phpMyAdmin installations have default credentials, and a further 2% do not require authentication at all

2% of Cisco devices with an accessible administrative interface have default credentials

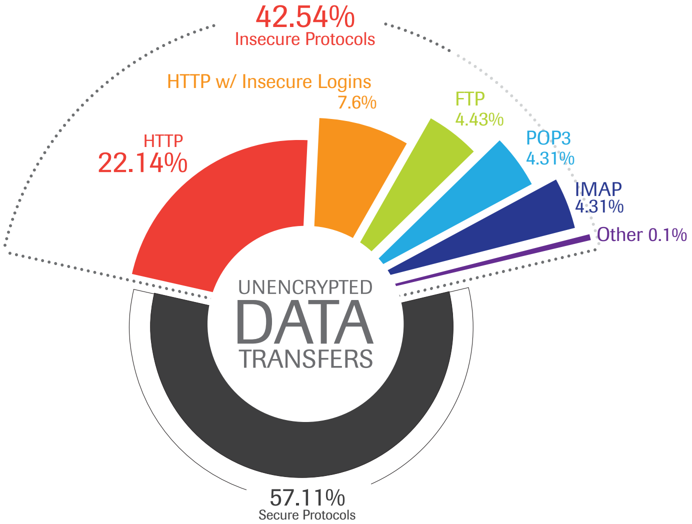
For many common applications and devices, Trustwave TrustKeeper® vulnerability scans show which are left with default credentials. These include applications that could allow an attacker to compromise other applications or servers, or gain direct access to sensitive data stored on internal databases. phpMyAdmin, in particular, has been linked with several notable breaches, including the 2011 breach of Dutch certificate authority Gemnet, in which the attackers gained access through a phpMyAdmin server that did not require authentication.

[7] Delivered through the Trustwave TrustKeeper® platform, Trustwave's vulnerability scanning service scanned more than 2,000,000 customers in 2011. These customers elect to have network and application vulnerability scans perform at various intervals throughout the year. Trustwave SpiderLabs developed the proprietary scanning technology and maintains the vulnerability signatures for TrustKeeper by providing weekly (or more frequent, if critical) updates to our cloud-based scanning engines.

[8] Default credentials to nearly every commercial product can be found online easily. For example, http://cirt.net/passwords contains a database of more than 450 vendors representing nearly 2000 passwords.

Unencrypted Data Transfers

Although mainstream encrypted protocols for transferring Web pages, email, and other files and data have existed for more than a decade, their insecure predecessors continue to predominate. While legitimate applications may exist for the use of unencrypted protocols across the Internet (e.g., websites with no sensitive content or functionality), in many cases the insecure protocols are used to transfer sensitive data. More than a quarter of all HTTP services scanned by TrustKeeper had login pages that transmitted credentials unencrypted.



Overly Permissive Network Access

10% of all organizations scanned by TrustKeeper allowed connections from the Internet to internal database servers; 85% of these were MySQL database servers

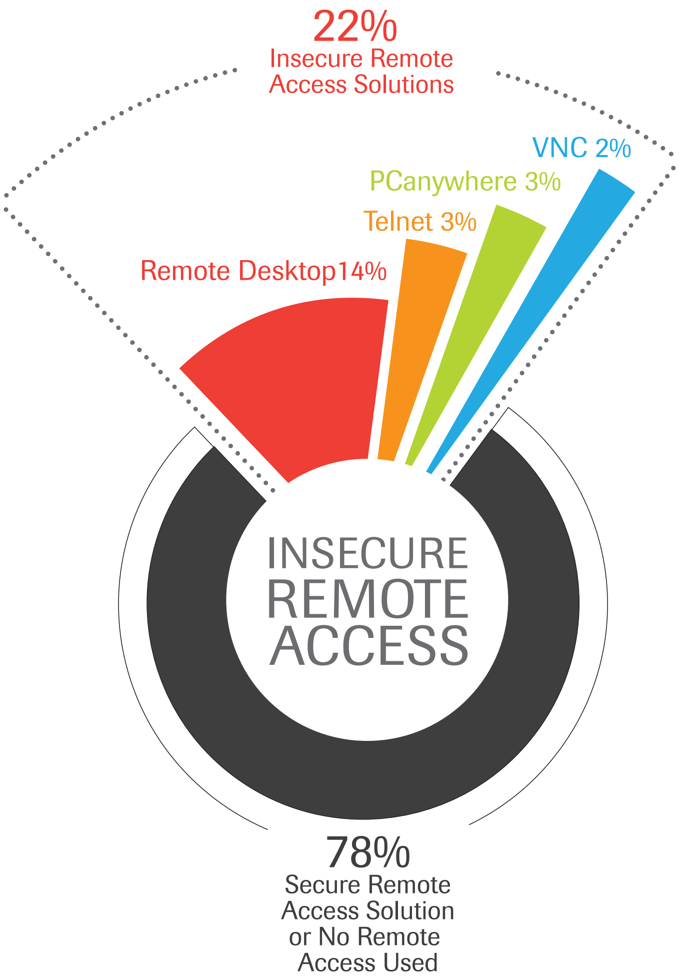
3% of all organizations scanned by TrustKeeper had results suggesting that one or more of their systems were essentially not protected by a firewall

TrustKeeper scans reveal that a significant number of organizations do not adequately protect network services that should not be exposed to the Internet, such as database servers and Windows networking services. Whether due to misguided policies, firewall misconfiguration or lack of firewalls in the first place, these services end up accessible to the Internet. Database servers, particularly MySQL, are the most frequent victims, and a significant number of these appear to come from shared hosting providers.

Exposing these services provides attackers an avenue of access to sensitive information, allowing them to directly attack a database server, which may have default passwords. Or they may be able to uncover missing security updates, rather than discovering flaws in a Web application, allowing an indirect attack against the server.

Insecure Remote Access

Despite the wide availability of secure VPN solutions, 22% of organizations continue to use insecure remote access applications. Without robust authentication and data encryption, these applications do not provide adequate security for remote access, potentially exposing usernames, passwords and other sensitive data. Additionally, the applications provide direct access to a computer or device, giving attackers more areas to attack, increasing the risk of compromise for those hosts.



Top 10 Network Risks

Below is a top ten list of the issues found during the more than 2,000 penetration tests conducted in 2011.[10]

1 Weak or Blank Password for an Administrative System Account

Windows or Unix Systems may have an easily guessed or null password for an administrative level account.	CVSSv2 Score 6.7

2 Sensitive Information Transmitted Unencrypted on the Wire

Sensitive information such as CHD, PII or SSN is not encrypted while traversing internal networks.	CVSSv2 Score 6.7

3 MS-SQL Server with Weak or No Credentials for Administrative Account

Microsoft (MS) SQL server may have an easily guessed or null password for administrative accounts such as the system administrator account.	CVSSv2 Score 4.7

4 Address Resolution Protocol (ARP) Cache Poisoning

ARP cache poisoning, or ARP spoofing, is an OSI Layer 2 attack. A gratuitous ARP message is sent to one or more machines on the subnet stating that the MAC address has changed; the message usually contains the attacker's MAC as a substitute. When the attacker turns on IP forwarding, sent packets will be routed through the attacker's machine.	CVSSv2 Score 10

5 Wireless Clients Probe for ESSID's from Stored Profiles When Not Connected

A Karma attack occurs when an attacker starts up a bogus wireless AP that will allow association and access for any client probe from a stored profile. In this way the client connects to the Karma AP instead of the intended AP. If the attacker's AP has Internet connectivity and is configured to route traffic, the victim can perform tasks normally but not know they are connected to an attacker.	CVSSv2 Score 4.7

6 Continued Use of Wired Equivalent Privacy (WEP) Encryption

WEP is a protocol for encrypting transmissions over IEE802.11 wireless networks. Packets are encrypted using the stream cipher RC4 under a root key shared by all radio stations. Security analyses of WEP show that it is inherently flawed; an exploit tool exists for almost every step in the encryption process.	CVSSv2 Score 8

7 Client Sends LAN Manager (LM) Response for NTLM Authentication

Any number of mechanisms can "trick" a client into attempting to authenticate to a malicious server/service (e.g., MITM, DNS or DHCP attacks, embedded links in Web pages) making this vector easy to implement. If a user is an administrator of his or her own system (very common), compromise of the host is easier to accomplish and an attacker will have access to the local system, domain or domain administrator credentials. By implementing a server with a known NTLM 8-byte challenge, it is possible to perform cryptographic attacks against a captured LM client hash using a combination of pre-computed hash tables (rainbow tables) and brute force to reveal the plaintext password.	CVSSv2 Score 4.7

8 Misconfigured Firewall Rules Permit Access to Internal Resources

Depending on the complexity of the firewall access control list, mistakes can cause data to be forwarded to hosts inside the network.	CVSSv2 Score 4.7

9 Storage of Sensitive Information Outside the Designated Secured Zone

Sensitive information is stored in unencrypted files on local workstations or network file shares.	CVSSv2 Score 3.3

10 Sensitive Information Transmitted Over Bluetooth

2011 has seen developments in tools that can be used to sniff sensitive information if it is transmitted over Bluetooth. Because of this an eavesdropping attacker can sniff this information.	CVSSv2 Score 4.5

[10] Note: For each risk, we documented the Common Vulnerability Scoring System Version 2.0 (CVSSv2) score as documented and maintained by the Forum of Incident Response and Security Teams (FIRST) in which Trustwave SpiderLabs is a member. For more information, visit http://www.first.org/cvss/cvss-guide.html.

New threats and emerging attack vectors continue to receive the most attention from security departments and budgets, while older problems remain unaddressed. Many issues found in network penetration tests and vulnerability scans are well-known, some more than 10 years old, and others date back to the very beginning of shared and networked computing. These vulnerabilities are actively exploited by attackers and often represent the path of least resistance. Older, widely known vulnerabilities make exploitation simpler and the tools to exploit these issues are mature, several revisions deep, and even feature rich.

As the saying goes, those that fail to learn from history are doomed to repeat it. Organizations must look at these old issues and address them.

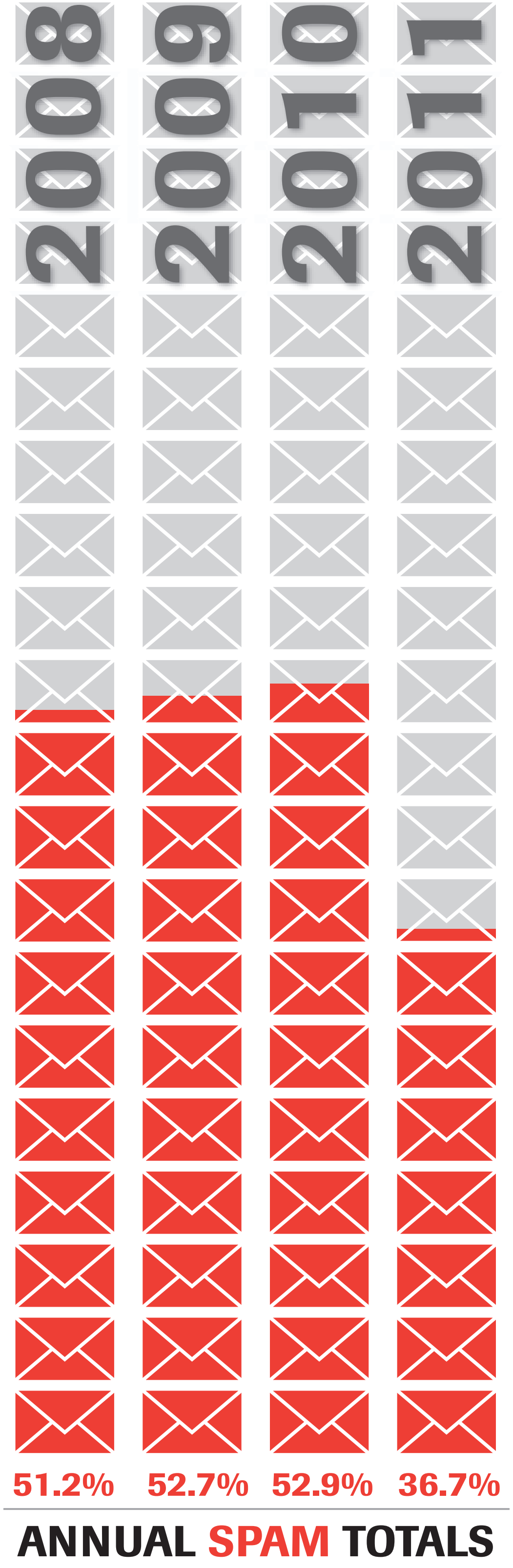
What's in Our Inbox? 2011 Email Trends[11]

Spam and junk mail peaked in 2008; the percentage of "good" emails has slowly increased each year since. Although spam and junk mail have declined, mail containing viruses and malicious executables have nearly doubled year over year (although they still represent less than 1% of all email being processed). Attackers were more likely to send malicious emails during the early hours of the morning, peaking between 8 a.m. and 9 a.m. Eastern Standard Time, slowly tapering off over the course of the day. Similar to the trend observed in 2010, attackers are moving away from mass quantity email (although it still exists). Rather, attackers are becoming more focused on targeting users with emails containing malware and malicious Web links.

Email Statistics

Trustwave mailMAX processes more than four billion email messages every year. To make sure that every message sent is clean before entering or leaving the network the messages are thoroughly scanned for viruses, spam and unauthorized content. Spam messages and other unsolicited emails waste time and cost businesses money.

The percentage of email messages processed as spam dropped noticeably from the fifty-percentile range (where it had maintained the previous three years) to 36.7% during 2011. Part of the drop-off of messages categorized as spam may be due to the improved use of additional real-time blacklists (RBLs), implemented in late 2010. RBLs block known bad email servers by default, limiting the need for further computationally expensive analysis. Trustwave saw a 7% increase in email stopped by RBLs in 2011 compared to the previous year. Further aiding the decrease of spam, a number of large botnets were taken down during the year, including Rustock, believed to be responsible for sending 40% of all Internet spam.[12]



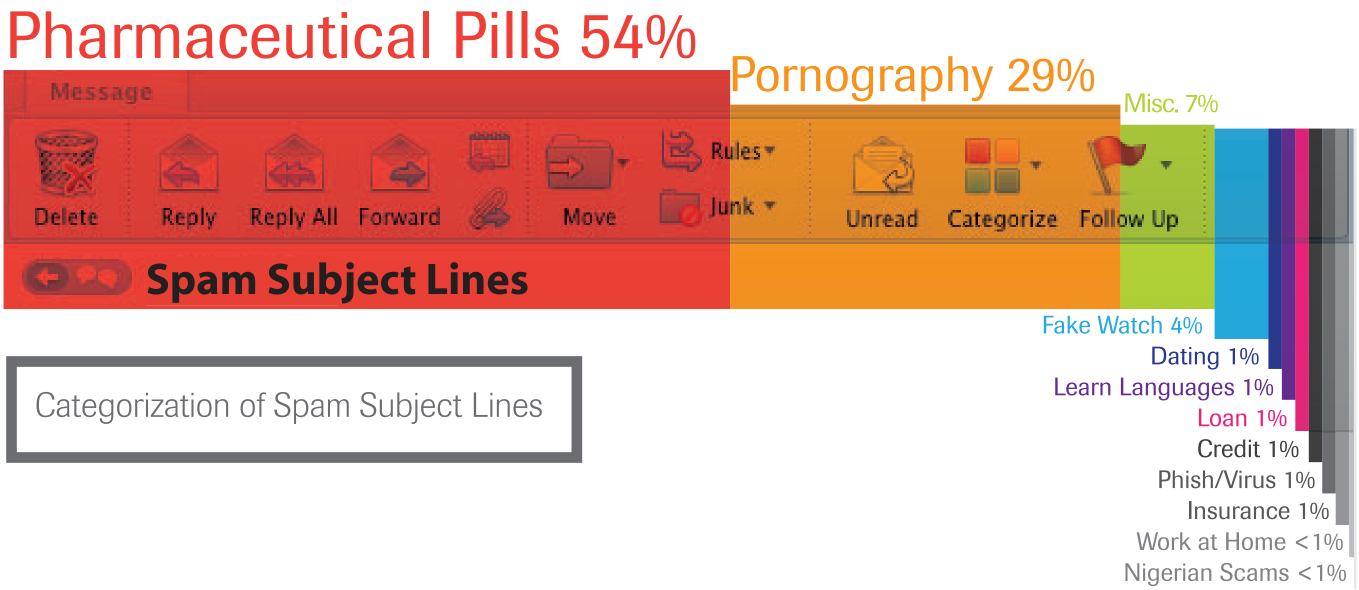
A review of the percentages of spam messages received for all of 2011 and comparing them to the three previous years.

[11] Data in this section is based on Trustwave mailMAX. mailMAX is a solution for spam filtering, email encryption and archiving. Between the years 2008 and 2011 the system processed and analyzed more than 16 billion emails for our clients.

[12] "Rustock botnet responsible for 40 percent of spam."
http://www.goodgearguide.com.au/article/358165/rustock_botnet_responsible_40_percent_spam/

Spam Subject Lines

The majority of all spam identified–83%–consists of two categories: pharmaceutical pills and pornography. The remaining categories cover a range of topics, such as imitation wristwatch spam (4%). While Nigerian advance-fee fraud scams are often talked about, they represented less than 1% of all spam processed in 2011.

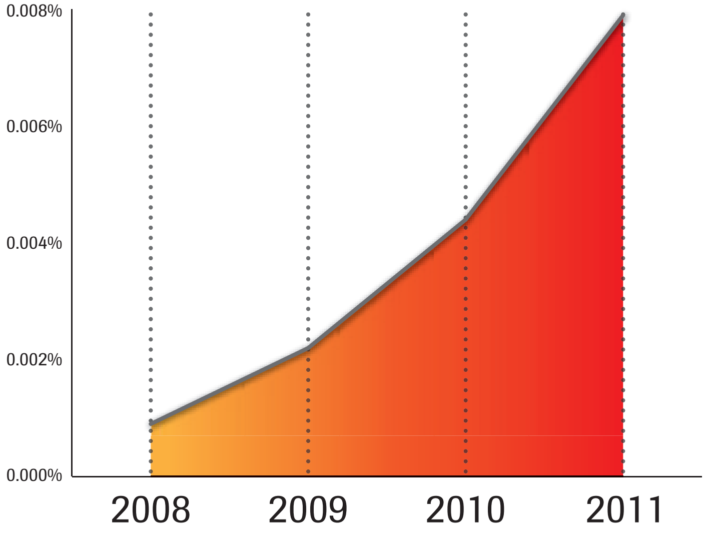


Categorization of Spam Subject Lines

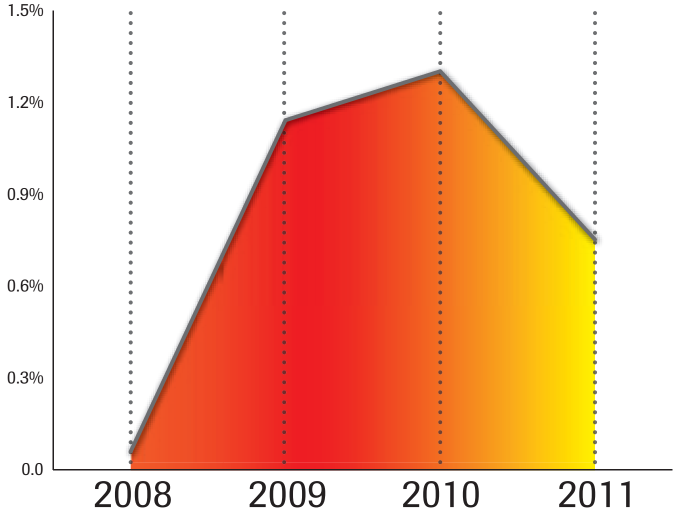
Dangerous Files

Interception of executable files via email has almost doubled every year since 2008. Blocking dangerous files such as executables sent through email helps restrict the spread of malicious worms and Trojans that may be attempting to spread to new hosts.

Known viruses detected in emails dropped to three quarters of a percentage point in 2011 after three years of steadily increasing. This decline further attests to the fact attackers are moving away from broad-based attacks and becoming more targeted in their approach.



Percentage of Executable Attachments



Percentage of Viruses Detected

Temporal Analysis

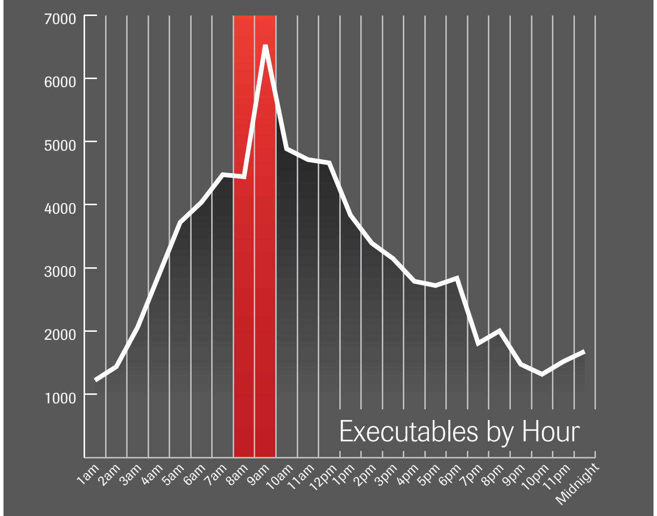
Analyzing the maximum peak spikes by time-of-day, month and year, some interesting conclusions based on the results can be drawn.

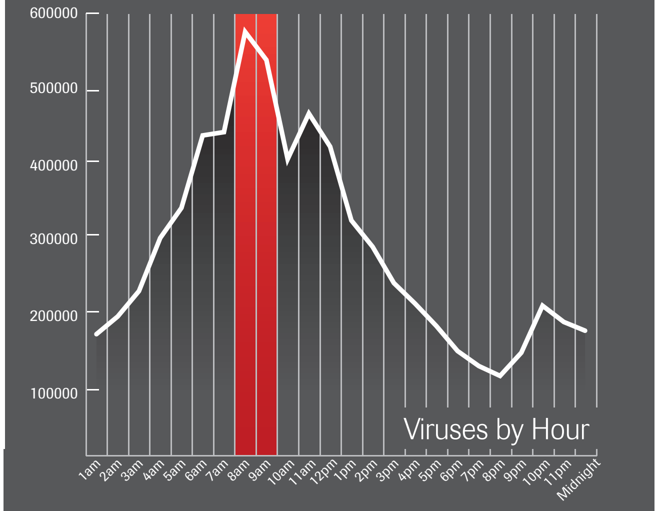
The number of executables and viruses sent in the early morning hours increased, eventually hitting a maximum between 8 a.m. and 9 a.m. Eastern Standard Time before tapering off throughout the rest of the day. The spike is likely an attempt to catch people as they check emails at the beginning of the day.

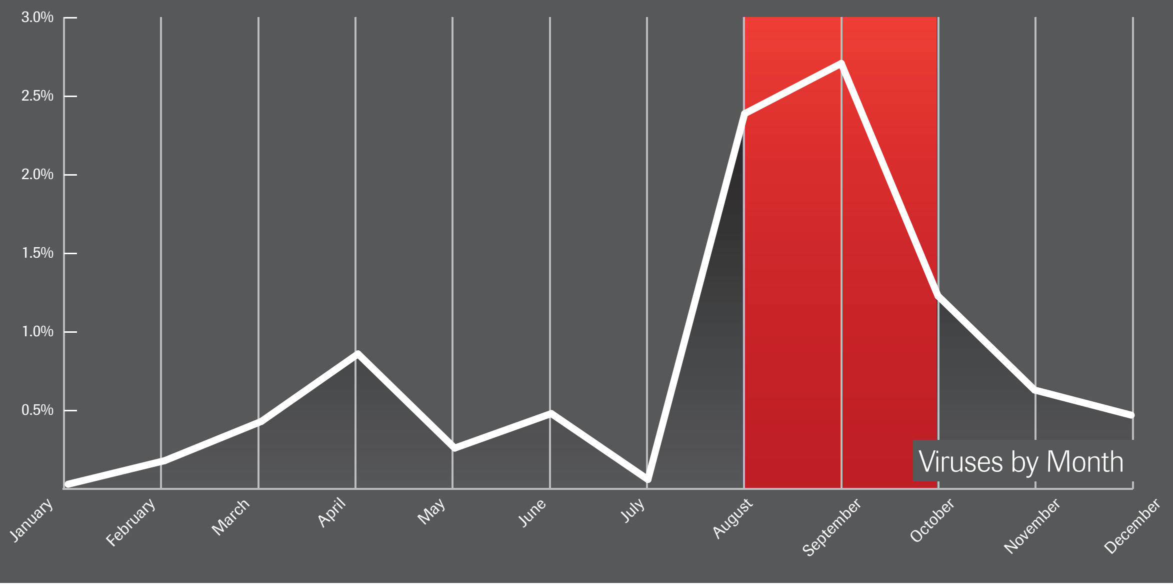
Executables and viruses accounted for almost 3% of all electronic mail in August and September 2011. Based on this data, an individual was most likely to be emailed a virus between 8am and 9am during the month of September 2011. The time from compromise to detection in most environments is about six months; therefore, if these methods were successful, March 2012 should be a busy month for incident responders and breach disclosures.

Email remains one of the most prevalent and pervasive targets for cyber attack today. According to a 2011 Pew Internet Survey[13], using email is tied at 92% with using search engines as the most popular activities performed by online adults. Since many attackers tend to be opportunistic, the popularity of email and its ability for dynamic action makes it a natural choice as an attack vector. Attackers go where the victims are, and more users on a particular platform translate into more potential victims for the attacker.

In a year of headlines constantly warning of new cyber threats it is important to remember the basics. A healthy amount of skepticism and adherence to security best practices, such as not opening unexpected attachments, will help prevent the initial vulnerability attackers look for. Awareness, education and communication should be the security mantra as attacks continue to evolve and test our defenses.







[13] "Search and email still top the list of most popular online activities."
http://www.pewinternet.org/Reports/2011/Search-and-email/Report.aspx

The Web – Multi-Vector Analysis of Modern Attack Techniques

What motivates attackers to hack Web applications? What methods are used? What vulnerabilities are exploited? Organizations are struggling to find answers to these critical questions. Numerous community security projects exist to track Web application vulnerabilities, such as CVE and Bugtraq, however, they only provide data for one dimension of the standard risk equation:

RISK = THREAT x VULNERABILITY x IMPACT

Real-world, Web application breaches, on the other hand, provide additional information, such as exploit likelihood, to enable research into actual cyber threat trends. This information helps to identify the types of organizations attacked, the motivation behind the attacks and the sources of the attacks. The Web Hacking Incident Database (WHID)[14] is a project dedicated to maintaining a list of publicly disclosed Web application-related security incidents. The WHID first serves as a tool for raising awareness of Web application security problems, and second, aids risk-rating methodology processes by providing statistics of real-world Web application security incidents. Unlike other resources covering website security, which focus on the technical aspect of the incident, the WHID focuses on the impact of the attack. To be included in the WHID, an incident must be publicly reported, be associated with Web application security vulnerabilities and have an identified outcome.

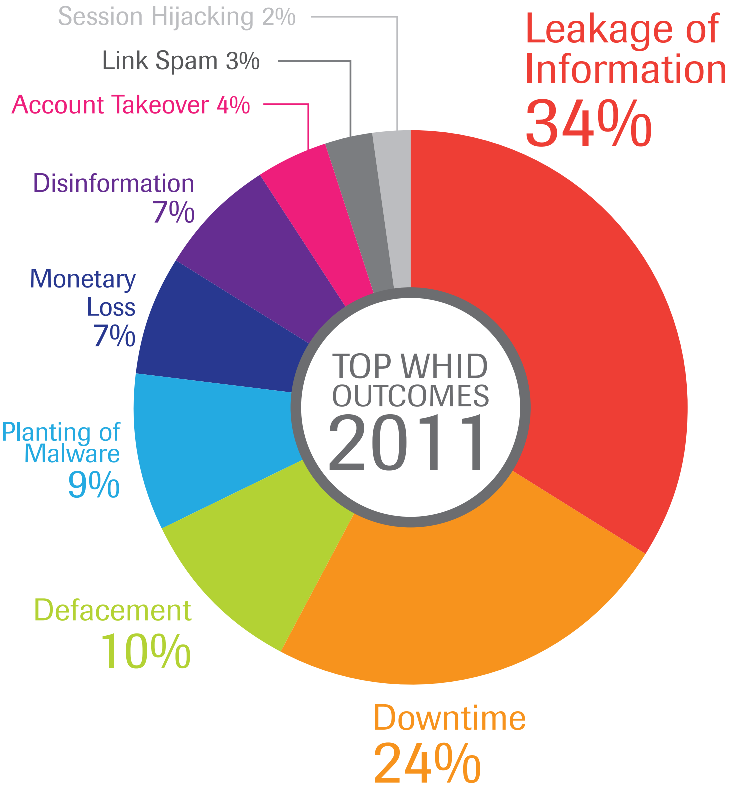
WHID Statistics for 2011

The criteria for the WHID are restrictive by definition, and the number of incidents that are included is not very large — approximately 300 incidents were included in the database for 2011. This is a sample of the overall Web application compromises that occurred but are not publicly disclosed and/or reported on by media outlets. Therefore, the analysis in this document is based on relative percentage rather than absolute numbers.[15]

There are two main motivations driving the bulk of Web application attacks that we see today: hacking for profit and ideological hacking.

Hacking for Profit

Professional criminals are increasingly developing new ways to generate revenue from compromising Web applications. The top outcome in 2011, leakage of information, is largely due to criminals extracting sensitive customer data from e-commerce websites. This data can then be sold on the black-market for identify theft and fraud purposes.



Monetary loss, occurring in 7% of incidents, is largely the result of criminals utilizing various methods of fraudulently transferring funds out of victim's online bank accounts. They leverage client-side banking Trojans (such as Zeus and SpyEye), which monitor a user's Web activity and, when a user interacts with online banking sites, it either steals their login credentials or alters the transfer to request data.

Planting of malware results in a related outcome: by adding malicious code to the attacked websites the attackers convert hacked websites into a primary method of using client-side attacks to further the propagation of malware, such as banking Trojans.

Ideological Hacking

Hacktivists are ideologists who use the Internet to convey their message. Their goals are most often: downtime (24%) and defacement (10%).

Similar to real-world civil disobedience demonstrations such as "Occupy Wall Street," online hacktivist groups aim to bring down websites in order to disrupt normal business operations. While any amount of downtime for a website is undesirable, there are often critical time windows where being offline can cause major damage. Sample scenarios of critical timeframes include: fund raising efforts and seasonal shopping, such as Cyber Monday.

[14] 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.

[15] The WHID should not be seen an exhaustive source of data to demonstrate real-world threats, but it does provide evidence that Web application attacks happen frequently.

Besides downtime, another hacktivist goal is website defacement. Web defacements are a serious problem and a critical barometer for estimating exploitable vulnerabilities in websites. Defacement statistics are valuable as they are one of the few incidents that are publicly facing and thus cannot easily be swept under the rug.

Traditionally, defacements are labeled as a low severity issue as the focus is on the impact or outcome of these attacks (the defacement) rather than the fact that the Web applications are vulnerable to this level of exploitation. What should not be overlooked, however, is that the threat and vulnerability components of the equation still exist. What happens if the defacers decided to not simply alter some homepage content and instead placed malicious content within the site? Web defacement attacks should not be underestimated.

The majority of Web defacements were of a political nature, targeting political parties, candidates and government departments, often with a very specific message related to a campaign.

Attack Method Analysis

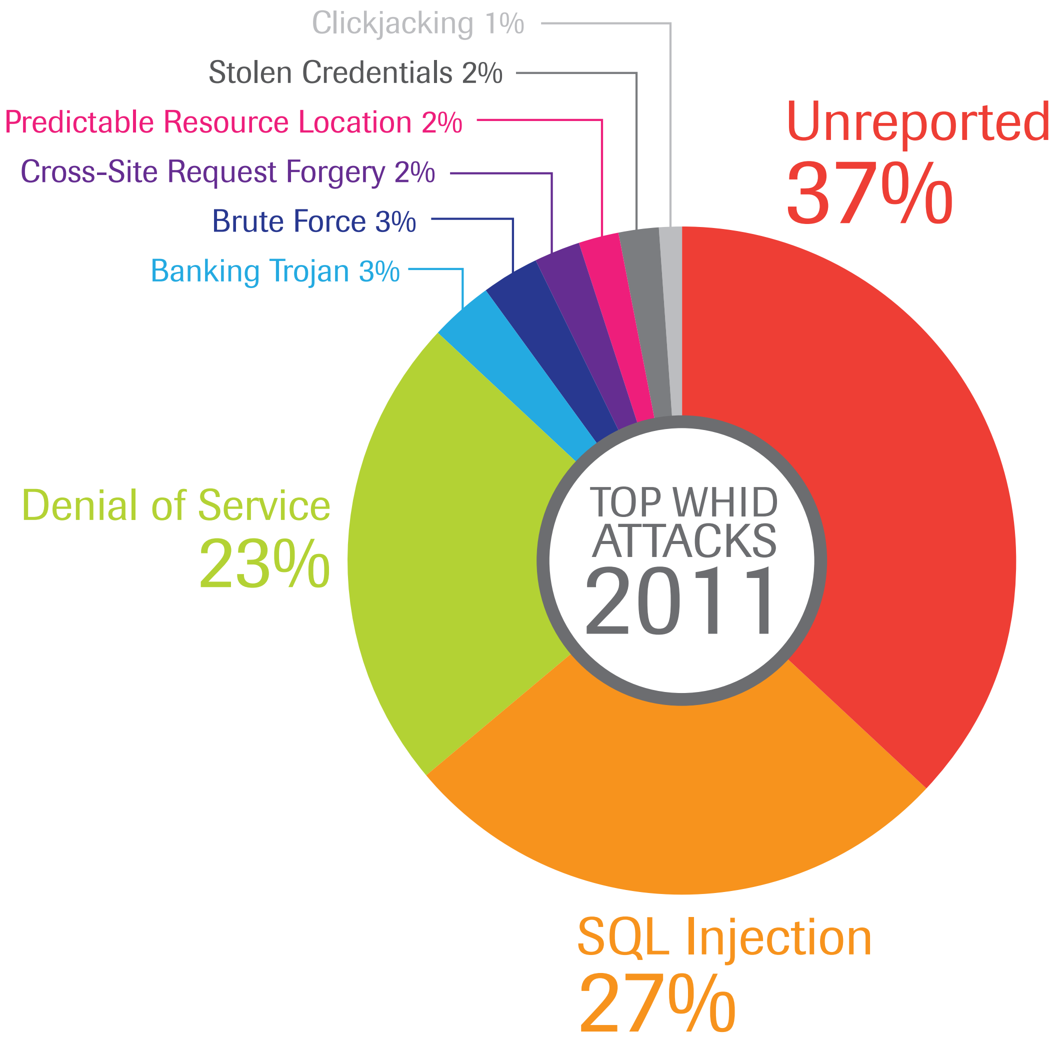
The top attack category is “unreported.” This means that 37% of the incidents reported did not specify a specific attack method, likely attributed to:

Insufficient Logging

Organizations may not have properly configured their Web application infrastructure in a way to provide adequate monitoring and logging mechanisms. If proper monitoring mechanisms are not in place, attacks and successful compromises may go by 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.

Public Disclosure Resistance

Most organizations are reluctant to publicly disclose the details of the compromise for fear of public perception and possible impact to customer confidence or competitive advantage.



Top Attack Method per Vertical

Government
Denial of Service 41%

Entertainment
SQL Injection 43%

Web 2.0
Cross-Site Request Forgery 14%

Finance
Banking Trojan 36%

Retail
SQL Injection 27%

Technology
SQL Injection 37%

Hosting Providers
Cross-Site Request Forgery 14%

Media
SQL Injection 17%

Education
SQL Injection 40%

Politics
Denial of Service 78%

In many cases this lack of disclosure, apart from skewing statistics, prevents the fixing of the root cause of the problem. This is most noticeable in malware-planting incidents, in which the focus of the remediation process is removing the malware from the site rather than fixing the vulnerabilities that enabled attackers to gain access in the first place.

For the other top known attack methods, they correspond to the outcomes covered previously. SQL injection is number one and it most often results in leakage of information outcomes. Denial of service, at number two for known attack methods, results in downtime for the target websites. Specifically, application-layer denial of service attacks is a huge concern for two main reasons:

Bypass Network Security

There are many methods for rendering a Web application inaccessible rather than network bandwidth saturation. Web applications are relatively fragile and attackers are able to send precise requests, which target Web application resources that require large processing power, and thus may more easily consume the site's available resources. These types of application layer attacks are not normally flagged by networking infrastructure security devices.

Often Excluded From Application Penetration Testing

Due to restricted rules of engagement, most organizations do not actively test application layer denial of service attacks when conducting penetration tests. This is the main reason why this attack type is not listed in the Top 10 Web Application Risks found on page 32.

Attack Method per Vertical Market Analysis

A few interesting conclusion can be drawn from attack methods by vertical. First, attack methods may be cross vertical — both SQL injection and denial of service attacks are vertical market agnostic. They may essentially be used against any website regardless of what type of market it is in.

However, some attacks are used more depending on the vertical market. For example, banking Trojan software is very specific and targeted at not only the banking industry but also to work against specific banking websites themselves. Additionally, cross-site request forgery (CSRF) attacks can theoretically be used on any Web application, although they are most commonly used by attackers on Web 2.0 social media websites such as Facebook and Twitter.

The takeaway for organizations is that this data should be correlated in a threat modeling process to ensure that proper prioritization is applied to these attack vectors.

Top 10 Web Application Risks

The vulnerabilities and attacks listed below are ranked by collective risk, based on the frequency of vulnerability findings, difficulty in launching the attack, exploit likelihood and the potential impact when exploited by criminals. For example, while SQL injection flaws are not the most common vulnerability encountered during application assessments, it is the number one attack vector found in both the Web Hacking Incident Database and the number one Web-based method of entry in incident response investigations. Combined with the potential impact of bulk extraction of sensitive data makes SQL injection the number one Web application risk of 2011. Conversely, CSRF is one of the most common application vulnerabilities found in application assessments, but requires a more complicated attack scheme, relegating it to eighth on the list.

1. SQL Injection

Risk Ranking Analysis:

SQL Injection is the number one risk for Web applications in all three of our data sources: internal application assessments, internal incident response/forensic investigations Web-based method of entry and the WHID attack method.

Application Weakness Reference:

CWE-89: Improper neutralization of special elements used in a SQL command
http://cwe.mitre.org/data/definitions/89.html

Attack Method Reference:

CAPEC-66: SQL injection
http://capec.mitre.org/data/definitions/66.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S329834ql6g

2. Logic Flaw

Risk Ranking Analysis:

Logic flaws are tricky as they are not easily integrated into automated dynamic application scanning tools (DAST) and are difficult to spot within standard Web application logging mechanisms. The results of these two issues are that most organizations cannot identify logic flaws and then are not able to spot if or when criminals exploit them. Only through manual application assessment can business logic flaws be identified.

Application Weakness Reference:

CWE-841: Improper enforcement of behavioral workflow
http://cwe.mitre.org/data/definitions/841.html

Attack Method Reference:

CAPEC-77: Manipulating user-controlled variables
http://capec.mitre.org/data/definitions/77.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S329845bfBR

3. Cross-Site Scripting (XSS)

Risk Ranking Analysis:

While XSS flaws are the prevalent finding within Web applications, the resulting risk level is lower than SQL injection as attackers are not leveraging them as much in profit-driven attack scenarios.

Application Weakness Reference:

CWE-79: Improper input neutralization during Web page generation
http://cwe.mitre.org/data/definitions/79.html

Attack Method Reference:

CAPEC-63: Simple Script Injection
http://capec.mitre.org/data/definitions/63.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S329845bfBR

4. Authorization Bypass

Risk Ranking Analysis:

Authorization bypass is the result of unenforced access control profiles (i.e., users should not be able to access other users' data). Authorization and access controls are often not consistently applied to all resources.

Application Weakness Reference:

CWE-862: Missing authorization
http://cwe.mitre.org/data/definitions/862.html

Attack Method Reference:

CAPEC-87: Forceful browsing
http://capec.mitre.org/data/definitions/87.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S3298656i9X

5. Session Handling Flaws

Risk Ranking Analysis:

Session handling flaws allow attackers to impersonate a valid and authenticated user. Attackers may manipulate Session IDs (credential prediction), trick end users into authenticating a Session ID (session fixation) or use XSS attacks to steal a Session ID (session hijacking).

Application Weakness Reference:

CWE-642: External control of critical state data
http://cwe.mitre.org/data/definitions/642.html

Attack Method Reference:

CAPEC-196: Session credential falsification through forging
http://capec.mitre.org/data/definitions/196.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S329956MqHr

6. Authentication Bypass

Risk Ranking Analysis:

To protect sensitive data or functions, applications rely on authentication controls as a first defense. Attackers can sometimes bypass these controls to access the application without credentials. This is a common vulnerability in Rich Internet Applications (RIA) and thick-client architectures. Web services are another culprit as they do not prevent attackers from directly accessing them and instead assume that authentication controls will be handled by the main user interface.

Application Weakness Reference:

CWE-306: Missing authentication for critical function

http://cwe.mitre.org/data/definitions/306.html

Attack Method Reference:

CAPEC-36: Using unpublished Web service APIs

http://capec.mitre.org/data/definitions/36.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S329897Ft92

7. Cross-Site Request Forgery (CSRF)

Risk Ranking Analysis:

CSRF allows a malicious website to force a legitimate user to execute commands on the targeted Web application, possible when the command is formatted in a predictable manner known by the attacker. Unless the Web application uses request validation tokens, it is most likely vulnerable to CSRF attacks.

Application Weakness Reference:

CWE-345: Insufficient verification of data authenticity

http://cwe.mitre.org/data/definitions/345.html

Attack Method Reference:

CAPEC-62: Cross-site request forgery

http://capec.mitre.org/data/definitions/62.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S329890UMOT

8. Source Code Disclosure

Risk Ranking Analysis:

Proprietary application source code can be disclosed through a number of methods, such as code left by developers in browsable directories or misconfiguration in the Web servers file handlers. Web application firewalls are often used to identify code leakages and can block pages from being served to the client.

Application Weakness Reference:

CWE-540: Information exposure through source code

http://cwe.mitre.org/data/definitions/540.html

Attack Method Reference:

CAPEC-116: Data excavation attacks

http://capec.mitre.org/data/definitions/116.html

9. Detailed Error Messages

Risk Ranking Analysis:

Verbose error messages can provide significant aid to an attacker. The error messages can provide configuration data, source code or other useful information for fine-tuning attack payloads. Error pages are also often used as the conduit for data exfiltration when using SQL Injection attacks.

Application Weakness Reference:

CWE-209: Information exposure through an error message

http://cwe.mitre.org/data/definitions/209.html

Attack Method Reference:

CAPEC-54: Probing an application through targeting its error reporting

http://capec.mitre.org/data/definitions/54.htm

10. Vulnerable Third-Party Software

Risk Ranking Analysis:

An application can only be as secure as the infrastructure it runs on (i.e., application frameworks or servers). PHP applications have a number of Remote File Inclusion (RFI) issues where an attacker can trick the Web application into downloading code from a third party site and executing it. The main goals of these attacks are either botnet recruitment or installing a Trojan/backdoor interface for executing commands on the server.

Application Weakness Reference:

CWE-830: Inclusion of Web functionality from an untrusted source

http://cwe.mitre.org/data/definitions/830.html

Attack Method Reference:

CAPEC-175: Code inclusion

http://capec.mitre.org/data/definitions/175.html

WHID Incidents:

http://www.google.com/fusiontables/DataSource?snapid=S331015Y6ZO

Blind Faith in Mobile

A mobile device such as a smartphone or tablet computer is often mistaken for a miniature PC. Unfortunately this confusion has led to many implementation mistakes and trust assumptions over the past few years by organizations of all sizes and industries.

Most, if not all, mobile devices are consumer-grade technology. Consumer-grade mobile devices are designed to 1) attract the widest spectrum of users, 2) be simple to use, and 3) drive sales of media, games and other content. Until recently, mobile device security has been slow to develop. Attack trends are starting to appear, though, and taking a proactive approach today can help mitigate risk tomorrow.

In the past year, existing PC-based malware proliferated in the mobile space. Mobile devices can provide malware with information such as location tracking and access to photos, video, and even audio. The Android platform is a major focus for malware developers due to the availability of third-party market places for applications and the ease of gaining root access.

Mobile Integration of Banking Trojans

2011 saw an increase in mobile versions of the largely PC-based banking Trojan malware market. The release of Zeus source code, and its eventual merge with SpyEye malware, included Android and iPhone components used to capture Mobile Transaction Authentication Numbers (mTAN) and mobile one-time passwords. By capturing mTANs, bot authors are able to access the banking information of those infected with SpyEye.
With mobile payment systems gaining traction, including virtual wallets and near-field communication payment mechanisms built into phone hardware, malware targeting financial and payment card data continues to be a pressing concern. By abusing the mTAN authentication process, malware authors are demonstrating their ability to keep up with security mechanisms meant to secure transactions.

In 2011, the propagation of mobile banking malware has mainly been limited to social engineering rather than forced downloads or worm-type replication. With the strong trend toward developing malware for Android (discussed below), it seems only a matter of time before a systemic vulnerability leads to greater infection rates through direct attacks and replication.

Location-Aware Malware

Carriers aren't the only ones tracking the location of mobile devices. Malware targeted at mobile platforms often collects GPS and other location information, reporting back with other stolen data. While it isn't clear why attackers are collecting location information, it is not difficult to imagine the ways to generate value from it. For instance, stolen payment card information used in a region local to the legitimate user is less likely to activate fraud detection.

In the past several months both iOS and Android have come under scrutiny for excessive and persistent collection of location data. Additionally, several carriers have been criticized for not disclosing the nature of the built-in diagnostic utilities on their devices. Malware authors are certain to find ways to monetize such a rich data source.

Android Focus for New Malware

The trend toward Android as the target platform of choice for malware authors should come as no surprise. Android dominates the worldwide smartphone market, powering 56% of devices.[16] Android's ability to install applications from third-party stores provides a direct route to consumers for malware authors. Foreign marketplaces and those catering to pirated applications are breeding grounds for counterfeit applications or legitimate applications modified to include malware.

While Apple has had some short-term success at stymieing attempts to jailbreak their current iOS 5, strong desire from the user base to install non-approved applications eventually resulted in a jailbreak in that platform. One can now expect to see an increase in the release of new iOS malware. Although a highly visible segment of the market, iOS still represents a minority of the market with only 18% of devices. Much like Apple has experienced in the world of traditional, computer-targeting malware, their somewhat limited market share may assist in reducing the platform's attractiveness as a target.

Mobile security faces challenges on several fronts. As mobile device adoption increases, malware developers will think up new ways to penetrate this insecure market. At the same time, traditional malware is being updated to include mobile components, furthering its reach. Increasing amounts of sensitive data are stored on our mobile devices, in turn increasing the relative value of each device to an attacker. Evolving mobile platforms must not only fight with each other for market share, but must compete on features, including security and transparency. With such a young yet ubiquitous technology, it is hard to pinpoint exactly where the next security concern will arise, but it is fair to say that 2012 will bring its own share of interesting threat developments in this space.

[16] "Android market share reaches 56 percent; RIM's, Microsoft's cut in half."
http://www.dailytech.com/Android+Market+Share+Reaches+56+Percent+RIMs+Microsofts+Cut+in+Half/article22852.htm

Our Defenses: Four Basic Controls

A perfect system does not exist. Under enough scrutiny, everything has its flaws. Through identification and analysis of those flaws and sharing this analysis with industry, marked improvements in security postures can be made.

In this section, four different types of defenses are reviewed by looking at the weakness that exists within the implementation of some of the most common security controls: business passwords, data transmission encryption, anti-virus and the firewall.

No organization can do without these four basic controls. Unfortunately, when controls are not implemented correctly or flawed from the start, there is a false sense of security imparted upon the adopting organization, impacting both the security posture and the operating budget.

Business Password Analysis

Passwords continue to be a pertinent topic of discussion and study within both the security community and the world of technology at large. However, few studies have had the advantage of large amounts of real-world data. In this section, passwords from Trustwave's client businesses are analyzed.

Password Risks Unrelated to Password Choices

The strongest password choice may not matter if the underlying system is weak, whether due to a cryptographic weakness, exploit or external factors. Even with solid technological foundations, a variety of human fallibilities can undermine the security of the system as a whole.

Even users proactive in ensuring account safety can experience a system compromise by attack vectors unrelated to their password selection. An ever-present example is the MS08-067 SMB vulnerability for Microsoft Windows 2000, XP/Server 2003, and Vista/Server 2008.[17] This four-year-old vulnerability is trivial to exploit and enables an attacker to compromise a system in seconds without requiring a single user password.

Patched systems can also become compromised as a result of third-party services installed on a user's system. This ranges from unpatched services such as an Apache Web Server that enables an attacker to exploit a buffer overflow, or more commonly, remote access tools that bypass a user's login credentials or that only require a secondary password, such as free editions of VNC. Installed by an end-user to enable remote access, VNC utilizes secondary passwords that bypass a user's system login, even if a secondary password is set. By default, VNC does not encrypt communications between the client and server making a user's machine susceptible to man-in-the-middle attacks that can capture a VNC password, if one is even set.

Networks susceptible to man–in-the-middle attacks leave a user's account vulnerable to compromise regardless of the user's password complexity. An attacker that captures a user's LM or NTLMv1 hash as they're authenticating against an Active Directory Service can simply pass the hash without even having to worry about cracking the password. NTLMv2 is not susceptible to passing the hash and requires offline cracking where the strength of a user's password would be tested.

Weaknesses in Cryptographic Methods

Another factor that can contribute to an account compromise is the cryptographic algorithm used to encrypt a password. If a weakness exists in the algorithm, an attacker will take advantage of that weakness rather than resorting to attacks on the password.

An example is the use of LAN Manager (LM) hashes to store Microsoft Windows passwords. LM hashing is considered to be a legacy algorithm but is still in use in many environments today. It was used as the primary hashing algorithm for pre-Windows NT systems, and was carried over and enabled by default in later versions of Windows in order to maintain legacy support. LM hashes can be cracked with rainbow tables in a matter of minutes because of the way the hash is designed. When an LM hash is created the user's plain-text password is converted to all upper case characters followed by null-padding the password up to 14-bytes. This "fixed-length" password is two 7-byte DES encrypted hashes. Instead of needing to crack the entire password, an attacker can crack each half individually then merge the two results together.

Microsoft finally disabled LM hashing by default starting with Windows Vista and Server 2008, but it is still commonly seen in Windows XP/2003 implementations. An LM hash has a 14-character limitation. If a user's password is over 14 characters, Windows will not hash the password with LM and only hash using NTLM, thereby mitigating the issue. Other examples where attacking the cryptographic weakness is better than attacking the actual password itself is for WEP enabled wireless networks.

Old-Fashioned Methods

Writing down passwords is still prevalent within the workplace, especially in organizations that implement complexity requirements, frequent password expiration and password histories to prevent password recycling. The effect of increasing password complexity policies is often reduced memorability, a key requirement for a password. In approximately 15% of physical security tests performed at client sites in 2011, written passwords were found on and around user workstations.

A tried and true method of attacks is the installation of a keystroke logger. To successfully install a keystroke logger, an attacker needs a user to leave their machine for only a matter of seconds. Keystroke loggers can also be installed remotely if a user's machine is vulnerable to remotely executable exploits.

[17] "Microsoft Security Bulletin MS08-067 – Critical. Vulnerability in Server Service Could Allow Remote Code Execution (958644)." http://technet.microsoft.com/en-us/security/bulletin/ms08-067

Social engineering is increasingly being used by attackers to obtain user account information. In this method, attackers take advantage of the trusting nature of people in an attempt to convince them to divulge sensitive information. Phishing attacks focused on social networking websites are now commonplace, and pose a danger to the corporate environment because of the associated risk of users using similar passwords for everything ranging from Twitter and Facebook to their Active Directory account at work. Social engineering attacks can also involve an attacker interacting with the user whose account they are attempting to steal. Whether the attacker poses as the new IT administrator or uses bribery, extortion or intimidation, this non-technical attack vector has proven to be useful for attackers.

Password Pitfalls

In response to strong password policies, users are finding creative ways to override these policies. Common examples include:

- Setting usernames as the password in cases where complexity requirements aren't enforced
- Adding simple variations to fit usernames within complexity requirements, such as capitalizing the first letter and adding an exclamation point to the end
- Using dictionary words verbatim or applying simple modifications to adhere to complexity requirements

Companies are also assigning poor default passwords for new employees with examples such as "changeme" and "Welcome." At times, users are not required to change such default passwords upon login.

Service accounts, especially ones that are automatically generated (e.g., accounts used between applications and back-end databases), were discovered to also include poor default passwords, and IT administrators forgot to change them. A frequently occurring example was Microsoft SQL Server's common system administrator (sa) username and password combination. Domain administrators in Active Directory environments can also ignore password policies if setting a user's password through Active Directory Users and Computers.

Shared Passwords

Shared passwords can cripple an IT environment if compromised. Shared passwords among services and machines are a common tradeoff for manageability over security. Shared local administrator passwords make administration of large numbers of machines by IT staff possible, but do pose an inherent but generally accepted risk. Another example includes accounts that are utilized by common services across multiple machines that typically require administrative access. A prevalent example would be accounts used to initiate backup software on machines within an environment. Accounts for the Backupexec suite are commonly discovered in Active Directory environments to have domain admin privileges. Accounts that are used for automatically logging into a machine typically utilize a shared password, specifically on POS machines in retail locations.

Shared accounts leave an environment open to a complete compromise if just one machine is compromised. It also enables an attacker to focus on a couple of machines with exploitable vulnerabilities; with this access, the attacker can obtain and crack passwords for shared accounts. Readily available tools such as Medusa quickly allow an attacker to determine whether the account they've just obtained is in fact used elsewhere on other machines.

Poor Password Selection

Users are not creative when it comes to passwords, and creativity was found to decrease with each successive password in our study. User passwords featured local sports teams or activities near their location. Users also created passwords based off their company, whether a variation of the company's name or products in their password.

Passwords were also correlated to the time period in which the password was set. Users established a base password and modified it with the time period in which they needed to reset their password, whether as a specific month, year or season. With this kind of predictability, an attacker need only crack a historical password then make intelligent guesses on what the user's current password might be.

Incremental passwords were also a common practice. Users set a base password then simply added one number to the end, incrementing it from there when time came to change their password, leaving the password open to attack by predictability.

IT administrators should be aware of what passes as a complex password, especially in Active Directory environments. Users can create passwords that meet complexity requirements because they contain the minimum amount of characters and include a couple of character variations. The Active Directory password complexity policy states that a password is required to have a minimum of eight characters and three of the five character types (Lower Case/Upper Case/Numbers/Special/Unicode.) With that, "Password1" completely adheres to these policies, as does "Password2" and "Password3." Users are creating passwords that meet the bare minimum requirements for length and character types, to aid with the memorability of the password.

Password Complexity versus Length

Users and IT administrators often believe that simply adding complexity to a password will make it inherently more secure. While this might be the case when it comes to someone guessing individual passwords, it's not the case when it comes to utilizing password-cracking tools. Character substitution or "L33tsp33k" is often used in passwords to (in theory) increase the difficulty of cracking a password.

Some character substitution examples are:

Original Character	Replacement Character
A	@ or 4
E	3
I	!
S	5

Character substitution defends against a dictionary attack; if there isn't an exact match for that password in the dictionary list, it is missed. However, when a password-cracking tool is utilized in a brute force attack, the tool is already using all possible character combinations and is not going to increase the difficulty or time required to crack the password. However, simply increasing the number of characters has a dramatic effect on the difficulty of cracking a password. Every character added to a password increases the possible combinations exponentially for a password, making brute force attacks on longer passwords impractical.

Below are examples of the total possible combinations for a password at a given length, utilizing a brute force attack. These figures assume a standard 95 character U.S.-English keyboard.

Password Length	Password Possibilities
10	5.98737x10^{19}
9	6.30249x10^{17}
8	6.6342x10^{15}
7	69,833,729,609,375
6	735,091,890,625
5	7,737,809,375
4	81,450,625
3	857,375
2	9025
1	95

Total Number of IPv4 Addresses for Size Reference: 4,228,250,625
Total Number of IPv6 Addresses for Size Reference: 3.40282x10^{38}

Trustwave Password Study Methodology

Trustwave obtained the source for passwords from Trustwave SpiderLabs investigations, most often from Windows Active Directory servers, and a system to recover ("crack") them.

Windows Active Directory was chosen as a password repository for several reasons. First, it was the largest source of password examples; nearly every organization has an Active Directory domain for user account storage. Second, unlike Internet forum passwords, Active Directory accounts are generally subject to higher scrutiny and more restrictions in regard to complexity. This makes them better examples of "honest" password choices by users. Third, Windows passwords are recoverable by a wide variety of tools, such as John the Ripper, Cain and others. Finally, the continued use of weak Windows LAN Manager for storage of password hashes makes recovery an easy task.

Password cracking was performed on a custom system built using off-the-shelf parts totaling less than $1,500. The system was built with an EVGA Motherboard, a quad core AMD processor, 16 gigabytes of RAM, and utilized three NVIDIA 460GTX graphics cards (GPUs) as the primary medium for the password cracking process.

A number of password cracking methods were utilized:

1. The password cracking process began with an attack against all LM hashes. Using Cryptohaze Multiforcer[18], a free publicly available brute forcing tool, Trustwave launched a brute force attack to recover the plaintext passwords for all LM hashes containing standard ASCII characters.

2. Using the recovered plaintext passwords from the Cryptohaze Multiforcer attack as a wordlist, Trustwave then used John the Ripper, another free publicly available tool, coupled with a set of word mangling rules against all NT hashes.

These attacks took roughly 10 hours and recovered more than 200,000 of the 2,521,248 passwords analyzed.

3. Using a third free and publicly available tool called oclHashcat-plus from the Hashcat suite[19] Trustwave used publicly available wordlists coupled with the Kore-Logic[20] word mangling rules set in an attempt to recover the remaining unrecovered NT hashes.

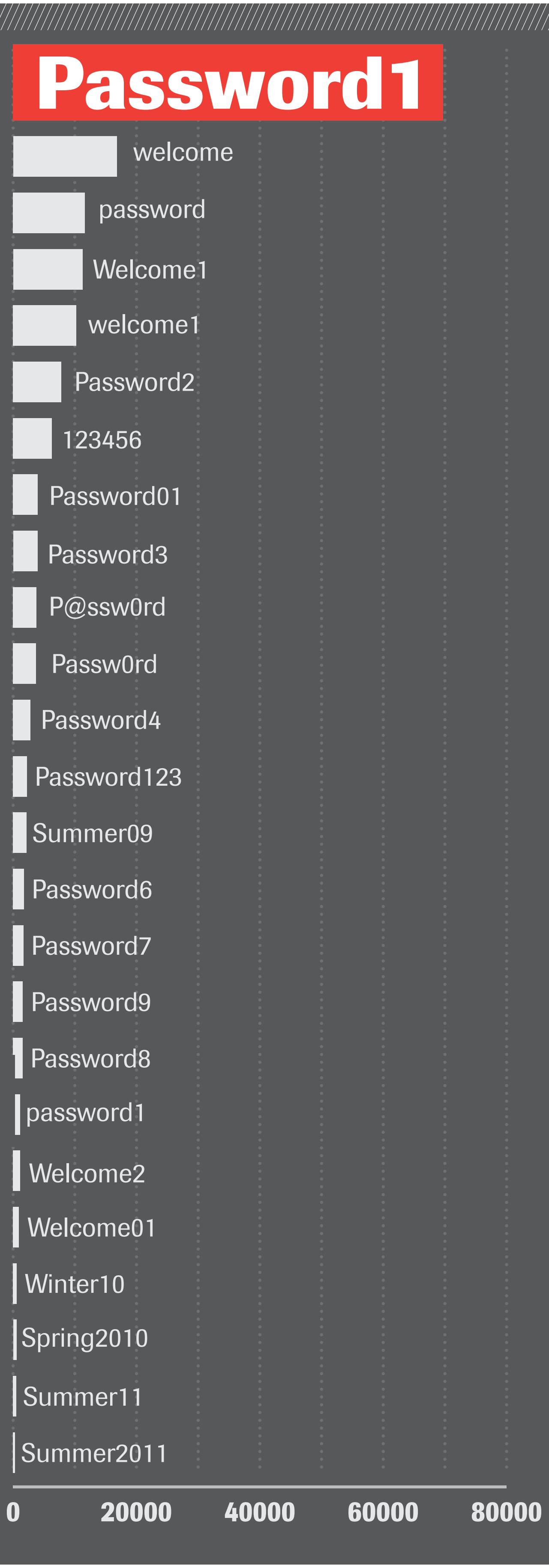
4. A fourth attack, known as a masking attack, was coupled with oclHashcat and the same publicly available wordlists to recover additional passwords for a total of 2,521,248 passwords analyzed.

To ensure client confidentiality, Trustwave filtered and anonymized all passwords by removing identifying data (such as usernames and domains) as well as randomizing password hashes before recovery.

Top 25 Passwords

This list was created through accumulated data combined with limited filtering (i.e., statistical bias, industry-specific passwords, etc.).

Variations of "password" made up about 5% of passwords and 1.3% used "welcome" in some form.



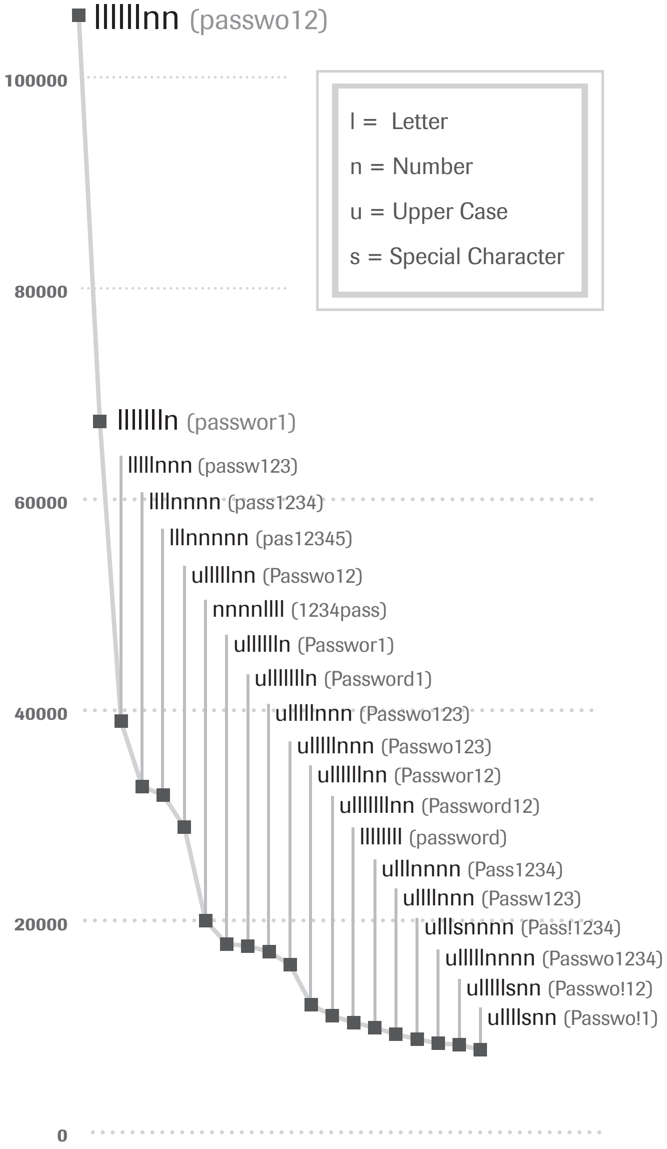
[18] Cryptohaze Multiforcer. http://www.cryptohaze.com/multiforcer.php

[19] Hashcat. http://hashcat.net/oclhashcat-plus/

[20] "Crack Me If You Can" – DEFCON 2010. http://contest-2010.korelogic.com/rules.html

Top 20 Sequences

Password complexity can be affected by character sequencing. In the following examples, the top user choices of the sequence of letter (l), number (n), and special character (s) can be seen.

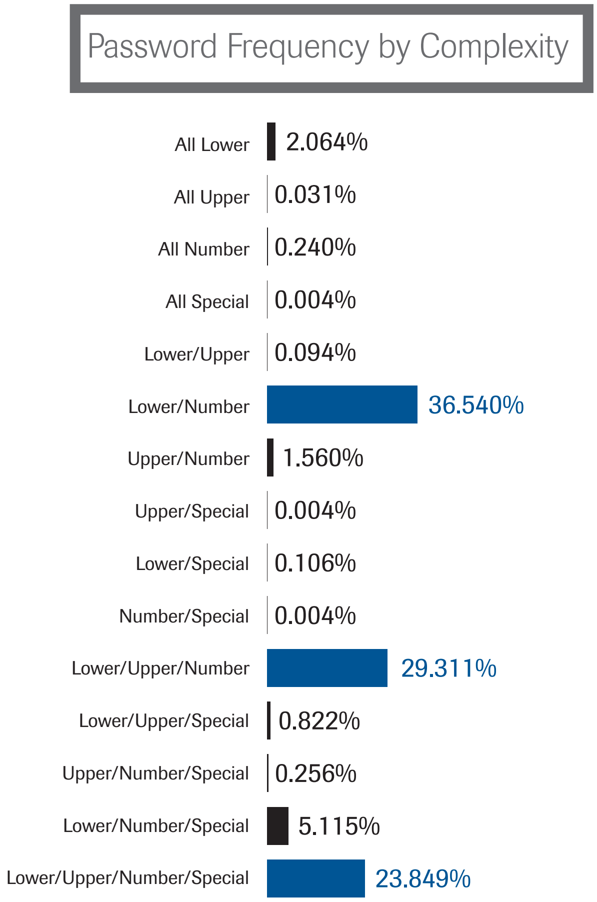


The most common sequence for passwords appears to utilize six letters and two numbers, followed closely by seven letters and one number. This is a typical result for many Active Directory installations as it correlates with easy to type and remember user choices. However, this also results in easy to guess user choices: nearly all the combinations of these two sequences could be guessed by basic rule set changes in password recovery tools.

Of additional note is that passwords containing special characters do not appear until the 16th most popular choice. This would indicate that users appear to avoid special characters, and not subscribe to using them as substitutions for popular letters ("L33tSp33k").

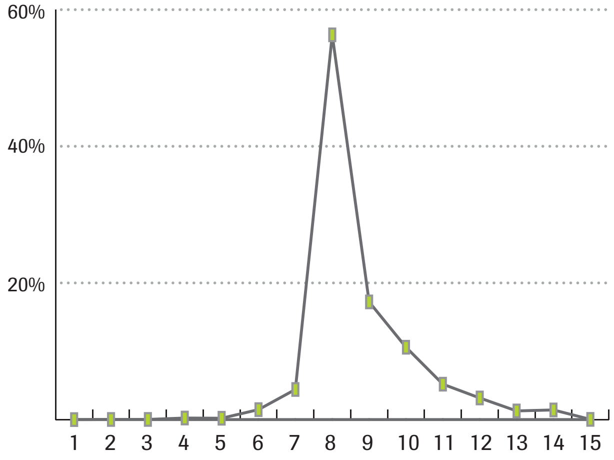
Password Complexity

In this category, user choices are broken down by use of one or more of each type of character in passwords. As before, users appear to lean towards letters and numbers, most specifically lower case.



Password Length

In this category, the overall length of analyzed user passwords can be seen:



The most common password length appears to be eight characters. The most likely reason for this is that eight characters tend to be the accepted length for many Active Directory installations.

Keyword Usage

The following statistics showcase some common user keywords:

Months	27,191 passwords used English spelling of months (January – December)
U.S. States	72,389 passwords used U.S. States (Illinois, California)
Seasons	74,368 passwords used seasons (spring, fall)
Baby Names	170,013 passwords used names in the "top 100 male and female baby names of 2011" list.

These categories were sometimes expanded to local sports teams, city nicknames or any information pertinent to the organization's location.

Implications

When ground rules are set for security, users will often conform to the lowest level of complexity that satisfies the requirements. For example, the default "use complexity" setting in Windows Active Directory requires:

- The password is at least six characters long.
- The password contains characters from at least three of the following five categories:
  - English uppercase characters (A - Z)
  - English lowercase characters (a - z)
  - Base 10 digits (0 - 9)
  - Non-alphanumeric (For example: !, $, #, or %)
  - Unicode characters
- The password does not contain three or more characters from the user's account name.

As a result, "Password1," while a terrible password choice, meets the same complexity requirements that "X$nc*(24" does. Most users opt for the easier to remember password, and as such they conform to the least required options that satisfy the requirements.

Also of note is that within the default set of Windows AD rules, there is no protection from similar password choices between password histories. So while passwords cannot be the same for incremental passwords (depending on the policy for the domain), there is no native rule to prevent users from numerically incrementing passwords. Thus, "Password2" could follow "Password1," and so on.

Recommendations

The solution to password security starts with eliminating weaker, older and insecure technologies. In the case of Windows AD, the use of LAN Manager for password storage simply needs to go. NT Hash-based storage, while not without issues of its own, at least allows for a larger key space (128 characters, Unicode) than LAN Manager. On top of this, assistive cryptographic techniques to slow down dictionary attacks would be a welcome addition. Many of these items are already available in Unix-based systems but require third-party additions to work with Windows products.

No solution is complete without some component of user education and awareness. Users need to be instructed and encouraged to avoid policy overrides – especially in the case of those users with an administrative capacity. Whether it's setting an artificially weak password for a domain service, or eliminating user password incrementing, these changes will enhance the baseline robustness of user password choices.

What should users consider in their password choices? For one, it's time to stop thinking of passwords as words, and more as phrases.

"ThisIsMyPasswordNoReallyItIs" is, all things considered, a far harder to guess passphrase than the previously mentioned "X$nc*(24". Given that many rainbow tables have reached eight to nine or more characters for recovering NT passwords, length is one of the few effective constraints left. Standing in the way of this, of course, is the ease of remembering the password. A passphrase allows for the benefit of length and memory without overt complexity.

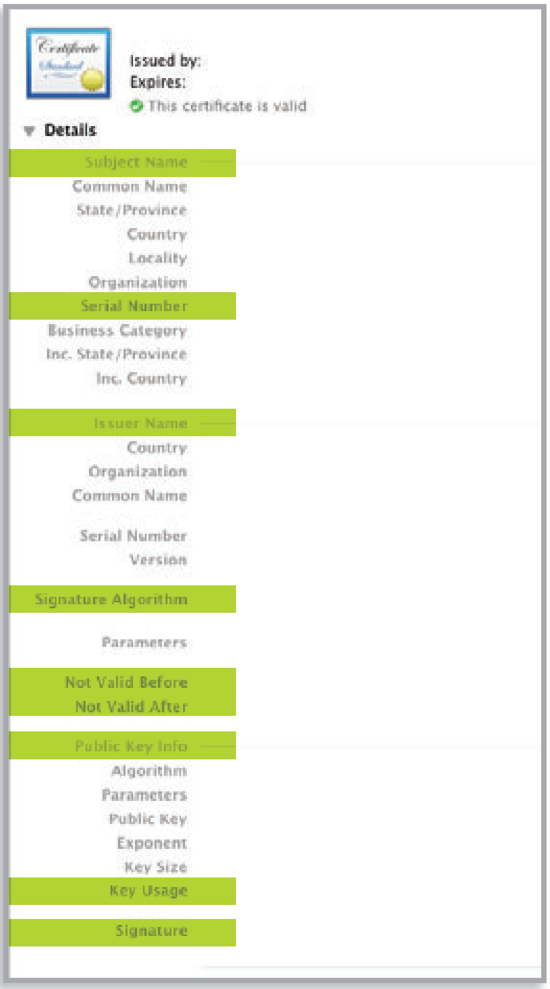
A combination of a properly designed password storage method and a properly designed methodology/policy for user password choice goes a long way. If either of these is weakened, the entire system is weakened; therefore some organizations may opt to explore alternatives to passwords where possible in their environment. Many areas of an organization can use two-factor authentication to eliminate the reliance on user choice in the security equation for particular authentication schemes.

A Study of SSL

The story of Secure Sockets Layer (SSL) is intertwined in the origins of e-commerce. Originally released by Netscape in 1995 in an effort to assure customers of the safety of Internet transactions, it has been adopted and extended considerably over the years. The first public release, version 2.0, contained a number of security flaws that were later addressed as part of a redesign, which resulted in version 3.0. This version is the basis for the SSL implementation we use today.

SSL Certificate

Subject	The fully qualified domain name of the server
Serial number	A unique identifier used to identify the certificate
Issuer	The Certificate Authority that created the certificate
Signature algorithm	Specification of the algorithm used, SSL certificates almost exclusively use SHA-1 / RSA
Validity	Start and end date during which the certificate is valid
Public key	The actual key
Purposes	Specifies what the certificate may be used for
Signature	A cryptographic hash of the key



Issued by:
Expires:
This certificate is valid

Details

Subject Name
Common Name
State/Province
Country
Locality
Organization
Serial Number
Business Category
Inc. State/Province
Inc. Country

Issuer Name
Country
Organization
Common Name

Serial Number
Version

Signature Algorithm

Parameters

Not Valid Before
Not Valid After

Public Key Info
Algorithm
Parameters
Public Key
Exponent
Key Size
Key Usage

Signature

From a security perspective, the makeup of SSL certificates found on active Internet systems provides an interesting view into ecommerce security. In order to gather a large sample set to pull data from, Trustwave's SSL team scanned more than 17 million internet-facing systems for SSL certificates and processed the results. This process yielded 289,926 unique certificates, which were categorized according to a number of attributes.

Bit Strength

The strength of a key is generally associated with its bit strength, referring to how long the key is, considering that each additional bit increases the amount of possible values that an attacker would need to test. This type of attack is referred to as brute force, where an attacker tries every possible permutation of values until the key is found.

Most modern cryptography relies on computational security, a methodology that increases bit strength as computational power increases in order to stay ahead of the attacker's capabilities. Security researchers and even possibly criminals have had recent success factoring 512-bit RSA keys, due to the computational power available via cloud services. In turn, this has caused Certificate Authorities (CAs) to refrain from offering this type of certificate, again raising the bar as part of the ongoing battle between attackers and defenders.[21] Cloud services will likely accelerate this process due to the large-scale, cost-effective amount of processing that the model offers.

Certificate Authorities (CAs) are trusted organizations that issue certificates used in the secure identification and encryption of network transactions. Trustwave is a Certificate Authority and a top 10 global issuer of SSL certificates.

[21] "RSA-512 certificates abused in the wild."
http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/

Total Certificates by Bit Strength

A number of valid 512-bit certificates still exist on active Internet systems, although adoption of 1024 and 2048-bit keys has been predominant. As there have been no published instances of a 1024-bit key being factored (the term used for discovering the key when discussing asymmetric algorithms such as RSA), it is encouraging that this strength of key is being used in 41% of certificates. 2048-bit certificates also offer good security and are a strong choice for the near future.

Expired and Self-Signed Certificates

Every SSL certificate contains a field that denotes its validity period. These fields often read as "not before" and "not after," and allow a client to ensure that the certificate is in good standing. The use of a certificate after its valid period expires suggests that the organization is not in good standing with the Certificate Authority, and should be taken as an indication that the session is not secure.

Certificates that are not issued by a trusted CA are known as "self-signed" and represent another security concern in regard to SSL. Self-signed certificates are only vouched for by the entity itself, with no third-party validation whatsoever. There are valid use cases for these certificates in specific situations, such as internal resources in cases where clients' Trusted Root is pre-populated with the organization's self-signed certificates, but they should not be relied on in general.

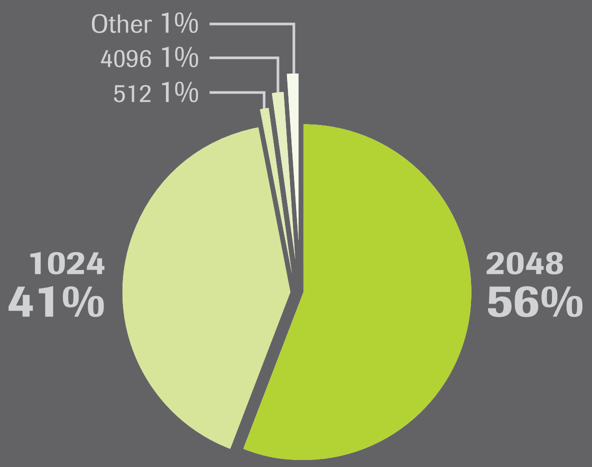
Hosts using Expired, Self-Signed and Valid Certificates

Self-signed certificates expired without renewal in 20% of cases. Many of these invalid certificates came from instances of Web hosting control panels, such as CPanel and Plesk. Several Hewlett-Packard printers were discovered as well, hosting expired and self-signed certificates. These platforms simply do not receive the same level of attention or scrutiny that e-commerce servers do, and often get overlooked in terms of SSL certificate security. Self-signed certificates offer the client no assurances to the validity of the server to which they are communicating. In addition, organizations relying on self-signed certificates cannot revoke those certificates as they are not listed on the two primary mechanisms that exist to perform revocation: Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP).

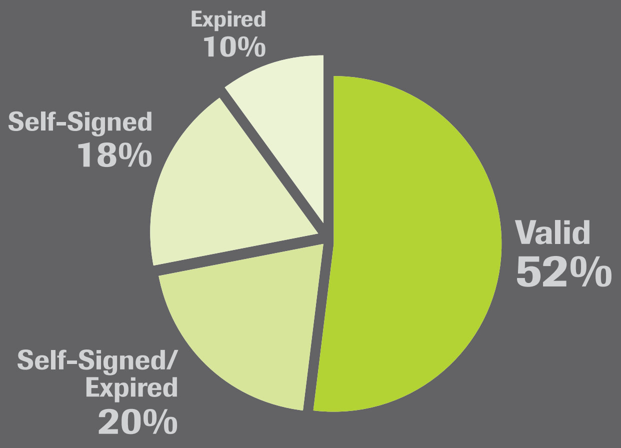
Self-Signed Certificates by Bit Strength

Self-signed certificates trend more towards 1024-bit encryption than their CA-issued counterparts. The relatively small number of 512-bit certificates found here is encouraging.

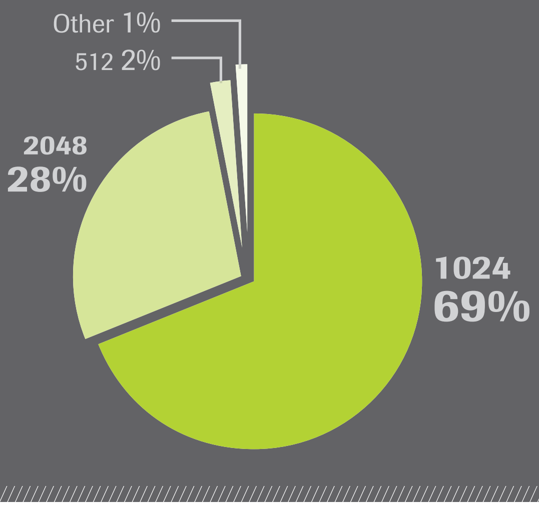
Total Certificates by Bit Strength



Expired, Self-Signed and Valid Certificates

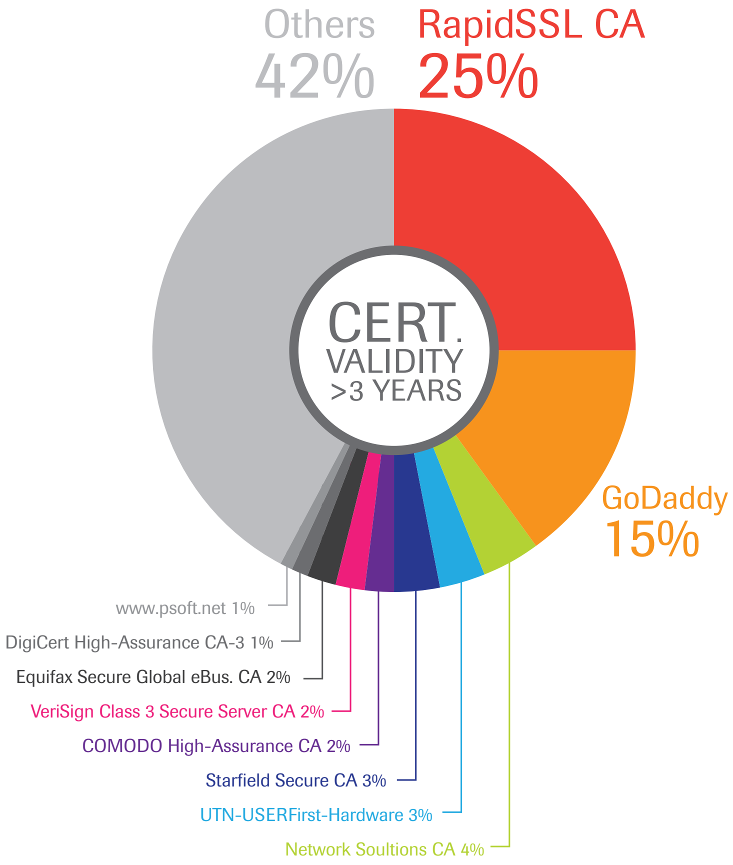


Self-Signed Certificates by Bit Strength



Long Validation Periods

Limiting a certificate's lifetime ensures that an entity revalidate their ownership of the domain in question on a regular basis. Trustwave imposes a limit of three years on any certificate issued, which is a generally accepted standard among Certificate Authorities. Certificates that are valid beyond three years are considered unusual, and as the time limit increases the reliability of the certificate's validity decreases.



Surprisingly most of the issuers are trusted CAs. The top two CAs listed make up 40% of this segment, illustrating the disparity between different CAs' approaches to revalidation requirements.

Key Usage

Certificates can be used for a range of functions, and each certificate provides information about its own authorized uses. In addition to Web server authentication, key uses also include certificate signing, code signing, client authentication and other security roles. Roles are defined in the key usage and extended key usage values of a certificate. These two fields have some common elements. If the elements are not in agreement on the certificate it is technically considered invalid. For example, a certificate that specifies the "TLS Web server authentication" role in the extended key usage field would also normally call out "digital signature" and "key encipherment" in the key usage field to be consistent. This is because in order for a Web server to establish its authenticity, it needs to provide a certificate that can authenticate itself (digital signature) and allows encryption of data (key encipherment).

Extended Key Usage	Common Key Usage Values
TLS Web Server Authentication	Digital Signature, Key Encipherment
TLS Web Client Authentication	Digital Signature
Sign Executable Code	Digital Signature
Email Protection	Digital Signature, Non-Repudiation, Key Encipherment

CAs offer certificates with the certificate-signing attribute, among other key usage values. Certificate signing is the value that allows a CA to validate and sign certificates belonging to other entities; this value separates a CA from other entities in the SSL trust model.

The Web browser, according to what is called a certificate chain, enforces the certificate signing key usage value. A valid certificate chain may have a number of entities, each performing validation for the entity below. Each of these entities that signs a certificate must also possess a certificate that includes the Certificate Signing attribute. If not, the Web browser should generate an error that the certificate presented is invalid.

Certificate 1:

Entrust.net Secure Server Certification Authority

Key Usage: Certificate Signing

Certificate 2:

SecureTrust CA

Key Usage: Certificate Signing

Certificate 3:

www.trustwave.com

Key Usage: TLS Web Server Authentication

Key Usage Security Concerns

Certificate implementations naturally vary across software vendors. To allow compatibility for any variance, Web browsers often accept certificates even if certain fields are missing or incomplete.

Data gathered by Trustwave has uncovered an interesting statistic in this area: a small but significant number of hosts that offer certificates lack any type of key usage extension. In some cases, this is due to the use of the older X.509 version 1 standard, which does not support the key usage extensions. In other instances, the certificate in question uses version 3, but omits these extensions altogether.

The full ramifications of the version 3 certificates are unclear, considering that each Web browser could handle them differently. This scenario introduces uncertainty – it is a condition that should not occur according to the specifications. Although by virtue of being "extensions," key usage can be omitted completely. The result depends on how a browser programmer deals with this unexpected case.

OCSP Findings

As a Certificate Authority, Trustwave maintains an Online Certificate Status Protocol (OSCP) server that allows Web browsers to confirm the validity of an issued certificate. OCSP was created as a more flexible alternative to the Certificate Revocation List (CRL) method to provide controls for certificates after they have been issued. From a statistical perspective, OCSP data offers an interesting view into the client-side adoption of this relatively new protocol.

Apple's mobile platform iOS is among the top requesters of OCSP data, even more so than Apple's desktop operating system. This suggests a tightly coupled integration of OCSP into the iOS platform.

Also of interest is the predominant position of Windows in these statistics, especially considering that Firefox represents a larger share of the requests when compared to Internet Explorer (IE) and Google Chrome combined. (The latter two statistics are combined due to the fact that IE and Chrome share an OCSP library.) The strong showing of Windows XP hosts confirms that Microsoft's 10-year-old operating system is still maintaining a significant market share. Windows 98 made an appearance, using a Mozilla browser to perform OCSP on an unsupported platform.

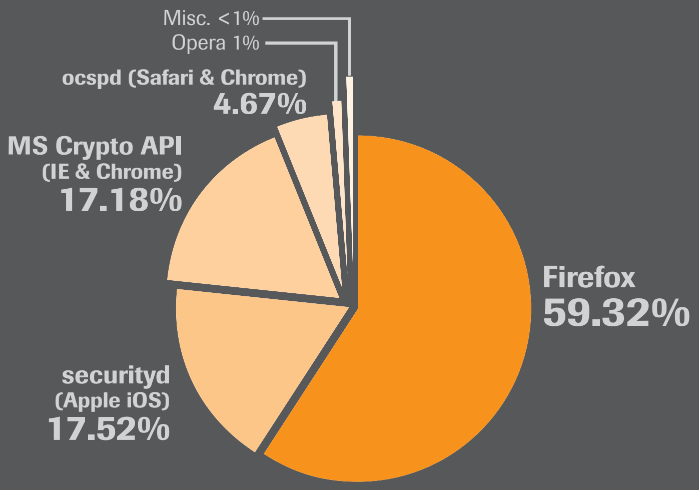
The ever-expanding use of SSL, coupled with recent news of successful attacks against Certificate Authorities and SSL technologies themselves, are bringing more interest to this field than ever before. As the sampling of data provided here has shown, behavior can vary to a surprising degree across SSL implementations. Whether talking about key usage values, bit strength, certificate status checking or validation periods, every issuer and browser developer has a unique take on implementation.

Number of Hosts Using Certificates Without Key Usage (KU or EKU) by Issuer

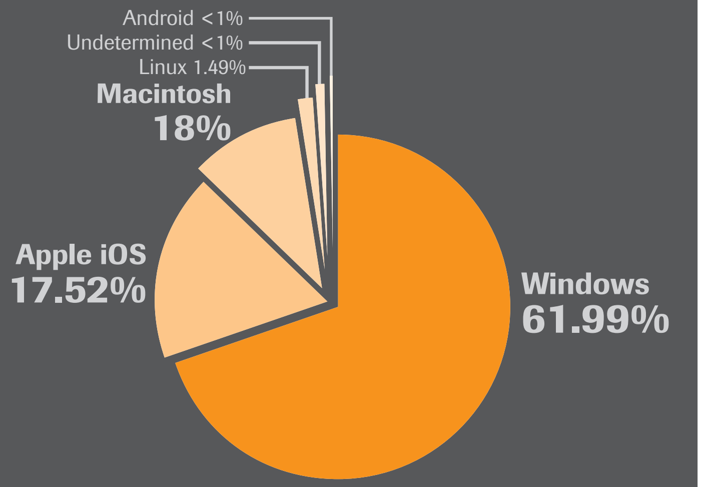
Hosts	Issuer	x.509 Version
294	www.psoft.net	1
258	lifesize.com	1
167	UM Web CA	3
156	PCoIP Root CA	3
123	TAA ROOT CA	3
111	localhost CA	3
84	Foo Bar, Inc	1
66	Infrastructure Certificate Authority	66
58	dummy_ca.thecus.com	3
52	Spiceworks Desktop Install CA	1
50	Google Internet Authority	3
47	Snake Oil CA	3
43	Dev CA	3
38	ca.three12.com	1
35	Lebshama CA	1
35	Siemens Com ESY HD Security Office	3
34	DMSBU CA (1024 bit RSA)	1
34	ImageScape CA	1
34	University of Connecticut Certificate Authority 2017	3
32	mmca.merunetworks.com	3
1699	Other hosts	Various

The SSL industry has matured considerably in the last decade. OCSP greatly improves the ability to revoke certificates over CRL, and Extended Validation offers clients another level of assurance about the validity of a certificate. It is important that, as an industry, we continue to convert security findings into security improvements. The SSL system is a cornerstone of Internet trust, and like any stone, should not remain unturned.

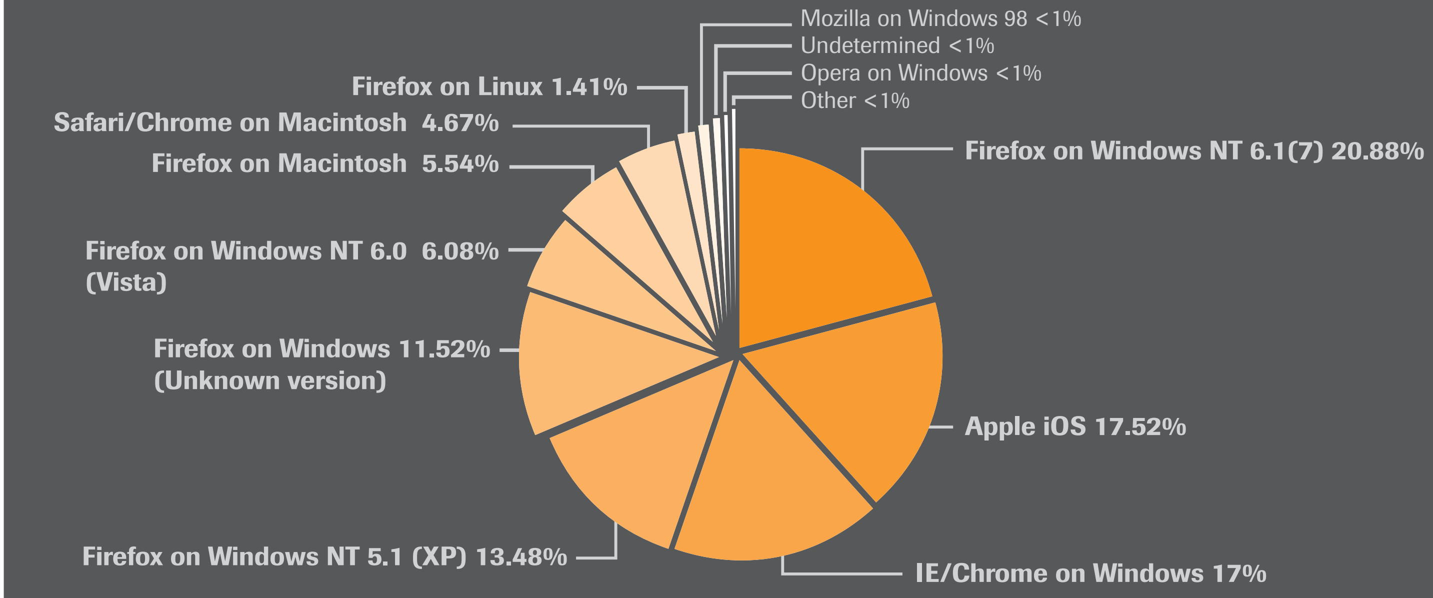
OCSP Requests by Browser / Library



OCSP Requests by Operating System



OCSP Requests by Operating System and Browser



Anti-Virus: The Elephant in the Room

"We have anti-virus, shouldn't we be protected?" is often heard during Trustwave investigations. The historical perception of anti-virus and the sometimes blind faith in its ability to detect and stop malware is one of the reasons attackers are so successful in what they do. The accepted industry approach when a malicious sample is discovered is to create a signature that can then be added to the anti-virus signatures for future detection.

The process of signature creation starts with identifying new malware, whether during a forensics investigation, witnessed on a honeypot system, or received via a submission to an online service. Once detected, a signature must be created for the sample. It is during this phase that the battle between accuracy and speed is fought. Detections are constantly performed and signatures created and there is customer demand for immediate protection from anti-virus companies.

Signatures need to maintain a level of quality in order to properly detect malicious samples. If signatures are created using a method that is too generic, there is a possibility that false positives may occur, leading to benign samples being detected as malicious. Conversely, if signatures are too specific, there is a possibility that a slight variant to a malicious sample will not be detected at all, leading to false negatives. All of these factors are taken into consideration when a signature is created.

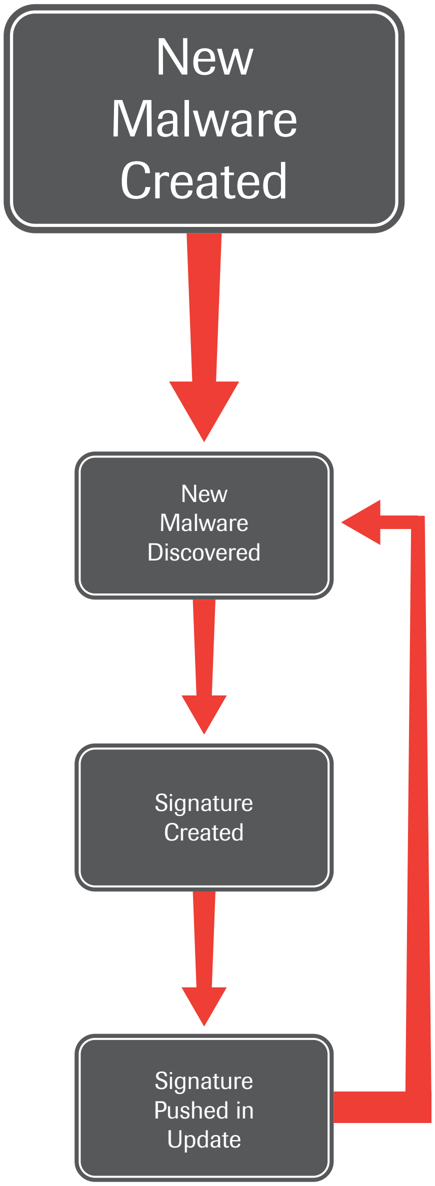
After creation, signatures are pushed into the quality assurance (QA) phase in order to ensure no harm is caused to client systems when deployed. Historically, there have been a few instances where signatures have been pushed to customers that flag critical files on the host operating system as malicious. This led to those systems crashing, as the critical files were either deleted or quarantined by the anti-virus solution.[22] In one of the stranger instances, Microsoft Security Essentials flagged and removed Google Chrome as a banking Trojan.[23] The QA phase is often coupled with the signature development cycle.

After the signature development phase, a final phase is enacted, where updates containing the new signatures are pushed to clients, requiring them to download the update. After client systems have been updated, protections against this specific malware sample or family of samples have been put into place.

When malicious samples first appeared and anti-virus was in its infancy, this signature creation process made sense. However, as the number of malicious files increased, problems using the above method quickly surfaced. The delay in time between when a malicious file is created and when the average user has protection on their system leaves end users unprotected for long periods. Even when detections are put in place, end users are only protected against previously encountered, known malicious files.

Malware targeting specific companies or products will often go undetected by anti-virus products simply because these vendors never encounter this malware.

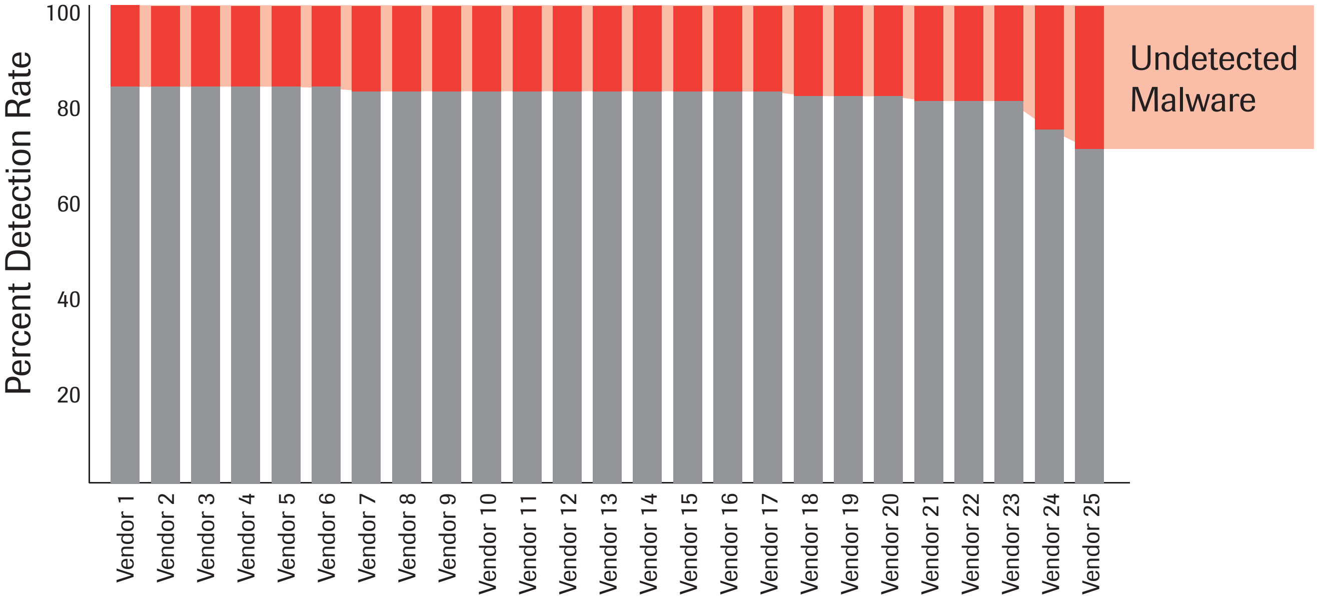
New methods of detection, such as heuristics, have been developed to detect previously undiscovered malicious files as they appear. However, this technology is still in development and has not reached a state of maturity that allows it to be used as the primary method of detection in most anti-virus solutions.



Signature Creation Process

[22] "Horror AVG update ballsup bricks Windows." http://www.theregister.co.uk/2010/12/02/avg_auto_immune_update/

[23] "MSE false positive detection forces Google to update Chrome." http://www.theinquirer.net/inquirer/news/2113892/mse-false-positive-detection-forces-google-update-chrome



The Results

Trustwave SpiderLabs aggregated more than 70,000 malicious samples in 2011 utilizing a propriety correlation and analysis database. Samples were used to perform an analysis on anti-virus coverage, overall and among vendors. On average, anti-virus identified 81% of all samples analyzed (four out of five malicious samples). The highest rate of detection came in at around 83%, while the lowest rate of detection was found to be 70%.

Though 81% may be a passing grade for a student, when it concerns the security of an organization, it demonstrates that relying on anti-virus as a core component of the information security program still exposes the organization to malware threats.

Anti-virus will almost always be a key component in any information security budget, but it should not be relied upon with the level of confidence that many instill in it. Instead, it should be treated and viewed for what it is: a single layer of defense against attackers, but one that will be often and easily bypassed. Anti-virus should always be used in conjunction with other techniques in order to detect a threat against the host and/or network. Such techniques include, but are not limited to, intrusion prevention systems, log analysis, proper network segmentation, and properly configured firewalls between segments.

Walking through Firewalls

A firewall, at its core, is a simple technology. It takes a set of instructions given by an administrator and implements those instructions to influence whether a set of traffic can pass through the device. Nearly 25 years after its introduction, and despite the plethora of competing technologies that have been introduced in recent years, it is still critical for IT security.

Modern day firewalls have a variety of new features, including application-level intelligence, onboard intrusion prevention, anti-virus modules, load balancing, reputation intelligence and others. Modern firewalls have very specific and contextual knowledge of a given traffic stream to enforce a much more granular level of control than their predecessors.

Network Address Translation (NAT) is one firewall technology that surfaced in the early 1990s. NAT was proposed as a stopgap solution to interconnect devices with the public Internet without consuming as much public address space. It also made the internal addresses un-routable on the external Internet by using private address space (defined in RFC1918), familiar to most network users as:

RFC1918 Private Address Space

Start IP Address	Destination IP Address	Prefix
10.0.0.0	10.255.255.255	10/8
172.16.0.0	172.31.255.255	172.16/12
192.168.0.0	192.168.255.255	192.168/16

When hosts from a private address range wish to communicate with a public address, they need to go through NAT. There are two basic forms of NAT in use today: Source Network Address Translation (SNAT) and Destination Network Address Translation (DNAT). SNAT performs modification of source addresses to a public IP as traffic traverses from private to public address space to ensure a return path. DNAT compliments this by performing modification of destination addresses as traffic traverses from

Outbound Traffic (SNAT)

Security Zone	Source IP Address	Destination IP Address
Private	192.168.1.1	1.1.1.1

——MODIFIES SRC IP ONLY——

Public	**2.2.2.2**	1.1.1.1

Inbound Traffic (DNAT)

Security Zone	Source IP Address	Destination IP Address
Private	1.1.1.1	2.2.2.2

——MODIFIES DEST IP ONLY——

Public	1.1.1.1	**192.168.1.1**

public to private address space to ensure the traffic hits the true initiator. SNAT and DNAT are able to accomplish these tasks by maintaining a state table of which devices are communicating to and from private and publicly addressed networks.

Despite the maturity of firewalls, little progress has been made to improve security of the underlying components. Vulnerabilities present in lower-level functions, such as NAT, can confuse higher-level functions resulting in a degraded security state. It is also likely, that as organizations and product companies begin to focus on advanced functionality they lose sight of the underlying core importance of foundational firewall and border device components of such as stateful inspection, traffic flow and network address translation.

Increased network complexity is slowly creating gaps in defenses. These gaps may not introduce substantial risk by themselves but, taken as a whole, they can have a significant adverse effect on the overall security posture of a given network. In response, organizations are asking professionals to specialize more, creating an experience gap at the ground level where networking and security meet. We often see this during our incident response investigations; the network and security administrators may sit across from each other, but assume certain aspects of the environment are being managed by the other. In actuality, no one is managing those aspects.

Due to these growing gaps, Trustwave SpiderLabs performed research to determine ways in which this core function could be exploited. During this process we identified a new attack vector, dubbed “Broken NAT” (BNAT), which could be exploited by malicious users to gain access to internal devices previously thought inaccessible.

BNAT in its most basic form is observed during TCP session initiation. When a client wants to initiate a normal TCP session with a server they need to perform a TCP 3-way handshake as follows[24] :

1. 192.168.1.1 --------> SYN --------> 192.168.2.1
2. 192.168.1.1 <------ SYN/ACK <------ 192.168.2.1
3. 192.168.1.1 --------> ACK --------> 192.168.2.1

When looking at a simple BNAT scenario, we see a slightly different result, which results in a broken communication channel.

1. 192.168.1.1 --------> SYN --------> 192.168.2.1
2. 192.168.1.1 <------ SYN/ACK <------ **192.168.2.2**
3. 192.168.1.1 --------> **RST** --------> **192.168.2.2**

In this case, because 192.168.2.2 responded to our request instead of 192.168.2.1, our client terminates the connection with a TCP RST, as we were trying to talk to 192.168.2.1 and not 192.168.2.2.

BNAT scenarios are usually a result of a device misconfiguration or device subsystem malfunction. They are more likely to occur in complex networks, such as when an organization deploys multiple infrastructure vendors without a consistent vision of the overall network traffic flow. BNAT commonly exists in environments where asymmetric routing is present. Asymmetric routing is IP communication that takes different paths from source to destination and destination to source.

Trustwave’s Managed Security Services team frequently identifies BNAT conditions and helps organizations correct these scenarios when installing unified threat management (UTM) and other stateful enforcement devices into customer environments. When BNAT scenarios go unidentified and uncorrected, the traffic flow through a network can cause improper NAT actions, resulting in a broken communications channel similar to the initial BNAT scenario example noted previously.

Trustwave SpiderLabs recently identified “BNAT hijacking”: a malicious user successfully makes use of broken communications channels and converts them into valid TCP sessions with little effort. BNAT hijacking is achieved by making the local TCP stack of the malicious user more forgiving when receiving responses from an uninitiated target by “Reflectively ACKing”(rather than RSTing) and then pivoting to the SYN/ACK responder for the remainder of the communication session.

[24] TCP 3-way handshake defined in RFC 793, Figure 7. http://www.ietf.org/rfc/rfc793.txt

1. 192.168.1.1 --------> SYN ----------> 192.168.2.1
2. 192.168.1.1 <------ SYN/ACK<------ **192.168.2.2**
3. 192.168.1.1 --------> **ACK** --------> **192.168.2.2**
4. 192.168.1.1------>**PSH/ACK**------>**192.168.2.2**
5. 192.168.1.1 <------- **ACK** <-------- **192.168.2.2**

Note: 192.168.2.1 only sees the first SYN packet; the remainder of the connection traverses through 192.168.2.2

This new process accomplishes a number of things that could be useful to a malicious individual trying to exploit a BNAT service:

1. Allows completion of the TCP 3-way handshake with a service that was previously unreachable
2. Allows bypass of stateful inspection and other advance application controls
3. Allows inbound initiated communication through an egress-only device
4. Allows exploitation of vulnerabilities that may exist

Trustwave SpiderLabs analyzed 250,000 public IP addresses from 132 countries to determine whether or not BNAT exists on open Internet and how prevalent it really is in the wild.

This analysis included a port scan of each host on each of the services listed in the tables to the right. If the host responded with a TCP SYN/ACK response with a matching sequence number (+1 of the ISN) then it was included in our data set. If the host responded with a TCP SYN/ACK response matching the port and sequence number, but not IP, the service is a BNAT service.

Port	Service
21	FTP
22	SSH
25	SMTP
80	HTTP
443	HTTPS
445	Microsoft-DS
1433	MS-SQL
1521	Oracle DB
3306	MySQL
3389	RDP

Of the 250,000 IP addresses scanned, only those that responded to a TCP SYN request with a TCP SYN/ACK on one or more the services listed above were considered in scope. These yielded approximately 60,000 live hosts with the following distribution of TCP services:

Port	Service	Percent
21	FTP	9%
22	SSH	9%
25	SMTP	10%
80	HTTP	34%
443	HTTPS	34%
445	Microsoft-DS	1%
1433	MS-SQL	2%
1521	Oracle DB	0%
3306	MySQL	1%
3389	RDF	2%

Note: Percent value is the number of instances of each service over all instances found.

This data is not surprising as Web and email are two of the top three of services used on the Internet today. Within these services, a subset of BNAT services existed. This means that the service responded, but the response traffic received did not match the IP address requested.

Port	Service	Percent
21	FTP	4%
22	SSH	1%
25	SMTP	8%
80	HTTP	9%
443	HTTPS	74%
445	Microsoft-DS	1%
1433	MS-SQL	1%
1521	Oracle DB	0%
3306	MySQL	0%
3389	RDF	1%

Note: Percent value is the number of instances of each BNAT service over all BNAT instances found.

The most surprising result of the service distribution of the identified BNAT services was that although HTTP and HTTPS shared about 35% of the total services identified, HTTPS was eight times more likely to yield a BNAT service than HTTP. This is likely due to various asymmetric routes that are introduced when load balancers of e-commerce systems are performed.

Country	Percentage
Ireland	0.96%
Hong Kong	0.81%
Canada	0.72%
Japan	0.53%
Mexico	0.46%
United Kingdom	0.21%
United States	0.05%

Note: Country distribution is not a representative sample of each country as a whole.

Note 2: 71% of all BNAT instances discovered were located in one of the seven countries listed above.

Note 3: Percent value is number of BNAT instances found over all services for each country.

In a number of countries where a series of IP addresses were scanned, a large number of active services were found but absolutely no BNAT services. These countries, in order of size, were: Australia, Germany, Sweden and China.

Overall, Trustwave positively confirmed that all but two of the services identified above (Oracle DB and MySQL) were present on the Internet. An average of one BNAT service existed for every 790 live hosts identified by the scans. When comparing these results to the current number of live Internet hosts (about 850 million hosts) reported by the Internet Systems Consortium in July of 2011, the number of hosts exhibiting BNAT services is estimated at more than one million.

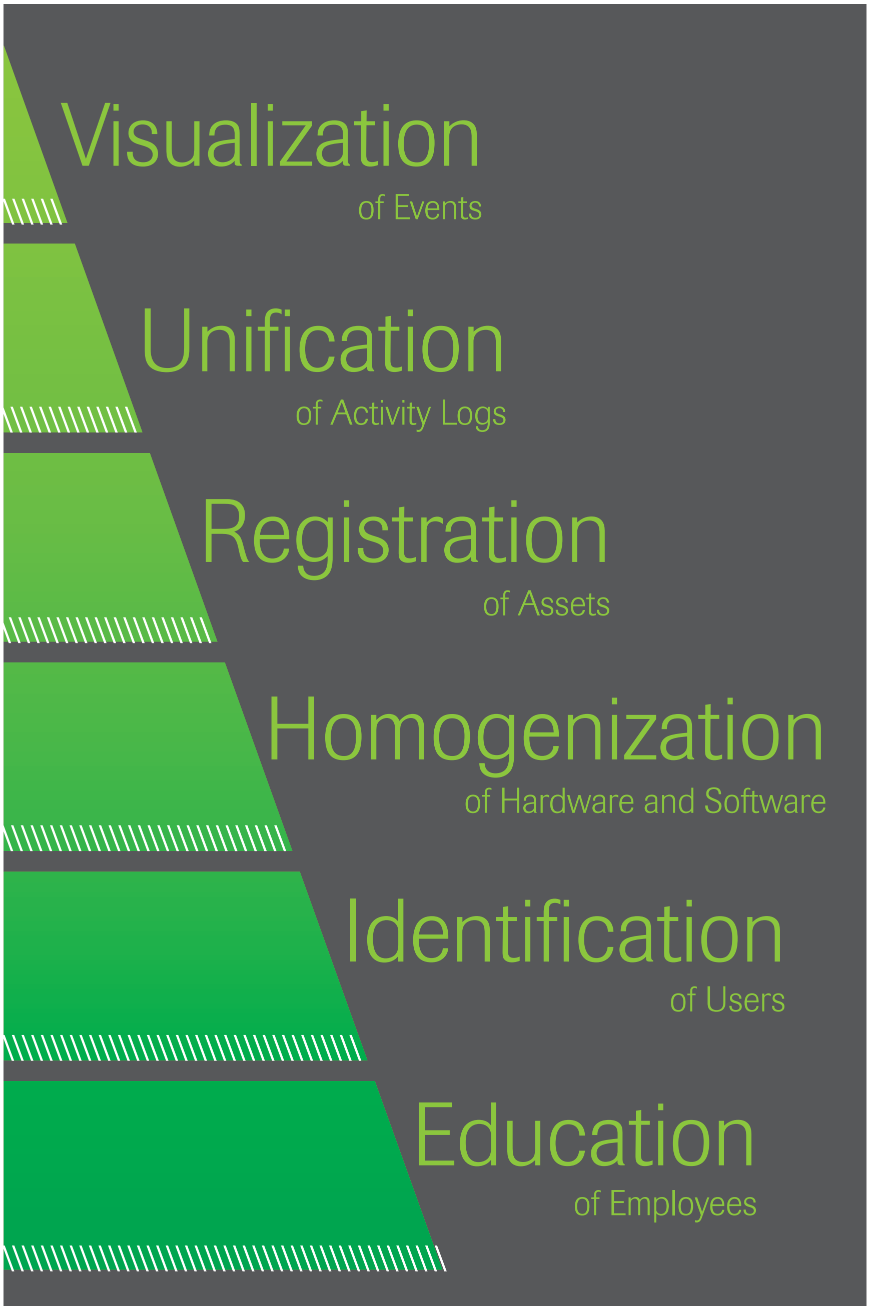
BNAT exists in the wild across various services and multiple geographic boundaries. It is highly recommended that organizations that have a publicly facing Internet presence assess their environment to ensure that they do not have exposed BNAT services. These services effectively hide from modern port and vulnerability scanners, and can go long periods without detection. Recently, Trustwave SpiderLabs added BNAT detection to its TrustKeeper vulnerability scanning solution and has been assisting customers in fixing the issues identified.

It is recommended that professional service organizations, like IT auditors, penetration testers and security consultants alike scan for BNAT when performing assessments for their clients to ensure they are protected. Detecting BNAT with the right tools is easy and not much more work than a simple port scan.[25]

[25] Trustwave currently maintains a set of open source tools on GitHub called "BNAT-Suite" (github.com/spiderlabs/BNAT-Suite) that can be used not only to detect, but also to hijack BNAT scenarios to better help organizations and security industry professional understand this new attack vector.

Information Security Strategy Pyramid for 2012

Improving the security posture of an organization may not be an easy task. If 2011 was any indication of what the future will bring, it is no longer a matter of “if” you will be attacked, but “when.” The security goals for 2012 should be to prevent as many cyber attacks as possible, as well as streamline information security processes to identify attacks when they occur and resolve related problems quickly. Trustwave SpiderLabs recommends six areas for all organizations to focus on in 2012:



Each area, if implemented fully, will support and enhance the area placed above it. Once the top is reached, the process starts over at the bottom — it is a continuous effort work to refine security programs. The pyramid can be explained from the bottom up.

Education of 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 to liabilities.

Attackers are motivated to use phishing attacks as they require only a small percentage of recipients to perform actions that assist the attacker in gaining unauthorized access. Untrained employees click links to malicious websites, opening a backdoor into the corporate network, or expose their corporate credentials by logging into what appears to be a legitimate (but is actually attacker-controlled) corporate website. These actions can result in loss of intellectual property and exposure of customer data, leading to incident response investigations, costly fines, and a detrimental effect on an organization’s reputation and brand.

An alternative to casting such a wide net is focused phishing attacks against specific individuals. For instance, the attacker may be very interested in a person with privileged access to sensitive systems, applications and data within the target organization.

With proper education, a targeted employee can be the first detector of an attack that would otherwise circumvent preventative technical controls. Security-aware employees are better able to determine if an email is malicious and will follow proper procedures to alert security staff.

Physical security awareness is just as important. Tailgating and social engineering are less effective when personnel have been taught the importance of their individual responsibilities for physical security. In many respects, it requires education around why social norms (like holding an access door open for the person behind you) can have a negative impact on security for the organization.

Employees should be encouraged to challenge unknown individuals in the correct circumstances and to ensure those around them follow the correct physical access control procedures. This can help prevent losses and ultimately save organizations money. In some cases, it can also protect the lives of employees should the person tailgating or attempting to bypass controls have intent to physically harm employees.

By changing the mindset and behavior of employees through education and reinforcement of positive behaviors, businesses build a solid foundation for a security program. In the 2012 security pyramid, Visualization isn't remotely possible if employees, especially those tasked with security, do not have situational awareness to sound the alarm when something doesn't look, feel or sound like it should.

Initiatives and technology to support this area:

Security Awareness Training

Regular training of staff on both core security techniques and topical issues is important to build a successful security foundation.

Security Awareness Campaigns

Repetition is key; regularly featured security topics will help staff awareness levels and help maintain employee vigilance.

Rewards for Incident Identification

Monetary or other rewards can help encourage employees to be observant and report security events.

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.

Identification of Users

Once employees are educated on their roles in protecting their organization's assets, they need to be properly identified. Every user-initiated action should be tagged to a specific employee, consultant or other third party. This may seem a lofty goal, but it is achievable in most environments.

The first task is the eliminations of generic, shared, vendor and default accounts. Every single 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, attackers utilize a shared vendor or default account that should have been changed before the application was placed into production.

This level of security must be adhered to in the physical world as well. Employees may wear badges and key cards for access control and logging of movement within a facility, but as soon as an employee forgets their badge, all they need to do is request a temporary keycard for the day. Ensure every single person who has access to facilities and systems is identified as they traverse the physical and digital environment.

Initiatives and technology to support this area:

Logical Access Management Reviews

Performing periodic analysis of all user and group roles will improve security around employee access levels and may even identify accounts that are no longer needed.

Password Complexity Policies

Set password policies of high complexity and educate staff on best practice password techniques, such as using passphrases.

Two-factor Authentication

Two-factor authentication allows users to authenticate by both what they know (a password) and what they have (a device or certificate). This should not only be applied to the digital world, but also the physical world. Combining key-card access with PINs is a way to accomplish this.

Biometrics

Beyond passwords and other authentication mechanisms, biometrics may be necessary for more sensitive areas of the workplace, such as data centers and R&D environments.

Homogenization of Hardware and Software

Fragmentation of enterprise computing platforms is an enemy to security. IT departments are often busy just keeping systems up and running, and security takes a back seat. If platforms and devices become unmanageable from an inventory standpoint, keeping tabs on security-related issues can become unmanageable as well.

Fragmented environments can require unrealistic maintenance efforts and cause major security issues. One day it is an issue with an Internet browser that 20% of employees like to use, the next day it is a document reader on all the Mac devices, and on the third day it is a flaw affecting only those using Android on a certain hardware platform.

The more diverse the hardware and software population in the environment, the more IT and security teams need to react to problems. Reducing this fragmentation through standardization and decommissioning of old systems will homogenize the environment, making it easier to manage, maintain and secure.

Initiatives and technology to support this area:

Policies

Defined based upon risk assessment exercises, policies should dictate how future decisions are made in regards to platforms and software packages used by employees.

Hardware Standards

Identify standards to adopt a "less is more" strategy. Fewer standards can help to reduce complexity, an enemy of security.

Decommissioning of Old Systems

Too often, through both our investigation and penetration tests, we find vulnerabilities in systems that are no longer needed for business purposes. Work to aggressively turn off and unplug these systems from the environment. Upgrade or replace systems to align with policies and standards. In circumstances where this is not a business option, triage (understanding the security issues and risks) and treatment (applying compensating security controls) are options that should be considered.

Registration of Assets

Educated, identifiable users armed with specific approved devices, running specific applications, is a good place to start to create an easier environment to navigate from a security standpoint. We now need to know which devices are entering our networks and when, and at the same time understand their individual security posture.

Networked devices are widespread in organizations today. It is more important than ever to have a complete inventory or registry of valid devices.

Bring Your Own Device (BYOD) is a burgeoning trend; employees are accessing the corporate network via their own smartphones, tablets and even laptops. Allowing users to use any device they want with no security controls, however, will destine the security program for failure.

Businesses that adopt a BYOD policy 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 on this accurately, making a survey of devices unreliable. Without a device registration process, a BYOD business is never sure that a vulnerable device doesn't exist on the network.

From desktops to laptops, from 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. By implementing a device registration process and limiting BYOD, businesses will have better oversight of what devices access corporate networks when and for what purpose.

Security controls also play a strong role this area. 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.

Initiatives and technology to support this area:

Asset Management

Institute a system to track devices, applications and other assets owned.

Network Access Control (NAC)

NAC can control access to various network environment based upon defined rules. It can also be used to remove devices from the network if and when security issues are identified.

Patch Management

When there is an active threat understanding the patch levels of systems and applications are critical.

Vulnerability Scanning

Even with the above solutions in place, there will still be instances where configurations or the combinations of various services will introduce vulnerability. Regular scanning of both internal and external systems should be performed.

Unification of Activity Logs

Combining the physical world with the digital affords organizations new ways to identify security events more quickly. Most businesses today treat physical controls 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 systems and other security technology.

From the results of our investigations, it is clear 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. Consider the following scenario:

A world-wide business employs many individuals who regularly travel for their jobs. While waiting for a flight, one such individual attempts to access their email on a laptop. A certificate warning pops up but is ignored (see Education above). Their credentials are intercepted and stolen. A few days pass and the employee is back in the New York office. While he is sitting at his desk, the attacker connects to the environment via the email account information he obtained and begins to download email.

In most organizations, this scenario would not raise an alarm. When the attacker logs in, the IT environment registers that act as an employee accessing his email while outside the office. However, the employee is currently physically located in a New York office, logged into the domain from the office network, and not traveling (see Registration above). This scenario becomes more serious when the employee is a high-profile individual with access to sensitive data.

The first step to addressing this attack scenario is to reduce the number of consoles. Instead of viewing multiple consoles and attempting to correlate data across all, feed the logs of these point solutions into a single console. During this process, review each point solution to ensure they are: 1) configured correctly, and 2) they are logging as much as possible.

Too often many tools are in place but administrators have tuned them down to reduce the "noise," and they no longer provide anything of value. Instead of tuning, use a tool, such as security information and event management (SIEM) technology, to take over the processing of these logs; all "noise" will just be data for this technology.

Unification of systems will benefit awareness of the attack scenario described above and other types of events, as well as help improve the accuracy of Visualization. In a unified scenario of this example, the office badge swipe combines with the local domain login and the company issued computer. Correlating this information with the act of email accessed from a location outside the office from a non-company-issued machine yields a red flag.

Initiatives and technology to support this area:

Logging Option Analysis

Logs are sometimes turned off or tuned down to the point where they become useless in identifying security events. Analysis should be performed to maximize the amount of events captured.

Point Security Solution Tuning

Over time security logs may not be reviewed as frequently and may even be tuned to limit the "noise" they are generating. Tuning these solutions regularly to ensure proper data capture and review is happening is recommended.

Security Information and Event Management:

A SIEM helps achieve log normalization and correlation, and allows for rules to be applied to trigger security events.

Visualization of Events

Daily business activities take place millions to billions of times per day in most environments, but all it takes is one security event for a company to make the headlines for the wrong reasons.

Security event visualization in the enterprise isn't practiced frequently, most of the time it is just considered log review. Many security professionals still use spreadsheets to perform their analysis — after the event has occurred and the damage has been done. In the previous section we wrote about the Unification of data using tools like a SIEM. For most organizations today, this is where the path ends. The ultimate goal should be to develop an environment that allows for security events to be discovered by seemingly innate observations by both the people who are tasked at protecting the environment and those who are not. Data aggregation or correlation as seen in a SIEM is a precursor to real-time security event visualization and notification.

After automating analysis, acknowledge there are tasks computers can't do very well and design analysis processes to coordinate employees working with computers. Present items to administrators that a computer can't understand in a way that the validity of the action can quickly be determined, or that would encourage further investigation.

Consider using colors and sounds as data is presented to employees. Trustwave SpiderLabs research in this area revealed that "urgent" flashes of light or beeps are not effective at gaining attention or driving actions. Over time people ignore them. Employees are more likely to notice subtle changes in color or audible tones.

Initiatives and technology to support this area:

Custom Visual / Environmental Controls:

Explore tying the physical environments in which administrators work with the potential security changes occurring in the digital environment.

Experimental

Trustwave SpiderLabs' cerealbox is a tool that demonstrates a method of tying various events on computer systems to visual indications. The goal is to prompt the user to investigate when something is different or looks odd, rather than having to constantly review logs or receive pop-up messages on their console to indicate so. The tool can be found at https://github.com/SpiderLabs/cerealbox.

Global Conclusions

In 2012 and beyond, some predictions and recommendations can be made. First, cyber attacks are increasing, as evidenced by the frequency of media reports and the growing queue of incident investigations conducted by Trustwave SpiderLabs. There is no sign of abatement.

Possession of customer records makes businesses a target. The risk is even greater for businesses frequented by consumers and brand name chains. Technology may be necessary to protect the network, such as Web application firewalls and network access control, and the data itself, such as encryption and data loss prevention.

Outsourcing IT and business systems to a third party increases risk, as many of those organizations may not have client security interests in the forefront. When those third-party systems are used for remote access, criminals are more able to access the corporate environment due to weak and default passwords. Change default passwords and work with vendors to ensure they are following security best practices and adhering to industry requirements.

Employees will continue to choose poor passwords. Enacting and enforcing stronger policies, and encouraging longer passphrases, will help mitigate this risk.

Out-of-the-box anti-virus is not effective against many classes of threat. Don’t rely on anti-virus to solve security problems. Instead, adopt a security plan that uses both automated and manual testing techniques to identify unknown vulnerabilities and security gaps.

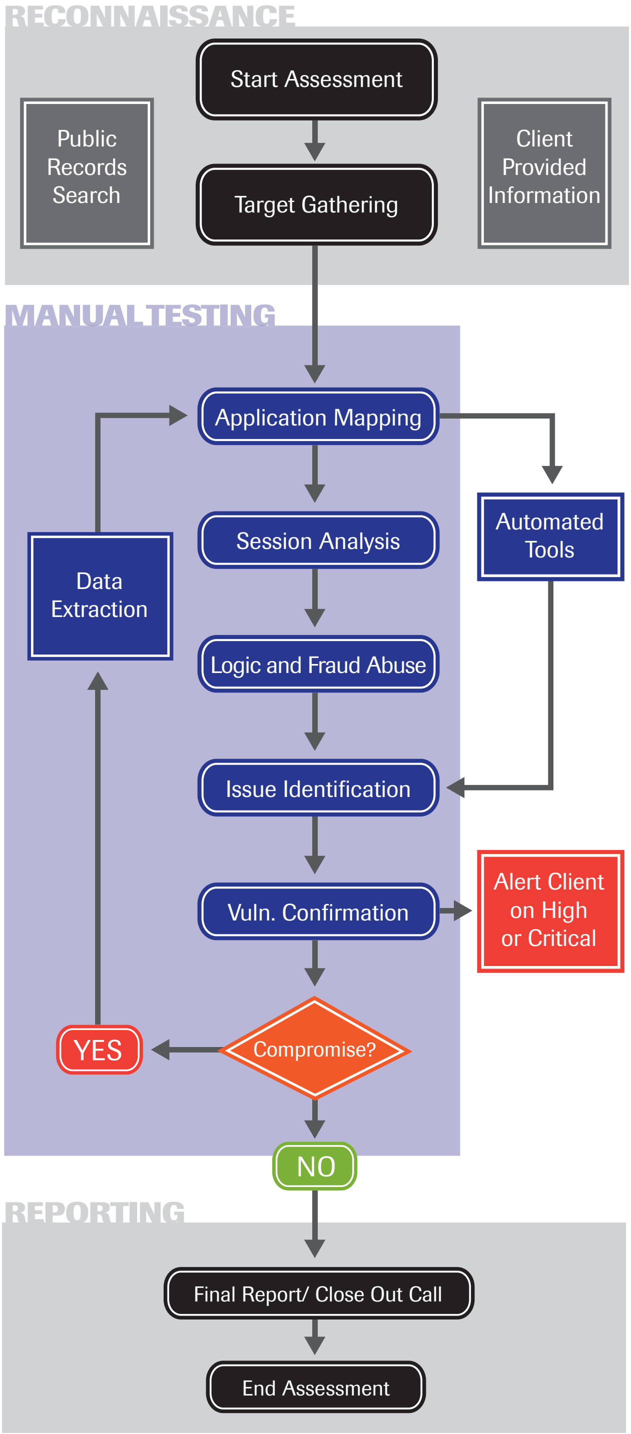
Finally, firewalls deployed years ago are often no longer effective due to flaws in the original design or its use. Review the configuration of firewalls and make a plan to update or install a modern implementation.

Organizations that approach their security initiatives in a committed manner and as an integrated requirement for 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, they’ll also safeguard their reputation.

The Trustwave 2012 Global Security Report identifies many areas where organizations can improve or implement new procedures and technologies. By learning from the misfortunes of others, and applying tactical and strategic changes outlined in this report, organizations worldwide can build better security programs and frustrate cyber criminals everywhere.

Appendix
What is a Penetration Test?

Testing data protection strategies by using the same tools and techniques an attacker would use is one of the most useful ways to be assured those strategies work. This method is called penetration testing. It is a controlled engagement whereby a qualified professional attempts to test network and application security controls by trying to gain unauthorized levels of access, ultimately to access sensitive data.



Why Vulnerability Scanning is not Penetration Testing?

Vulnerability scans are automatic tools that attempt to identify vulnerabilities that an attacker might be able to exploit. They are often used for finding “low-hanging fruit,” such as basic or common configuration mistakes that could be exploited by an attacker.

Vulnerability scanners can’t understand data like a human can, so an automated scanner would not know if it was dealing with a mundane document, or highly sensitive board room minutes. Nor can vulnerability scanners understand the background context of a security test, meaning they are very poor at assessing the impact of a specific vulnerability. Finally they are also not able to identify certain classes of security issue, such as subtle business logic flaws (perhaps related to a complex approval process within a supply chain management application). It is precisely these security issues that often have the most serious consequences!

Organizations should ask these questions before engaging in a penetration test or scanning service:

- Are we trying to defend against a low-skilled attacker who is able to download and run a vulnerability scanner against us?
- Are we trying to defend against intelligent adversaries who can cleverly exploit a chain of vulnerabilities, possibly across seemingly unrelated assets, to gain access to our sensitive data?

The answer is yes to both. Just running a vulnerability scanner against IT assets is not enough to secure an organization. Trustwave SpiderLabs consistently finds critical and high-risk material vulnerabilities in environments that undergo regular, automated vulnerability scanning.

Who Needs Penetration Testing?

Organizations with sensitive information, such as customer data, personally identifiable information, payroll data, payment card data, intellectual property and other data types should consider penetration testing.

Some organizations use a data classification policy (with associated procedures) that describes how different types of data within the business should be protected and handled. However, even the most detailed data protection strategies can have vulnerabilities.

Any organization that has electronic data that they would not want exposed publicly should consider regular penetration testing. Trustwave SpiderLabs conducts penetration tests against networks and applications for many different types of sensitive data. The entire testing process is primarily manual to limit generic results often received from scanners and checklist methods used in general vulnerability assessments. In this way, Trustwave can focus the engagement on directed attack logic-based testing against systems and networks

What is the Difference Between Network and Application Penetration Testing?

A network penetration test typically includes entire networks and many hosts, the testing of which is focused at the network layer. This type of assessment is typically performed “blackbox” (without any authentication credentials or privileges). Network layer penetration tests should be performed both externally (against Internet-facing servers and supporting infrastructure) and internally (against internal corporate information systems assets, including servers, workstations, routing and switching equipment, printers and IP telephony systems).

Application penetration testing involves a targeted assessment of an individual (commonly, although not exclusively, Web) application. This application could either be on the Internet or accessible only internally to employees and third-party customers or partners.

Application penetration tests will almost always require that the penetration tester receive authentication credentials to the applications, specifically two sets of credentials for each type of “user role” that exists within the application. The reason for this is two-fold:

- Typically the dynamic data creating/reading/updating/deleting functions of an application are only accessible post-authentication. Security vulnerabilities within these areas of functionality are likely to be most serious;
- Tests to ensure one user cannot create/read/update/delete data belonging to, or by pretending to be, another user require two users at each user role.

Often organizations believe that only the corporate website needs application penetration testing. However, the corporate website is typically one of many Web applications an enterprise would have facing the Internet. Trustwave SpiderLabs has worked with individual customers that have more than 1,000 business applications.

About Trustwave®

Trustwave is a leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organizations faced with today’s challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions including SIEM, WAF, EV SSL certificates and secure digital certificates. Trustwave has helped hundreds of thousands of organizations-ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers-manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, Asia and Australia.

For more information: https://www.trustwave.com.

About Trustwave SpiderLabs®

SpiderLabs is the advanced security team within Trustwave focused on forensics, ethical hacking and application security testing for our premier clients. The team has performed hundreds of forensic investigations, thousands of ethical hacking exercises and hundreds of application security tests globally. In addition, the SpiderLabs research team provides intelligence through bleeding-edge research and proof of concept tool development to enhance Trustwave’s products and services.

For more information: https://www.trustwave.com/spiderLabs.php.

About Trustwave®

Trustwave is a leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions including SIEM, WAF, EV SSL certificates and secure digital certificates. Trustwave has helped hundreds of thousands of organizations-ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers-manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, Asia and Australia.

For more information: https://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

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

APAC Headquarters
Level 26
44 Market Street
Sydney NSW 2000, Australia

P: +61 2 9089 8870
F: +61 2 9089 8989

Trustwave®
Security begins with Trust℠