Global Security Report 2011

Trustwave® SpiderLabs®

Dear Reader:

Trustwave's SpiderLabs is committed to delivering advanced information security services to our clients and actively supporting the community at large through our research and industry participation. Since Spiderlabs' 2005 inception, we have grown to become a global services organization supporting Trustwave's clients and providing a range of services, including application security, incident response, penetration testing, physical security and security research.

When we published the Global Security Report 2010, we did not foresee the impact it would have on our industry. Over the last year, the 2010 report was often referenced for its real-world insight into the state of the information security posture of companies worldwide. Universities around the globe are also using it as a teaching aid within information security and assurance curriculums.

We also received feedback from readers asking for more and different data analysis in the next release. Over the past year, we spent a great deal of time digging deeper to provide you with the most comprehensive information security report available. This year, we not only include expanded analysis of our compromise investigations, but also take a new look at the expanding and evolving landscape of data security vulnerabilities.

In addition to the data analysis, members of the SpiderLabs team contributed various topical essays that we felt further define the state of the industry in 2011—beyond what can be depicted with statistics and graphs.

It is with great pride that I present Trustwave's Global Security Report 2011. I hope you enjoy reading it as much as we did creating it.

Sincerely,

Nicholas J. Percoco
Senior Vice President and Head of SpiderLabs

Table of Contents

Introduction

In 2010, SpiderLabs performed more than 220 investigations worldwide. In 85% of the investigations, a system breach was confirmed. Of those entities in which a system breach was confirmed, 90% involved the actual theft of sensitive data, representing criminals' effectiveness in extracting data once system access is obtained. Cybercriminals simply selected a target, accessed data from that target and harvested sensitive data with little to no resistance.

Cybercriminals are repeatedly portrayed as individuals or a loosely connected band of individuals. But our research demonstrates that cybercriminals have evolved to integrate with the world's organized crime rings. These criminal organizations are highly structured and are now investing in technology and technically skilled people to assist them in a primary goal: defrauding businesses worldwide.

Often the simplest solution to prevent cyber attacks is the one that most easily thwarts the attackers' efforts. We see such information security solutions working every day. Unfortunately, many organizations take a tentative approach to information security due to the perceived complexity of the solutions to the problems they face.

Each year SpiderLabs is called upon by thousands of organizations around the world to assist them in better understanding their security posture (i.e., their risk of compromise via penetration testing), as well as determining and detailing what went wrong when a breach actually has occurred (i.e., incident response and forensics).

The foundation of Trustwave's Global Security Report 2011 is data from real-world investigations and research that SpiderLabs performed in 2010. To assist with the planning and security efforts of our readers, this report offers analyses of data compromise investigations, offensive exercises and defense strategies taken directly from Trustwave's expansive global client base. Similar to last year's report, the 2011 report is separated into three distinct sections:

1. 2010 Incident Response Investigations: This section features analyses of more than 220 investigations conducted as a result of suspected security breaches, identified by either the target organization or a third party (e.g., regulatory body, credit card brands, business partners, consumer, etc.). The section details the tools and techniques used by attackers to gain access to sensitive data.
2. Attack Vector Evolution: In this section we reviewed vulnerabilities of the last 30 years, to illustrate how attack vectors have evolved, and the scope of the security problems we face today.
3. Strategic Initiatives for 2011: In order to help organizations avoid becoming a statistic in our 2012 report, we've identified 11 strategic initiatives that every organization should strongly consider prior to embarking on their own security endeavors.

The overall methodology incorporated firsthand evidence collected in 2010 by Trustwave's SpiderLabs. Results are based on information gathered during data breach investigations, penetration testing and other security-as-a-service (SaaS) activities conducted for our clients. Standardized tools were used to record data, as well as 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 the aggregate only.

2010 Incident Response Investigations

Analysis of Sample Set

Unique Data Source and Methodology

SpiderLabs' initial goal is to investigate how the breach occurred and to quantify the damage inflicted. The results of these investigations are often required by not only the affected party, but also a regulatory body that has an interest in the investigation. For instance, the major card brands dictate specific milestones in the investigation of a payment card breach and require a formal report of the findings. In many cases, SpiderLabs' investigative information is used by law enforcement to assist in identifying and apprehending the party responsible for the breach.

Responsiveness and accuracy are both essential to properly contain a compromise and limit exposure. Following a thorough analysis, a containment and remediation plan is implemented to reduce the risk of re-occurrence, with the additional purpose of minimizing recovery time and costs.

Early in its existence, SpiderLabs recognized that traditional incident response and forensic methodologies were quickly becoming irrelevant in the constantly evolving threat landscape. As criminals became more resourceful, the complexity of computer forensics increased exponentially. In addition, as a result of the growing size of data storage devices, it quickly became impossible to even consider imaging tens of hundreds of terabytes of affected data.

Through logic and data reduction techniques based on forensic evidence extracted from live analysis, SpiderLabs developed a streamlined methodology. With this highly accurate and efficient methodology, SpiderLabs has consistently delivered results to the interested parties two to three times faster than other investigation firms.

Countries Represented

Australia
Brazil
Canada
China
Dominican Republic
Germany
Ghana
Israel
Japan
Malaysia
Mexico
Nepal
Philippines
United Kingdom
United States of America

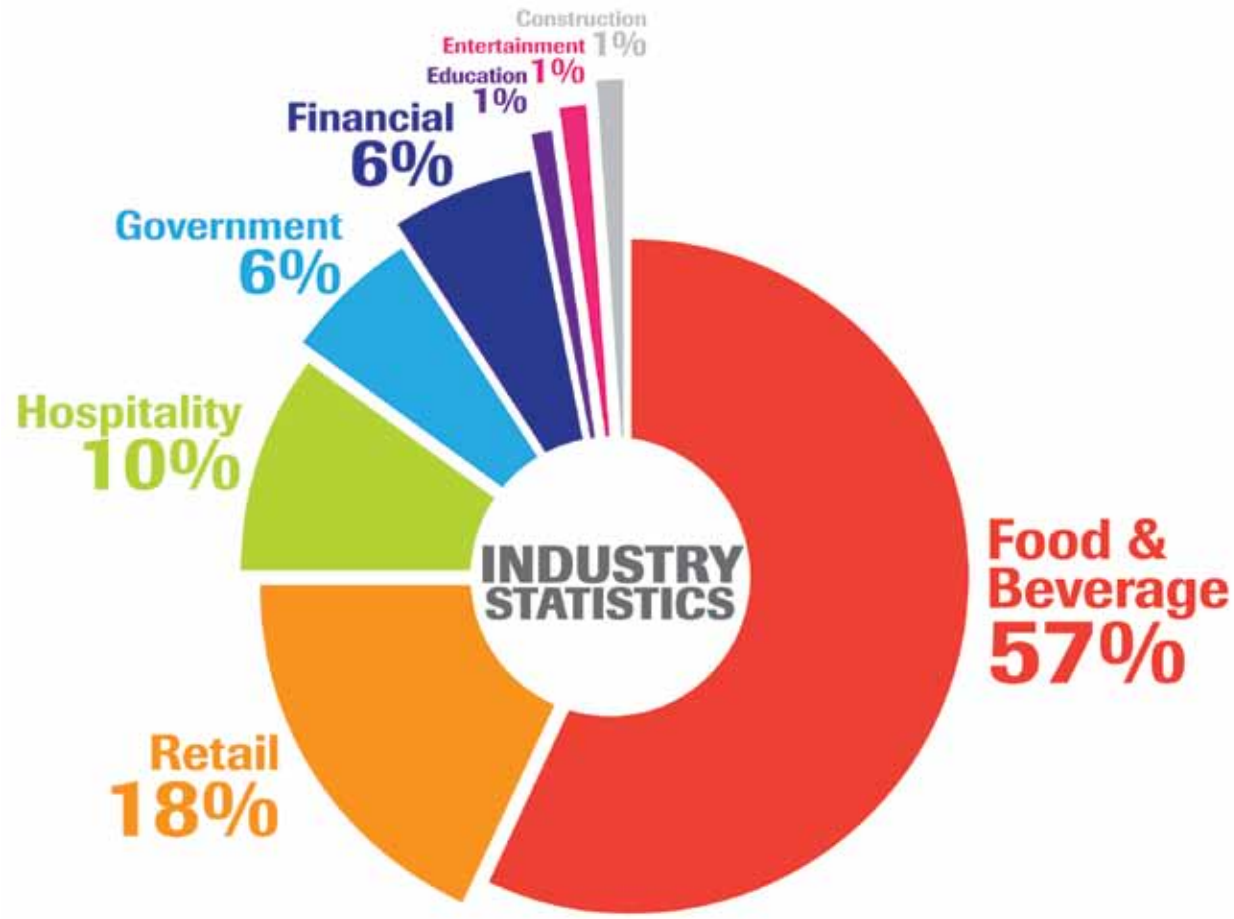
Working in a global environment presents its own set of unique challenges. Often we find ourselves not only responsible for meeting (and exceeding) our client's expectations, but also for abiding by all local data disclosure and protection laws. Our presence within specific regions may often be dictated by the maturity of regulatory requirements and compliance regimes. For instance, while the Payment Card Industry Data Security Standard (PCI DSS) requirements have been firmly established in North America and Europe, these mandates are just beginning to take hold in other regions.

For example, Latin America and Asia Pacific still lag behind other areas of the world in the identification and acknowledgement of a data breach, which adversely affects the global effort to combat attacker behavior. In these regions it is widely known that many organizations under-report breaches in order to protect their brand. This is similar to what occurred in the United States prior to data breach disclosure laws and other regulatory requirements began to take hold.

Data breach disclosure makes the world a safer place for both businesses and their customers by allowing the necessary parties to understand what failed and how to remediate such failures, as well as provide law enforcement additional evidence to help bring criminals to justice.

Industries Represented

While our 2010 caseload was consistent with that in 2009 in terms of quantity, fewer industries were represented in 2010. In a trend consistent with pre-2009 levels, the food and beverage and retail industries shouldered the brunt of data breaches—accounting for 75% of all investigations.



While a reduction of breaches within the hospitality industry was observed from the prior year, hospitality businesses should remain on high alert. At this time, it appears that the organized crime group responsible for the majority of hospitality breaches in 2009 expanded their target list. Instead of focusing exclusively on the hospitality industry, this group became active within the food and beverage and retail markets as well. Evidence suggests this single organized crime group was responsible for 36% of all data breaches investigated by SpiderLabs in 2010.

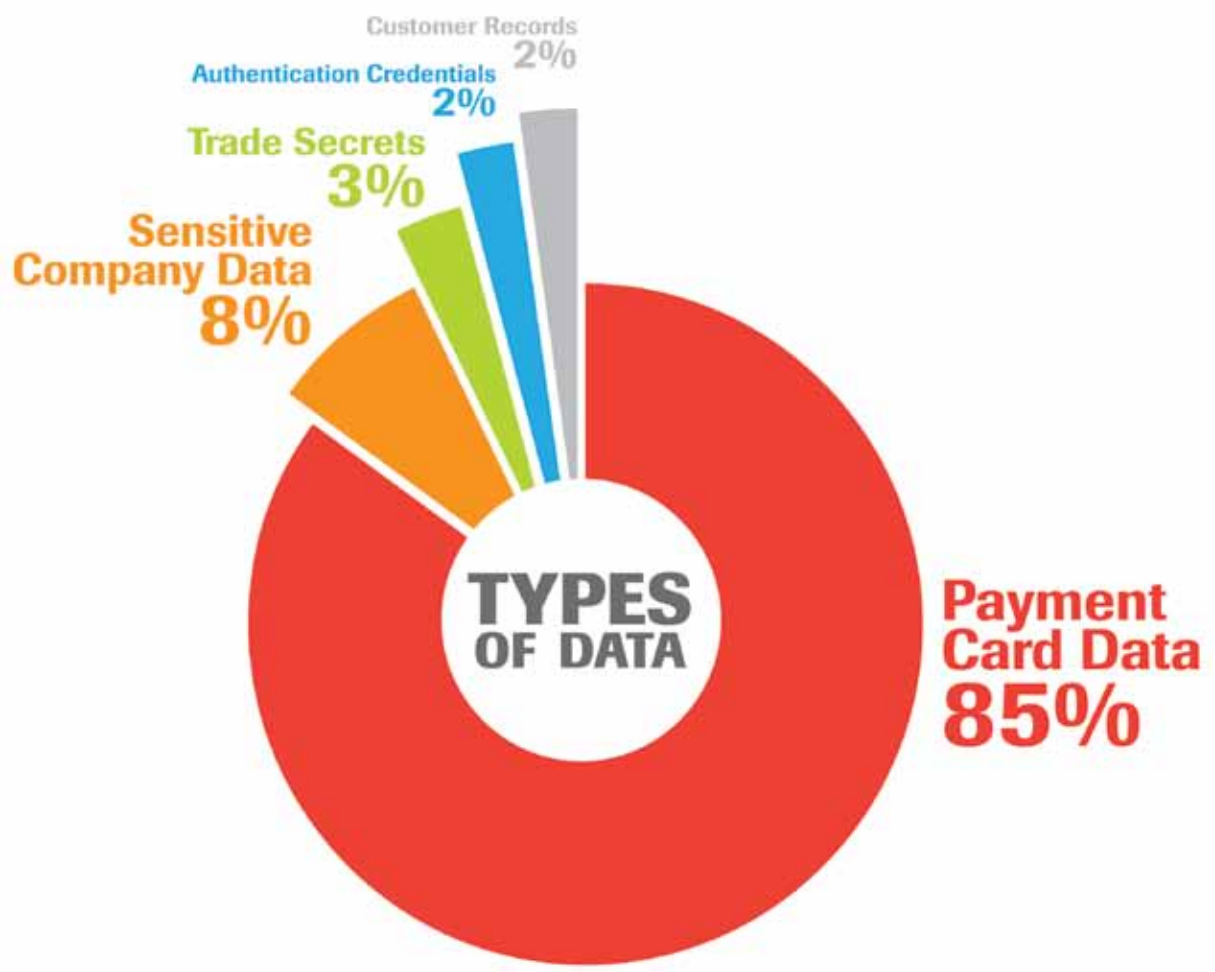
Our customers within the government services industry were on high alert as well. Unlike other industries, obtaining company trade secrets and proprietary information appeared to be the primary goal of these attackers. This industry experienced the greatest threat in terms of attacker persistence and skill level.

Analysis of Investigative Conclusions

Types of Data at Risk

As with prior years, the majority of our incident response caseload consisted of payment card data breaches. The targeting of payment card data is expected, as payment card fraud is an established business, and this data can be easily sold or laundered through established black market networks to realize financial gain.

Additionally, SpiderLabs is one of only a handful of teams authorized globally to perform payment card breach investigations on behalf of the major card brands (i.e., American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.).[1]



While the breach of authentication credentials only accounted for a fraction of our investigations, several of these investigations involved the theft of banking credentials via the ZeuS Botnet Trojan, which resulted in mass Automated Clearing House (ACH) fraud. Botnets are a growing threat and are targeting businesses that utilize computer systems to process financial transactions and governmental organizations with access to classified information. End users with access to public social networks and the ability to install client software packages will aid the operators, through either zero-day (unknown and without a fix available) vulnerabilities or end user carelessness, of various botnets in their quest to build the largest network possible.

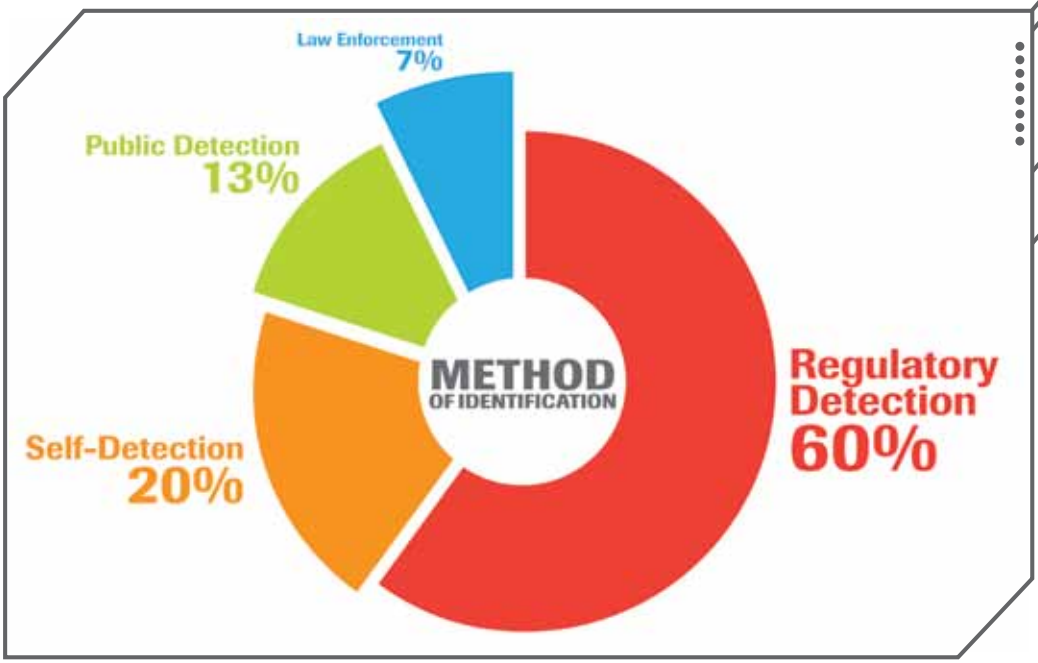
In addition, a joint cybersecurity advisory authored by several State and Federal agencies was released on March 12, 2010. "Information and Recommendations Regarding Unauthorized Wire Transfers Relating to Compromised Cyber Networks" offers more detail about the ZeuS threat encountered in our own investigations.[2]

[1]In 2011, the management of the investigation firms now falls under the oversight of the Payment Card Industry Security Standards Council (PCI SSC) with a newly formed program called the PCI Forensic Investigator (PFI). The SpiderLabs team is one of the first firms to be certified globally to perform PCI forensic investigations in 2011 and beyond.

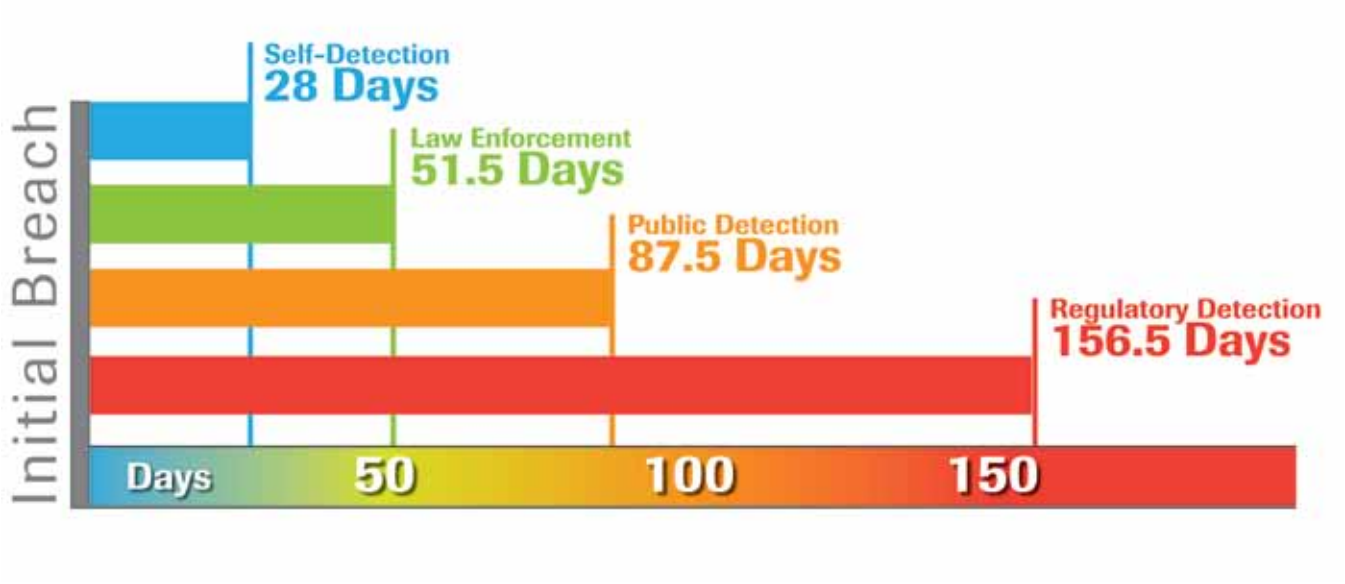
[2]http://www.msisac.org/documents/Wire-transfer-fraud-recommendations-2010.pdf

Detection

Incident response investigations are initiated in a variety of ways. Payment card issuers today utilize very advanced fraud-monitoring systems. When a card is reported stolen or anomalous activity is detected, this information is queried against legitimate payment card usage. Done on a large scale involving millions of transactions, a pattern often emerges. Most cardholders experiencing fraud used their card legitimately at a common merchant, called the common point of purchase (CPP), and this is where the theft of payment data likely occurred. This information is then funneled to the appropriate card brands and the suspect merchant's processing bank, where the bank then initiates an investigation of this business.



In 2009, 80% of investigations were initiated through regulatory detection. While regulatory detection was still the most common method in 2010, a 20% reduction was observed from the prior year. We also observed a modest reduction in the average lapse in time between the initial breach and detection of the incident. In 2009, the average lapse was 156 days. Meaning, the system was infiltrated over six months prior to detection of the incident. In 2010, this window decreased to 125.5 days on average.

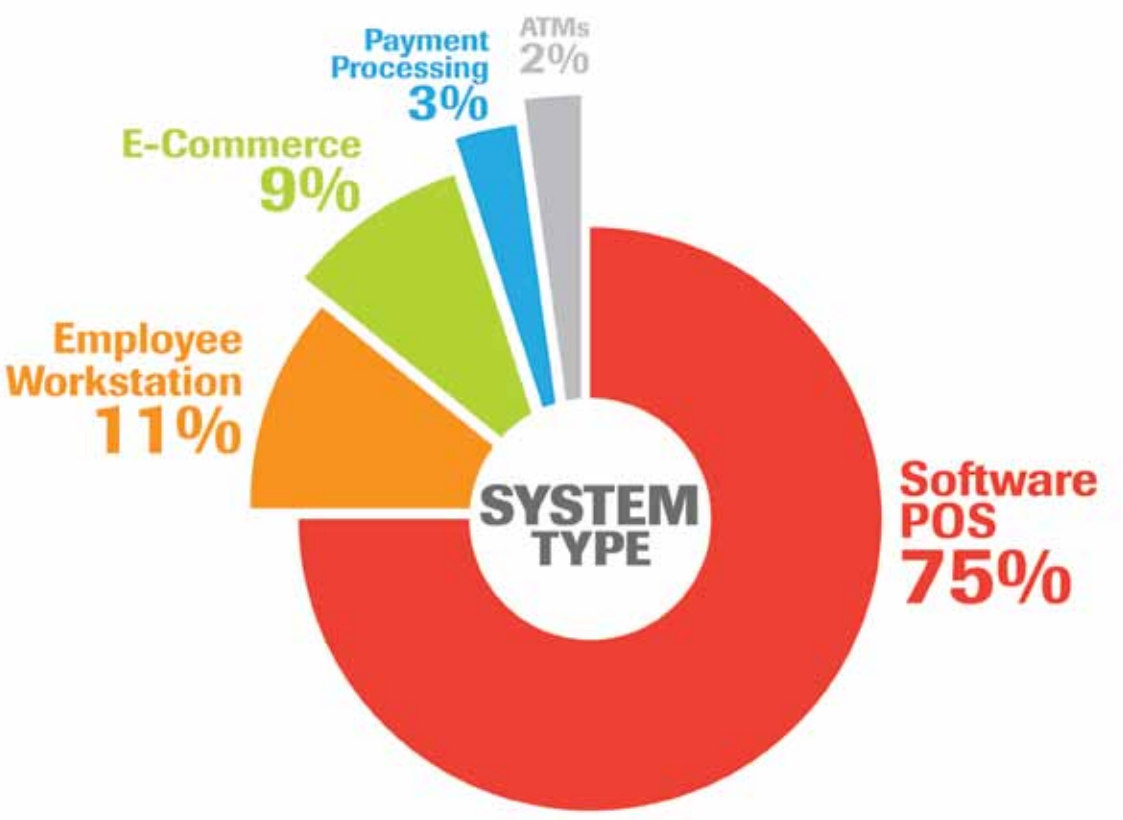


This year, we wanted to take a more detailed look concerning detection methods. Analysis demonstrates that those entities capable of discovering an incident themselves did so within a much shorter timeframe than entities who relied on others to identify the breach. In contrast, those entities that exclusively relied on a third party for detection, or just didn't detect the problem until a regulatory body did, could take up to five times longer to detect the breach. We have found that organizations with mature information security programs that include employee awareness training, regardless of size, are the most successful at detecting a breach.

Types of Target Assets

Software point-of-sale (POS) systems are responsible for the acceptance and transmission of payment card magnetic stripe data. Representing many targets and due to well-known vulnerabilities, POS systems continue to be the easiest method for criminals to obtain the data necessary to commit payment card fraud.

While the Payment Application Data Security Standard (PA-DSS) mandates that developers of software POS systems abide by a strict set of security controls, these controls are rarely implemented properly. Most small businesses investigated in 2010 relied exclusively on a third party for the support of their POS system. In our experience, many POS integrators are often not skilled in security best practices, leaving their clients open for attack. For instance, our investigations often uncover deficiencies in regards to basic security controls, such as the use of default passwords and single-factor remote access solutions. In 87% of POS breach cases, third party integrators used some form of default credentials with either remote access systems or at the operating systems layer. Businesses should work with their third party vendors to help ensure non-functional security requirements are part of the implementation and maintenance agreements.



E-commerce systems were involved in 9% of our cases, consistent with our 2009 report. Often, the public believes they are at greater risk of fraud when shopping online as opposed to a face-to-face purchase. But when magnetic strip data is not available criminals are limited to card-not-present fraud; they can only use the data they obtain from e-commerce attacks against other e-commerce or card-not-present businesses. E-commerce is most often not the primary target in large-scale payment fraud — the data just isn't as valuable.

In 2009, more e-commerce breaches seemed to be occurring within regions that had adopted secure payment card technology, such as EMV (often called "chip and PIN"). But in 2010, investigations concerning e-commerce systems were consistent between all regions and cybercriminals were more likely to target card-present environments. Even countries with EMV mandates were still a target for card-present data compromises, as POS systems for consumers with magnetic stripe-based cards are still in use within those regions.

Payment processing environment breaches were few, but the damage inflicted was severe. Attackers successfully infiltrated payment environments housing the financial transaction switch and related financial application programming interfaces. Highly sophisticated or customized software was used in this type of breach, and there were often multiple tiers of systems, even Hardware Security Modules (HSMs), involved in the transaction process flow. Attackers were able to obtain magnetic stripe and PIN data, allowing direct access to cash through globally coordinated cash-out exercises.

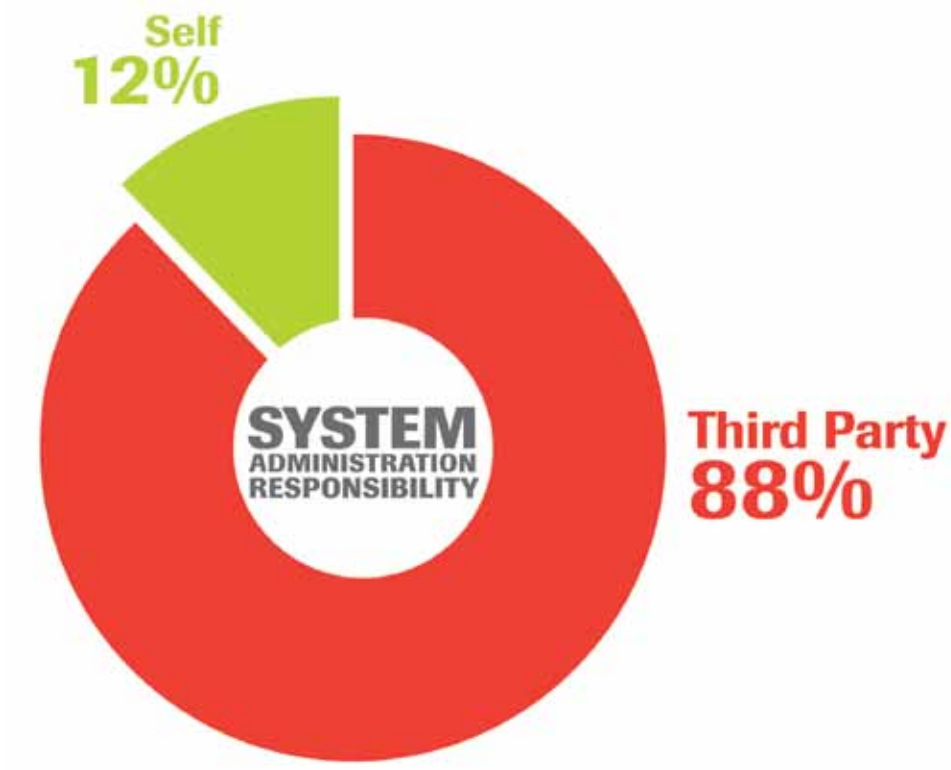
Previously, automated teller machine (ATM) breaches were often the result of hardware tampering, such as the insertion of skimming devices and hidden cameras. In 2010, ATM breaches investigated by SpiderLabs were exclusively the result of the installation of custom, ATM-specific malware. We reported on the initial appearance of this malware in Europe in 2009. Our cases this year suggest new malware authors and new strains of ATM-specific malware in both North and Latin America. This new malware proved to be much less sophisticated than the 2009 versions that were investigated and reported. These were not credential pieces of malware with alternative graphical user interfaces (GUIs), but rather information stealers focused on the physical presence of a USB thumb drive for installation and data retrieval. While these breaches have been limited to specific geographic regions and required physical access to the system, financial institutions need to be aware of this emerging threat. Attackers are working hard to find ways to reduce the steps from data to cash and the ATM is a perfect vector to make this a reality. In 2011 and beyond, we expect to see techniques developed that facilitate network-based malware propagation on ATM networks.

Utilized as a foothold to gain entry into additional systems, employee workstations represent the majority of cases involving the theft of authentication credentials, sensitive company data and trade secrets. Several cases involving employee workstation assets involved the theft of banking credentials via the ZeuS Botnet Trojan. In these cases, the Trojan was delivered via a malicious e-mail attachment sent to the internal employee. Subsequently, banking credentials were captured and mass ACH fraud was perpetrated by the criminals, resulting in the loss of more than $100,000 per company.

The employee workstation is a commonly overlooked security asset and may be more difficult to secure due to volume and mobilitiy. As companies continue to secure the borders of their network, the employee workstation is becoming more enticing as a means to gain entry. More about this attack vector appears in the second part of this report.

System Administration Responsibility

Compromises introduced by a third party increased from 2009; 88% of investigations involved deficiencies such as default vendor-supplied credentials and unsecure remote access applications.



Businesses should first make security requirements for all implementation and maintenance key components of their vendor agreements, then properly validate these partners as skilled in security best practices and compliance requirements. They must also ensure that self-managed security controls are properly implemented and maintained. Rarely is a third party responsible for security of the system in its entirety, but only a subset of controls. Businesses are often not aware of this gap between a third party's responsibilities and the company's responsibilities. Taking advantage of this large gap, criminals easily access and exfiltrate thousands of customer records without the business owner realizing a breach and/or theft has occurred.

The Breach Triad

At its most basic level, a data breach consists of three elements:

BREACH

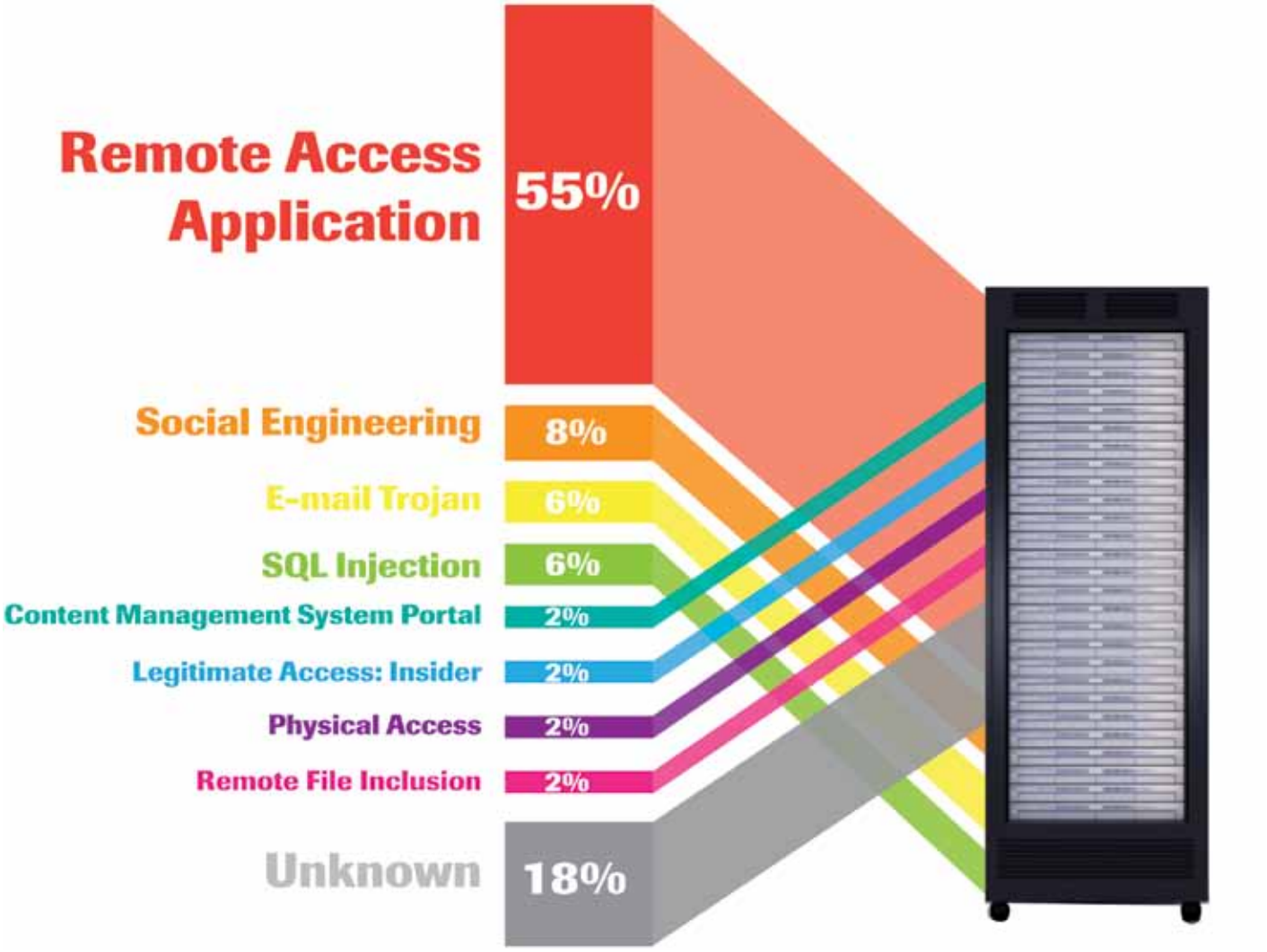
Infiltration
Aggregation
Exfiltration

Only by differentiating between these elements can we begin to clearly understand the anatomy of a data breach.

Infiltration, or Method of Entry

Method of entry can vary and is most dependent on asset type. In 63% of our investigations in which a method of entry could be determined, the attacker simply leveraged an available remote access application. Couple this technique with default vendor-supplied credentials (i.e., logins and passwords) in use on the target system and access is trivial even to the novice attacker.

In many cases, the breached entity was unaware that a remote access application was even present and exposed to the Internet. This was a typical scenario for those entities experiencing a POS system breach in which the third party utilized the application for remote maintenance of the system. In approximately 18% of cases, the method of entry could not be determined, mainly attributed to a lack of evidentiary support due to improper detective and monitoring controls along with nonexistent perimeter security.

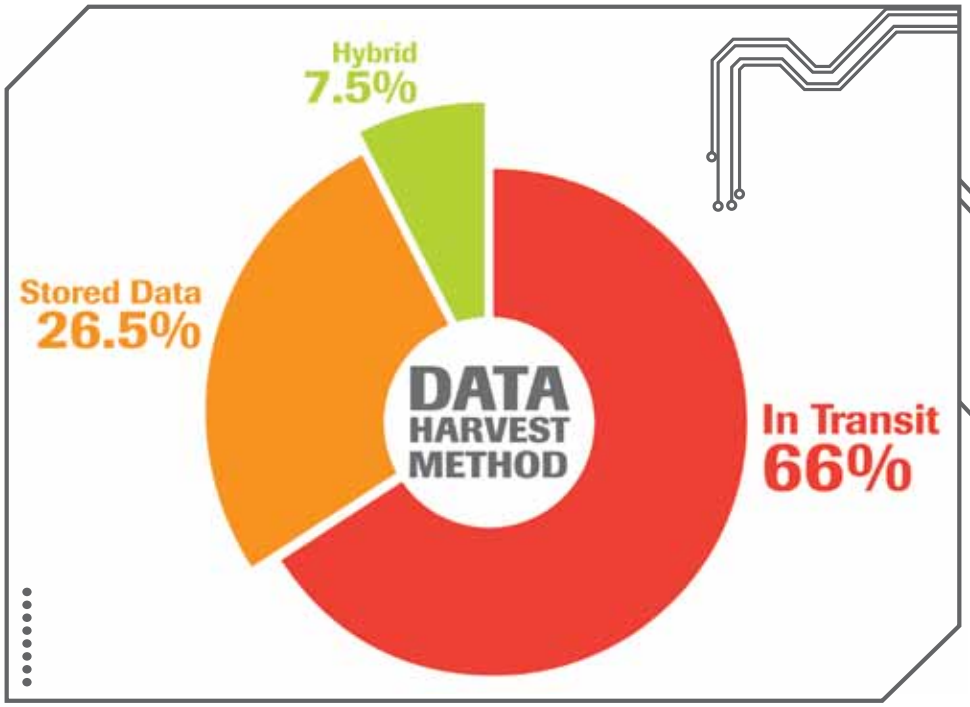


Multiple forms of social engineering attacks were also quite successful in gaining entry to the targeted entity. In many cases, highly targeted phishing e-mails were sent to select employees containing malicious PDF documents. In several other cases, attackers posed as individuals from their IT support company and convinced low-level employees via the phone to install a malicious remote access application on the target system—resulting in system ownership by the attackers.

Even after a decade, SQL injection continues to be the most popular method of entry for Web-based applications; it is a perfect example of attackers only working hard enough to identify a vulnerability affecting many or all payment applications, and then take advantage of it. In 2010, more SQL injection attacks resulting in system-level shell access were observed. Traditional SQL injection attacks typically result only in the extraction of data residing within the backend database. As entities continued to eradicate the storage of unencrypted data within these databases, attackers relied on advanced SQL injection techniques to obtain access to usable data. In most instances, advanced SQL injection allowed attackers to obtain system-level shell access and to then modify Web code to harvest sensitive data during the submission of the data within the Web form.

Propagation

In 16% of cases, the attacker was able to propagate to additional physically dispersed targets through site-to-site internal network connections, such as MPLS. Though the hospitality industry was less represented this year, additional franchised industries experienced similar propagation techniques by attackers resulting in large-scale data breaches affecting multiple locations.



In these cases, many of these multi-location breaches were recently "upgraded" to fully shared connectivity across locations resulting in criminals being able to access many locations at once. Perhaps this was just an oversight in planning by corporate entity IT or security staff; however, a few hours of additional analysis and planning to develop simple network access rules could have prevented this type of propagation.

Aggregation, or Data Harvesting

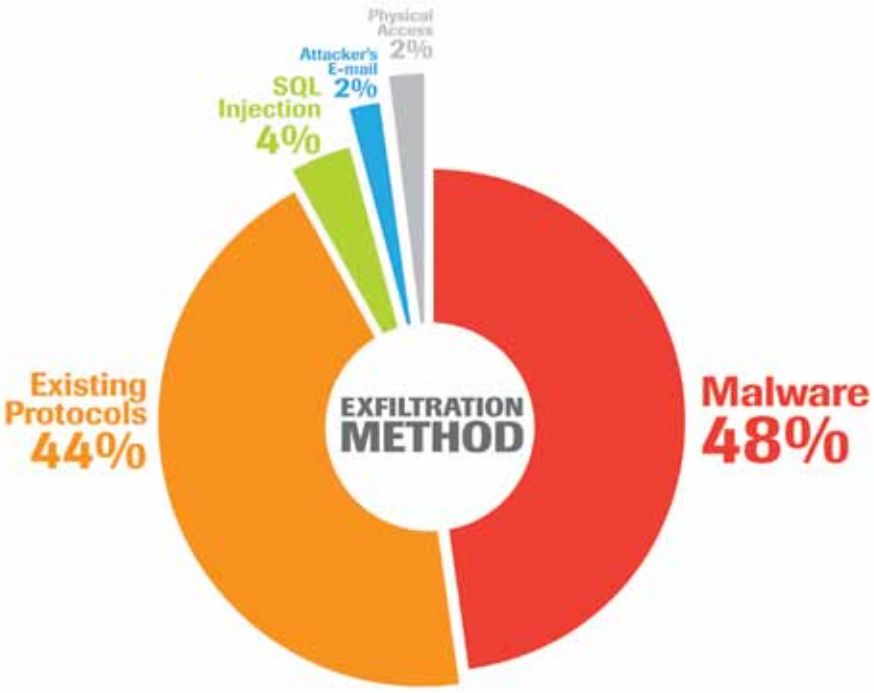
We continued to see a shift away from basic "smash and grab" attacks targeting stored data to more complex methods of data harvesting in transit. There appears to be two reasons for this shift.

First, as various application security standards and regulatory requirements (i.e., OWASP, PA-DSS, PCI DSS) continue to take hold, the elimination of insecure storage practices has increased. Archived data is becoming less available to criminals.

Second, payment card data natively supports a "time to live;" payment card data is only valuable for an established time frame, apparent when viewing the expiration date of any credit or debit card. Archived data is not as appealing as harvesting data in transit. The increased complexity of obtaining real-time data is outweighed by the increased confidence that the data captured with be usable.

In approximately 66% of our investigations, attackers opted to harvest data in-transit, while stored data was only targeted 26.5% of the time. These two methods are not inclusive. In 7.5% of cases, attackers utilized multiple methods to harvest locally stored data, as well as capturing data in transit.

Criminals are continuing to utilize custom or off-the-shelf malware to harvest data from target systems; data-harvesting malware occurred in 76% of our investigations — a 23% increase from 2009. There is a positive correlation between in-transit attacks and the use of malware. In order to capture data in transit, attackers must utilize malware. This is not to say that malware is limited to in-transit attacks. Many of the malware samples involved in our breaches were capable of parsing stored data from disk. We take a deeper look at malware later in this section of the report.



Exfiltration

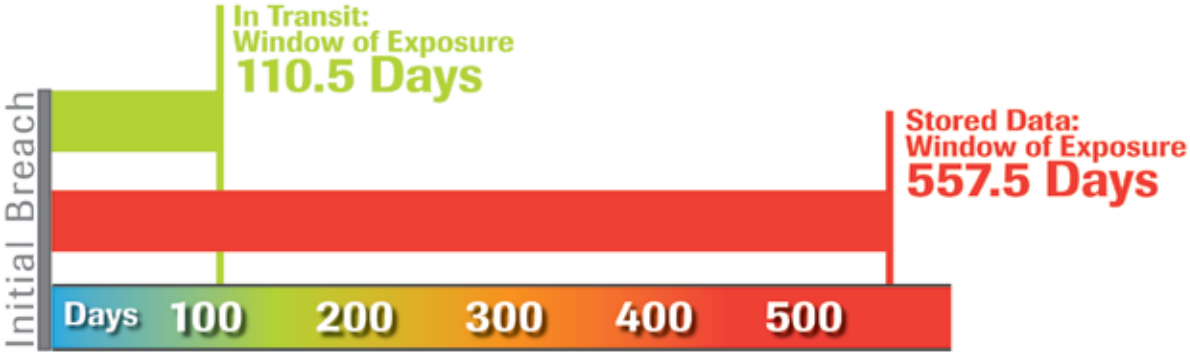
Exfiltration is usually accomplished by copying the data from the system via a network channel, although removable media or physical theft can also be utilized.

Data-harvesting malware is often falsely believed to contain functionality to exfiltrate data from the target system. In 44% of cases where the exfiltration method was determined, however, the attacker exfiltrated via the same method used to enter the environment. Subsequently the malware output file containing harvested data was uploaded using a native application on the target system, such as FTP, HTTP or SMB. Network egress filtering is a security control that restricts the number of routes on a network. This control can help identify unusual activity by performaing traffic volume analysis.

Some instances of data obfuscation or encryption were observed being used by criminals, but more often they exported the data in clear text. Technologies such as data loss prevention (DLP) were not present in any of the environments we investigated. Even the simplest DLP implementation would have flagged sensitive data leaving the victims' networks in the clear.

Window of Data Exposure

A window of data exposure is much more telling than a basic accounting of data records exposed. In our experience, an accurate accounting of compromised records cannot be determined in most cases. This is especially true when the majority of cases involved the harvesting of payment card data in transit. Typically, in payment card data breaches, the payment card data is written to an output file and retrieved by the attacker on a reoccurring basis or in real time if malware exfiltration functionality exists. Therefore, an investigating firm will often only have access to a fraction of the harvested data when the investigation begins.



Recognizing this, the impacted card brands and processing banks do not rely exclusively on an accounting of card data supplied by the investigating firm, but on the window of card data exposure. When this window is supplied, the processing bank can then query their own records to supply all transactions processed during that timeframe. Unfortunately, this process can take months after completion of the investigation. Therefore, the investigating firm is often not privileged to this final accurate accounting of records exposed.

Additionally, if we rely on an accounting of records exposed, small businesses are often not equally represented when compared to larger enterprises. This is especially true when dealing with payment card breaches in which records are

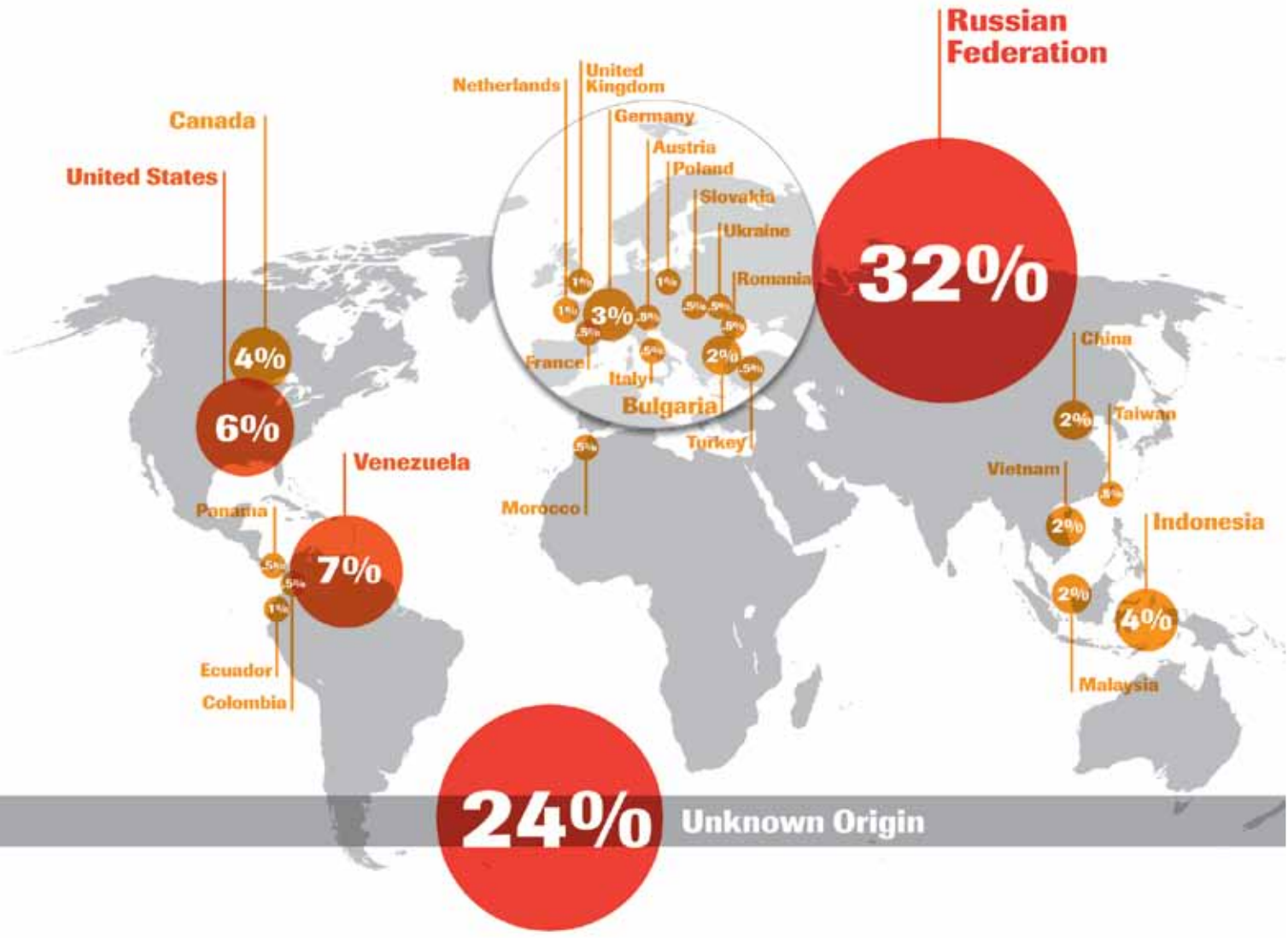
accepted and processed on an ongoing basis. While 100,000 records may represent only a week in terms of exposure for a large enterprise customer, this same amount may represent a year's worth of transactions for a small business. By examining windows of exposure, one trend is worth noting: data breaches involving the harvest of data in transit averaged a window of exposure of approximately 110 days, while breaches targeting stored data averaged approximately 557 days. Similar trends were observed last year and strengthen the argument that the elimination of stored data in a vulnerable form (i.e., clear-text) is instrumental in minimizing the impact of a data breach.

Origin of Attack

Anyone in cybersecurity understands that the process to anonymize origin on the Internet in order to hide source IP address is trivial. Dozens of methods exist to hide a point of origin. For example, attackers can proxy their traffic through various anonymity services, or utilize exploited systems to attack additional targets (i.e., jumpbox).

We cannot exclusively rely on the source IP address as the primary means to establish where an attacker is physically located, however, the origin of attack can still be of value. For instance, the origin can represent a jumpbox, and intelligence regarding the attacker and additional victims can be gathered when this system is analyzed.

It is important to know that our SpiderLabs team often has the ability to gather additional intelligence on the origin of an attacker. We frequently provide various law enforcement agencies with data to assist in apprehending criminals. When appropriate, supplementary intelligence is often shared and this partnership between private firms, such as Trustwave, and law enforcement is instrumental to fight cybercrime.



Payment Card Industry Compliance

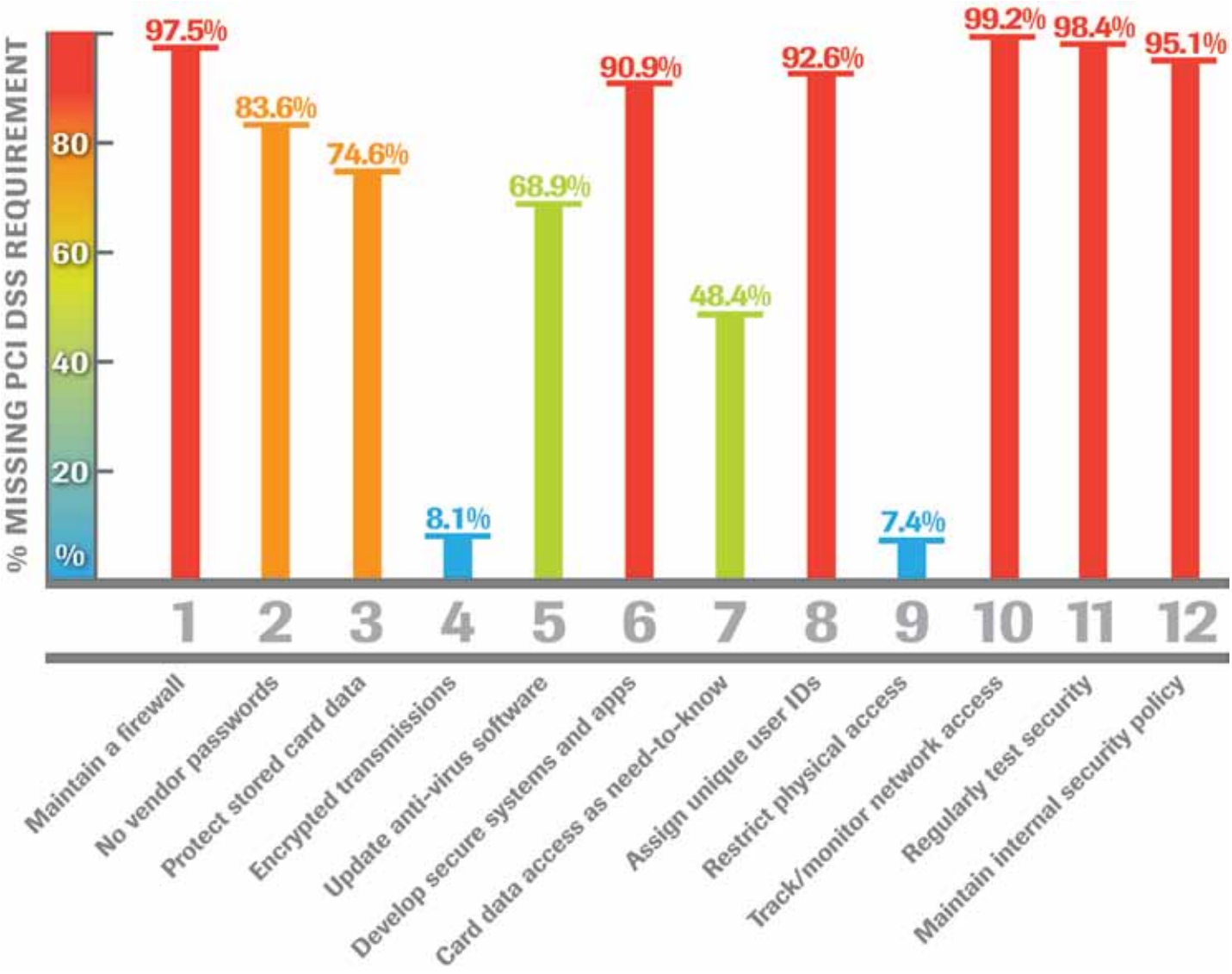
In the vast majority of cases in which payment card data was breached, we observed overwhelming numbers of infractions with PCI DSS compliance at the time of compromise. This suggests that most breaches are the result of mass security deficiencies brought about over time, not a single violation in terms of a specific security requirement.

Many of the entities receiving incident response services believed they had purchased a "PCI compliant" system and that this purchase ensured ongoing compliance. Unfortunately, the term "PCI compliance" is often used incorrectly by those vendors selling products and services responsible for the handling of payment card data.

A properly validated application or system can support PCI compliance when configured correctly, but additional (and ongoing) steps will most likely be required on behalf of the vendor to ensure that the system is properly secured and compliance requirements are met. This misconception is illustrated in the high rate of failure to meet PCI DSS Requirement 1, which mandates the installation and maintenance of a firewall configuration to protect cardholder data.

Breached organizations did not have a firewall policy that properly protected the payment environment at the network border in 97.5% of our cases. Of those organizations, 84% lacked a firewall completely. The lack of a firewall was not usually a deliberate attempt to cut corners, but a belief that the purchase of a "PCI compliant" system was all that was required.

While the merchant is ultimately responsible for compliance, evidence suggests third party integrators are often hindering compliance, observed in the breakdown of Requirements 2 and 8. Time and time again, default vendor-supplied credentials and insecure single-factor remote access solutions are still being used for third party support of the payment system.



Various initiatives have mandated the use of PA-DSS validated payment systems. PA-DSS sets forth to ensure that entities that develop payment applications meet rigorous security requirements, such as elimination of prohibited payment data stored within merchant and processor environments.

Despite these mandates, 48% of compromised entities were not utilizing PA-DSS approved systems. While PA-DSS validation helps to ensure that the payment system does not store restricted card data, 43% of systems running PA-DSS validated applications were found to contain restricted cardholder data. In many of these cases, the system was not storing restricted data for current transactions, but was storing archived data that was not scrubbed properly upon upgrade to a validated version. Integrators must ensure their upgrade methodologies sufficiently remove archived data when upgrading a non-compliant version to a compliant version.

Malware Statistics

Introduction to Malware Attacks

Until the early 1990s, malicious software, or malware, was considered more of a prank or a proof of concept (PoC) software program than a tool to be used for data theft. The landscape has changed dramatically in the last twenty years. Global Internet access, increased broadband connection accessibility and the emergence of the Internet as a business platform brought many entrepreneurial individuals online, some of whom chose to make their money by stealing it.

Using malicious software is a natural progression for cyber attacks. In the real world, a bank heist is a one-off job; breaking into a bank and then staying there for an extended period is just not feasible. Bank robbers steal money and then attempt a fast getaway. The cyberworld is completely different. A long-term, steady flow of stolen cards from a compromised environment is highly lucrative. The PCI DSS requirements attempt to enforce very specific rules on all the stakeholders in a transaction process; the cardholder data (in a compliant implementation) is no longer stored on the systems for longer than necessary. The only way for attackers to obtain data, then, is to look at the transaction flow and sniff the valuable information as it is being processed.

The attackers' approach resembles the "just-in-time" strategy. The advantage of stealing "data in transit" is that the extracted data is always fresh, whereas in the "smash and grab" attacks, attackers have to verify the validity of card numbers.

As malware started to be used for cyber attacks, the makeup of malware developers also changed. Malware is now developed by a single individual with access to endless Internet resources or a team of such individuals. We have also observed increased modularization of malicious components combined into deployable kits. Such kits allow anyone from a skilled attacker to a novice to install and operate a botnet.

Analysis of malware observed during SpiderLabs' investigations shows interesting patterns. Generic, widespread malware is slowly becoming more customized, one-off pieces of software — a trend that is challenging the foundation of the anti-virus industry. The ease with which one can create a variant of malware that is undetectable by anti-virus companies is well-known. The less often discussed issue is the fact that attackers do not always rely on custom code. Samples we have uncovered in compromised environments are often unmodified, off-the-shelf key logging products that can be easily found and purchased online. The compromised systems often use leading anti-virus solutions with the up-to-date virus definitions but most custom malware cannot be categorized as viruses or Trojans.

Malicious software frequently employs techniques to extract data known from "normal," legitimate operations that are similar to what an application developer would use. One example could be sniffing of the data across the network; such operation is carried out by many IT administrators who want to understand and test their networks. The attackers use this technique to intercept data that is moving from POS terminals to a back-of-house (BOH) or back office processing server.

Another example is the memory dumping attack similar to a technique used by Microsoft Windows Operating System upon application crash. The goal is to preserve the memory and the state of the application in order to analyze what caused the crash. Malware can't be easily flagged by traditional anti-virus because it is targeted and the techniques used are similar to those used by system administrators to troubleshoot networks and systems. It is impossible to write a generic detection for a snippet of code that can be represented in many ways and may also be used for a legitimate purpose. On the other hand, there is always a potential for behavioral detection, something that in many ways is more accurate than traditional anti-virus against targeted malware attacks. Until behavioral detection tools are widely available, organizations should consider implementing a method of base-lining end point security through software white listing, enforced software restriction policy and file system integrity monitoring.

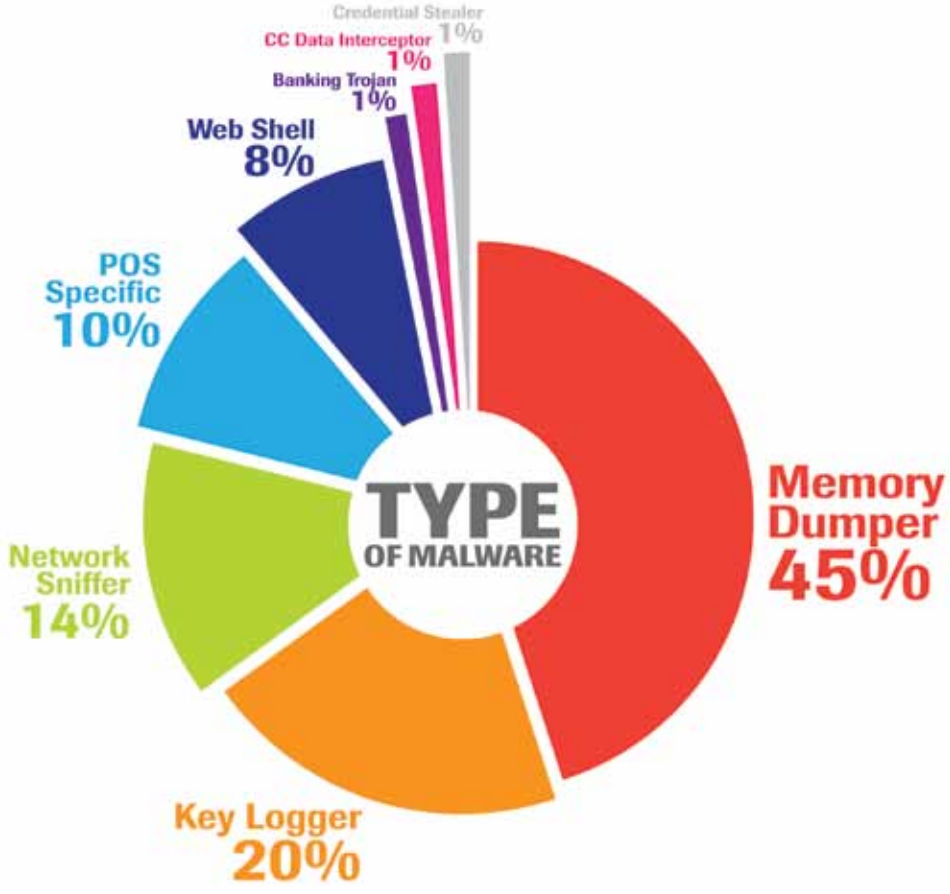
Malware: Data Points of Interest*

In 2010, memory parser malware led the way, accounting for 45% of all malware investigated by SpiderLabs. Keystroke logging malware and network sniffing malware came in second and third, respectively. A keystroke logger intercepts data as it is being entered at a computer terminal via the keyboard, touch screen or external data entry device (i.e., card reader). A network sniffer is a device or software application that listens to traffic on a network much as a phone tap listens to verbal conversations.

New malware uncovered in 2010 was a POS application-specific malware. The POS-specific malware is the most sophisticated malware we have seen, and similar to the ATM malware we saw in 2009, as it requires deep knowledge about the workings of the POS application. The ATM malware, also called credentialed malware, is multi-user malware with the ability to control access to various functions using a method of authentication, typically a physical token, like an ATM card.

SpiderLabs found that two different POS applications were targeted with the new malware. For one of those applications, attackers identified its data decryption algorithm and used that method to extract encrypted data from the system.

Web-based malware made up 8% of investigations. Use of Web-based shell (Web malware) to extract data was one trend evident in e-commerce breaches. Custom Web shells were made specific to victims' database schema to extract the temporary data kept in the database for returns/order modification purposes. Attackers wrote custom code to extract data from those temporary tables at regular intervals. SpiderLabs also encountered a few types of banking malware targeted at gaining credentials of financial sites, and introduced through social engineering methods.



Development Platform

Most malware SpiderLabs uncovered in recent years was written in popular high-level languages, such as in C, C++, Delphi, Perl and .NET. Code was often compiled with very old compilers (circa 1991-2001), suggesting attackers habitually reuse code or modify existing malware. The multiple technologies employed by attackers in their malicious creations show the code to be relatively low quality and give the impression that it was copied and pasted from another source. We sometimes saw advanced creations, but as with "mainstream" malware, these made up a very small percentage in a pile of copycat code.

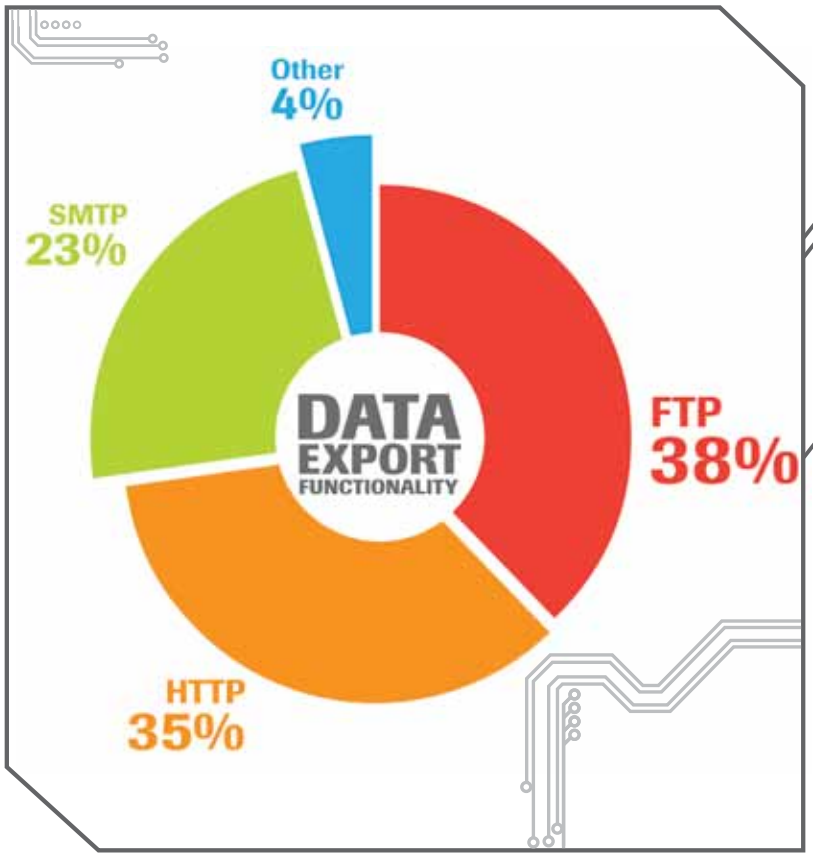
Propagation Functionality

Traditionally, malware authors implement a propagation mechanism in their programs so they can infect a single or small number of systems and then observe how it spreads from afar. This is not the case for payment card malware. The simplest examples of payment card-targeting malware enable a debugging mode of the POS application through modification of a single file to force the applications to log sensitive data. Other malware is often limited to specific functionality, for example, to sniff data from the wire, parse for track data and save it to a file. The need for spreading or mass-infection does not exist since the attackers "own the box" and because propagation mechanisms could generate events indicating security incident activity. The only propagation mechanisms SpiderLabs observed thus far is a distribution via insecure patch management.

* For a taxonomy of software tools, see Appendix A: Tool Description.

Data Export Functionality

About 48% of malware had automated exfiltration features. File Transfer Protocol (FTP) was still the top exfiltration method used by malware; about 38% used FTP functionality. Many organizations are conscious of ingress filtering, but have not widely adopted egress filtering. Simple Mail Transfer Protocol (SMTP) (an e-mail protocol for sending messages) was another prominent way to export data; about 23% of malware used an SMTP server to send data.

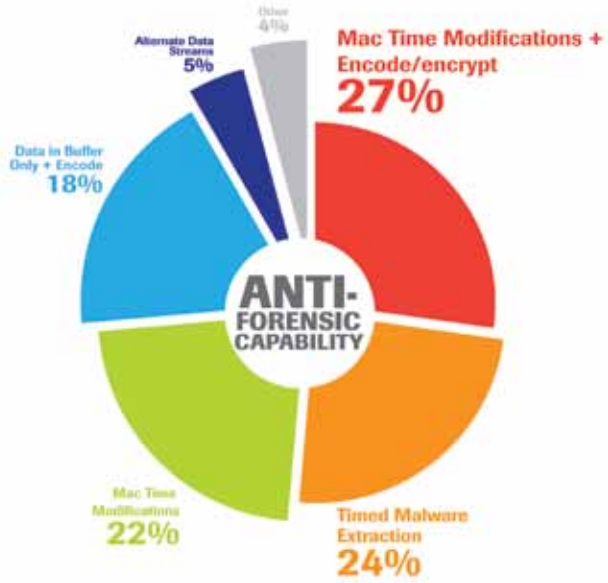


The emerging method in 2010 was exfiltration of data via HTTP; 35% used HTTP as the exfiltration mechanism. Significantly, even the more mature security organizations allow outbound access on Web ports, such as TCP port 80 (HTTP) and TCP port 443 (HTTPS). Substantial Web traffic occurs on most networks, so analyzing Web traffic for malware output is not an easy task, especially if the malware sends encoded or encrypted data via HTTP. Some malware investigated by SpiderLabs had built-in features to encode the data before exporting it via HTTP.

Compared to last year, SpiderLabs did not see network shares for data exfiltration, perhaps because many organizations now close those ports on the firewall. An interesting pattern was evident in the exfiltration of data via Remote Desktop Protocol (RDP) access. This exfiltration is facilitated by a supplementary malware which functions only when there is an established RDP connection by the attacker. With this connection from the attacker's to the victim's system, the attacker can mount their local drive to the victim's system and then copy the data as if the copying occurred in the internal network or attached storage devices.

Anti-Forensics Capability

In the past year, malware development has made leaps and bounds over 2009. Astoundingly, 45% of malware had at least one anti-forensics feature, if not multiple. About 27% of the malware had file time modification features to deceive the investigators and system administrators. Out of this 27%, 12% of the samples included a data encryption feature.



Malware with hidden features and binaries appeared in about 24% of cases; this malware would be revealed at a specific time, usually in the middle of the night to avoid close monitoring. The unpacking of additional malware executable code at a certain time and then immediate deletion was an interesting development.

About 45% of the malware with anti-forensic capability had encryption or encoding features to attempt to elude intrusion detection systems and data loss prevention (DLP) software.

Malware with a feature for storing output data in a buffer only, thus no storage on disk, occurred in 18% of these samples; common searches for sensitive data by investigators would fail to detect the malware output. Even the data in buffers was encoded to defeat RAM analysis.

In addition to these major techniques, obfuscation of malware and malware running code in alternate data streams was also observed.

These anti-forensic features of malware make memory analysis a must for all data forensic investigators. Anyone who is using old techniques is simply missing all of the action in today's malware attacks.

Beyond Counterfeiting Cash:
The US Secret Service

As the original guardians of our nation's financial infrastructure, the U.S. Secret Service was founded in 1865 to investigate and suppress counterfeit currency. Over the years, the authority of the Secret Service has expanded, and the scope of the agency's investigations has grown exponentially. Today, the Secret Service's expertise and approach to investigating financial and cyber-related crime is recognized worldwide.

In 2001, by the enactment of the USA PATRIOT Act, the Secret Service was mandated to establish and maintain a nationwide network of electronic crime task forces (ECTFs). This legislation recognized a Secret Service philosophy, learned from the organization's protective mission, that success resides in the ability to bring partners, such as academia, law enforcement and private industry, together. The goal of the ECTFs is to establish, promote and continue these robust public/private partnerships based on the Secret Service's historic strategic alliances with federal, state and local law enforcement agencies, private industry and academic institutions. The ECTFs respond, confront and suppress cybercrime, malicious uses of cyberspace, and threats to cyber security which endanger the integrity of our nation's financial payments systems and critical infrastructure. Currently, the Secret Service has a total of 31 ECTFs, 29 domestic ECTFs and two overseas, in Rome, Italy and London, England.

To further combat the growing scope and volume of Internet-related crimes, the Secret Service established a proactive investigative and support element of the Criminal Investigative Division: the Cyber Intelligence Section (CIS). This section is comprised of special agents and intelligence analysts who focus on investigating and preventing cyber attacks. CIS serves as a central repository for the collection of data generated through a three pronged approach of media collection, proactive investigations and partnerships.

In 2007, the Secret Service partnered with federal, state and local agencies to create the National Computer Forensics Institute (NCFI). This facility trains state and local law enforcement officers, prosecutors, and judges in the field of cybercrime and computer forensics.

Special agents and ECTF partners have achieved success in investigating a wide variety of financial and cybercrimes, including but not limited to: network intrusions, botnets, phishing, skimming, identity theft, access device fraud, bank and wire fraud, copyright offenses, violations of the CAN-SPAM Act, and the use and deployment of malicious software.

In fiscal year 2010, the Secret Service arrested more than 1,200 suspects for cybercrime violations, associated with more than $500 million in actual fraud loss. These cases prevented approximately $7 billion in total losses.

The tactics employed by the Secret Service are unique and largely centered on exploiting vulnerabilities associated with the cybercriminal community. In order to identify these vulnerabilities Secret Service investigations are consistently devised to penetrate, disrupt and dismantle the greater cybercriminal community infrastructure.

Over the past decade, the Secret Service successfully investigated some of the biggest cybercrime incidents in this country, including Operation Firewall, which dismantled a major English language carding portal, the LexisNexis data theft investigation, the E-Gold digital currency investigation, and the TJX and Heartland Payments Systems investigation. According to the U.S. Department of Justice, the Heartland investigation was the "biggest identity theft case ever prosecuted in the United States."

The agency's continuing effort to investigate cybercriminals also extends to those in supporting roles. An example of this would be the Secret Service's investigation of those in the financial cybercrime "supply chain." The agency continues to target the people or organizations that provide services such as illicit online hosting companies, malware developers/providers, stolen data distributors as well as those that compromise point of sale systems. To properly investigate these cases, the Secret Service must have the cooperation and assistance of the victims and private sector partners. Working together, all parties achieve positive results in targeting, arresting and prosecuting these attackers.

The Secret Service continues to partner with private industry to identify current trends in network vulnerabilities. Further, the Secret Service has prevented data theft by providing intelligence recovered during criminal investigations to victim companies in order to mitigate exposure of network assets.

— Kenneth Jenkins, Special Agent in Charge, Criminal Investigative Division

Attack Vector Evolution

Introduction

Nearly two-thirds of Trustwave's SpiderLabs team is responsible for penetration testing. While the security market trends towards the placement of automated penetration test technology, and while we believe automated technology has a place in a strong security strategy, our methodology still primarily relies on manual testing by seasoned security professionals. Our clients demand we attack their environment with the full force and determination that a motivated criminal would use, and we comply, in order to provide the best view of their risk to compromise.

In 2010, we performed more than 2,300 penetration tests in all of the top 20 GDP countries, as well as many others. In reviewing the results, we observed that various attack vectors being used by criminals today fell naturally into categorization by decades of time. While hacking of phone systems, first, and computers later, has been in the mainstream since the 1970s, we begin our review of attack vectors in the 1980s. Between the 1980s and today, sensitive and private business information began to hemorrhage through attack vectors introduced by technology innovations. Unfortunately, for all the effort and emphasis placed upon information security, new attack vectors keep cropping up before older, existing ones can be locked down.

How the Decade Sections Work:

In each decade section, attack vectors are highlighted by the decade in which they were most often utilized:

1980 Physical
1990 Network
2000 E-mail, Application, Wireless
2010 Client-Side, Mobile, Social Networking

In addition to an introduction about the attack vector or vectors, each section also includes:

Top 10 Methods of Attack for 2010 within the Vector

- Business Impact
- Percentage of Attacks for 2010
- Percentage Increase or Decrease from 2009 Data

Attack Visual

Known Incidents from 2010

Topical Essay

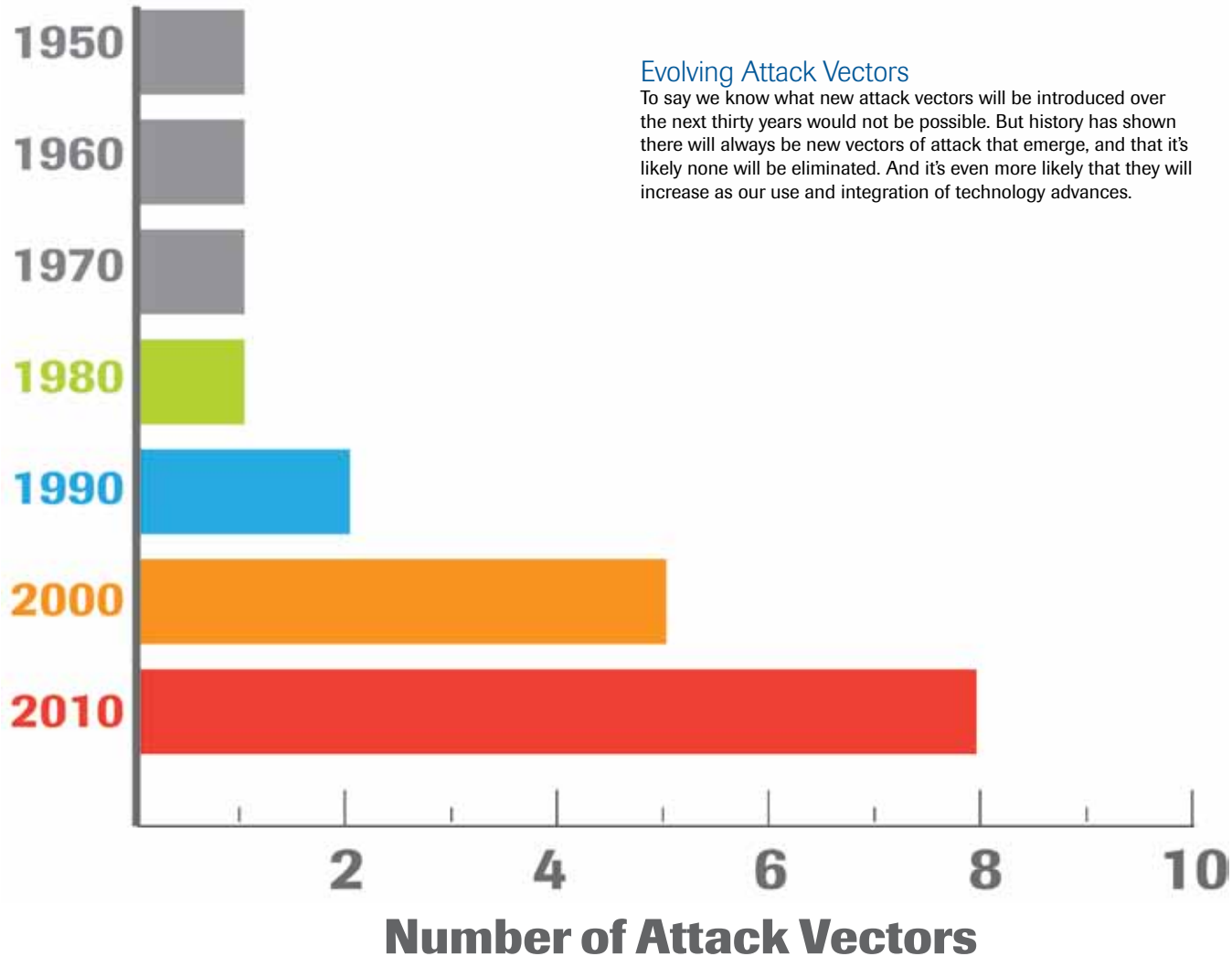
In the 1980s, data and information were most often communicated via media such as print, radio, television and film. The postal service was used to exchange business documents; memos were typed and filed in cabinets. People went to the bank to make a deposit or withdrawal, and they used the telephone to talk with colleagues and business partners. While cybercriminals were well on their way towards learning how to form attacks and commit computer fraud, businesses were still most vulnerable to attack against their information assets via physical means.

The world changed in the 1990s. The information super highway was born and everything and everyone went "online." While most businesses invested in connectivity and access for their employees, security was an afterthought; it wasn't until the late 1990s when organizations started to invest in people, processes and technology to reduce their risk to compromise. The defining moment within this decade were the release of tools called Netbus and-

Back Orifice by a Swedish programmer named Carl-Fredrik Neikter and the hacker group known as Cult of the Dead Cow (cDc) respectively. These tools, coupled with network vulnerabilities, allowed an attacker to control a victim's computer over the Internet. Functionality included being able to read files and see desktop activity, along with other detrimental activity. Networks as an attack vector became a much sought-after target throughout this decade.

By the start of the 21st century, many industries were taking advantage of productivity gains offered by online connectivity, and e-mail became widespread for personal and business use. It was in this decade that the idea one could form an entire business around an application accessible by the internal and private business network, as well as the Internet, came into popular practice. Three attack vectors gained prominence: e-mail, application and wireless.

All five attack vectors—physical, network, e-mail, application and wireless—have been used in varying degrees over the last three decades. Until 2010, the majority of all data breaches were only perpetrated via one of these five vectors. But as the richness and the availability of bandwidth to people all over the world increased over the last decade, so has the richness of the content and applications utilizing these networks. When complexity is added to any client-side application, browser or viewer, the attack surface increases for someone to find an exploit that can be performed against the end user. As we have moved away from desktops and laptops to mobile devices and tablets, the security principles developed and enforced over the last two decades were forgotten or ignored. Privacy, once coveted, is decreasing with the advent of social media tools. Intent on accessing private data, the new attack vectors from 2010 are none other than client-side, mobile and social networking.



Evolving Attack Vectors

To say we know what new attack vectors will be introduced over the next thirty years would not be possible. But history has shown there will always be new vectors of attack that emerge, and that it's likely none will be eliminated. And it's even more likely that they will increase as our use and integration of technology advances.

1980s

Physical

Physical security and the attacks against it have likely been around since the dawn of humankind. Predominant in the 1980s, today these attacks take advantage of a weakness in the protecting technology or a gap in protection measures surrounding the assets. Many physical attacks are easy to successfully execute, some even used by authorized individuals as workarounds to gain speed and efficiency. A successful physical attack exposes data, equipment and other physical assets to theft, damage, espionage or sabotage.

Physical security is returning as a more common attack vector since companies are more focused on becoming proficient at securing their network access from remote areas, such as the Internet. For a determined attacker, physical access is now the path of least resistance, and more likely to be successful with less time and effort.

Successful exploitation can involve an immediate loss of assets and data, and can also lead to new back doors into facilities and network access points created by the attacker for continued use. By using a variety of affordable devices, or "leave behinds," an attacker can maintain access to a network or a facility for as long as it takes a target to realize that their physical security has been breached.

Method	Description	Business Impact	% from 2010	Change from 2009
1 Sensitive Data Left in Plain View	Employees leave sensitive data on their desks, taped to a computer monitor or otherwise in plain view.	Anyone walking through the office (friend or foe) can access sensitive data, including passwords and personally identifiable information (PII).	15%	↑
2 Unlocked and Otherwise Accessible Computer Devices	Workstations not locked when unattended could provide unapproved access to the internal network and password files. This includes laptops and other mobile devices not properly secured when outside a facility.	Unlocked devices could be used to infect the internal network with virus or worm traffic or, in a targeted attack, allow the attacker to place malware (i.e., key loggers, connect-back shells) for later access to the corporate network. Stolen laptops and other mobile devices can give attackers access to sensitive information as well.	13%	↑
3 Sensitive Data Cabling is Accessible from Public Areas	In an otherwise secured building, cabling for the private data network runs through accessible wall panels or ceiling tiles of public areas, such as hallways or public restrooms.	An attacker entering the public area can tap into the private data network by moving a wall panel or ceiling tile, possibly resulting in compromise of the internal data network.	11%	↑
4 Physical Security Device Management Systems	Larger buildings maintain and monitor physical assets, including door access, camera recording and control, and HVAC systems.	Due to lack of patches or use of default passwords, attackers can remotely monitor a building through video camera feeds, open doors and read access logs. Other possibilities include disabling alarms, HVAC control and elevator control. Compromised systems results in partial or complete physical control of the facility by an attacker, usually remotely via the Internet.	11%	NEW
5 Security Camera Placement and Monitoring	Either the placement of security cameras leaves a gap in coverage, or the coverage is complete but too many cameras make it difficult for staff to monitor properly.	A gap in camera coverage can allow an attacker to perform malicious actions without being noticed or recorded. Too many cameras will record the actions taken, but will not be noticed until well after the attack has occurred, if at all.	10%	NEW
6 Lack of Plate Covering Gap from Door Latch to Strike Plate	Electronic locks require a proximity card or other authentication means to release a magnetic retainer in the strike plate to open the door. If the latch is accessible through the door gap, the lock can be bypassed with a stiff card or needle nose pliers.	The lack of a cover plate over the latch and strike plate could allow an attacker to bypass an electronic lock and open a door in a matter of seconds. For only a few dollars, a simple steel plate can mitigate this.	10%	↑

7	Motion Sensors to Allow Egress from Highly Sensitive Areas	Electronic locks that require a proximity card or other authentication means sometimes entail a motion sensor used to automatically open the door upon leaving that area. A coat hanger, balloon, piece of paper, or other materials inserted through the door gap on the secured side can trigger the motion sensor on the other side.	This could allow an attacker to bypass an electronic door lock and access a secured area.	6%	
8	Motion Sensors Mounted Incorrectly Creating a Zone of No Coverage	Motion sensors have certain ranges where they can detect a moving object. A sensor mounted incorrectly may cause a significant gap in coverage where it will not detect motion.	This could allow an attacker to bypass triggering an alarm system and gain access to a highly sensitive area.	8%	
9	Dumpsters are Accessible and Unlocked	Employees do not always follow policy for discarding sensitive documents and some organizations do not have these policies in place at all.	Information such as financial records, ID photocopies, canceled checks, signatures, network diagrams, passwords, and other sensitive data could be stolen, and data and systems compromised.	8%	
10	Bypass Route from the Public Area to the Secured Area is Available	An organization may have locks on all doors and in/out access control; however, there may be a path that leads from the unsecured area into the secured area that bypasses the locked doors.	This could allow an attacker to bypass an electronic door lock and access a secured area.	4%	

Known Incidents from 2010

Loss of 46,000 Customer Records

In August 2010, Zurich UK received a £2.28 million fine from the Financial Services Authority (FSA) for losing a disk containing customer information. The loss occurred when one of Zurich UK's contractors, Zurich Insurance Company South Africa Limited (Zurich SA) lost an unencrypted back-up tape during a routine transfer to a data storage facility. The back-up tape included customers' bank and credit card numbers, and details about insured assets.

Although the actual incident took place in 2008, the lack of a proper reporting structure lead to Zurich UK not learning of the incident until a year later. The fine levied against the company in 2010 is the highest fine levied in the UK against a single firm for a data security compromise. This particular case underscores the importance of hard drive encryption, not just for workstations and laptops, but also for every device that will contain the sensitive information of a company or individuals.

Corporate Network Compromise

A lobby or other entrance area is commonplace for many businesses and almost any person is able to gain access to it. When a building is constructed, network and power drops are often located in these areas. During an authorized and controlled physical security test, a SpiderLabs team member entered a facility's lobby carrying a newspaper. They were left alone while reading the paper. When the reception desk employee was distracted, the team member removed a small PC, the size of a power plug, and connected it to the power and network sockets located next to the chair he was in. After leaving the facility, this SpiderLabs expert was able to connect his laptop to this PC. From that connection, they broke into the network, utilizing common network-based attacks and vulnerabilities. Over the course of two hours, our expert was able to gather logins and passwords, read corporate e-mails, and harvest sensitive customer data.

A true attacker would not always take the precautions that our SpiderLabs team member did, such as securing the wireless connection. This type of attack would not only allow the primary attacker access to the corporate network, but also anyone else in the area that stumbled across the wireless connection.

While a common problem, situations such as this are easily resolved. With proper camera coverage and monitoring, a SpiderLabs' expert's activities would have been noticed by security, even though the receptionist was otherwise occupied. Additionally, proper access controls on the network access port would have prevented a successful network connection for the left-behind PC and denied the SpiderLabs team member access to the data he gained through the course of the test.

Loss of Corporate and Private Assets

In May 2010, a lone thief broke into a Paris art museum in the middle of the night and stole five paintings worth hundreds of millions of Euros. Multiple physical security failures were discovered during the investigation:

1. A weak padlock on a gate was easily broken by the thief.
2. The alarm system had not been working for multiple weeks and was simply not turned on.
3. A low-level window was smashed by the thief and used as his entry and exit point.
4. The three security guards monitoring the CCTV system were never alerted to the thief during the course of the theft.

As concerning as it is that no alarm ever sounded, bypassing alarm systems, even when turned on, is not an impossible feat. However, the thief was not cautious and was caught on multiple security cameras during the heist. While at least three security guards are on staff at all times in this museum, none saw the thief in the video footage until the next morning when the video was being reviewed for evidence.

If a proper monitoring system had been in place, even with the alarm being turned off, security guards would have witnessed the thief on camera in the act of stealing. When trying to actively monitor a facility with large numbers of cameras in place, it is important to take advantage of motion sensing software. When this software is in place, instances of motion are brought front and center to the monitor's attention immediately, instead of the commonplace cycle rotation of camera views.

Improperly Monitored Security Cameras Can Lead to Data Theft

Conclusions

Physical security attacks are on the rise. As new solutions for network and application security are introduced to deter and detect attempts against those vectors, attackers are beginning to switch to the path of least resistance. Much time and money has been spent on securing the IT infrastructure, and physical security has slowly faded into an afterthought, allowing for weak implementation of new solutions and poor maintenance of existing ones. Attackers are discovering that the risk, time and effort involved in exploiting the physical weaknesses are currently lower than the other vectors, and the payouts are just as high, if not higher.

Advantages and Disadvantages of Security Convergence

The term security convergence refers to the combining of two security functions inside companies that were maintained separately in the past (physical security and information security). Security convergence evolved from the realization that information-based assets are increasingly critical to organizations, and that there is a need for these assets to be protected physically as much as they are logically. An industry organization called The Alliance for Enterprise Security Risk Management (AESRM) has been formed by ASIS International, Information Systems Security Association (ISSA), and Information Systems Audit and Control Association (ISACA) in order to help advance the adoption of security convergence by more businesses.

Advantages of Security Convergence

Management systems for logical security are already in use at a large number of companies, providing a single point for the operation, administration and provisioning of information assets. In a security convergence scenario, these types of systems would place the physical security operations and systems under the same area of capabilities already provided to the information systems. This merging would create a time and cost-saving advantages for a company, as well as a more secure corporate environment.

In a security convergence scenario, when an employee is hired, they might receive a single physical access card. This card maintains physical access to facilities and is the second factor of authentication for logging into systems, applications and remote access devices. This same card could also provide two-factor authentication for mobile corporate assets, such as laptops, ensuring a higher level of security when used outside the company. This situation allows for the rapid removal of both physical and logical access in the event of the employee leaving voluntarily or forcefully.

In the event of a physical or network breach alert, both physical and logical access logs can be reviewed in sync to ascertain exactly how far the intruder went. This helps form a more complete risk assessment of the situation and the potential damage. Furthermore, a security convergence investment can provide additional capabilities and decrease the time used for daily tasks.

Disadvantages of Security Convergence

Certain issues should be considered when deciding whether or not to adopt this type of security approach. One issue that has prevented some companies from moving forward with security convergence is a single point of failure. For example, the introduction of a virus in a network may not only cause network and server problems, but can also affect physical security, and users may experience difficulty with something as simple as physically entering their offices. In the event of a network breach, control of certain networked assets is no longer the only concern; an attacker's control over physical assets–such as closed circuit TV (CCTV) cameras, elevators, HVAC and door controls–can possibly cause more havoc with business operations than a simple server compromise.

Another issue is the combination of two historically separate groups: physical/facilities security and network/IT security. While both teams are "security" groups, each has its own methodologies and capabilities. A merging of these two groups may cause strife, as people from one group may feel left out from decision making in the new group, leading to a lack of cooperation.

Finally, while a cost benefit may be realized over time, the initial cost of combining the two practices is usually very high. Current security systems may not meet the needs of security convergence and therefore must be upgraded and replaced. Education may be required to ensure proper implementation of systems to administer the combined physical and logical controls. These initial costs can prohibit the adoption of a combined security capability, especially for mid- to small-size companies, or companies hard hit by the economic recession.

Conclusion

Security convergence is a method of protection and risk management that will help reduce compromises of corporate assets. However, it is not a plug-and-play solution. It requires careful planning and consideration, not just of current physical and logical controls, but also of the initial costs of implementation and changes in corporate structure. While security convergence is a goal worth achieving, each organization must examine its own capabilities, personnel and method of doing business to decide if it is the right goal for the organization.

1990s

Network

Network attacks focus on the compromise of remote hosts in order to obtain administrative access and/or sensitive data. Network attacks often take advantage of the infrastructure itself, whether by manipulating networking equipment, or protocols used to facilitate interoperation. Successful network attacks can be severe and difficult to detect.

Successful exploitation is often followed by the installation of backdoors to allow for successive phases of attack. Using a compromised host in this way is called "pivoting," since the attacker will often have access to more attack surface at each point of insertion. By loading tools onto each compromised host and pivoting, the attacker works to gain more and more access until the goal is achieved.

Method	Description	Business Impact	% from 2010	Change from 2009
1 Weak or Blank Password for an Administrative Level Windows or Unix Account	Windows or Unix systems may have an easily guessed or null password for accounts with administrative privileges.	An attacker with this level of access can read sensitive information such as the security account manager (SAM) hive, which stores users' passwords, or the shadow file. This vulnerability allows full system access to the operating system. If the system is a domain controller or back-up domain controller, it could provide administrative access to the entire Windows Domain.	17%	
2 Microsoft 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.	Using the xp_cmdshell stored procedure gives an unauthorized user full system level access to the Windows operating system.	16%	N/A
3 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 many machines on the subnet stating that the MAC address of the subnet gateway has changed; the message usually contains an attacker's MAC address as a substitute. When the attacker turns on IP forwarding, sent packets will be routed through the attacker's machine.	Any authentication via services such as POP, Telnet and FTP through a man-in-the-middle (MITM) host will expose a user's login credentials. Older implementations of remote desktop protocol (RDP) and secure sockets layer (SSL) communications with clients using browsers with broken root certificates are also susceptible to a proxy style attack. This technique can lead to advanced attacks such as the LANMAN / HALFLM challenge attack, and can be used for anything from passive eavesdropping to active MITM techniques. Credential mining, session hijacking and delivering malware are all possible. Because the vulnerability is inherent to the way the IP MAC layer works, network access control (NAC) is usually the best defense.	12%	
4 Sensitive Information Transmitted Unencrypted on the Wire	Sensitive information, such as CHD, PII or social security numbers, is not encrypted while traversing internal networks.	When combined with a technique such as ARP cache poisoning, attackers will have access to data in transit on a network.	12%	

5	Client Sends LAN Manager (LM) Response for NTLM Authentication	Windows NT is a suite of operating systems produced by Microsoft, and NT LAN manager (NTLM) is a Microsoft authentication protocol. NTLM is sometimes referred to as NT Challenge/Response (NTCR). The server authenticates the client by sending an 8-byte random number, the challenge. The client performs an operation involving the challenge and a secret shared between client and server, such as a password. The password is used twice to generate an NT password hash and an LM password hash (for backwards compatibility with older systems). The client then sends the response (hashes) to the server. The server verifies that the client has computed the correct result, and from this infers the identity of the client.	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.	9%	
6	Vulnerable Legacy Services (Buffer Overflow Attacks)	These issues occur when an accessible server is running an older or unpatched service that is vulnerable to a buffer overflow attack and exploit code is available.	Buffer overflow attacks against enterprise services are becoming rare and harder to exploit, but some legacy servers are still vulnerable to these attacks. When exploitable, the system hosting the vulnerable service can be compromised by an attacker running commands on the server itself with the privilege level of the vulnerable service.	9%	
7	Virtual Network Computing Authentication Bypass	Versions of virtual network computing (VNC) are susceptible to authentication-bypass due to a flaw in the authentication process of the affected package. Attackers use the null authentication method to gain unauthenticated, remote access to the VNC servers.	This exploitable version of the VNC remote access software is still widely used in environments today, and can lead to user or administrator access to the system running it.	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.	Often occurring when port-forwarding is in place, an erroneous rule here can give an outsider access to an internal machine. Poorly implemented firewall rules can provide access to the firewall itself. Scanning all ports open to the outside and performing service fingerprinting tactics can allow unsecured local test databases to be used to gain access to the internal infrastructure, resulting in an internal network compromise from the Internet.	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.	Sensitive data stored, contrary to policy and/or on the wrong systems, in lower security environments allows an attacker easy access.	7%	**No Change**
10	DNS Updates Permitted Due to Dynamic DNS Misconfiguration	DNS servers support dynamic updates to records, allowing internal hosts to be easily located by name inside the network. This configuration is sometimes deployed externally, allowing anonymous users to add and change DNS records for valid hosts.	An attacker can redirect all site traffic to their own system, gathering credentials, transaction information and other sensitive data.	4%	**NEW**

Compromise of POS System Code Execution Environment

Windows Domain controllers will often allow an unauthenticated user to gather a list of valid usernames through remote procedure call (RPC) queries. Once this list is recovered, an attacker can sometimes gain credentials by testing each username using two common passwords: null (blank), and the same value as the username. Using this method, a SpiderLabs expert was able to discover a user account with access to a shared drive while conducting an internal penetration test.

Reviewing the shared folders, the SpiderLabs team member identified a file share that led to privileged escalation. This share contained different binaries used by the POS application. Our expert's approach to escalate privilege was to modify the binaries, injecting a custom backdoor within, such that when the POS system restarted it was compromised without creating any abnormal behavior. The binaries were modified in such a way that they continued to work properly.

This incident highlights the importance of a strict password policy for all user accounts, even those that are created for non-interactive service accounts, and those added for new employees. User accounts such as these are often left in an unsecured state, at least for a short period of time, allowing an attacker to compromise the account and pivot into a more sensitive area. In this case, the execution environment of POS systems, a valuable resource, was exposed.

Manipulation of Microsoft SQL Data in Transit

During penetration testing of an internal network, a SpiderLabs team member was able to perform ARP cache poisoning in order to monitor all communications between client devices. Successful execution of this attack allowed our expert to see all unencrypted data traversing between the client's device and the upstream network gateway.

Of particular note was a session that contained SQL commands. This traffic, based on the port being used and some syntactical clues, was identified as Microsoft SQL data. Database protocols often encrypt the credentials used to establish a session, but the data itself is many times unencrypted. The SpiderLabs team member monitored communications, but did not witness the target data during this passive phase.

In order to gain access to the desired data, the SpiderLabs team member performed session injection. This tactic allows an attacker to modify data, using the established session as a vehicle to enter their own commands. Our expert's attack was successful, and the inserted SQL commands created another administrative account that was then used to access the entire contents of the database at will.

Compromise of Systems During the Provisioning Process

In large organizations, IT departments frequently maintain a network for the sole purpose of provisioning new user desktop and laptop systems. The security of these networks is rarely considered. In ideal situations they are properly segmented from production systems, but this is not always the case.

A SpiderLabs team member, using a network scanner, was able to locate one of these networks during a penetration test. The environment was recognized by the different threat posture of the machines contained within. While systems in the production environment were patched and firewalls were installed according to best practices, these machines were vulnerable to many older flaws and did not employ any packet filtering. Indeed, these systems were in the process of being provisioned, and Windows security patches were several revisions behind. They were still going through the lengthy process of downloading and installing the patches released since the Windows install media had been produced.

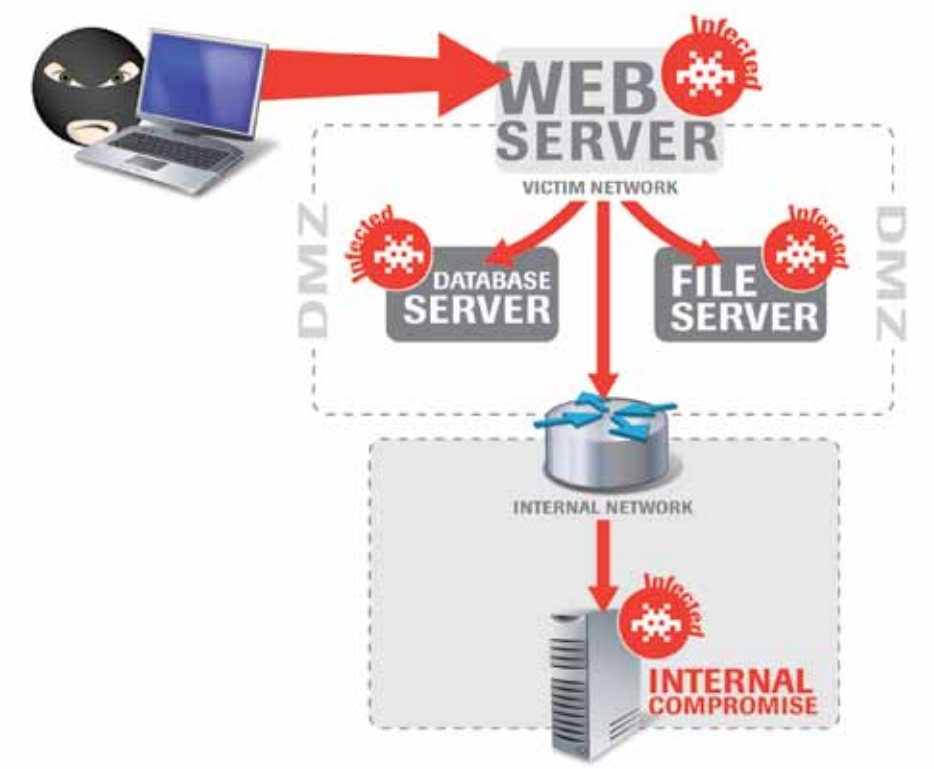
Using a commonly known Windows exploit, MS08-067, our expert gained access to these systems while they were being configured. After compromise, keystroke loggers and network sniffers were installed, revealing sensitive information. The SpiderLabs expert watched the IT staff connect to various network shares and other resources during the provisioning process, using their own credentials. In effect, this team member could monitor everything required to create a production system.

Conclusions

New methods for attacking particular network services are frequently discovered, but often remain largely unaddressed. ARP cache poisoning, as it provides the capability to intercept and manipulate data while in transit, is widespread when it comes to internal attacks. Default credentials also hinder efforts to secure the network, serving as a very weak link in what can be an otherwise strong defense.

Visibility is most often lacking, making the reconnaissance phase of a penetration test one of its most valuable deliverables. We can't secure what we don't know about, and the ease with which new devices are added to modern networks is one of its biggest vulnerabilities. Future efforts should focus on closing the known gaps that exist in the network infrastructure and finding ways to better monitor the use of this vital resource.

External Network Attack Leading to Internal Network Attack



The Network: A Security Retrospective

Early Network Attacks

The network represents one of the most utilized attack vectors; attacker's have the ability to perform attacks remotely, with relative anonymity, via networks. Modern network attacks evolved and started to become mainstream during the 1990s. While the Internet has been in existence since late 1969, when it was born as ARPANET, businesses started to really explore this new communication medium at the beginning of the 90s.

Network attacks during this era bore a strong resemblance to modern network attacks. Instead of scanning for vulnerable IP addresses as part of reconnaissance, dial-up attackers performed "wardialing." Through the use of a script, an attacker instructed a modem to dial a large chunk of telephone numbers, perform a connection attempt and then disconnect. Any numbers that resulted in a connection with a modem would be noted along with any banners received. The attacker would review these records, looking for systems that might store valuable data. Phone numbers might also be cross-referenced with public records to determine the likely owner of the modem.

At this stage, network attack methodologies employed during this era were identical to those used today. With modem access to a login prompt–or worse, an actual application–the attacker would begin to test the remote system using various inputs and default credentials. The main disadvantage for these attackers, compared to their modern counterparts, was information. Attackers were limited to electronic reference tools, such as Usenet and Gopher (an early protocol used to search Web documents), or large libraries of books.

Local Area Networks

The local area network (LAN) allowed businesses to network disparate PCs in order to distribute processing and enable greater collaboration. This was in contrast to the central processing model utilized by mainframes, where each thin client received all data over serial protocols such as the one utilized by IBM 3270 terminals. LAN technology, such as Ethernet and Token Ring, allowed peers to communicate in an ad-hoc manner, each one able to offer its own services, such as print and file sharing. This shifted control away from IT staff and into the hands of users, and brought with it a slew of new security threats, some of which remain with us today.

One such threat is address resolution protocol (ARP) poisoning, made possible because of the inherent trusting nature of LAN protocols. The very concept of data networking, during its formative years, was considered an academic pursuit where all participants would behave according to certain protocols. These protocols were documented and often required both sides of the communication stream to behave in a particular way in order for the transaction to be successful. Little thought went into network security at the business level during this time, as the idea of trusted and distrusted parties was beyond the scope of the design.

Inevitably, attackers used LAN-connected PCs to manipulate protocols and early LAN attacks simply involved the use of a "sniffer"–a program that put the network card into "promiscuous mode"–in order to gather all traffic, regardless of its actual destination. The use of Ethernet hubs, which forwarded each packet to all connected systems, allowed this to work. This inefficiency was addressed through the use of switches, which could locate and direct traffic according to each packet's destination. ARP poisoning was established in response to this limitation and still facilitates man-in-the-middle (MITM) attacks in many modern networks.

Internet Attacks

The mid-1990s saw explosive growth in the number of Internet users and Internet service providers (ISPs) that cropped up in response, offering dial-up access to the Internet for a per-minute or per-month fee. Popular ISPs during this time included America Online (AOL), EarthLink, CompuServe and Prodigy.

Operating systems also embraced this shift. Microsoft Windows 95 was a popular choice for home PCs, due to its built-in Internet connectivity features. The focus on ease-of-use proved detrimental from a security standpoint, however, and a considerable number of tools were released during this time to target and exploit Windows' weaknesses. Attackers commonly found instances of exposed Windows file sharing services, often configured with poor or non-existent passwords. Installing and running malware was trivial and almost undetectable by Windows users.

Malware distribution through e-mail also became widespread during this period. Again, preying on user naiveté, attackers sent malware in executable form over e-mail to unsuspecting users, often claiming that the file was something innocuous, such as a new screensaver. Compromised machines were often used to further spread the malware to other systems, posing as the compromised user to gain trust with other users in their address book.

Advances in Internet connectivity during the latter part of the decade only exacerbated this problem. These "always-on" connections, as opposed to the intermittent dial-up connections that users were familiar with, dramatically raised the value of compromised hosts. With a predictable connection, these machines could be used to launch attacks against other sites, send large amounts of unsolicited messages and monitor keystrokes for sensitive data. Large collections of compromised hosts, or "bots," became known as "botnets." Central command-and-control mechanisms were setup to maintain, or "herd," these devices. Their controllers, known as "bot herders," experienced an unprecedented level of control over other devices. Accordingly, control of these bots, and the data they gathered, quickly became monetized. Bot herders could hire out their collection of compromised machines for any number of purposes, including distributed denial of service (DDoS) attacks, spamming and sensitive data gathering.

Modern Network Attacks

Technology incorporated into modern networks has improved in terms of reliability and speed, but security remains a concern. Better software development practices, and the implementation of perimeter defenses such as firewalls and intrusion prevention systems, have strengthened the exterior, but weaknesses in client operating systems and internal networks continue to provide attackers with an ample attack surface.

The internal network in particular has seen little change since the 1990s. ARP cache poisoning is still in use and continues to permit MITM attacks against application data. Although this attack requires local access to a data network, the proliferation of user-owned devices, the rise of client-side attacks and the availability of wireless access points, makes this requirement less of a challenge than it was in previous years.

Whether launched locally or delivered remotely, network attacks are shifting toward the client. Where server administrators can be vigilant about the software they run, the common user does not have the same level of experience to make this decision. A majority of modern code execution takes place without manual prompting and the end users have no indication that an attack has occurred. Opening a Web page, for example, can initiate any number of plug-ins and create one or more virtual machines, all transparently from the user's perspective. If one of these plug-ins, the virtual machines (Flash and Java, for example), or the browser itself contains exploitable code, compromise is possible. This represents significantly more attack surface than most external networks offer.

Conclusion

Networks connect us not only with other well-intentioned colleagues, partners, customers and friends, but also unintentionally with those who aim to do us or our businesses harm. When reviewing the history of networking and network security, one fact becomes clear: hacking has been an intrinsic consequence right from the start. When advances or improvements seem to be made in one area, there are always those that immediately begin looking for ways to counteract, circumvent or take advantage of that progress for personal gain. Although it seems counterintuitive, there may actually be an arguably beneficial consequence of this: the cycle of hack/counter-hack has helped the industry to more rapidly mature. It is important to remember, however, that more mature doesn't necessarily mean more secure. There are still many unresolved challenges, many new and some very old, that continue to pose significant risk.

2000s

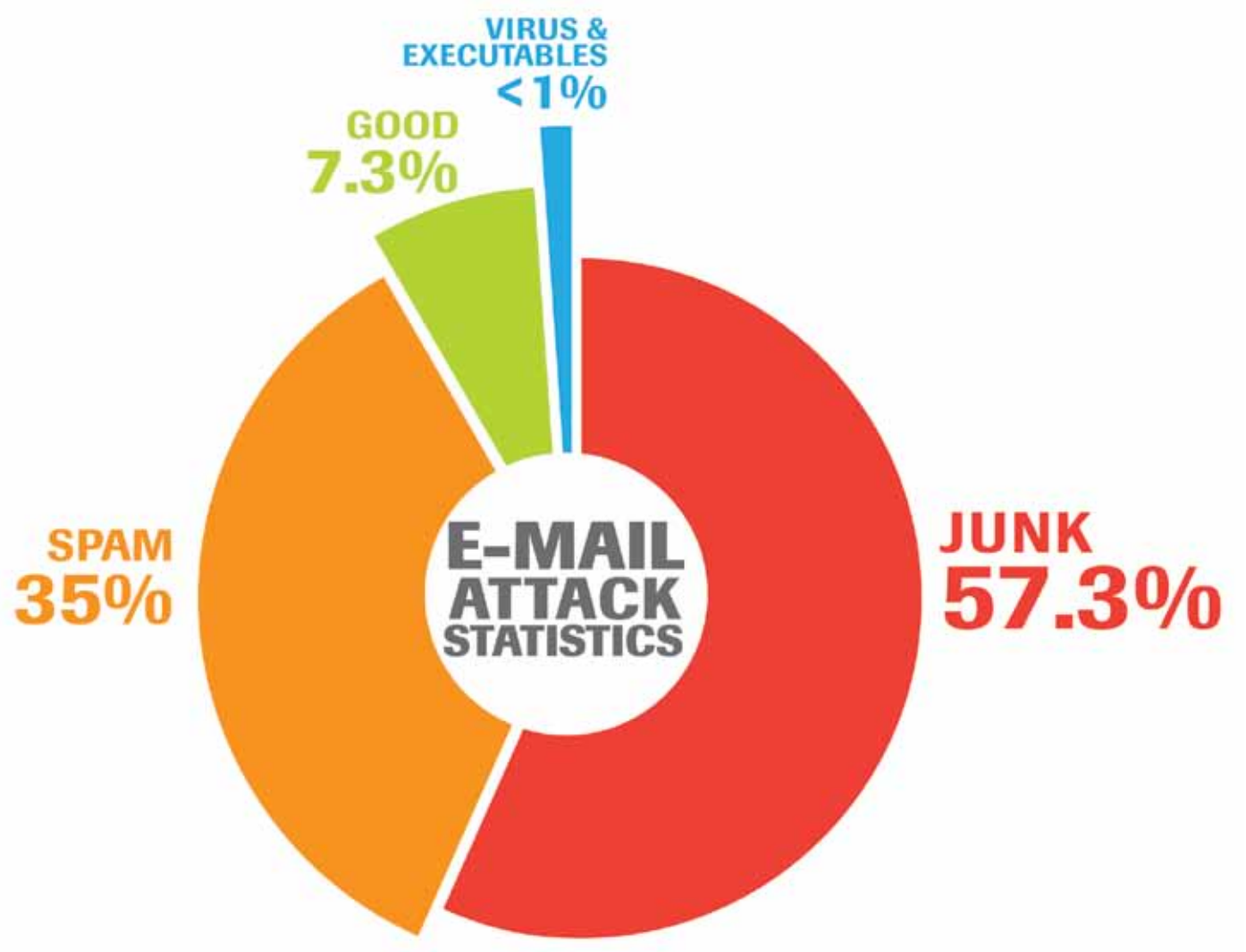
E-mail

Electronic mail (e-mail) attacks can be broken into three primary vectors: attachments, links to remote malware and malformed messages. By attaching files to an e-mail, the attacker attempts to deliver malware directly to the target's system hoping to entice the user to execute the malicious payload (i.e., malware) locally. Including links within an e-mail, an attacker seeks to lure the user into following the link to where the malicious code is stored remotely. Lastly, attackers directly target the e-mail clients used to view the messages and the servers used to send and receive the messages by creating malformed messages. Successful attacks by any of these means can result in the complete compromise of the targeted system.

E-mail Attack Statistics

Instead of providing a top 10 list of e-mail attacks being used to target business users, we've taken a look at the historical data archived within Trustwave's mailMAX environment. mailMAX is a solution for spam filtering, e-mail encryption and archiving. Between the years 2006 and 2010 the system processed and analyzed more than 15 billion e-mails for our clients. Using this data we've identified a number of interesting trends.

We found that spam and junk mail peaked in 2008 while the percentage of "good" e-mails remained static. Although spam and junk mail have declined since then, mail containing viruses and executables increased. The trend seems to be against sending spam-based e-mail in mass quantity; rather, it is focusedon targeting users with e-mails containing malware.



Zeus Spear Fishing[4,5]

Users of the popular online social networking site Facebook were e-mailed links to a fictitious new login system from a spoofed account appearing to be from the official Facebook team with the victim's username already populated. User credentials could be compromised, as well as the infected host potentially becoming a member of the Zeus botnet.

Haitian Earthquake Relief Scam[6]

An e-mail scam was sent in early 2010 requesting financial aid to help the victims of an earthquake that had occurred in Haiti. Funds were not used to aid the earthquake victims.

UPS Package Tracking Malware E-mail

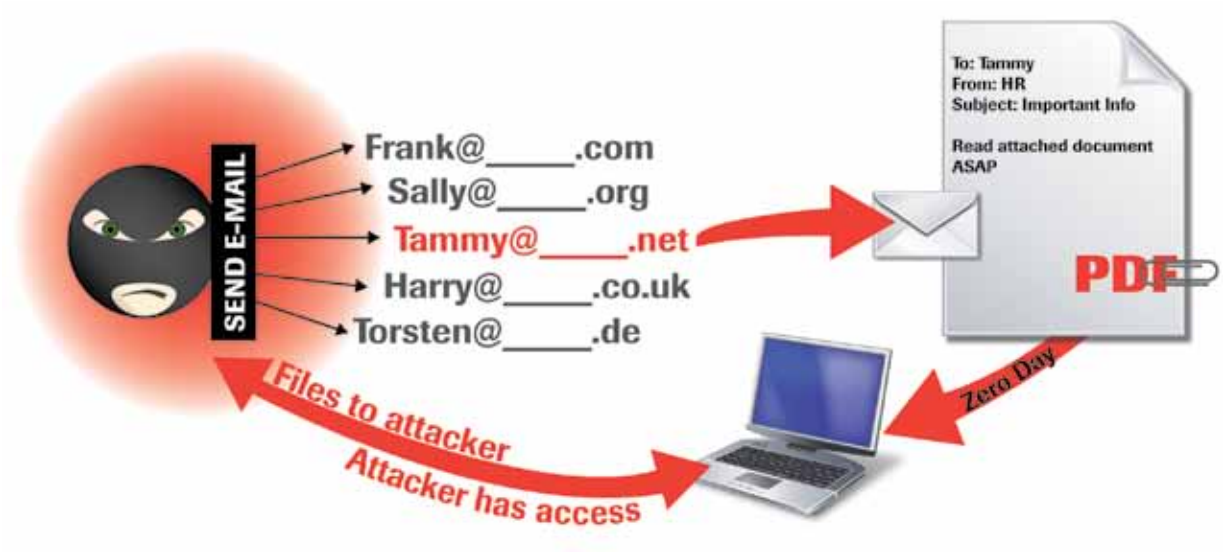
An e-mail seemingly from UPS stated that the package that was sent could not be delivered to its destination. A file attached to the e-mail masqueraded as an invoice. Opening the attachment infected the computer with a Trojan.

Conclusions

E-mail attacks, including spam, make up an overwhelming majority of all e-mails sent. Inboxes are under constant assault by attackers attempting to find any weak spot in the defenses. Spammers and malware authors quickly hop from campaign to campaign with the average attack lasting less than 24 hours in duration. The one trend that does continue is that of attack diversity. We can expect to detect more previously unknown attacks upon our resources and should be prepared to counter with a solution.

Public awareness and open communication regarding current threats are keys to protecting end users. Moving forward, efforts in these areas should include keeping potential victims up-to-date on the latest discoveries of the information security community. Understanding the threat is the first step to preventing compromise.

Depiction of an E-mail Attack



[4] "Facebook Phishing Attack Powered by Zeus Botnet, Researchers say." http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=221100157

[5] "Facebook Virus: "newloginsystem" email ALERT!!!" https://www.facebook.com/note.php?note_id=169607741767

[6] "Haitian Earthquake Relief Fraud Alert." January 13, 2010 http://www.fbi.gov/scams-safety/e-scams

Spear Phishing: Targeted Attacks

Phishing can mislead a user into revealing sensitive information such as passwords, credit card numbers or other personal financial information. A typical phishing campaign involves sending millions of e-mail messages that appear to originate from popular and highly recognizable sources, such as e-commerce sites, large banks, social networks or government agencies. These e-mails may contain malicious attachments or links to websites that imitate legitimate sites in an attempt to harvest data from unsuspecting visitors.

Phishing is not a new threat. As with most computer-based attacks, there are analogous attacks pre-dating the modern digital system, such as fake charity donation collections. But criminals have adapted to the digital world as we all have. For example, in early 2010 the FBI issued an alert about an e-mail scam attempting to solicit funds under the guise of providing aid to earthquake victims in Haiti.[6]

Taking phishing one step further, attackers are now targeting specific individuals, giving rise to the term "spear phishing." Using specific personal data, this type of attack can easily dupe users. Attackers are frequently able to gather personal contacts and information needed for this type of attack from social media sites. Variants of the Zeus crimeware botnet took advantage of this susceptibility in its attacks on Facebook users; they were e-mailed links to a fictitious new login system from a spoofed account appearing to be from the official Facebook Team with the victim's username already populated.[4, 5]

E-mail continues to be an important part of day-to-day business and personal lives, but social media tools are also increasingly used for regular communication and storage of personal information. Attackers will attempt to use these channels to gain an online dossier on potential targets in an attempt to gain profit at the victim's expense. As threats to online users evolve, continued personal vigilance and awareness are key weapons in defending against spear phishing and other types of targeted online attacks.

Application

In the 21st century, small organizations often have more than one custom application to support their work processes, whereas large companies can easily have hundreds of applications, if not more. The critical roles applications play in business today mean that application security is a key element in any risk management program.

Application penetration tests are the most popular and effective method for identifying vulnerabilities. After mapping out the application's functionality, a professional and ethical security specialist uses cutting-edge attack techniques to discover a variety of vulnerabilities.

The vulnerabilities listed below are ranked by collective threat, based on the frequency of findings, difficulty in launching the attack and the potential impact when exploited by criminals. For example, while SQL injection is not the most common vulnerability we encounter, the potential for the bulk extraction of sensitive data makes it the number one threat of 2010. Conversely, cross-site request forgery (CSRF) is one of the most common application vulnerabilities, but requires a more complicated attack scheme, relegating it to eighth on the list.

Method	Description	Business Impact	% from 2010	Change from 2009
1 SQL Injection	SQL injection allows an attacker to insert arbitrary commands into a SQL query or statement. This attack is possible when user-supplied input is not properly sanitized before being used in a command sent to the database server.	SQL injection can be used to extract any data stored in the targeted database, to modify data, execute arbitrary operating system commands, read and write local files, and even tunnel internal network traffic to the Internet. This flaw can lead to the compromise of applications storing large amounts of data, such as payment card numbers or financial information.	7%	**No Change**
2 Logic Flaws	A logic flaw vulnerability allows an attacker to bypass business rules that should be enforced by the application. A simple, yet common example is when an attacker can arbitrarily set the price of goods on a website.	The impact is typically fraud-related; the nature of the fraud depends on the application. Online stores are a frequent target and exploitation typically results in theft of goods. Depending on the application, a simple logic flaw could have devastating effects on the data being used within the application. Many logic flaws do not require traditional "hacking" skills to exploit, making the threat even more severe.	7%	**No Change**

3 Authorization Bypass	Authorization bypass is the result of unenforced access control profiles (i.e., users should not be able to access other users' data). Privilege escalation to administrative functions is another common scenario. Applications with external users (i.e., consumers) may be particularly vulnerable.	The impact is closely tied to the type of data stored by the system. Financial services applications can be a target for authorization bypass since the result can be the theft of hard assets. When scripted attacks are possible, bulk extraction of other valuable data, such as payment card numbers or social security numbers, can still be profitable for criminals.	5%	No Change
4 Cross-site Scripting (XSS)	XSS vulnerabilities allow an attacker to insert arbitrary client-side scripts (typically JavaScript) into Web content that will be viewed by another user. Most XSS is classified as "reflected," meaning the attack is not permanently stored by the application. Less common, but more severe, is "persistent" XSS, typically stored in the application's database.	Once an XSS attack has been launched, the attacker can modify a Web page in any manner. Prompting the user for authentication credentials or for purchase information (i.e., credit card) are two possible outcomes. The attack can also monitor user keystrokes, force the user's browser to attack other websites, or even tunnel network traffic through the browser.	26%	
5 Authentication Bypass	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.	When combined with a technique such as ARP cache poisoning, attackers will have access to data in transit on a network.	8%	No Change
6 Vulnerable Third-party Software	An application can only be as secure as the infrastructure it runs on (i.e., application frameworks or servers). Poorly coded applications can introduce vulnerabilities.	Like many applications, this depends on the nature of the application. Typically, sensitive data is exposed, or business processes can be subverted.	3%	
7 Session Handling	Session handling flaws come in many varieties. When exploiting them, the attacker's goal is to impersonate a valid and authenticated user.	Depending on the flaw, attacks may be only possible against one user at a time. In some cases, the entire system can be compromised resulting in bulk data extraction. Regular patching and proper configuration management is the best way to prevent this vulnerability, as well as choosing a platform with a solid security history.	13%	
8 Cross-site Request Forgery (CSRF)	CSRF allows a malicious website to force a legitimate and authenticated user to execute commands on the targeted Web application. This is possible when the command is formatted in a predictable manner known by the attacker.	Like session handling flaws, this is dependent on the privileges of the victim user. Complete system compromise can be possible if the user is an administrator.	11%	No Change
9 Verbose Errors	Verbose error messages, long an issue for applications on all platforms, can provide significant aid to an attacker. The error messages can provide configuration data, source code or other useful information.	While they don't directly allow for fraudulent activity, verbose errors can reveal information about applications that makes other vulnerabilities far simpler to exploit.	13%	
10 Source Code Disclosure	Proprietary application source code can be disclosed through a number of methods, ultimately making things easier for attackers. The importance of source code security was highlighted by "Operation Aurora" in early 2010.	Many vulnerabilities are difficult to discover in a "black-box" attack scenario. When an attacker can access an application's source code, it becomes much simpler to identify flaws and craft effective exploits.	7%	NEW

Known Incidents from 2010

Operation Aurora[7]

One of the most notable incidents this year was a series of breaches at Google, dubbed "Operation Aurora" because of text in some of the attacks. The initial attack used a true zero-day vulnerability in Microsoft Internet Explorer. After workstations were compromised, the attackers created a tunnel into Google's internal network and gained access to Gmail accounts and to poorly secured source code repositories. Several other high-profile software companies reported similar attacks, but no breaches.

Google is generally well-regarded in respects to security, but this attack highlighted the importance of continued diligence no matter the company. The attack also used unpublished zero-day vulnerabilities, which are not common and are difficult to obtain. Finally, there were allegations by Google that the attacks were sponsored or performed by a foreign government.

Apache JIRA[8]

The Apache Software Foundation (Apache) supports the popular Apache HTTP server, along with many other high-profile open source projects. Apache is well-respected within the security industry for their commitment to security in their various projects. On April 5th, an attacker embedded a cross-site scripting (XSS) attack in Apache's bug tracking and project management website. The attack resulted in credentials being compromised from a number of administrator accounts, which attackers used to install back-doors on a number of servers and escalate privileges through a variety of techniques. Apache staff discovered their presence after four days and quickly shut down the affected systems.

Société Générale & Jérôme Kerviel

Headquartered in Paris, Société Générale is a global financial services company. Although the SocGen's trading scandal first came to light almost three years ago, it is worthy of this list because one of its employees, Jérôme Kerviel, was finally convicted October 5, 2010. By exploiting logic flaws in monitoring software and procedures, Kerviel was able to perform nearly 50 billion Euros worth of unauthorized trades. When the bank discovered the fraudulent transactions and reversed them, they resulted in losses of 4.9 billion Euros.

Kerviel was not a skilled cybercriminal. He wasn't even in SocGen's IT department. Instead, he accomplished the feat by becoming very familiar with the details of how the processes worked and identifying ways to subvert them through logic flaws. This should serve as a strong reminder that a wide variety of threat sources, including internal employees, need to be considered when securing applications.

Conclusions

Patience is a virtue practiced by criminals. Many of the high-profile attacks in 2010, including all three referenced above, required long-term planning and reconnaissance. Criminals now have sufficient skills to go after larger targets that require more than exploiting relatively simple vulnerabilities like SQL injection. Application owners cannot be satisfied with clearing out the low-hanging fruit of application vulnerabilities. Attention must be paid to complex vulnerabilities, which in turn requires a comprehensive approach to application security.

SQL Injection Attack

[7] "Google Hack Attack Was Ultra Sophisticated, New Details Show." http://www.wired.com/threatlevel/2010/01/operation-aurora/
[8] Incident Report from The Apache Software Foundation. http://blogs.apache.org/infra/entry/apache_org_04_09_2010

Application Security Sanity: There are No Silver Bullets

Within a competitive landscape, due to the constant drive to meet deployment deadlines, along with the perceived need for new technology, decision makers prefer quick solutions, and relegate security to an afterthought. The inherent problem with this strategy is that when security is addressed post-development, it becomes a more complex and expensive proposition.

Faced with this challenge, many organizations look for a "silver bullet" and some vendors within the industry are happy to oblige by promising a single, perfect application security solution cheaply.

Of course, no silver bullet exists for computer and data security, including application security. Application security is a complex requirement best served by a variety of complementary tools or processes at the appropriate stages of development and production. Since no individual application security technology or service can detect and prevent every flaw, the best approach is a plan that complements and blends a number of best-of-breed solutions.

The 24x7 availability of automated tools is complemented by analysis only available with manual testing. For example, logic flaws rank among the most severe and complex vulnerabilities. As a result, they cannot be discovered by automated testing or filtering tools; the only way to identify them is through human testing. Other common vulnerabilities, such as SQL injection, have nuanced variations that are unlikely to be detected by an automated tool.

Manual testing is extremely thorough, but few organizations have the budget to perform penetration tests against an application weekly, or even monthly. This is where automated tools shine. A Web application firewall (WAF) can provide 24x7 protection against attacks targeting common vulnerabilities such as simpler variations of SQL injection or XSS.

Security offense versus security defense is another way to match solutions:

Common Solutions for Security Offense:

- Application penetration testing
- Application scanning
- Code review
- Static code analysis

Common Solutions for Security Defense:

- WAFs
- Training
- Vulnerability patching

Regardless of the methods of discovery, the vulnerabilities discovered still need to be fixed. Development groups, pressured by delivery schedules and other deadlines, aren't always able to patch vulnerabilities immediately upon discovery, especially non-critical flaws. Continuous application protection can be had, however: "virtual patching" techniques possible on a WAF can protect the application from a vulnerability while the development team works to fix the flaw.

The shortest period between awareness of vulnerability and fixing it is best. Some security initiatives, however, are best as milestones. These milestones can often serve as a chance for the development team to take a deep-dive into the inner workings and true security posture of an application. Potential advantages of this approach are the immediate elimination of the vulnerability and the maintenance of the development team's scheduled release cycle. Indeed, periodic assessments partnered with a technology like virtual patching can be a robust approach to Web application security.

If an organization wants solid, complete application security, a variety of solutions must be implemented. By blending offensive and defensive techniques, manual and automated testing, and periodic and continuous updates, organizations position themselves for a better security outcome. A diversification strategy serves to protect against the threats of today, as well as better position a company to address the emerging threats of tomorrow.

Wireless

Wireless networks pose a unique security challenge, in part because of its wide adoption. Beyond the security considerations when implementing the 802.11 Wireless networking standards, there are numerous issues with the implementation of other technologies, such as Bluetooth, 802.15.4 ZigBee, 802.11p and others. Wireless networking technologies expand traditional physical boundaries, allowing attacks that once required physical access to a device or location to occur remotely — in some cases up to a mile away.

Like most attacks against information systems, attacks against wireless technology continue to evolve, keeping pace with security controls as they are developed and implemented.

Method	Description	Business Impact	% from 2010	Change from 2009
1 Wireless Clients Probe for and Associate with Wireless Nodes While Connected to Wired Network	Typically Windows clients will probe for and associate with wireless nodes even though they are already connected to a wired network. It is possible to create a wireless access point, which will answer to and allow association with, any request probe received. Any client that associates with this AP can be targeted for attack.	If the wired side network is a corporate network, and the attacker can gain access to the client from the wireless side, this client can be used as a jump point into the corporate network by an attacker.	33%	**No Change**
2 Wireless Clients Probe for ESSIDs from Stored Profiles When Not Connected (Karma Attack)	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 wireless stored profile. In this way the client connects to the Karma AP instead of the intended AP. If the attacker's Karma 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.	A Karma attack performed on a corporate campus or at a nearby location frequented by employees (i.e., cafe with Wi-Fi) can be devastating. Once connected, the victims can fall prey to MITM attacks that steal their credentials, download malware or a number of other MITM techniques. They then return to the corporate network with a compromised machine.	33%	**No Change**
3 Easily Determined WPA/WPA2 Pre-Shared Key (PSK)	Wi-Fi Protected Access (WPA) is another protocol for encrypting transmissions over IEE802.11 wireless networks. In one version of WPA/WPA2 based on a PSK, a single root key is shared by all radio stations. If the root key is a dictionary word or does not contain numbers of symbols, an attacker could use a dictionary attack to recover it.	Cloud computing services and high end graphics cards allow for faster cracking of a larger key space than ever before. And once an attacker has a root key they can decrypt all encrypted traffic captured over the air and in many cases, join the wireless network and interact with it.	10%	↑
4 Legacy IEEE 802.11 Frequency Hopping Spread Spectrum (FHSS) Wireless Networks With No or Minimal Controls	The 1999 IEEE 802.11 standard specified a method to use FHSS as a physical layer for the wireless network. Once widely implemented, FHSS fell from favor due to restrictions on transmission speed. Legacy networks still exist, however, often without security or access controls, or segmentation between wireless/wired networks. There is a misconception that these networks are inherently secure, but by using software radio attackers can find and connect to them the same way they connect to modern networks.	Due to the architecture and lack of security controls, once an attacker connects to these networks, they have remote access to the internal network.	5%	↑
5 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.	WEP does not properly protect wireless transmissions. In some cases an attacker can recover a WEP root key in as little as 40 seconds. WEP attacks allow—at a minimum—eavesdropping on wireless traffic and may provide the attacker with access to the wireless network.	5%	↓

6	Lack of Publicly Secure Packet Forwarding (PSPF) Features Enabled on Public or Guest Networks.	PSPF prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN. In public networks, the lack of these features allows an attacker access to attack other wireless clients.	Once connected, the victims can fall prey to MITM attacks, such as those that will steal their credentials or force a download malware. The lack of a PSPF feature could introduce virus or worm traffic to the internal network, or allow an attacker to place malware, such as key loggers, on the compromised device for later access to the corporate network.	5%	No Change
7	Wireless Clients Using the Public "Guest" Network Instead of Secured Private Network	Many organizations have a "guest" wireless AP for visitors, vendors or consultants to use. Attackers can access these guest networks as well. When employees start connecting to the guest network with corporate assets, an attacker can attack the corporate asset.	Once connected the victims can fall prey to MITM attacks that will steal their credentials or force a download of malware. When a victim returns to the corporate network, they return with a compromised machine which could introduce virus or worm traffic to the internal network.	3%	No Change
8	Wireless Device Configured to Connect to Secured Network Left Unattended	In retail environments or other businesses with public areas, wireless handheld devices or scanners are left unattended in an easy to access place. These devices contain all information necessary to connect to the wireless network. An attacker merely has to "borrow" the device for a few minutes to read the settings or dump the configuration.	This vulnerability provides the attacker with enough info to join the wireless network with an alternate device.	3%	
9	Lack of Segmentation or Access Controls Between Wireless and Wired Network Segments	Lack of network segmentation or properly implemented access controls means that once the wireless network is breached, it becomes a nearly trivial exercise for the attacker to breach internal network resources.	An attacker will have free reign to attack the internal corporate network and likely anything on the other side of a WAN connection as well.	2%	
10	Sensitive Information Transmitted Over Bluetooth	Recent research indicates that if sensitive information is transmitted over Bluetooth, an eavesdropping attacker can sniff this information.	An attacker can potentially gain access to sensitive information transmitted over Bluetooth.	1%	NEW

Known Incidents from 2010

Using Wireless to Hijack Sessions

Firesheep, a free open source plug in for the Firefox Web browser, is an easy-to-use, point-and-click method to hijack insecure Web sessions and capture a target's credentials while on any public wireless network. This tool was released at the ToorCon 12 information security conference in San Diego. Used on a public or private wireless network, this tool could compromise the accounts of any users who access non-HTTPs enabled websites that pass sessions information in the clear. This technique was used to target social networking sites such as Facebook.[9]

Largest Breaches in History Utilized the Wireless Attack Vector

Christopher Scott, sentenced to seven years in prison, pleaded guilty to breaching the wireless access points of several retailers between 2003 and 2007 to siphon credit and debit card numbers. Scott passed those numbers on to the noted cybercriminal Albert Gonzalez. The two men were reported to have stolen nearly 20 million credit card numbers, costing retailers nearly $200 million in fraud losses.[10]

Google's Mapping Drones Sniff Private Data

Google's Street View cars inadvertently collected e-mail addresses, passwords and other personal information while driving around the world's cities taking photos for their mapping service. The United State's Federal Communication Commission (FCC) in 2010 began a probe into whether or not Google broke federal laws in the process.[11]

Conclusions

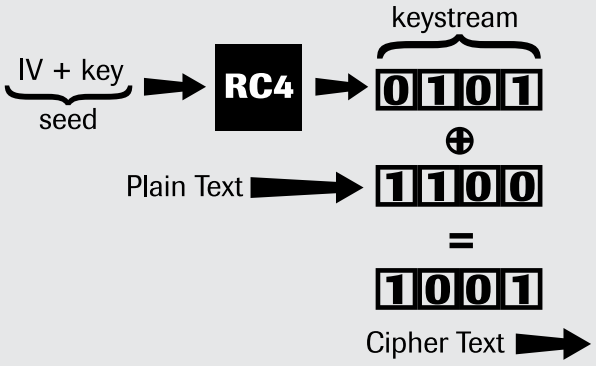
Attack vectors continue to shift from attacks against wireless infrastructure to wireless clients. Strong encryption is the only way to potentially mitigate client attacks since anything that is sent in the clear over a wireless network could be intercepted.

Depiction of Wireless Attacks

History of Wireless Attacks

Security issues with 802.11 began with theoretical attacks through the total destruction of the Wired Equivalency Privacy (WEP). The original IEEE standard 802.11-1997 and the later 802.11-1999 clarification defined WEP as an attempt to discourage eavesdropping on wireless network communications. It was meant to provide wired equivalent confidentiality to a wireless network. The original specification for WEP defined a 40-bit key length, with a version that used a 104-bit key length defined later. Both versions worked by concatenation of the provided key with a 24-bit initialization vector (IV), which were fed into the RC4 algorithm to produce a keystream. A binary mathematical operation called XOR was then used to produce the cyphertext.

Soon after, researchers began publishing academic papers detailing flaws in WEP; some of the most notable were "An Inductive Chosen Plaintext Attack against WEP/WEP2" published by William A. Arbaugh in May, 2001 and "Weaknesses in the Key Scheduling Algorithm of RC4" published by Fluhrer, Mantin and Shamir in August, 2001. The latter led to the implementation of a practical attack against WEP, known as the Fluhrer, Mantin and Shamir (FMS) attack.



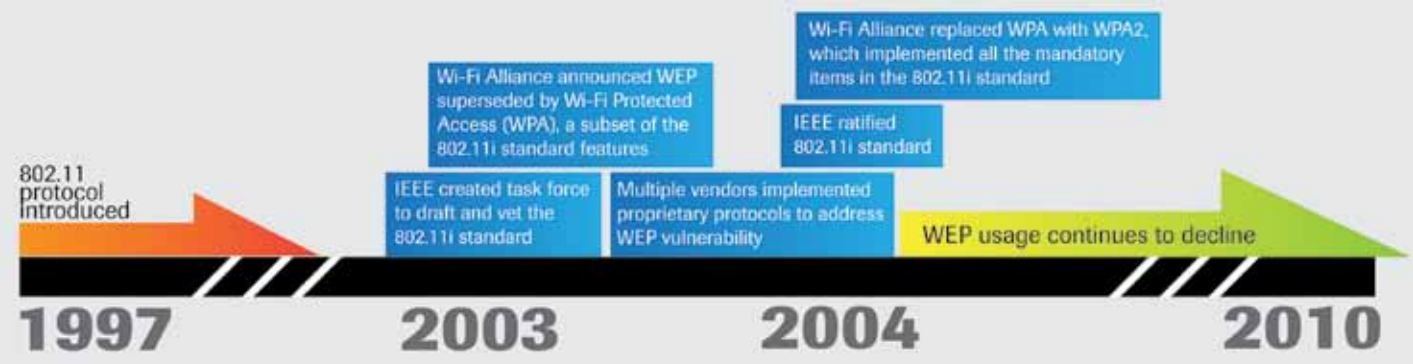
Shortly after the FMS attack was published, Adam Stubblefield, a summer intern at AT&T labs, published "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," which described the technique used to implement the FMS attack but did not include the tools. Within 20 days of the original RC4 publication, however, a group of security researchers published the tool AirSnort, a working implementation of the FMS attack. About the same time a tool called WEPcrack was also released. With these tools, attackers and researchers alike had a practical method to break WEP.

[9] http://codebutler.com/firesheep
[10] http://www.wired.com/threatlevel/2010/03/christopher-scott-sentencing
[11] http://latimesblogs.latimes.com/technology/2010/11/google-being-investigated-by-the-fcc-for-wireless-data-collection.html

Over time, techniques for breaking WEP only improved and in 2004 the Wi-Fi Alliance declared that all WEP implementation types were "deprecated as they fail to meet their security goals." The industry, however, persisted in widespread use of WEP, even as attacks against WEP got better, more reliable and faster.

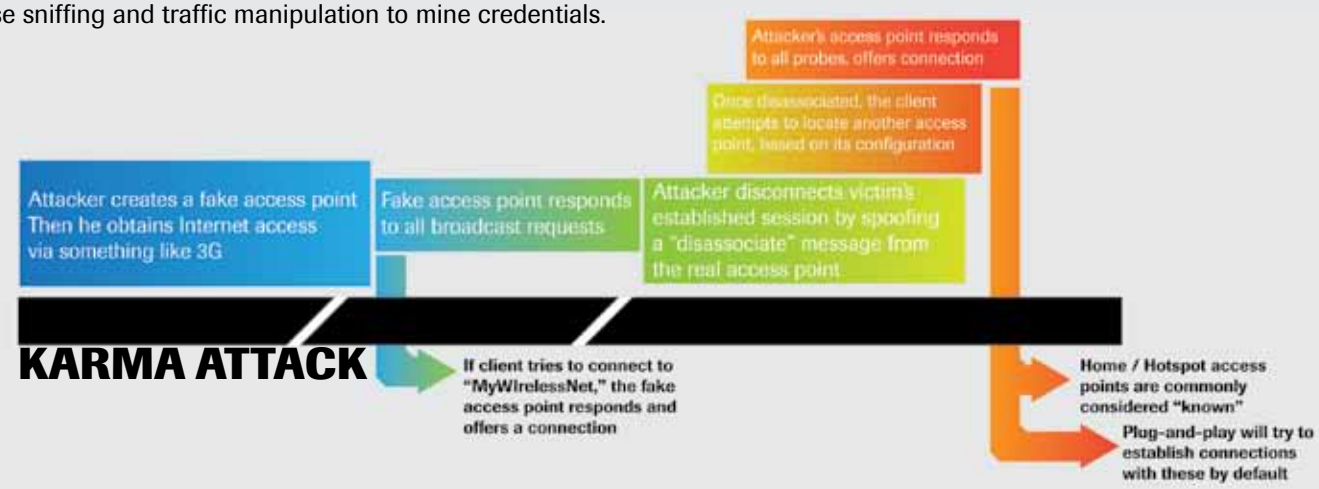
Many vendors and organizations tried to revive WEP by using tricks such as dynamic WEP keys that rotated periodically. The theory was that an attacker could not crack the keys fast enough before rotation. But in 2006 a new technique was published in a paper called "The Final Nail in WEP's Coffin," by Bittau, Handley and Lackey. This paper described a fragmentation attack that increased the speed of WEP cracking where even dynamic WEP keys could be defeated. Following this paper, three researchers, Erik Tews, Ralf-Philipp Weinmann and Andrei Pyshkin published a technique, known as a PTW attack, in a 2007 paper: "Breaking 104-bit WEP in Less Than 60 seconds."

But it wasn't until the spring of 2007 when the TJX Companies, Inc. (TJX) announced that attackers had infiltrated their systems and, over the course of several years, stolen millions of client credit card records that WEP usage showed a major decline. WEP, used on store wireless networks, was directly blamed for the initial compromise at TJX; later, it was discovered that Christopher Scott, one of the TJX attackers, did use WEP-encrypted networks as a starting point to breach several retailers between 2003 and 2007. Today WEP is little more than a speed bump for an attacker, but since it is supported in all Wi-Fi equipment from the oldest to the newest, it is still in use in some implementations.



Wireless Client Attacks

Wireless client attacks are hard to detect, still relatively unknown and often easy for attackers to accomplish. Most client attacks are variants of an attack known as "Karma." A Karma attack creates a fake wireless access point that can lure clients into connecting to it, and then act as a man-in-the-middle (MITM). An attacker can then either attack the client machine, or use sniffing and traffic manipulation to mine credentials.



While a Karma attack is in progress, many MITM avenues are open to the attacker; for example, they could gain information by creating a Web proxy or SSL proxy to sniff or control HTTP/HTTPS traffic. The attacker can start manipulation of network traffic (cause authentication events) or even create a phony "pay page" to collect cardholder data from multiple users in a public place.

Similar to the network attacks that were perfected in the 1990s, wireless targets are no different. Network access control, strict configuration standards applied to wireless infrastructure and installing the latest security updates on wireless devices are some of the best defenses against wireless threats.

2010

Client-Side

Malware attacks are nothing new and the evolution of computer threats closely follows the evolution of the computer software industry. In the 1980s, software was distributed via floppy drives, as were the computer viruses. During that time, client-side attacks were already a prolific attack vector. Not much changed in the 1990s, until Internet access became widespread. What followed was an avalanche of new propagation methods, from Microsoft Outlook worms, to malicious packets attacking servers, and then on to malware spreading via Usenet, IRC, IM and P2P software, with the most recent developments focusing on mobile phones.

The current availability of components, libraries, shared code and forums often simplifies and expedites the development of malicious code. The sheer number of malware samples available escapes statistics. Recent terms such as “malware as a service” and “malware operating system” are accurate descriptions; malicious code is simple to write, copy and improve — and to buy and sell.

Method	Description	Business Impact	% from 2010
1 Targeted Attack	Targeted attacks can occur when malicious content is hidden or provided in a legitimate-looking way to the victim. It can be an e-mail, a link posted by a “friend” or a USB drive left in the open.	Once a system is compromised via this attack, any information can be transferred out of the organization's systems. Next steps usually involve penetration of the network segment where the infected system is located. A simple PDF attack can lead to a large-scale attack on all accessible machines on the network.	5%
2 Drive-By Infection	Drive-by infection can occur when a victim visits a Web page that is hosting malicious code, typically in a complex, yet easily deployable package containing a set of exploits targeting old and recent (including zero-day) vulnerabilities in browsers, plug-ins and ActiveX controls.	Even if an attack is random, this attack has the ability to become targeted. While drive-by infection aims for mass-infection to create large botnets, it is not unusual for a botnet master to select some systems for further targeting.	60%
3 Manual Installation	Simply put, attackers exploit some vulnerability in the targeted system (e.g., default vendor passwords) to manually plant malware on the system.	Attackers that manually infect systems are a significant threat: they have full access to the system and privileges typically not available to malware authors undertaking automatic attacks. Manual installation positions attackers to steal large amounts of data, remain undetected and remove traces of their presence as long as possible.	20%
4 Social Engineering	In social engineering, an attacker attempts to manipulate a human victim into performing an action or sharing crucial information. Examples include websites that require users to download a "plug-in,” phishing e-mails, and intruders masquerading as legitimate service providers or vendors.	The only way to combat this is security awareness training, and perhaps a little common sense. Train all staff to be suspicious of unsolicited phone calls, visits or e-mail messages asking about employees or other internal information. Verify the identity of any unknown individual who claims to be from a legitimate organization. Be aware of malicious websites that may look identical to a valid site.	15%

Known Incidents from 2010

Stuxnet Worm[12]

The Stuxnet worm spread itself in many ways, but the method of initial infection was through the attachment of an infected USB memory stick to a vulnerable system. This previously unknown exploit, or "zero-day," infected systems even if auto run and auto play had been disabled. By spreading in this manner, Stuxnet infected systems on isolated networks that were not connected to the Internet.

Once on a system, Stuxnet employed another four unique exploits, two of which were used to escalate local privileges by leveraging vulnerabilities with both keyboard layout files and Task Scheduler files. This malware's arsenal was used to infect the system, raise its privileges on the device to the highest levels, and allow the code to execute and spread to other devices.

PIDIEF (PDF) Malware[13]

PIDIEF malware works by enticing a user to open a maliciously crafted Portable Document Format (PDF) file via a common file distribution medium: website, e-mail attachment, removable media or a network share. If the file is opened with a vulnerable version of Adobe® Acrobat® or Reader®, the attacker is able to execute arbitrary code on the system. An executable file is then decoded from the PDF and written to the device. Depending on the variant of the specific malware, a Trojan will normally be installed at this point. Then, the attacker typically downloads additional tools, disables anti-virus software, monitors keystrokes and harvests the target's website credentials.

PDF files have become the de facto standard of file-based malware attacks, out numbering older popular formats such as Office documents and binary files. The large number of media rich features supported by the open format combined with its wide adoption provides malware authors with many potential avenues for new exploit development.

Qakbot Trojan[14]

The primary infection occurs when a user visits a malicious website and clicks on links that attempt to exploit known vulnerabilities in Web browsers and media players. If the victim has not applied the relevant patches to the system, the Qakbot Trojan/Worm will install itself to the system and attempt to spread itself via shared networks.

Once the system has been infected, the Qakbot specifically targets sensitive information on the device with special attention to any financial credentials. While harvesting this data, any identified financial information is sorted out locally before being sent out of the network via File Transfer Protocol (FTP). Attackers then use this data to attempt ACH fraud, transferring money to accounts in their control.

Conclusions

Malicious attacks on the client side are one of the most common ways for attackers to build botnets and deliver payloads in targeted attacks. In the last 25 years, constant development has taken place in this field. Mobile phones, smartphones, tablets and other devices are all similar at the macro level, and the more devices, interfaces, layers, and nested relations between hardware and software, the more chance there is for something to go wrong.

Most importantly, the attackers are no longer random individuals, but more often groups of highly technical, advanced specialists that form criminal organizations. In the next few years, we expect to see continuous growth of client-side attacks. Thus far, these attacks have relied heavily on popular platforms; we have seen growth of zero-day exploits for Microsoft Office, Adobe Acrobat, Adobe Flash, Sun (now Oracle) and Java. As more customized attacks develop, it is highly possible for the next generation of zero-day exploits to hit additional platforms. With the possibility of limited visibility into the code of these platforms, discovering such attacks will present many new challenges.

[12] "Stuxnet Attacker Used 4 Windows Zero-day Exploits."
http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347
[13] "CVE-2010-0188. Patched Adobe Reader Vulnerability is Actively Exploited in the Wild."
http://blogs.technet.com/b/mmpc/archive/2010/03/08/cve-2010-0188-patched-adobe-reader-vulnerability-is-actively-exploited-in-the-wild.aspx
[14] "New, Improved Trojans Target Banks."
http://www.bankinfosecurity.com/articles.php?art_id=3075

Anatomy of a PDF Attack

Let's look at a typical scenario of a targeted PDF attack. John, a long-time employee working for a large U.S. Defense contractor receives an e-mail with a PDF attachment from a sender that he trusts. The name of the attachment indicates there are recent updates to a conference that John is planning to attend in Las Vegas. He clicks on the attachment, Acrobat Reader opens, but there is a small delay before the document fully opens. As John begins reading through the document, he doesn't even notice that the hard drive starts making a little bit more noise than usual.

John is completely unaware that by opening the attachment, he inadvertently initiated an unstoppable, inevitable cycle of events. First, the e-mail client he was using looked up in the Windows Registry what software is associated with the .pdf file extension. Next, the associated program, in this case Acrobat Reader, was launched. Reader then received a command to access the malicious PDF file that had been stored in a temporary folder by the mail client. Acrobat Reader loaded the file and started processing the structure of the PDF. As it was processing the file, it came across a section storing JavaScript code. The built-in JavaScript engine was then loaded, and the JavaScript code was executed.

The polymorphic JavaScript code contained a simple routine. It allocated a lot of memory, filling it with a small but clever machine code. As the memory allocation progresses, the program reaches a point of no return and the vulnerability triggered by the Heap Spraying technique is exploited. The code, also known as a shell code, is executed and the attack reaches a milestone: remote code execution (RCE).

The binary code contains a "recipe" for disaster; it resolves a few addresses of operating system APIs and uses them to load the encrypted data from the original PDF. The encrypted data is decrypted and then written to a temporary file. The file is then launched and the second milestone of the attack is reached: payload execution.

The payload is a small program with the ability to connect to a remote site where it can either download further payloads or act as a reverse shell. It connects to the remote site and polls possible commands that the attacker passes to it in an interactive or predefined way. From this point on, the system is controlled by the attacker.

The final milestone of this attack is opening the clean PDF file that was also transported inside the malicious PDF attachment. The clean PDF file is launched at the end of the infection, allowing John to view the conference information the attacker copied from the conference website and happily sent to John (using a spoofed sender e-mail address).

John closes the document and smiles, anticipating his upcoming trip, thinking (mistakenly) that he's having a great day.

PIDIEF Malware Attack

Mobile

Mobile devices are a growing target for attacks using conventional exploitation methods, as well as new vectors unique to mobile platforms. Mobile security trends have changed dramatically; in the 80s and early to mid-90s, cell phones were popular targets for fraud and cloning due to inherent weaknesses in the cellular network architecture. Since most modern mobile networks have moved to GSM and CDMA, these vulnerabilities have decreased. While CDMA cloning is still possible, GSM cloning attacks are very difficult. Carriers are much more vigilant about detection and deterrence as well.

Method	Description	Business Impact	% from 2010
1 Mobile Phishing Attacks	Many of the same e-mail and Web-based phishing attacks on PCs have been used against mobile devices. However, other existing variations use mobile-specific technologies such as SMS. A common variation of mobile phishing involves fooling victims into texting premium-rate numbers.	Phishing attacks vary in impact and severity. An attacker may target victims with premium paid SMS text messaging services, malware installation on the mobile device, or harvesting banking or other sensitive user information. Because of easy implementation and immediate monetization of the attack, mobile phishing is currently the most prevalent and may sometimes be part of a larger malware infection.	60%
2 Mobile Ransomware	Ransomware is malware designed to infect a user's device and actively prevents or threatens the user from using the infected device, demanding payment for removal or release of a device lock. The attack often also involves stealing sensitive user information such as SMS, voicemail and e-mail messages.	Ransomware attacks can be severe; if an attacker compromised a device as part of the infection, the user's data may not be available unless they pay the ransom or, if the attack has harvested potentially compromising information from the user, this attack may even develop into full-fledged blackmail. To date, multiple ransomware attacks targeted platforms including Symbian S60, Blackberry and Windows Mobile.	15%
3 Fake Firmware and Jailbreaks	Fake firmware and jailbreaks are similar to phishing attacks, but specifically target a user on their PC system, enticing them with phony new versions of firmware or a jailbreak. Though in some cases the fake firmware or jailbreak installation program may work, they are malware designed to infect the user's computer.	In many cases, this malware also (or exclusively) targets the PC it is run on. The attack may compromise sensitive user and corporate information on both a mobile device as well as a victim's PC.	13%
4 Mobile Trojans/ Bots/Worms	Infecting devices without the user's knowledge, these attacks aim to provide the attacker with harvested sensitive user information and, in many cases, remote control of the infected system. Mobile botnets, Trojans, worms and other malware have been used to specifically target mobile users. Infection varies from luring victims into accepting malicious programs to exploiting mobile software vulnerabilities.	A mobile device infected with malware may be fully accessible to an attacker, although on some occasions, full system level access may not be possible due to mobile sandboxing techniques. In this attack malware seeks to compromise sensitive user information such as banking information, user credentials e-mail (corporate and personal), and other sensitive communications. On mobile devices, even voice calls, geographical location, SMS texting and other unique features are also at the mercy of an attacker.	8%
5 Client-Side Exploitation and Forced Jailbreaks	Client-side vulnerabilities and exploits are an increasingly common vector of attack on mobile devices. As more security research is done on mobile platforms, the bar is being lowered for exploitation. An increasing body of knowledge is being developed in the white- and black-hat hacking communities as relates to low-level system details on mobile devices. For some platforms, the bar is somewhat lower since a large amount of the architecture is based on open source software (e.g.., Android). However, even more proprietary platforms such as the iPhone commonly use a large amount of open source code as well.	To date, this form of attack has been less common than other counterparts due to the inherent complexity of implementing it successfully. The primary reason the bar is higher is that an attacker needs a working exploit for an un-patched vulnerability. However, there have already been cases to date of mobile device vulnerabilities being used to install rootkits and other malware on victims' devices. We have also seen a steadily growing trend of new vulnerabilities being found and exploited on mobile devices in general, so it is anticipated that the frequency will only increase for this form of attack in the future.	4%

Mobile device technology advancements of the last decade have led to always connected, Internet-enabled phones and other devices. At the beginning of 2010, around 500 million devices existed on 3G enabled networks. A typical smartphone today has the same processing power as a PC from eight years ago, but also supports an array of advanced hardware capabilities such as built-in audio, video and geographical location. And about 60% of users carry their devices with them at all times.

As the security of mobile networks has improved, mobile devices themselves are increasingly a target for attack. In the early 2000s, a flurry of real-world malware attacks begin to evolve against popular smartphone platforms such as Symbian, Blackberry and a wider class of J2ME-enabled devices. With the advent of new mobile device platforms, such as Microsoft's Windows Mobile, Apple's iPhone and Google's Android, comes additional malicious attacks and security research.

Known Incidents from 2010

Weaponized Remote iPhone Jailbreak Rootkit Proof of Concept

Released in August 2010, a new jailbreak for iPhone used a previously undisclosed vulnerability in the PDF-rendering engine for Mobile Safari coupled with local privilege escalation kernel vulnerability to achieve full compromise on any modern iOS device. The jailbreak was intended for users to jailbreak their own iPhone devices. However, the characteristics of the vulnerability indicated it could also be used by malicious attackers to compromise iPhones without an owner's knowledge.

Several unconfirmed reports of drive-by download MITM attacks targeting the jailbreakme.com website occurred in August during the Defcon 2010 security conference right after the jailbreakme.com site was launched. Seeking confirmation, SpiderLabs researched and presented a successful proof of concept exploit derived from the jailbreakme.com implementation at Ekoparty in September 2010 and again, with additional research, in October 2010 at Toorcon.[15, 16]

First Android SMS Trojan Found in the Wild

A new Android Trojan was discovered by Kaspersky Labs anti-virus and dubbed Trojan-SMS.AndroidOS.FakePlayer-A in August 2010. The application posed as a media player application but was designed to steal money from those who installed it by sending fraudulent SMS paid text messages.

TROJAN-SMS.Fakeplayer was not the first malware for Android to be found in the wild, but it is the first example to date that exploits SMS premium-paid text messages for financial gain. This type of malware has become common on older platforms such as Symbian S60 and Windows Mobile, but until this case, had not been used against newer generation devices such as Android.[17, 18, 19]

Zeus Mobile Bot Variants Discovered in the Wild

The infamous Zeus botnet is an increasingly prevalent threat against PC Windows systems. In September 2010, however, we also saw new Zeus bot variants designed specifically for mobile devices. Monitoring of the Zeus botnet by Fortinet exposed new variations running on Symbian S60 and Blackberry devices in the wild. Symbian, Blackberry and J2ME malware had already been quite prevalent. Significantly, this bot infection was being used by attackers specifically to intercept mTAN banking authorization messages via SMS and access victims' online bank accounts.[20, 21, 22]

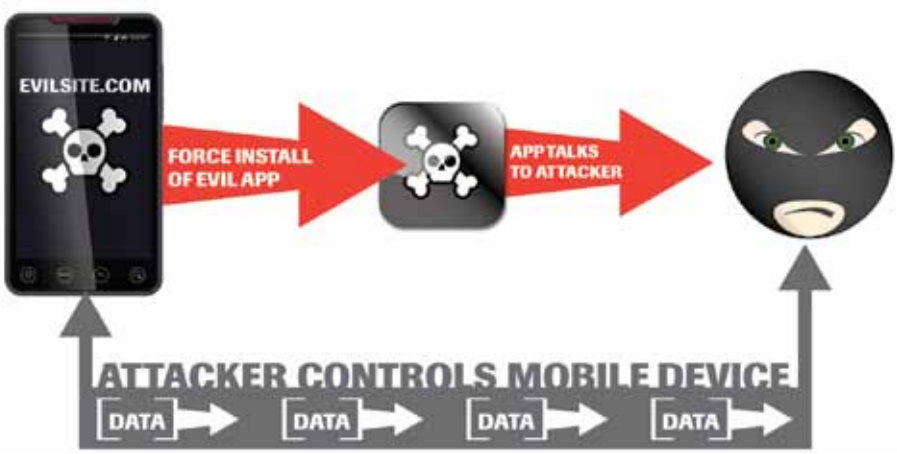
Conclusions

The mobile device space demonstrates that traditional barriers in embedded security are falling down. For a long time, a certain level of security through obscurity existed in mobile devices and other embedded systems. As we see more developments in mobile security, the lessons learned correlate closely with other proprietary embedded systems.

We expect to see even more malware attacks targeting mobile devices as sophistication of attacks develop and new technologies mature. Other trends we expect may develop in coming years is the advancement of further security research and real-world implementations in the wild of GSM protocol attacks at the RF layer.

[15] "iPhone Jailbreak Tool Sets Stage for Mobile Malware." http://threatpost.com/en_us/blogs/iphone-jailbreak-tool-sets-stage-mobile-malware-102310
[16] "Toorcon 2010: iPhone Rootkits? There's an App for That." http://www.slideshare.net/esmonti/toorcon-2010-iphone-rootkits-theres-an-app-for-that
[17] "Popular Porn Sites Distribute a New Trojan Targeting Android Smartphones." http://www.kaspersky.com/news?id=207576175
[18] "First SMS Trojan for Android is in the Wild." http://www.theregister.co.uk/2010/08/10/android_sms_trojan/
[19] "Dexcode Teardown of the Android SMS Trojan." http://jon.oberheide.org/blog/2010/08/10/dexcode-teardown-of-the-android-sms-trojan/

Mobile Phishing Attack



Mobile Platforms: An Attackers Perspective

The sophisticated software and hardware on mobile device platforms offers new opportunity for attackers. The same classes of vulnerabilities that were popular eight years ago have found new life in the mobile world, as many mobile devices do not support newer security features commonly found in desktops and laptops.

Security threat trends are proportional to the profitability of attacks and mobile hacking trends have been no exception to this rule.[23] As mobile devices are used by more people to share information, access bank accounts and store data, one can expect that the frequency and sophistication of attacks will only increase.

Mobile Malware: In the Wild

The mobile operating system ecosystem is much more diverse than the desktop computing world. Mobile platforms have varied frequently in terms of use and popularity. In the late 1990s through the early to mid-2000s, Symbian S60 was the leader in smartphone and mobile market share, followed by Blackberry. Symbian's success is owed largely to the popularity of the Nokia phones on which it ran. With the release of Windows Mobile by Microsoft and several new mobile smartphones running it, Symbian's dominance began to wane. Apple's iPhone and Google's Android have only increased in popularity since their release.

Malware trends typically correlate with platform popularity. Through the early to mid-2000s, Symbian malware samples were being discovered in the wild at an increasing rate, with several malware families developing and evolving into variants during this time. A significant number of J2ME-based malware attacks began to surface during this time as well. These attack implementations were more portable between multiple platforms, as Symbian and a large number of other device OS platforms also supported J2ME application compatibility. Third party J2ME runtimes were even available for Windows Mobile.[24]

SpiderLabs witnessed several malware incidents targeting next generation platforms such as Windows Mobile, followed by iPhone and Android. We also saw new malware targeting Symbian, Blackberry and J2ME devices, albeit at a slower pace.

Mobile Rootkits

Known mobile malware incidents are still immature compared to PC and enterprise malware attacks. But real-world attacks and research findings are growing steadily in severity, sophistication and frequency. To date, modern smartphone malware targeting iPhone and Android has been uncommon and of limited sophistication. Earlier this year, however, SpiderLabs presented ongoing research in advanced mobile rootkit techniques and mitigations which targeted both Android and iPhone platforms.

[20] "Zeus Malware Purveyors Target Symbian, BlackBerry Devices." http://www.eweek.com/c/a/Security/Zeus-Malware-Purveyors-Target-Symbian-BlackBerry-Devices-800557/

[21] "Zeus In The Mobile (Zitmo): Online Banking's Two Factor Authentication Defeated." http://blog.fortinet.com/zeus-in-the-mobile-zitmo-online-bankings-two-factor-authentication-defeated/

[22] "ZeuS Mitmo: Man-in-the-middle (I)." http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html

Many techniques developed as part of this research are similar to well-established PC rootkits including loadable kernel modules, foreign process library injection and basic backdoor user-land programs added to the system. Leading mobile platforms such as iPhone, Android and Windows Mobile have much in common with their corresponding PC operating system architectures, respectively Mac OS X, Linux, and Windows. The techniques used for creating backdoors on mobile devices can therefore draw upon a wide body of pre-existing research and techniques in the area of rootkit development.

Attacks on Mobile E-mail and Web Browsers

Both e-mail and Web-based attacks exist, whether developed initially for PCs or specifically targeted against mobile devices. Malware attacks targeting phone platforms either exploit mobile software vulnerabilities or lure users into accepting Trojans through phishing attacks. Some attacks target users via directed e-mail, while in a few cases client-side software vulnerabilities were exploited via Web browsers and e-mail messages.

Attacks on SMS and MSS Weaknesses

Short message service (SMS) and multimedia messaging service (MMS) are popular features exploited by mobile malware. Symbian and J2ME-based mobile platforms have historically been targeted by Trojan horses that send SMS messages to premium-rate numbers without user consent.

SMS has also been used in various fraud and phishing attacks as well. At the 2009 Black Hat security conference, two separate groups of researchers published information on attacks targeting SMS vulnerabilities in both carrier networks and mobile devices themselves.[25, 26] The latter class of attacks exposed vulnerabilities in SMS handling on several mobile phone platforms. SMS security threats require continued research and vigilance, particularly in regard to attacks on mobile transaction authentication numbers used by online banking and other businesses.

Attacks on Mobile Transaction Authentication Number (mTAN)

Mobile Transaction Authentication Number (mTAN or SMS-TAN) is an easily deployed, two-factor authentication used by online banking and other industries.[27, 28] Considered difficult for attackers to obtain, authentication data is used to send one-time passwords via SMS to the customer to authenticate various online transactions. mTAN is also used to authenticate sensitive operations online, such as password resets.

By compromising a victim's SMS messages, an attacker can intercept mTAN one-time credentials to transfer funds out of a bank account or perform other actions. SpiderLabs research into smartphone rootkits in 2010 demonstrated how easily they could be implemented using Android and iPhone platforms. Shortly thereafter, reports on mobile malware in the wild implementing this attack against multiple online banking sites via Blackberry and Symbian-based phones surfaced.[29] Samples of a Zeus mobile botnet variant were identified in use to break into victims' online bank accounts via mTAN attacks. This Zeus malware variant uses SMS for botnet command and control (C&C) communications back to the botmaster. Several high-profile arrests of Zeus botnet operators in the EU were also announced around the same time.

Conclusion

We have much to learn in the area of mobile security, but the lessons are strikingly similar to those that we've encountered before. No device or network is inherently trustworthy, and any technology that handles our personal information, including mobile devices, must be treated with security in mind.

[23] "Hacker Spoofs Cell Phone Tower to Intercept Calls." http://www.wired.com/threatlevel/tag/chris-paget/
[24] "Mobile Malware Will Increase Proportionally to Profitability." http://unplugged.rcrwireless.com/index.php/20100930/news/3952/mobile-malware-will-increase-proportionally-to-profitability/
[25] "J2ME Programming/MS Windows Mobile and J2ME." http://en.wikibooks.org/wiki/J2ME_Programming/MS_WindowsMobile_and_J2ME
[26] "Researchers can attack mobile phones via spoofed SMS messages." http://news.cnet.com/8301-27080_3-10300174-245.html
[27] "Researchers attack my iPhone via SMS." http://news.cnet.com/8301-27080_3-10299378-245.html
[28] "Transaction Authentication Number." http://en.wikipedia.org/wiki/Transaction_authentication_number
[29] "Zeus Mitmo: Man in the Mobile." http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html

Social Networking

Social networking sites allow users to potentially share their personal information with friends, peers and the public at large. They also can act as malware propagation engines for both general and targeted attacks, and present security challenges that the computer security industry is only recently beginning to understand and address.

Like initial e-mail and IM attacks, the first generation of social networking attacks took a shotgun approach, targeting many users in hopes a small percentage of them would fall victim to the attack. There have been many effective phishing campaigns on Twitter, variants of Koobface have infected millions of Facebook users and social networking sites have been used to expand and propagate botnets. Industry experts have claimed social networking sites are the most targeted vertical in recent years. More recently, attacks have become sophisticated and targeted, through the use of geographical location data and other methods.

Method	Description	Business Impact	% from 2010
1 Malware Propagation	Presenting an application or link through social networks that appears to be a game or questionnaire, but infects the user's account and/or computer.	This attack has been used to create botnets for later use by attackers. These uses include spamming, hosting phishing sites, or harvesting information for use or sale (banking or credit card information). The attack can also be used for causing personal or corporate damage to the owner of the attacked profile by creating false information or stealing data previously thought to be "private" on the social site.	25%
2 Personal Information Exposure	Individuals place personal information, such as phone numbers, birth dates, spouse information, travel plans or other items on a public profile.	An attacker can gather a variety of information from various social networking sites to profile where an individual will be, when and how to contact them through various means. This can be used to assist in stalking, theft of property or otherwise causing harm.	30%
3 Data Mining	Data mining information from public profiles to use in other attack vectors.	An attacker can mine the information that known employees of a target organization make available on social networks to discover names, corporate infrastructure, events and other information. By further use of social engineering, an attacker could manipulate that employee into providing additional information.	20%
4 Exposure of Corporate Data	Employees post sensitive corporate data in public forums.	This allows an attacker to search through a public profile of an employee much as they would a hard drive in a compromised system.	20%
5 Brand/Reputation Manipulation/ Destruction	Creating a false account on a social network site to seed disinformation about a brand or person.	An attacker can create a profile while posing as an employee of a target organization. After becoming an established "member" of the target organization, the attacker can then spread disinformation or lies to manipulate the public's opinion of that organization.	5%

Malware

Multiple applications and links spread malware through social networks, usually taking the form of an application or a link advertised as something the user would find interesting. In some cases, the malware harvested all of the user's data, public or private, and then propagated itself to all the friends the user had on that particular social network. In other cases, installed software resulted in that machine becoming part of a larger botnet to be used for future spamming, phishing and other malicious activities.

With social networks, attackers are able to spread malware more quickly across a wide range of users. An instance of malware spread through Twitter took two and a half hours to infect the same number of users that would normally take a day or two through non-social networking attacks.

Command and Control

SpiderLabs observed that Twitter and other social networks have been used for sending commands to infected systems that have then become part of botnets. Attackers start by creating multiple accounts on a social network. Once created, encrypted commands are written into the profile of the account. As systems become infected with malware, they are controlled and instructed to check a particular profile for commands, ranging from looking for other machines to infect, to starting a keylogger to monitor user typing, to identifying other accounts on that social network that can be used in the event that the originating account is detected and deleted.

Besides allowing attackers to hide in plain sight, this method allows them to control systems that may be infected but are behind network security measures that are configured properly. Attackers can prevent such systems from receiving commands via other communication styles; the infected system will appear to be requesting a website over a commonly used port, such as port 80 (HTTP) and port 443 (HTTPS).

Phishing Attack

Facebook users have publicly requested additional functionality in the form of a "dislike" button. Since Facebook has elected to not provide the functionality, malware developers created an application that advertised this functionality. Called "The Official Dislike Button," the application requested the following levels of access:

- Access basic information
- Posting to the wall
- Accessing data at any time

After successful installation, the malware directed the user to an online survey. Following its completion, the user was directed to a Firefox plug-in page to install add-on software for their Web browser. Finally, the application posted on the user's wall to advertise to other Facebook users.

Though this particular malware seems harmless, future iterations of the same style of attack could be used for more malicious activity, including installation of Trojan software and capturing of logins and passwords.

Conclusions

Social networks, with millions of users and more people joining every day, are an attractive target for spreading malicious software and information gathering to identify users from a particular company for use in future social engineering attacks. Individuals and businesses should exercise caution in posting potentially sensitive information as well as pay attention to what access levels social "applications" are requesting. Proper education and awareness can help all social network users realize the simple fact that "a friend of my friend is not necessarily my friend."

Dealing with Employees and Social Networks

Friends and families use social networks to stay in touch and up-to-date with each other across physical distances, and companies are embracing it as a free marketing tool and possible revenue stream. Both individuals and organizations can overlook certain details when utilizing, or planning to utilize, these portals to the masses.

Employees are already on these sites with the ability, whether they know it or not, to affect a company's image and Internet presence. Social networking has the potential to turn every employee into a public relations nightmare. Because of the social nature of these sites, people discuss their jobs, complain about internal problems, and disclose, inadvertently or intentionally, proprietary information.

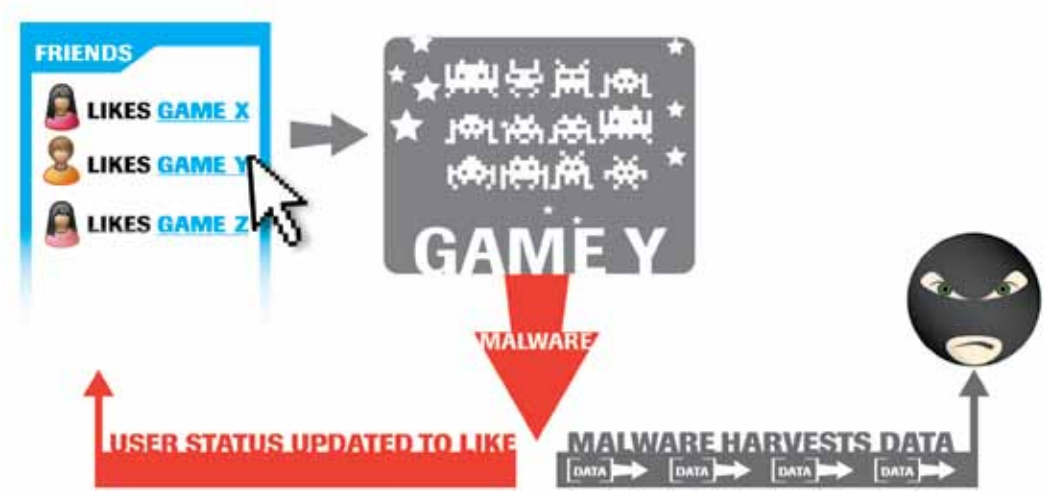
Most of the time, this act of sharing information is not intended to be malicious. It could be something as simple as an employee sharing his excitement about a future move the organization hopes to make, but forgetting that his profile is public and accessible by 1,298 "friends." Regardless of intent, the information is now public, has been indexed and archived by search engines and is now a permanent part of the Internet's recorded history.

Some companies block access to social networking sites and others monitor their employees' accounts. The first technique may have been useful in the past, when employees did not have access to high-speed, data-enabled mobile devices, but these days the idea of blocking a user from a site is useless and obsolete. Monitoring is still an achievable tactic, but there is no guarantee a company knows all of its employees' accounts. Furthermore, an employee's post is instant and monitoring only lets the company know what has been exposed after the fact.

Education is the key to this problem. Without proper education, employees will not always realize what information is appropriate or remember that their posts are seen by hundreds of people at once, who possibly will repeat it to hundreds more. People also don't always realize how much personal information they are exposing across these sites; information leaks can not only be used against an individual, but also against an individual's employer.

With proper employee education, organizations will not just help protect themselves from data loss across social networks, but can also help improve the security awareness and safety of their own staff when they visit these sites.

Malware Propagation through Social Network



11 Strategic Initiatives for 2011

At the end of each engagement or research effort, the SpiderLabs team analyzes and consolidates the information, knowledge and experience gained to provide to our clients guidance for the coming year.

For executives and managers who are tasked with ensuring their company does not suffer a security event, this section of the Global Security Report 2011 will provide that guidance. While many believe these initiatives are already in practice, our experience has shown that attacks are often successful in organizations that thought they were completely covered. Whether this list is used to define a comprehensive data security strategy or as a second opinion, it can help any organization reduce its risk of a security compromise.

The Top 11 Strategic Initiatives for Every Organization

1 Assess, Reduce and Monitor Client-side Attack Surface

Why: In 2010, we saw client-side attacks occurring faster than anyone would have predicted. Software developers of browsers, plug-ins and viewers were at times issuing security updates every couple of weeks.

How: For various classes of applications, create an organizational standard. Monitor those versions and develop a method of inventorying the applications to measure adherence to standards. Finally, develop a method of evaluating risks, communicating them if needed and rapidly patching them when required.

2 Embrace Social Networking, but Educate Staff

Why: The medium is not going away anytime soon; social networking is being used to improve brand awareness, reduce costs and connect with customers. Along with official business uses, employees are going to join the ranks of everyone else on the planet from age 2 to 102. With this come risks, such as public exposure of private company information or cybercriminals identifying targets by mining social profiles for personal information.

How: Establish a policy on what company information and activities can be shared by unofficial users. Educate staff on this policy and provide them additional awareness training on how they can protect themselves and the organization against social networking based attacks.

3 Develop a Mobile Security Program

Why: Staff with company issued smartphones, laptops and other devices carry their organization's intellectual property with them wherever they go.

How: Evaluate the various platforms used by employees, identify those that cannot enforce enterprise profiles and decide how to phase them out. Over the next few years, mobile attacks may surpass those against desktops. Gaining as much control over the configurations of mobile devices as there is for desktop and service environments will help organizations begin to reduce risk.

4 Use Multifactor Authentication

Why: People choose easy to remember (poor) passwords if they are allowed. Even with the enforcement of password complexity rules, many often still choose passwords that are weak in strength.

How: Multifactor authentication does not work everywhere, but should be strongly considered where possible. Critically important for perimeter access such as VPN or Remote Access, the cost of implementing a multifactor solution is far less than the impact of a major breach of the corporate network and loss of data.

5 Eradicate Clear-text Traffic

Why: Cybercriminals know that businesses send sensitive data over private networks in the clear.

How: This is as simple as implementing SSL certificates for Web-based transactions, using e-mail encryption or using end-to-end encryption for transaction processing systems.

6 Virtually Patch Web Applications Until Fixed

Why: Both internal and external Web applications should be tested on a continuous basis using both manual and automated means to identify security issues. Vulnerabilities can then receive a virtual patch until a full patch can be developed.

How: Implement a Web application firewall and apply a virtual patch to protect applications based upon the result of the security testing. The development teams can then create a fix for the vulnerability; once it has been validated the Virtual Patch can be safely removed from the WAF.

7 Empower Incident Response Teams

Why: An organization's internal incident response team should be investigating anomalies. If there is no incident response team, consider creating and maintaining one.

How: The incident response team should have access to the security team's notifications or information stored within log aggregation or analysis systems, such as a security information and event management (SIEM) system. Empower the team to investigate even the most obscure issues. While investigating a data breach, SpiderLabs often learned there were minor signs of criminal activity identified by the organization's internal staff several months before we arrived, but no one investigated. Security teams are often told to wait for the next large breach or HR-issued directive to take action, rather than seeking out signs of initial attack activity.

8 Enforce Security Upon Third-Party Relationships

Why: Third-party vendors and their products introduce vulnerabilities, mostly as a result of default, vendor-supplied credentials and insecure remote access implementations.

How: Organizations need to be aware of what regulations or industry requirements apply to them, and what is required of their third-party vendors to be able to know if those vendors are compliant. For large strategic partnerships, organizations should require their partners to undergo third-party security testing on a regular basis, with the results shared with the security team. In addition to functional testing, organizations should strive to include non-functional security requirements for implementation, maintenance and support services in their agreements with vendors.

9 Implement Network Access Control

Why: Most internal network environments tested by SpiderLabs had a weak security posture. Externally, attackers can only utilize Layer 3 (the network layer on the Open Systems Interconnection [OSI] model, and above to perform their attacks. On the internal network, they can start at OSI Layer 2. This means that an attack, such as MITM, is not only effective, but easily performed in most corporate environments.

How: A network access control solution combined with a segmentation strategy can help the internal network be just as resilient against attack as the externally protected perimeter.

10 Analyze All Events

Why: Network devices, servers, workstations and applications can all generate events. We often don't let them because the "noise" they create can overwhelm the security staff. However, these events frequently serve as an early indicator of the origins of an actual attack.

How: Implement a security information and event management (SIEM) system to help turn noise into action by applying policy and workflows to environments events.

11 Implement an Organization-wide Security Awareness Program

Why: Security awareness training may not stop an insider with malicious intent, but it can mean earlier detection and notification of a potential incident. Even an entry-level employee may notice something amiss if trained to be more security aware. Such security awareness training for employees can be especially effective in combating the risks posed by social engineering.

How: Organizations should look to implement a security awareness training program and make it mandatory for every employee, regardless of title or function. This training should be repeated at least annually and made it part of all new hire orientation.

Global Conclusions

In 2010, the information security landscape changed before our eyes. The intended target of attacks shifted from the infrastructure, to endpoint devices and their users allowing attackers to access applications hosting sensitive data. Individuals, often by their own actions, became even more personally identifiable to their attackers. Malicious tools became more customized, covert, automated and persistent. New devices, applications and other media continued to provide new ways for attackers to compromise private and sensitive information from businesses, customers and users.

We expect these trends to continue as organizations continue to innovate and grow, many which won't include security or privacy as an integral part of that process. In 2011 and beyond, organizations that approach their initiatives firmly committed to including security as an integrated requirement, and not just as a checkbox, will be most resilient to attack, reduce their risk to compromise, and be able to best protect both sensitive data and reputation.

Appendix A: Tool Description

Tool Description

Tool	Description
Archiving Utility	Often required to transfer data outside the compromised system. The most common tools used by attackers include WinRar and 7z.
File Manager	Used when attackers gain access to the system via RDP (Terminal Services); examples include FAR Manager.
Hacking Tool	Could be a well-known security assessment tool, or a customized tool used for finding vulnerabilities in the attacked networks.
Infostealer (User Accounts Credentials Thief)	Could be a well-known security assessment tool, or a customized tool used for gaining access to user accounts (passwords); examples include password retrievers, password hash dumpers and MS Gina hacking tools.
Infostealer / Keylogger	Most often an off-the-shelf keylogging or monitoring utility that comes with a rich set of functionality including, but not limited to: keystrokes and mouse click capture, screens capture, Web camera streaming, audio eavesdropping, and data extortion; examples include Blazing Tools Software's Perfect Keylogger and RelyTec's All-In-One Keylogger.
Local Reconnaissance Tool (Cardholder Data Scanner)	A dedicated scanner that walks through the file system searching for files potentially storing cardholder data (i.e., Track 1 or Track 2). It helps the attacker to verify whether the system is within the scope of their interest.
Local Reconnaissance Tool (Network Resources Enumerator)	Could be a well-known security assessment tool or a customized tool used for network resources enumeration. The most commonly used traverse the network shares and/or domain controller resources collecting information about systems, users and sometimes testing whether they are prone to a dictionary attack.
Local Reconnaissance Tool (Network Scanner)	Could be a well-known security assessment tool or a customized tool used for network shares enumeration.
Local Reconnaissance Tool (Send Mail Tester)	A simple tool that tries to send a test e-mail to an external point; if successful can help the attackers to extract the data via e-mail.
Local Reconnaissance Tool (UI Language Identifier)	A simple tool that identifies the location and language of the attacked system.
Memory Dumper	A simple tool that enumerates processes and dumps memory of all of them, or dumps a memory of a specific process.
Memory Dumper and Parser	A simple tool that combines the memory dumping with parsing; it usually targets a specific process' memory and parses it looking for track data; the output is saved to a file that the attacker collects occasionally.

Tool	Description
Network Sniffer	A tool that modifies the NIC's state into a monitoring (promiscuous) mode. Once enabled, it can intercept the data from the network card.
Patcher	A simple tool that modifies the targeted application; patching may involve a binary patching (code/data modification), or configuration change (e.g., enabling transaction logs or debugging information).
Local Process Launcher	A tool that helps in launching specific commands on a local computer; most often part of the reverse shell.
Remote Process Launcher	A tool that helps in launching specific commands on a local computer; the most commonly used is psexec from Microsoft/Sysinternals.
Time-stomping Utility	A tool that modifies the timestamps associated with a file; once modified, the timestamps make the file "blend" with the files located on the system and only forensic investigators or experienced users can detect such files.
Utility (Network Share Adding)	A simple tool that helps in adding shares.
Utility (Process Termination)	Terminates specific processes.
Utility (Remote Service Deletion)	Helps in launching services placed on remote systems.
Kernel Mode Modules Loader	Places a kernel module in memory and launches it as a service.

Contributors

Authors

Ryan Barnett
Rob Havelt
Charles Henderson
Jibran Ilyas
Ryan Jones
Ryan Merritt
Eric Monti
Steve Ocepek
Nicholas J. Percoco (Lead)
Colin Sheppard
John Yeo

Editor

Sarah B. Brown

Art Direction and Design

Nathan Glick

Contact Us

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

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

+1 312 873-7500

GSR2011@trustwave.com

https://www.trustwave.com/spiderlabs

Twitter: @SpiderLabs / @Trustwave

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure—from the network to the application layer—to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

Corporate Headquarters
70 West Madison St.
Suite 1050
Chicago, IL 60602

P: 312.873.7500
F: 312.443.8028

EMEA Headquarters
Westminster Tower
8th floor
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) 3521-7314
F: +55 (11) 3521-7070

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℠

Copyright © 2011 Trustwave Holdings, Inc.
All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions.

Trustwave and Trustwave's SpiderLabs names and logos are trademarks of Trustwave. Such trademarks shall not be used, copied or disseminated in any manner without the prior written permission of Trustwave.