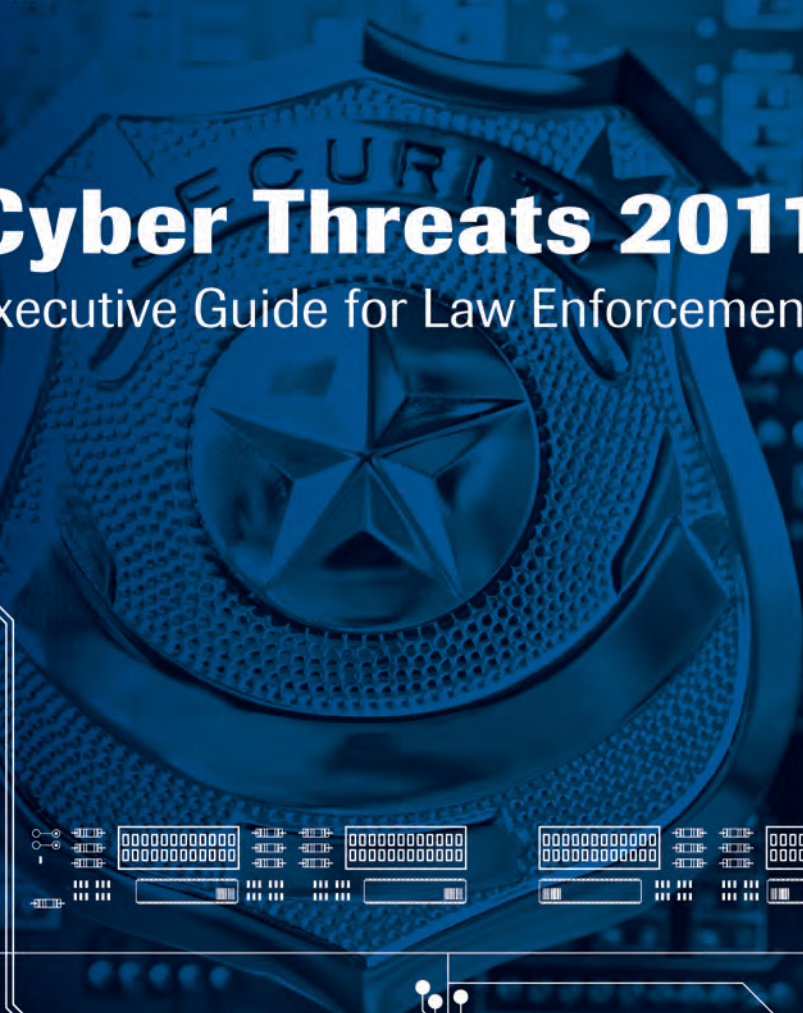




Cyber Threats 2011

Executive Guide for Law Enforcement



Contact Us

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

+1 312 288-4875

leoguide@trustwave.com

<https://www.trustwave.com>

Twitter: @Trustwave / @SpiderLabs

To the Chief:

The law enforcement community has unique needs and concerns that the commercial world does not — if mistakes are made and information compromised, lives may be in danger, and investigations and subsequent litigation may be negatively impacted. With cyber criminals using technology advances to gain an advantage over law enforcement, it is now more important than ever to develop a defense-in-depth strategy to protect information about undercover personnel, confidential informants and other sensitive measures. *Cyber Threats 2011: Executive Guide for Law Enforcement* aims to assist law enforcement in better understanding and addressing today's cyber security threats.

Each year, Trustwave SpiderLabs conducts hundreds of data breach investigations, and thousands of technical application and network penetration tests. By coupling this information with intelligence gleaned from ongoing investigations, technical testing and collaborative efforts with law enforcement, we produced this guide specifically for chiefs of police and other executive law administrators.

In this guide, we identify the top vulnerabilities encountered in 2010 and provide an actionable list of strategic initiatives for law enforcement to improve its' overall security. Our goal is simple: share information to help reduce the risk of compromise and thereby reduce the risk of harm to your officers, employees, victims, witnesses and ongoing investigations.

Trustwave has many law enforcement roots; in addition to personnel experienced in federal and military criminal investigations, prosecution, military and intelligence analysis, and operational work, we collaborate with federal, state and local law enforcement in support of their criminal investigation mission. For more than 10 years, Trustwave has trained law enforcement on the methods and techniques to conduct digital investigations, such as through our widely popular, "Sniper Forensic" course. We have conducted more than 1,000 data breach investigations in coordination with law enforcement and police agencies.

Trustwave has built its business on trust by providing comprehensive security strategies that incorporate cutting edge solutions and trained subject matter experts to help organizations continuously protect their most sensitive data. The guide draws from this commitment and is intended to provide you with the current state of information security, as well as recommendations on how to secure your data. Your feedback is essential and we welcome the opportunity to collaborate on future projects for the law enforcement community!

Thank you for your hard work and dedication in keeping our communities safe.

Sincerely,



Robert J. McCullen
Chairman, CEO and President of Trustwave



Introduction

In today's world, confidential data and access to that data is a major battlefield in an ongoing cyber war. The law enforcement community is not immune, and is frequently a target for cyber attacks. Whether the motivations are political, criminal or retaliatory, the methods used by cyber attackers will be the same. Overcoming these threats requires an understanding of the major attack vectors and the strategy needed to fortify the IT environment. In this document you will learn about both established and emerging ways in which cyber criminals access sensitive information, as well as the methods you can deploy to reduce and prevent their activities.

Areas of focus include:

- Network Security
- Application Security
- Mobile Devices
- Social Networking

In addition, we offer a list of 10 questions to ask the head of information technology (IT) or Chief Information Security Officer (CISO) about the information security efforts being employed to protect digital assets from attack.

The Network

The network represents one of the most utilized attack vectors; attackers have the ability to perform attacks remotely, with relative anonymity, via the Internet. If your department has access to the Internet or hosts a website, you are exposed to potential network-based attacks. 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 weaknesses within the infrastructure, either by manipulating networking equipment or the protocols used to facilitate interoperation. Successful network attacks can be severe and are frequently difficult to detect.

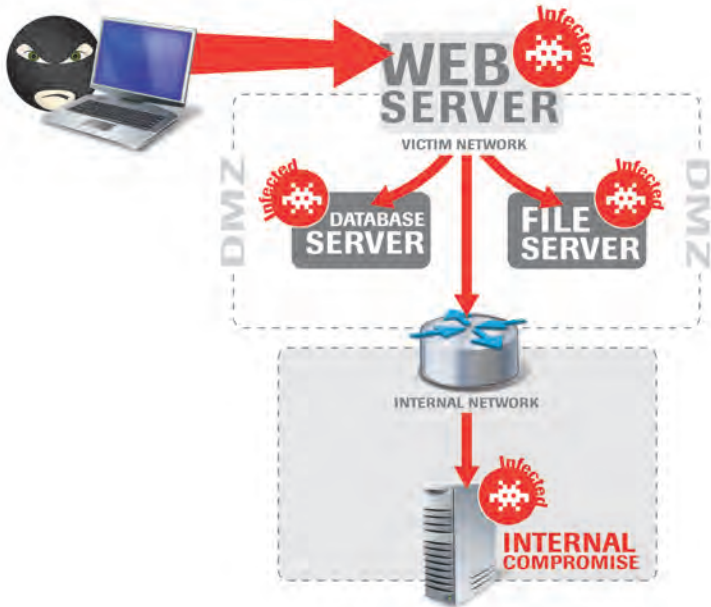
Successful exploitation is often followed by the installation of backdoors to facilitate successive phases of attack. Using a compromised host in this way is called "pivoting," since the attacker will often have access to more attack surface at each point of insertion. By loading tools onto each compromised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

New methods of attack to gain access to internal networks are constantly evolving, however, they often remain unaddressed. Once an attacker is inside your network, they can intercept and manipulate data while in transit, harvest user credentials (user

names and passwords), and identify additional potential targets. Default credentials also hinder efforts to secure the network, serving as a very weak link in what can be an otherwise strong defense.

Trustwave SpiderLabs developed a Top 10 list of network vulnerabilities based on more than 2,300 penetration tests conducted in 2010:

1. Weak or Blank Passwords for an Administrative Level Accounts
2. Data Base Servers with Weak or No Passwords for Administrative Accounts
3. Address Resolutions Protocol (ARP) Cache Poisoning Possible on Internal Networks
4. Sensitive Information Transmitted Unencrypted on Internal Networks
5. Client Sends LAN Manager (LM) Response for NTLM Authentication
6. Vulnerable Legacy Services (Buffer Overflow Attacks)
7. Virtual Network Computing (VNC) Authentication Bypass
8. Misconfigured Firewall Rules Permit Access to Internal Resources from the Internet
9. Storage of Sensitive Information Outside the Designated Secured Zone
10. DNS Updates Permitted Due to Dynamic DNS Misconfiguration



External Network Attack Leading to Internal Network Attack

Visibility into which systems house critical information, where those systems exist, and how they are accessed is most often lacking, making the reconnaissance phase of an attack vector one of the most important. You can't secure what you 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 identifying critical assets, closing the known gaps that exist in the network infrastructure, and finding ways to better monitor the use of this vital resource.

Recommendations for Network Security

Proper configuration and implementation of the following solutions can lower the risk of network attacks:

- Firewall
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Security information and event management (SIEM)
- Network access control (NAC)

CASE STUDY

Real-Time Street Views

Recently, Trustwave assisted with a unique deployment of technology for a mid-sized municipality. The city, and their associated police and fire departments, wanted to integrate traffic cameras and cameras in police cars, allowing their Chief and the threat intelligence section to have a first-hand, real-time view of crime scenes. This solution would also allow command staff to have same-time insight into the actions of their officers.

While this concept merged technology and creativity to offer real-time, unaltered intel, it also led to several possible vulnerabilities. Failure to properly implement security measures could allow hackers, whether employed by organized crime or not, to exploit unaddressed vulnerabilities. They could gain access and control of the cameras, potentially repositioning them, resulting in false intelligence to first responders. Cameras in squad cars could also be disabled prior to a planned physical attack on an officer. Understanding the cyber threats and taking the proper steps to reduce the risk of compromise are critical.



CASE STUDY

Compromise of Systems during the Provisioning Process

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 since they are not traditionally viewed as part of the organization's "production environment." In ideal situations they are properly segmented from production systems, but this is not always the case.

A Trustwave SpiderLabs team member, using a basic network scanner, was able to locate one of these networks during a penetration test. The environment was recognized by the different vulnerabilities located on 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 the firewalls did not employ any packet filtering. Additionally, 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 install media had been produced by the manufacture.

Our expert gained access to these systems while they were still being configured. After compromise, keystroke loggers and network sniffers were installed on the target systems, allowing access to sensitive information. As a result of our activities, we were able to infect the target organization's employee systems before they were given to the end users.

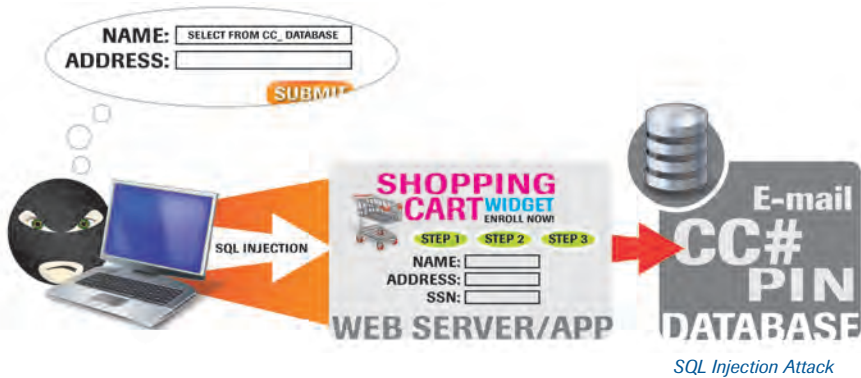
This lack of security in the IT department provisioning process could result in attackers infiltrating employee systems for on-going exploration and data exfiltration. Properly assessing all networks in an organization's environment, and in turn using their risk profile to map an increased level of security to critical systems, would have prevented this type of attack.

Application Security Sanity: There are No Silver Bullets

Today, small police departments may have no more than three custom applications to support their work processes, whereas large departments can easily have dozens of applications, if not more. Applications play critical roles in daily operations; application security is a key element to protecting departmental data.

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-implementation, it becomes more complex and exponentially more expensive.

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



Of course, no silver bullet exists. Application security is a multifaceted undertaking 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.

If your systems are online, it is likely that someone is “testing” them for you, looking for the gaps that will allow them a way in. You need to test for the same gaps in order to identify and fix application security flaws that exist, before someone else finds and exploits them.

The 24x7 availability of automated tools for system testing is complemented by analysis only available with manual testing by security experts. For example, application 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 Structured Query Language (SQL) injection, have nuanced multiple variations that are unlikely to be detected by an automated tool.

In contrast, manual testing is much more thorough, and should be performed at least annually. For ongoing security checks, automated scans can easily be performed as frequently as weekly against your department's applications. In addition, a Web application firewall (WAF) can provide 24x7 protection against attacks targeting common vulnerabilities such as simpler variations of SQL injection or XSS.

Regardless of the methods of discovery, identified vulnerabilities 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 those that appear to be non-critical. Continuous application protection can be had with "virtual patching" techniques with a Web application firewall (WAF). Virtual patching can protect the application from a threat while the development team works to fix the flaw.

The shortest period between awareness of vulnerability and fixing it is best. However, some security initiatives are best implemented 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 more comprehensive security posture. 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.

Recommendations for Application Security

Common Solutions for Security Offense:

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

Common Solutions for Security Defense:

- Web application firewalls (WAFs)
- Developer training
- Vulnerability patching

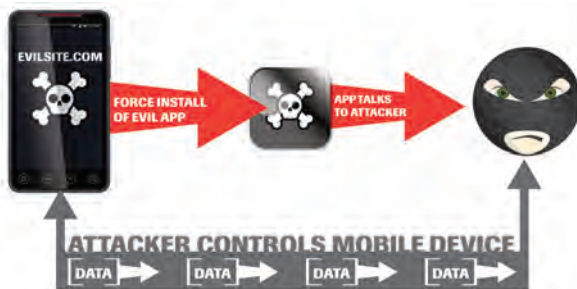
Mobile Devices: What You Need to Know

Mobile devices are now standard equipment for law enforcement officers. Internet-enabled smartphones and other devices, such as tablets and laptops, provide many capabilities that officers either depend on today, or will depend on in the future. Embracing mobile technology has many benefits but also some risk.

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.

At the beginning of 2010, around 500 million devices existed on 3G enabled networks. A typical smartphone today not only 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 integrated GPS. It is estimated that approximately 60% of users carry their devices with them at all times.

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.

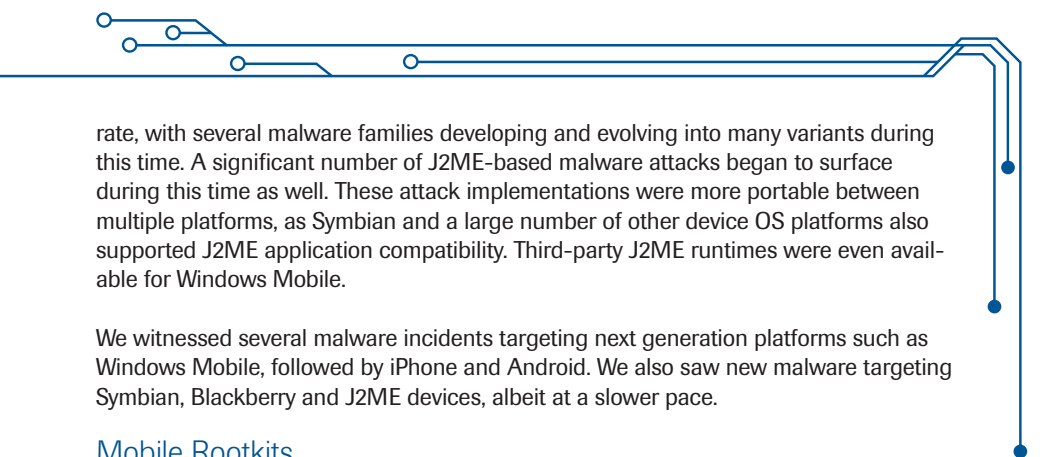


Mobile Phishing Attack

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 many 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.

We 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. However, Trustwave SpiderLabs has presented ongoing research in advanced mobile rootkit techniques and mitigation strategies that target both Android and iPhone platforms.

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 Email and Web Browsers

Both email 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 email, while in a few cases client-side software vulnerabilities were exploited via Web browsers and email 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. 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. Considered difficult for attackers to obtain, authentication data is used to send onetime 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. Trustwave SpiderLabs research on smartphone rootkits in 2010 demonstrated how easily they could be implemented using Android and iPhone platforms. Shortly thereafter, reports surfaced on mobile malware in the wild that leveraged this attack vector against multiple online banking sites via Blackberry and Symbian-based phones. 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.

As the security of mobile networks has improved, mobile devices themselves are increasingly a target for attack. In the early 2000s, a flurry of malware attacks began 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.

Security threat trends are proportional to the profitability of attacks and mobile hacking trends have been no exception to this rule. 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 likewise increase. No device or network is inherently trustworthy, and any technology that handles personal information, including mobile devices, must be designed, implemented and used with security in mind.

Recommendations for Mobile Security

- Mobile device management
- Security awareness education
- Email anti-virus

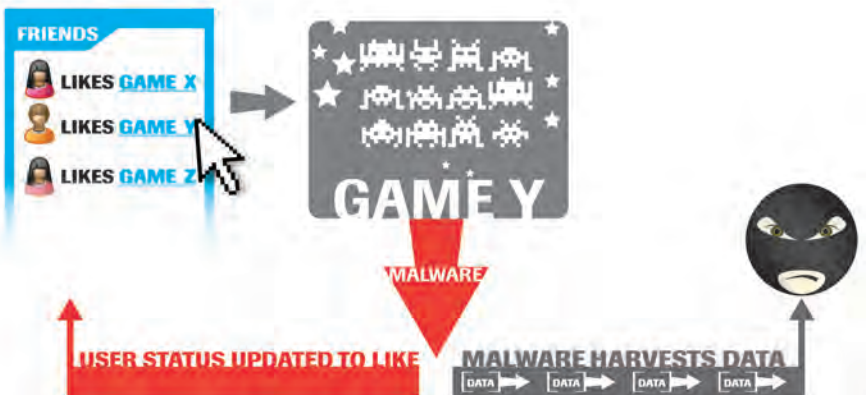
Social Networking: A Social Disaster?

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 and possibly sensitive company 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 organizations 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.



Malware Propagation through Social Network



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.

Social networking sites can also 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 email 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.

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."

Recommendations for Social Networking Security

- Security awareness education
- Social networking policies

10 Questions to Ask Your CISO

Cyber security threats are increasing as quickly as you can implement measures to counter them. Because of the constant onslaught of both new and old security threats, safeguarding data assets can be overwhelming for many security teams. Simultaneously, everyone is concerned with finding cost-effective ways to manage resources to ensure security throughout their department — without negatively affecting business operations.

Departments need to not only understand current trends in security threats, but also be able to identify inherent vulnerabilities within existing systems. Trustwave SpiderLabs offers an analysis of compromise investigations and the top vulnerabilities that potentially expose companies to security threats in their annual Global Security Report. To help executives identify an information security strategy, we developed the 10 questions you can ask your security teams.

1. Are we documenting our relationship with third-party vendors and are third party vendors being required to incorporate security controls?

In 80% of cases in 2010, third-party vendors and their products introduced vulnerabilities, mostly as a result of default, vendor-supplied credentials and insecure remote access implementations.


Choosing a platform and vendor with a solid security history is important, but monitoring those vendors to ensure they are following the same security practices as the hiring organization is equally important. Law enforcement departments should also ensure contracts with third-party vendors include security control requirements. If a vendor will not agree to security requirements, seek out a new vendor who will be responsive to your security needs.

2. Do we have an in-depth, comprehensive and relevant policies and procedures documentation to encourage department-wide buy in, support and increased awareness?

Consistency is the key to enforcing security because one weak link can “break the chain.” Many times well-meaning officers and staff can do things that jeopardize security — they don’t realize they’re doing it. By clearly articulating to staff strong policies for the department and the procedures necessary to fulfill those policies, departments can better ensure full understanding and adherence to those policies and procedures.

3. Should a security incident occur, do we have a team in place to assist at all levels?

Part of the difficulty in responding to a security event is the lack of a clearly defined and readily available procedure. Understanding how most incidents occur and where the breakdowns typically happen can play a role in developing a process flow and associated documentation. Equally important is forming an incident response team of trusted individuals from various operational groups within your department, including staff from the IT department, human resources, legal and public relations, among others. These individuals can be responsible for initial triage, establishing target goals, staffing, communications and goal accomplishment.



Over the past few years, the incident response industry has been flooded with inaccurate information regarding the best practices of first responders. The common theory has been to simply unplug the system, and hand it over to the forensic team. Doing this loses all of the volatile data, which is absolutely critical in incident response.

4. What security training is or should be offered for all staff?

Insider threat is growing and not just limited to employees with malicious intent. Unsuspecting staff may break security policy or expose sensitive information. Without the appropriate security training, they can pose one of the biggest threats to an organization.

Security awareness training for staff can mean earlier notification and detection of a potential incident; even low-level staff may notice something if trained to be security aware. Whether to meet compliance requirements or as part of a defense-in-depth strategy, organizations should look to implement a security awareness training program and make it mandatory for each and every employee, regardless of function. Repeat this training on an annual basis and make it part of new hire orientation. By educating staff, as well as suppliers, the chances that a department will become a victim of data security threats is reduced, and ensures that all staff can properly handle an incident should one occur.

5. How are we protecting our organization from threats to our systems and facilities?

One of the best (and least expensive) ways to protect an organization is through multi-factor authentication. Currently single-factor authentication is in widespread use; there are likely 10,000 applications that use single-factor authentication for every one using multifactor. Unfortunately, when given the choice, humans often create poor (weak) passwords. Even employees within the security industry – those that should know better – often choose weak passwords to protect their systems for one simple reason: strong passwords are harder to remember.

Multifactor authentication does not work everywhere, but should be strongly considered where it is possible. The cost of implementing a multifactor solution is far less than the impact of a major breach of the corporate network and loss of critical data.

Other initiatives organizations should undertake are the encryption of data, investigation of all anomalies and controlling user access and privileges to control software downloads.

6. Is there a risk management group that gathers regularly to discuss physical and local security issues?

An internal risk management group can lead the charge when it comes to assessing the department for risk on the whole or by specific areas. A risk management team has the ability to follow best practices by establishing benchmarks for risk acceptance levels and proper procedure for identifying and managing risks. It may be appropriate for this team to also manage security awareness training, follow and implement legal and regulatory compliance requirements, and work to identify new risks as the department changes.

7. Is there an inventory of all IT assets? Is there a schedule for the decommissioning of old systems?

Keeping an updated list of IT assets should be a priority; this will aid in the tracking and decommissioning of older systems. In its work with clients, Trustwave SpiderLabs often finds major vulnerabilities associated with older systems, but clients seem unconcerned about the vulnerabilities as these legacy systems have a planned decommission date. Coincidentally, many of these same clients use Trustwave SpiderLabs to re-test their environments in subsequent years. About 75% of SpiderLabs test results that included client responses of “system will be decommissioned” still have those same systems in production a year later.

At a minimum, the list should include: name of device, DNS names, type of device, operating system, IP address(es), MAC Address(es), date of installation, and owner. Once an asset list is established, all adds, deletes and changes should be logged so an up-to-date list can be obtained at any time. For decommissioning, establish an internal team with cross-competency work and tackle this problem.

8. Is security built into our IT and application development lifecycles?

We often train developers on how to code their applications securely or debrief them on the results of an application penetration test. Through an analysis of this work, Trustwave SpiderLabs found that the majority of organizations spend a great deal of time in the planning and implementation phases, but not a lot of time in the analysis, design and maintenance phases.


Organizations quickly go from idea to code to production. This means that a single individual makes both tactical and strategic decisions on their code, without input or oversight from others internal or external to the organization. When not properly implemented, a simple module like “reset my password” could result in major consequences to the security of an application and, potentially, to the entire organization.

Implementing a comprehensive development lifecycle process which, from the start includes security planning, review and testing, is crucial to successfully developing secure applications. Organizations should review their current development methodology, and make the necessary modifications to ensure that security is not simply addressed as an afterthought, but rather as an integral and indispensable part of their IT and application development process.

9. How is our wireless network structured?

Wireless is everywhere. Early adopters of this technology placed the access points inside their network so that employees could access resources without having to be tethered to a physical network jack. Even with the latest wireless security applied to the implementation, increased ways to crack or circumvent the security controls being used are being discovered by attackers.

We recommend law enforcement organizations never place wireless access points within their department's core network; instead, they should treat them as any other remote access medium. Users are able to use a wireless access point at a café or



hotel and securely connect back to department resources, so they should use the exact same process when they are in the office. The wireless access points should be placed outside the network and any security controls in place should keep unwanted visitors from using a department's Wi-Fi as an open access point to access the Internet.

10. What security investments should we consider? Are we an early adopter or is this a widespread practice?

Before undertaking an expensive product implementation that may not even resolve outstanding security issues, departments should review their infrastructure and identify any underlying security issues, ultimately resolving those issues.

Technology can go a long way towards fixing security issues if implemented correctly. A good, professional assessment can help identify security holes and suggest controls or technology to fix them. An assessment will also help prioritize security projects in respect to budget and the level of risk.

Cybercriminals will never stop trying to obtain valuable or proprietary data. By reviewing the information security infrastructure with the department's security team, paying particular attention to existing vulnerabilities, the assignment of security responsibilities to specific individuals or groups, and how data flows within the department, you can reduce the threat and impact of a security incident. A comprehensive, defense-in-depth strategy for information security can help reduce risk, protect sensitive information and ultimately safeguard the reputations of law enforcement departments and municipalities.

Conclusion

Advances in technology enhance our quality of life and help make our jobs more efficient. At the same time, cyber criminals are using the same technology to gain access to critical systems and sensitive data. Increasing numbers of individuals, businesses and now law enforcement experience the cataclysmic after effects of data breaches and theft. The law enforcement community is more frequently a target of organized crime syndicates as well as those who seek to embarrass public officials by exposing sensitive data and even operational information. Law enforcement needs to leverage technology to better protect its' sensitive data from compromise.

The security of your department starts with action — the action you take to first understand the security issues you are faced with and the action to apply proper protection methods to various networks, systems and applications within your organization's IT environment. Incremental improvement may occur at first, but over time these actions will decrease the risk of a successful cyber attack. Many major data breaches, against organizations of all types, could have been prevented if the digital asset owners first identified security flaws and second, made the effort to fix them.

References

- “Zeus Malware Purveyors Target Symbian, BlackBerry Devices.” <http://www.eweek.com/c/a/Security/Zeus-Malware-Purveyors-Target-Symbian-BlackBerry-Devices-800557/>
- “Zeus In The Mobile (Zitmo): Online Banking’s Two Factor Authentication Defeated.” <http://blog.fortinet.com/zeus-in-the-mobile-zitmo-online-bankings-twofactor-authentication-defeated/>
- “Zeus Mitmo: Man-in-the-middle (I).” <http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html>
- “Hacker Spoofs Cell Phone Tower to Intercept Calls.” <http://www.wired.com/threatlevel/tag/chris-paget/>
- “Mobile Malware Will Increase Proportionally to Profitability.” <http://unplugged.rcwireless.com/index.php/20100930/news/3952/mobile-malware-will-increaseproportionally-to-profitability/>
- “J2ME Programming/MS Windows Mobile and J2ME.” http://en.wikibooks.org/wiki/J2ME_Programming/MS_WindowsMobile_and_J2ME
- “Researchers can attack mobile phones via spoofed SMS messages.” http://news.cnet.com/8301-27080_3-10300174-245.html
- “Researchers attack my iPhone via SMS.” http://news.cnet.com/8301-27080_3-10299378-245.html
- “Transaction Authentication Number.” http://en.wikipedia.org/wiki/Transaction_authentication_number
- “Zeus Mitmo: Man in the Mobile.” <http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html>

About Trustwave®

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

Corporate Headquarters	EMEA Headquarters	LAC Headquarters	APAC Headquarters
70 West Madison St.	Westminster Tower	Rua Cincinato Braga,	Level 26
Suite 1050	3 Albert Embankment	340 n° 71 - Edifício Delta Plaza	44 Market Street
Chicago, IL 60602	London SE1 7SP	Bairro Bela Vista - São Paulo - SP CEP: 01333-010 - BRASIL	Sydney NSW 2000, Australia
P: 312.873.7500	P: +44 (0) 845 456 9611	P: +55 (11) 4064-6101	P: +61 2 9089 8870
F: 312.443.8028	F: +44 (0) 845 456 9612		F: +61 2 9089 8989



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.