White Paper

Security Trends

Security Trends for 2011

Imperva's Application Defense Center (ADC), has assembled its most comprehensive set of predictions for the threats security teams will address in 2011.

#10: Convergence of Data Security and Privacy Regulation Worldwide

#9: Cyber Security Becomes a Business Process

#8: Hackers Feeling the Heat

#7: Mobile Devices Compromise Data Security

#6: Data Security Goes to the Cloud

#5: File Security Takes Center Stage

#4: Misanthropes and Anti-socials: Privacy vs. Security in Social Networks

#3: Man in the Browser Attacks Will Man Up

#2: The Insider Threat – It's Much More than You Imagined

and #1...

> *If an attacker is really persistent in doing damage to the target, there is always another way to enter the organization. That is, through the insider.*

As 2011 approaches, data security continues to be a top priority. However, cyber security remains one of the most dynamic and fluid practices as hackers sharpen their skills and modify their attacks. Meanwhile, security teams worldwide are left to figure out the best ways to protect data from hackers while mollifying auditors, lawyers and their bosses.

Imperva's Application Defense Center (ADC), led by Imperva CTO Amichai Shulman, is exclusively focused on advancing the practice of data security to help companies shield themselves from the threat of hackers and insiders. In 2010, the ADC successfully predicted many of the key issues that would plague security teams in 2010 and beyond. For 2011, the ADC has assembled its most comprehensive set of predictions.

Trend #10:
Convergence of Data Security and Privacy Regulation Worldwide

As the Wall Street Journal features more companies that violate data privacy on its front page and security breaches appear daily, government regulators will continue to tighten the legal screws on enterprises. Recently, Google CEO Eric Schmidt said that people who don't like Google's Street View cars taking pictures of their homes and businesses "can just move." Typically, this executive bravado invites government regulation and scrutiny. For example, in Germany, Google has experienced many run ins with government privacy regulators. Privacy is only the latest thorn in the saddle.

Continuing data breaches force more and more governments – and even private industries – to consider more in-depth security regulations to protect citizens. But another interesting trend seems to be flying under the radar: as enterprises contend with additional data laws, a consolidation will take place across borders. Recently, for instance, the FTC reached out to the EU to begin the process of investigating where both sides of the Atlantic can unify data security laws. Companies will comply, but will find the task of complying with multiple mandates across borders very difficult. For example, Google is required to retain data about citizens for different amounts of time in different countries. Governments will respond – in fact already are – to define a common framework to make life easier for themselves and for enterprises housing data. Just last week, the White House announced on its blog a new privacy and security subcommittee.

The announcement stressed the need for a worldwide effort, stating that, "[given] the global nature of the digital economy and society, the Subcommittee will monitor and address global privacy policy challenges and develop approaches to meeting those challenges through coordinated U.S. government action."

Trend #9: Cyber Security Becomes a Business Process

Intel buys McAfee, HP buys Fortify, Oracle buys Secerno, IBM gets Guardium. Now rumors swirl about IBM and Fortinet. The consolidation taking place with security vendors implies, as Intel CEO Paul Otellini put it, "We have concluded that security has become the third pillar of computing." Vendors are seeing a big shift in security, what about enterprises?

From an enterprise standpoint, security is no longer a tactical technical activity, but is becoming a strategic business process. In the past, the objective of security was all about keeping the bad guys out while letting the good guys in. However, with the advent of insiders and as external hacking's focus shifted to data theft, the objective of security professionals changed dramatically. Data – and the transactions that moved data – meant security teams had to deploy security as a part of supply chains, online transactions and for online collaboration among customers, employees, partners and social networks. This process will be magnified where we see more traditional companies buying security companies as well as enterprises who increasingly integrate security practices within their business objectives.

Today, cyber security can't be separated from business operations. For this reason, how security teams must view and approach their roles has changed dramatically. For example, in the past, a CIO's role was laptop distribution. Today, CIOs build supply chains. In the past, CISOs distributed anti-virus and set up firewalls. Today, they must know where data resides, where it moves and how to protect it, which requires a serious, comprehensive data security practice. This means security teams need to become business process experts to keep the bad guys disarmed while keeping the good guys productive.

Forrester conducted a survey in August that nicely puts some statistical heft behind the trend. "Cyber Security Becomes a Business Process" highlights how security is gaining enterprise visibility:

> Senior executives and boards are increasingly more interested in the effectiveness of security controls within an organization. This is evident in the rising profile of the chief information security officer (CISO) and in the changing scope of responsibilities that security departments are taking on. In the third quarter of 2009, Forrester surveyed 2,199 North American and European IT security decision-makers at both small businesses and enterprises. They asked to what level in the organization their CISO reported. Almost 50% of enterprises replied that their CISO or equivalent reported to a C-level executive.
>
> Not only are security and risk departments moving up in the organization, but they're also expanding and taking on more responsibilities. Security organizations are assuming greater responsibilities in areas such as application security, business continuity, and risk management. The two ends of the security and risk continuum represent two very different types of security organizations. On one end is the strategy-focused security and risk organization, which is more focused on business expectations and priorities. At the other end is the operations-focused security and risk organization, whose main concern is to run the security operations efficiently and effectively on a day-to-day basis.

Trend #8: Hackers Feeling the Heat

Expect the 2011 cyber crime landscape to change in two ways. First, more and more smaller cyber-gangs will go out of business. Why? Security researchers will continue to look into the hacker operations and will unearth the smaller or less diligent criminals. In general, the hacker industry will react by investing more resources in their attack techniques and detection evasion. The hackers that cannot make this investment will go out of business. Other cyber-criminal organizations will "buy-out" other groups or merge their operations with other groups. This will lead to the second change. The current powerful cyber-crime organizations will consolidate their power and grow (after all, antitrust laws don't apply to them).

As the year 2010 draws to a close, it provides us with all the more examples of this accelerating trend:

- At the end of September, Zeus botnet ring leaders and operatives were arrested. This was the culmination of a year-long investigation that included the infiltration of the C&C servers by security researchers. Similarly, the master mind of the Bredolab botnet was arrested three weeks later.
- During mid October, the Avalanche phishing group completed their 2 year-long move from phishing techniques to distributing MitB Trojans.
- The end of October has seen the Iranian Cyber-Army (ICA), infamously known for engaging politically-motivated DDoS attacks, advertising their bots for rent.
- Also, towards the end of October, the bot code developers of the ever-competing spyEye and Zeus bots were showing signs of an upcoming merger.

The security industry can prepare to react by:

- Understading that all companies- of all sizes- are at risk – Regardless of the application size, small or large – they are attractive targets. Servers or workstations – those too are identified as potential targets.
- Beating automated attacks at their own game – The key player for cyber-criminals is automation. Slowing down an attack is most often the best way to make it ineffective. A second of delay will not be noticed by most users. But this can make the difference for an automated attack.
- Incorporating reputation controls – This also includes applying forensics from recent attacks.

Trend #7: Mobile Devices Compromise Data Security

The proliferation of sophisticated mobile devices (SmartPhones, Tablets, etc.) is going to have a substantial effect on application and data security in the coming years. In particular, we will see organizations struggle to accommodate the increase in number and variety of these devices, while maintaining traditional data and application security practices.

The past couple of years have witnessed a dramatic surge in the number of sophisticated mobile devices being used as access points to online services and enterprise networks. At the same time, these devices acquired more capabilities, in terms of storage size and web technology adoption. Apple's iPhone comes with up to 32GB of internal storage, while its bigger sibling iPad can accommodate up to 64GB of memory. (For context, one million records holding names, addresses, and social security numbers will occupy approximately 0.5GB.) Mobile devices are no longer mere address books or mail readers.

Add to the mix a growing variety of applications that are a gateway to enterprise systems, including CRM, ERP, and document management. While we are used to concerning ourselves with lost or stolen laptops, it turns out that missing mobile devices may be just as big of a pain point.

However, the storage of sensitive information is not the only new concern with mobile devices. As mobile devices become mainstream, online service providers must accommodate their offerings for these platforms; creating a special version of the applications to match each devices' capabilities. In this process, it is not uncommon to see older vulnerabilities surface once again. We have witnessed the online versions of well-protected mobile device applications display common vulnerabilities: the CitiGroup incident in 2009, a more recent CityGroup issue, and AT&T's well publicized mishap with respect to iPad owners. In particular, many mistakes are made around identification and authentication; where application programmers mistakenly trust attributes of the data stream that can be forged by an attacker without the particular mobile device. Thus, the applications themselves become more vulnerable.

Furthermore, some assumptions regarding "strong" multifactor authentication schemes are becoming obsolete. Take, for example, applications that use a one-time password (OTP) for validation of sensitive transactions; where the OTP is delivered through SMS to a phone number provided by the user. If the user is employing a smart mobile device for accessing the application, and that device is infected by a Trojan, then that Trojan is able to access the OTP delivered through SMS.

If you are surprised by the mentioning of Trojans in the context of your mobile phone, don't be. Mobile devices rely on sophisticated operating systems running complex applications. Malicious code is available for these platforms (e.g. Zitmo) and the complex applications (not to mention the usual human flaws) make it easy, if not easier, to infect a mobile device with malware, as with any standard desktop platform.

We expect exponential growth in the number of incidents related to mobile devices in the next few years. From theft or compromise of information in these devices, through massive infection campaigns, and up to frequent exploit of the vulnerabilities introduced into the server side.

Organizations need to start planning to secure the devices and their interaction with the enterprise networks. Tools and procedures need to be put into place, such as anti-malware, encryption, and authentication. Special monitoring requirements should be set for access of these devices to enterprise resources (databases, files, intranets). On the other hand, application providers need to get their act together with respect to serving these devices, including vulnerability mitigation, reevaluation of trust, and incorporation of new authentication/authorization channels.

Trend #6: Data Security Goes to the Cloud

We expect to see more application security offerings in the cloud throughout 2011, and predict some early data security in the cloud offerings. Offerings will need to respond to private and public clouds that are either self-serviced or managed as a service. This trend is a late response to the move of many applications and data stores to cloud technologies, and the industrialization of hacking, which dragged many smaller online businesses into the threat zone.

The past couple of years brought an extensive increase in the use of cloud technologies (and a definite abuse of the term "cloud technologies"). Each of these technologies contributes a different set of challenges with respect to data and application security. Cloud applications (SFDC.com, Gmail, MS BPOS, SuccessFactors) challenge their operators to maintain a bulletproof partition between datasets of different customers. At the same time, it challenges customers with respect to protecting data from the prying eyes of service administrators (e.g. European regulations require that PII will not be handed over to non EU individuals or entities).

Private clouds (in layman terms – clustered servers running virtual machines) create a challenge by having the same application or database server operate from a different physical server at different points in time, thus making it harder to monitor the communication path to the application.

Public clouds (hosting providers) challenge their operators to maintain partitions between applications and datasets of different users, and at the same time manage application and data security for a large multitude of different applications.

Self-service clouds (aka "platform as a service" or "infrastructure as a service" such as Amazon EC2 or MS Azzure) challenge their users with a new virtual platform and the need to protect data from cloud administrators.

Taking together all the types of cloud forms (private and public, SaaS, PaaS and IaaS) we can see a set of challenges for both providers and consumers. These can be summarized as following:

- Maintaining bulletproof partitions between datasets of different customers
- Providing different levels of data security to applications sharing the same logical or physical platforms
- Protecting customer data from the prying eyes of cloud administrators
- Providing solutions that operate over a specialized infrastructure (VM, Amazon AMI)
- Managing application and data security for a large number of applications inside the cloud

In the past year, we have become aware of numerous attempts by security providers and cloud providers to solve the conundrum of application and data security in the cloud. Traditional application security vendors are starting to provide their solutions over virtual platforms (VMWare, Amazon), while new vendors are creating models for application security solutions that are cloud-based (they route all traffic for their customers).

We expect that in 2011 good technical solutions for application security in the cloud will be available and gain traction, while data security solutions (protecting data stores in the cloud) will lag behind. Scale of manageability and different levels of security for applications that share the same platform will remain a major challenge for application security solutions. Data security solutions will continue to struggle with creating the right security model.

Organizations can now accelerate their adoption of cloud offerings without giving up on the security of their information by choosing the right solutions. Larger enterprises with private clouds will adopt the offerings of traditional vendors over virtual platforms. Smaller organizations may choose a cloud provider that is capable of delivering applications in a protected manner (managed application security), or choose to have their applications delivered by one provider and their application security by a dedicated security-in-the-cloud provider.

Trend #5: File Security Takes Center Stage

In 2011, we expect to see a growing number of data breaches where compromised data is in the form of files rather than database records. Consequently, organizations will rush to look for the proper tools to control access to repositories of unstructured data, mainly file servers. We estimate that the number of compromised files, and the number of organizations that suffer a massive file related security breach, will rise.

Even PCI 2.0 has recognized the security aspect of storing data in different locations. In October 2010, the PCI council released an updated version of their security standards. This new version included the clarification of controls to include all data containers likely to hold sensitive data that goes beyond databases.

While most business applications use structured storage (databases) to maintain and process sensitive and critical data, users are constantly creating and storing more and more unstructured content, based on the information taken from these systems. Recently, Gartner made a similar observation. Examples include: excel spreadsheets (based on data extracted from order processing systems), presentations (based on financial results taken from the ERP system), and medical lab results sent as letters to patients. These are just a few examples of the process in which sensitive information is disseminated from the structured to the unstructured world.

The volume of data is also growing, and is estimated to increase by 60 percent annually (IDC 11/09). Based on recent research, 80 percent of all data in the organization is stored in files. Increased sharing habits of data between users, as well as data retention policies that require organizations to store any work product for posterity, contribute to this growth.

With today's available tools, controlling access and usage of these files can be an extremely daunting task. Since each file is an autonomous entity, with respect to content ownership and access control (contrary to a database record), maintaining control of who can access a file is anything but possible. This is also true with regards to keeping track of access to those files that contain sensitive information. Each file is autonomous, with respect to its contents (unlike database records), and users are autonomous, with respect to contents of files they create (unlike database records that are created by pre-programmed applications). The inability to maintain control may result in excessive access privileges and an inadequate audit trail of access to sensitive information.

The variety of repositories that keep unstructured data is also growing. While traditional file servers still prevail, internal document management systems, such as SharePoint or Documentum, are increasing as well. At the same time, cloud-based offerings, such as GoogleDocs and Jive, are also becoming part of the enterprise IT.

Individuals often abuse this fragile situation by obtaining unauthorized access to large amounts of files, resulting in compromised contents. Incidents in 2010 suggest that massive leakage and compromise of sensitive information is indeed becoming a clear and present danger. The most notorious being the disclosure of 400,000 sensitive U.S. military documents related to the war in Iraq by Wikileaks (which followed a previous disclosure of 70,000 similar documents regarding the war in Afghanistan). While not confirmed by Wikileaks, these were deliberately handed to the site administers by a (very) small group of individuals.

In another incident, a former Goldman Sachs employee stole source code used for a proprietary high-frequency trading program. Court documents revealed that the software generated millions of dollars in profit each year. To steal the code, the former employee used his desktop to upload the code to a server based in Germany. The bank was able to identify his activity after observing large amounts of data leaving their servers, which lead to his arrest.

Although unstructured data breaches are mostly an internal threat, a recent attack on law firm ACS:Law demonstrates the potential for external threats as well. In this case, hackers obtained an unencrypted (archive) file stored on one of the firm's servers leading to the leakage of personal information from 500,000 files.

These examples, which include the DuPont case where documents were transferred to a Chinese competitor by a former employee, all follow earlier incidents related (mainly) to Cyber Espionage.

Organizations aiming to reduce the risk of file exposure should begin the process of budgeting and planning for the next generation of file access monitoring and governance tools. Key characteristics to look for include:

- Policies set and expressed by content of file, rather than metadata
- Flexible deployment, without impacting data stores or network architecture
- Adaptive deployment with focus on the most accessed files, without compromising the ability to track sensitive information in older files
- Ability to identify file owners and excessive rights to files

Trend #4:
Misanthropes and Anti-socials: Privacy vs. Security in Social Networks

In 2011, we will see prominent social networks, and tools, placing more efforts into security over privacy. This is not the result of resolved privacy issues, but rather an understanding of the real threats to the existence and proliferation of social networks.

In recent years, social networks, and tools – Facebook, LinkedIn, and Twitter – have invaded our personal and professional lives at a phenomenal pace and ignited numerous privacy complaints. Voices called out the "promiscuous" default settings, the lack of granular control, and even the entire interaction model. "Incidents," where personal details of users were "accidentally" disclosed, took center stage. Even the simple revelation that Facebook's public directory was available for download – doesn't the word "public" mean anything? – grabbed media attention. As a consequence, and an attempt to avoid public whipping, a great deal of effort has been invested – rather unsuccessfully – in preserving privacy of information. Facebook, for example, revamped its privacy setting scheme, implementing at least one major change in 2009 and another in the spring of 2010 that resulted in a very granular yet complex model.

Surprisingly, it seems that privacy issues have not had a detrimental effect on the rate at which users have joined social networks, or the amount of personal information that they are willing to provide. It turns out that people often join social networks to promote random interactions with other users, spurred by the information provided in profiles. With this in mind, it may be safe to say that if a user indicates their religion, or ethnicity, they do so because they want other users to know this information and are willing – even implicitly – to take the chance that a (hypothetical) KKK classification application will have access to it as well. It may also be safe to say that people who post a named defamation of their boss on their wall – or their friend's wall – are willing to take the chance that their boss may see the post.

Aside from privacy issues, additional factors will come into play in the coming year that may affect the development of social networks. The decrease in growth will not be a measurement of the number of members, but rather the inability for social networks to penetrate deeper into both our personal and professional lives.

There are two key factors at stake: security and trust. While privacy concerns the ability to keep personal information hidden from other application users, security operates with a much broader scope. Security controls the way in which people use the information of others. It is a way to ensure that people cannot invoke functionality on behalf of other users, and that delinquents cannot use the system to distribute malware. It is a way to make it difficult to hack into someone's account using a brute-force attack. Security enables us to integrate social networking applications into our business environment without affecting the integrity and confidentiality of business data. Trust, on the other hand, impacts our ability to make decisions based on the information we receive through social networks, such as the decision to accept requests from applications that have access to our information.

In today's social networking platform, both security and trust are in danger. Cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerabilities are quickly translating into massive worm out brakes. Examples:

- http://www.theregister.co.uk/2010/06/01/facebook_clickjacking_worm/
- http://www.pcworld.com/article/155039/facebook_worm_refuses_to_die.html
- http://blogs.msdn.com/b/tzink/archive/2010/01/29/new-facebook-worm.aspx
- http://gdeglin.blogspot.com/2010/09/reverse-engineering-latest-facebook.html

Even basic best practices, such as the use of SSL for authentication purposes, are not closely followed. Trust evaluation tools are nonexistent. Actually, if you ask users who contemplate installing a Facebook application, their measure of trust is often the number of other users who have already signed-up for the application. Clearly, anyone with an army of drone accounts can easily influence such decisions.

Nevertheless, we are starting to feel the winds of change. Recently, Facebook made changes to account SECURITY to reduce account hijacking incidents (device profiling, concurrent session sign out,and SMS OTP). Next year, we expect social platforms to invest more resources in improving the SECURITY posture of the platform, rather than continuing to struggle with controlling information overflow. These measures will provide improved protection against application layer attacks, stronger authentication and account control features, and better malware detection systems. Research into trust models is still in its early stages. Only a handful of companies have disclosed commercial offerings. We, therefore, do not expect to see much progress with trust in 2011.

Trend #3: Man in the Browser Attacks Will Man Up

In 2011, we expect to see growth in the role played by "Man-in-the-Browser" (MitB) attacks (a.k.a., Proxy Trojans) in cyber-criminal activity. MitB attack sophistication is going to increase, as well as its application to more types of online applications. As a consequence, more online service providers are going to include this in their list of priorities for 2011, shifting the responsibility for mitigating the risk from the consumers to the service providers.

MitB attacks consist of an attacker code running in the context of the victim's browser. They are a special breed of MitB attacks with two important characteristics. First, the attack plugs into the traffic flow without affecting Internet infrastructure (DNS, routers, etc.) since they plug into the traffic flow before the SSL encryption layer. Second, MitB attack code can access local resources on the victim's machine that are available for the application's genuine client-side code (e.g. key files).

The most primitive form of MitB code has been used to grab user credentials upon access to online banking applications. More advanced MitB code allows attackers to record and store entire browsing sessions. Even more advanced MitB code allows the attacker to inject HTML code in pages returned from the application server to the browser, thus allowing the attacker to entice the victim into disclosing even more information than merely credentials (e.g. PIN code for debit cards, credit card numbers, answers to security questions, etc.). The Trojan code usually sends out the grabbed information to a command and control (C&C) server on the Internet where the attacker can access it. Most prominent Trojans, such as ZeuS, Gozi, URLZone, Sinowal, Limbo and SpyEye, all have MitB capabilities that allow then to selectively intercept requests and replies and manipulate them based on configuration files delivered from the C&C. Quite commonly, such malware injects additional fields into HTML forms and sends out the information from the to the attacker.

As one-time passwords and two-factor authentication mechanisms become more common among online banking applications the credentials obtained by Proxy Trojans become less effective. Attackers, as a consequence, are now starting to improve the autonomous capabilities of the MitB code, allowing it to inject transactions into existing sessions or manipulate transactions initiated by the victim. The Silentbanker Trojan is a recent and potentially costly MitB attack targeting banking transactions. Targeting more than 400 banks and having the ability to intercept banking transactions – even those guarded by two-factor authentication – pushed Silentbanker into the limelight. At the same time, we are seeing MitB infections starting to target

more types of applications, on top of the traditional focus on online banking. Configuration files captured and analyzed show that Paypal and eBay are already being targeted and we assume that social networks and webmail platforms are soon to follow. Not only that, but MitB code, traditionally infecting only IE browsers, is now starting to appear on other common browser brands.

While avoiding infection by Proxy Trojans is presumably the responsibility of consumers, MitB attacks are quickly becoming a concern of online service providers. The actual rate of infection and the proliferation of the many types of MitB malware suggest that providers must be able to serve (and protect) customers who might be infected with one type of malware or another. Just as the evolution of vehicle safety drove manufacturers to include device such as ABS, Air Bags and ESP, rather than rely on us to drive carefully, so will online service providers need to invest in mechanisms that allow them to conduct business with allegedly infected consumers. Among the technologies that we foresee as helpful are strong device identification, client profiling, fast security code evolution, session flow tracking and site-to-client authentication.

Trend #2: The Insider Threat – it's much much more, than you had imagined

In this upcoming year, we expect to see a growing awareness to security incidents of an "insider job" nature. Attention will grow as a consequence of an increased flow of incident reports where data theft and security breaches are tied to employees and other insiders. The cause of this trend will be the emphasis put on new regulations covering the act of notification and disclosure (rather on the actual protection of data).

The enactment of the California data privacy act (SB 1386) was followed by a steep increase in the number of reported data leakage incidents, with customers receiving a constant stream of apologetic letters. Similarly, a UK ICO regulation from April 2010 encourages firms to engage affected individuals in case of a breach, or face a heavy (500,000 GBP!) fine. These laws and regulations, while generally discussing the need for security controls, place most of the emphasis on breach notification. In Germany, strict fines are imposed on companies that do not adhere to privacy laws discussing the publication of all data breaches affecting individuals. A surge in notifications due to an employee accessing the data in a way that violates business policy is bound to occur.

The increased visibility into insider-invoked breaches will close the alleged contradiction between the Verizon Business Investigations Report (VBIR) and that of Independent Oracle User Group (IOUG) reports. The former shows that breach investigations are heavily leaning towards hackers, in the traditional sense, from an external source. Yet, the IOUG report shows an inclination towards data breaches stemming from the Insider Threat. To explain this dissonance between the two, we must bear in mind that the VBIR is constructed out of incidents analyzed by VB. Breaches of an external nature are usually more complex to understand and trace. They require calling in the Verizon Business experts in order to conduct the required forensic analysis that would yield attack details – how it happened, what exactly happened, how to prevent future attacks and who was affected. On the other hand, internal data breaches are usually of a very simple technical nature and, quite often, easily tied to a specific person post-mortem. Thus, organizations rarely call VB experts to investigate internal breaches. As a consequence, the VBIR is inherently biased towards external attacks. The IOUG report is based on an anonymous survey among DBAs – those who are usually in the line of "hacker" fire. These are the individuals who can actually attest to the true extent of the insider threat.

As a matter of fact, a September survey by Imperva supports the findings of the bigger picture of the Insider Threat. This survey covered over 1100 security practitioners and has shown that data breaches due to malicious insiders account for 32% of all data breaches. Yet, external hacks account for just somewhat less – 29% of all dataWe will see these numbers better reflected in data breach notification due to new privacy regulations. To deter insider threats, organizations should therefore:

- Enforce access controls such that access is based only a business need-to-know level. This includes eliminating excessive privileges.
- Provide the proper access auditing tools to data centers. These auditing tools should monitor who accesses what data.

Trend #1: Advanced Persistent Threat (APT) Meets Industrialization

Advanced Persistent Threats (APTs) – politically motivated, specifically-targeted cyber-attacks – will incorporate concepts and techniques from the commercial hacker industry. These campaigns will contain a different malware payload than the traditional attacks conducted for monetary gain. However, these attacks will use similar techniques. The incorporation of industrialization techniques to APT seems quite natural. This past year alone has proven the success of cyber crime lords. The hacking industry is bursting with success stories. Why shouldn't the attack techniques then be adopted by the creators of nation-backed attacks? These APT attacks will borrow techniques, such as automation and viral distribution, making them all the more powerful and potentially more successful.

Towards the end of summer 2010, the name Stuxnet began circulating among security practitioners. It was a worm that specifically targeted SCADA systems. A threat with consequences to nations' underlying power systems and industrial infrastructure. Throughout the following months, researchers have analyzed the worm and the news emerged – this was no simple common worm. Stuxnet consisted of four different attack vectors, each exploiting a different vulnerability. The code, very deceptive, had to be written by a group of dedicated hackers, taking some six months of development. Although speculative, there is much agreement that this worm had one specific target – Iran. Much of the worm's deception laid in its propagation. In the course of reaching Iran, the worm also propagated itself in multiple countries: Germany, Russia, India and others. Upon arrival at the ultimate destination, Stuxnet called home and announced that the Eagle had landed.

Stuxnet was not searching for data to monetize, rather it was focused on gaining control of crucial infrastructure. And as mentioned, all fingers are pointing to government agencies as the Stuxnet driver.

However, as opposed to traditional APT attacks, the worm's target was not direct. Hopping around different countries and power plants, it seemed like the grand plan was to unleash the worm on the world. This technique sounds familiar: target as many systems, and sooner or later, there will be a victim. This notion is one of the underlying foundations of the hacker industry.

Looking back, we can see already that North Korea has also started mimicking the hacker industry. In mid-2009 botnet armies targeted US governmental institutions. When those did not fall prey to the attack, the attacks started targeting private US sites. Once again, the target shifted while the attacks were ROI focused. The attacking state has allegedly hired botnets from the hacker industry. And as they were already paid for and engaged in an attack, they were being used for a full-fledged campaign.

Both classes of attack (industry and APT) are going to use some of the same techniques so some security controls are applicable to both. On the positive side, given you're covered against the cyber-mafia you should have some of the controls to be protected from certain APT attacks. On the negative (scary?) side, as the name implies, APT is persistent. If a certain attack does not succeed, another one will come into play. The traditional security controls do not deter these relentless, state-sponsored hacker organizations. For the enterprise this means increasing monitoring visibility of traffic and setting security controls across all organization layers. Consider this, if an attacker is really persistent in doing damage to the target, there is always another way to enter the organization. That is, through the insider.

About Imperva

More organizations trust Imperva to protect their business applications and databases than any other vendor. Only Imperva delivers innovative technology to give full audit accountability and separation of duties to meet regulatory compliance. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring from the database to the accountable application user.

To learn more about Imperva's solution visit http://www.imperva.com.

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com