IBM X-Force Threat Intelligence Quarterly, 2Q 2015

Malicious or inadvertent, an insider threat to your enterprise "crown jewels" can cause significant damage. Explore ways to fight insider threats.

IBM

Contents

Executive overview

In our first IBM® X-Force® quarterly report this year, we provided a roundup of security incidents for 2014, in which we expressed just how significantly industries and foundational frameworks were compromised and how refined attacker techniques are changing the way we look at security.

While advanced threats and mega breaches continue to make headlines, in this second quarterly report we focus on the insider threat and why it remains an insidious and often-overlooked area of concern.

According to the latest IBM Security Services 2015 Cyber Security Intelligence Index, the insider threat continues to hold a top place in comparison to other attack types. While outsiders were found to be responsible for 45 percent of the attacks recorded in 2014, 55 percent of attacks were carried out by those who had insider access to organizations' systems.[1]

In this report, we take a look at how this type of threat is evolving and how companies might mitigate this exposure. The term insider threat can have many meanings, from a malicious employee who wants to do harm, to users who might inadvertently click on a suspicious email attachment, unknowingly exposing their system—and possibly the corporate network—to malware. Today, most spam is created by for-profit operators, who can attach any sort of malware to the spam message. From criminal intent to financial gain, any sort of adversary with the right motivation can hire a spam operator that will build a custom campaign to trick users to open an attachment or click on a link—thus, infecting the corporate network with ransomware or malware.

We also highlight the concern for the "quasi-insider" who could be considered a trusted third-party contract worker. This can include electricians, construction workers, phone or other type of repair personnel who come into physical locations or have access to networks. In the Target retail breach in the United States, abusing this type of third-party access demonstrated that attackers often steal credentials and gain access into networks.

Understanding how to protect valuable data and resources from compromise is top of mind for most organizations and we help to explain common best practices and recommendations to start readers thinking about how they can combat this area of risk.

We conclude by demonstrating how security intelligence, and specifically forensics, can help to detect insider threats and open the door to better analysis of what is occurring with both systems and networks.

Throughout the last year, we have seen how important preparedness can be for a company when it comes to understanding critical computer, network and physical security. Assessing the possible risk of a compromised network, whether from an insider or from outside your network, allows a company to know how it should respond when that future compromise presents itself.

Insider threats break the chain of trust

Do you know who is accessing your resources? Discover how to protect your critical assets in today's constantly changing business landscape.

For most corporations, "insider threats" historically meant that disgruntled or negligent employees were inflicting harm to the company's assets, either physical or electronic. With the increased level of corporate- and state-sponsored espionage over the last decade, there are now myriad additional scenarios to consider in order to safeguard all of your assets.

When assessing their risk for insider threats, many companies place considerable focus on "trusted" employees, especially those with higher privilege levels. Companies rely on these employees to meet strict privacy requirements when accessing and handling critical business and monetary assets. These privileged users are expected to stay within policy and not take advantage of their powerful access capabilities. As a result, companies must finely balance the trust and access privileges given to users within high-stakes business environments. Organizations want to trust employees, but they also must verify what activities are occurring with their most valuable assets—their "crown jewels" of intellectual property, financial data, product designs and other information that is vital to business success. Because of its value, this is precisely the data that insider threats typically target.

In today's job market, workers often change employment every few years in an attempt to get ahead, showing little devotion to any one organization. Often, when these employees move to a competitor, they may still have friends with access to resources at their former company. Add to the mix the possibility that they are disgruntled or looking for some sort of easy gain, and the result can be the many headlines about the latest security breach. The former employee may have created a "back door" before leaving a company that can be activated once he or she arrives at a new employer, providing outside access to hidden accounts or sensitive data. These are not new ideas, but are instead activities reported by companies virtually every day. To help stay aware, it can be useful to set up a recurring process to review access logs and network activity in order to look for these back doors or any other behavior that seems strange or out of the ordinary. Automated monitoring services are also available, but how to proceed often comes down to a balance of risk versus cost for the company.

A laid-back approach to protecting customer data should not be considered an acceptable practice. Recent insider threats have surprised even large vendors who maintain databases of customers' private information, and these vendors have well-established internal practices. For example, last year malicious insiders at a third-party vendor were able to steal customer data from a global telecom company—including birth dates and US Social Security numbers—and use this information to unlock mobile phones for resale on the black market.[2]

Computer networks that house the most valued assets should be monitored in a deliberate and purposeful way to make sure those assets are not exfiltrated, either through a network connection, email, USB device or other such means. Not only should a company limit the privileged access of private data (including customer data) to only those employees who require access, but it should also monitor for unusual employee activity.

Consumers, on the other hand, should be wary of a request by a vendor to simply hand over private details. Once a company has a consumer's private sensitive data, that consumer is subject to the data protection policies and practices of the company, which may be quite difficult for a consumer to evaluate or understand.

Many organizations make the choice to forgo security upgrades until something major happens, but by then it is often too late to spend money on certain security measures and to institute policies that should have been put into place years earlier. Far too often, keeping up with security, whether for technology assets, data or physical resources, has been considered a lower priority for many organizations because the cost to the business of ensuring security does not always result in a positive impact on the revenue stream.

From physical security to social engineering, threats are everywhere

Many people think IT-related security ends with the company's computer network and the various attached devices or technology. However, digital threats are not always limited to IT. In many instances, the digital network also allows access to a company's physical security system.

As a result, a digital threat can affect alarm systems, especially those that allow remote monitoring over the Internet. It can also affect Internet-ready telephone systems, which can be compromised from inside or outside the organization. A few years back, researchers demonstrated how easily they could remotely turn on a phone's microphone and eavesdrop from anywhere in the world.[3] If the Voice-over-Internet-Protocol (VoIP) phone had a webcam, they could also turn that on without anyone being the wiser.[3]

This research shows that when assessing threats to a computer network, it's vital to conduct due-diligence assessments for all your systems. For example, there could be a low-level threat to the company's paper copiers and fax machines. Most, if not all, of these machines now come equipped with some type of memory or hard drive and are often connected to an internal network. A person with the right technical knowledge, such as a repair technician, can access these storage devices quickly and steal important data. The storage device can also be accessed through the network.

In fact, some researchers have found sensitive documents on the hard drives of copiers bought on eBay, as well as copiers purchased from sales of obsolete corporate equipment and government equipment auctions. Computer hacking is not even required in these cases—just the ability to extract the hard drive and hook it up to a computer. In many cases, the drives are designed to work with Linux or Microsoft Windows. When replacing copy and fax machines, it is important to make sure the company—not a third party—either keeps the data or destroys it.

Attack vectors for insider threats

Digital entry points into physical systems—Attackers can use alarm systems, copy and fax machines, and Internet-ready telephone systems as entry points for accessing sensitive data.

Third-party contractors—Maintenance workers, field service technicians and cleaning crews often have unescorted access, enabling tampering of systems and access to passwords written down in employee workspaces.

The "quasi insider" is another type of threat to corporate security that could be considered low level, but should not be overlooked. This type of threat has been a staple of espionage tradecraft since long before electronic connectivity. Many corporations have contract workers from maintenance, repair, construction and cleaning companies who enter the workspace either after hours on weekdays or on weekends. These individuals typically have unescorted access to the entire corporate space, possibly including the C-suite and boardroom areas.

One example in which this third-party access actually resulted in compromise comes from the recent Target breach. In this case, attackers used credentials stolen from a refrigeration and HVAC contractor to successfully steal the personal and financial information of approximately 110 million people, comprising 11 GB of data.[4] This case illustrates the need to pay significant attention—including both time and expense—to securing more than "front door" entries to a company's website or web servers. Many companies also need to focus on controlling other points of entry that might be open to franchisers, contractors or partners.

What's more, on the international stage, security vulnerabilities caused by lack of oversight create situations that are ripe for nation states or other adversaries to infiltrate and gain access to corporate assets unnoticed. Work crews that are trained properly in espionage can implant a listening device in a C-suite office or boardroom in just minutes. Their "training" may be as simple as "plug this into the wall and put a plant in front of it," or it may be more thorough and complex.

In a matter of minutes, an unauthorized person could scour employee desks and find someone's passwords written down in a drawer, notebook or other location in the work area. If unauthorized individuals can gain access to the corporate network from an inside location such as an employee workstation, they can do a great deal of harm with little to no risk of detection. Access to a copier or fax machine can enable them to swap out or copy the storage device and download its contents in minutes. While it is possible to protect machines by locking them down or attaching tamper-resistant labels, they still may be compromised. Electronic sweeps of the C-suite and boardroom may also be warranted.

Regardless of whether a breach is the result of corporate or international espionage, or simply an individual seeking private gain, there are a number of defensive steps that a company can take if it feels it may be at risk. For example, businesses housed in a public building need to be aware of who owns the building. They should also know who their neighbors are down the hall as well as above and below their office space. Understanding and protecting the physical location where your data is stored is important. History has shown that it is extremely easy to attack assets from a close proximity.

Final thoughts and recommendations

In today's business environment, preventing the theft or the transfer of a company's critical assets has become more challenging because of adversaries on the inside and outside with the will, information, resources and patience to achieve unauthorized entry. Corporations should have budgetary allowances for safeguards to help prevent theft. These safeguards may include deploying proper controls for physical security as well as technology, and having a comprehensive understanding of the employees and contractors working for or on behalf of the organization.

A third-party assessment can be illuminating for organizations that have been trying to keep their crown jewels safe from digital enemies, but have ignored the potential threats from employees or contractors with inside access to those crown jewels. There are plenty of people with the knowledge and expertise who can help you by providing observations and recommendations regarding what they can easily see as weaknesses—but which may seem implausible to the corporate culture. Many of these experts will have had years of experience in the military or federal government, where they acquired the necessary skill sets during exposure to or investigation of espionage and counterintelligence activities.

A simple solution might be to have company personnel escort outsiders when providing them access to areas that contain sensitive data or equipment. This may seem like a burden or a waste of company assets, but it is relatively inexpensive in the long run when compared to a multi-million dollar intrusion or theft of crown jewels. In certain government offices, any contractor entering the office space must either be escorted or submit to a background check.

When it comes to hiring and retaining the best employees for sensitive positions, or contracting with people who are given access to essential company data, it is always a good idea to conduct a background check as part of the hiring process. Most companies do a pre-employment drug test and a criminal background check already for certain positions.

Insiders and the ongoing spam threat

Distribution of malware via spam is on the rise. Learn how to protect your business and keep users vigilant.

Threats may originate outside the organization, or with unauthorized or disgruntled insiders, but any insider, even those with the best of intentions, can inadvertently aid in an attack by clicking on a malicious link sent in a phishing email. To prevent this from happening, the organization's security team needs to recognize the danger of malware distributed by spam and take steps to block it. Every user should remain on constant alert and be aware that even the most innocent action can open the door for an attack.

Information security professionals sometimes regard garden-variety spam as more of a nuisance than a threat. Threats such as phishing or spear phishing attacks, malware or distributed denial of service (DDoS) keep their plates pretty full, after all. Recent IBM X-Force Advanced Research analysis indicates that the threat from spam is growing, however, and it may need to be taken more seriously.

When looking into current spam activity, a good starting point can be to understand the countries sending the spam. Figure 1 shows the trends in spam origination by country for the last two years.

In this chart, we see regular ups and downs within years as well as from year to year. Some key points include:

- In the first quarter of 2015, the US sent the most spam, accounting for more than 8 percent of the spam total, showing how widely distributed spam origination efforts have become.
- Vietnam dominated the scene at the end of last year, but is now merely the runner-up.
- Spain won the prize for sending the most spam several times during the last two years, but it now sits in third place.
- All other participants sent between 6.1 and 1.1 percent of the worldwide spam in the recent quarter and had several ups and downs within the last two years.

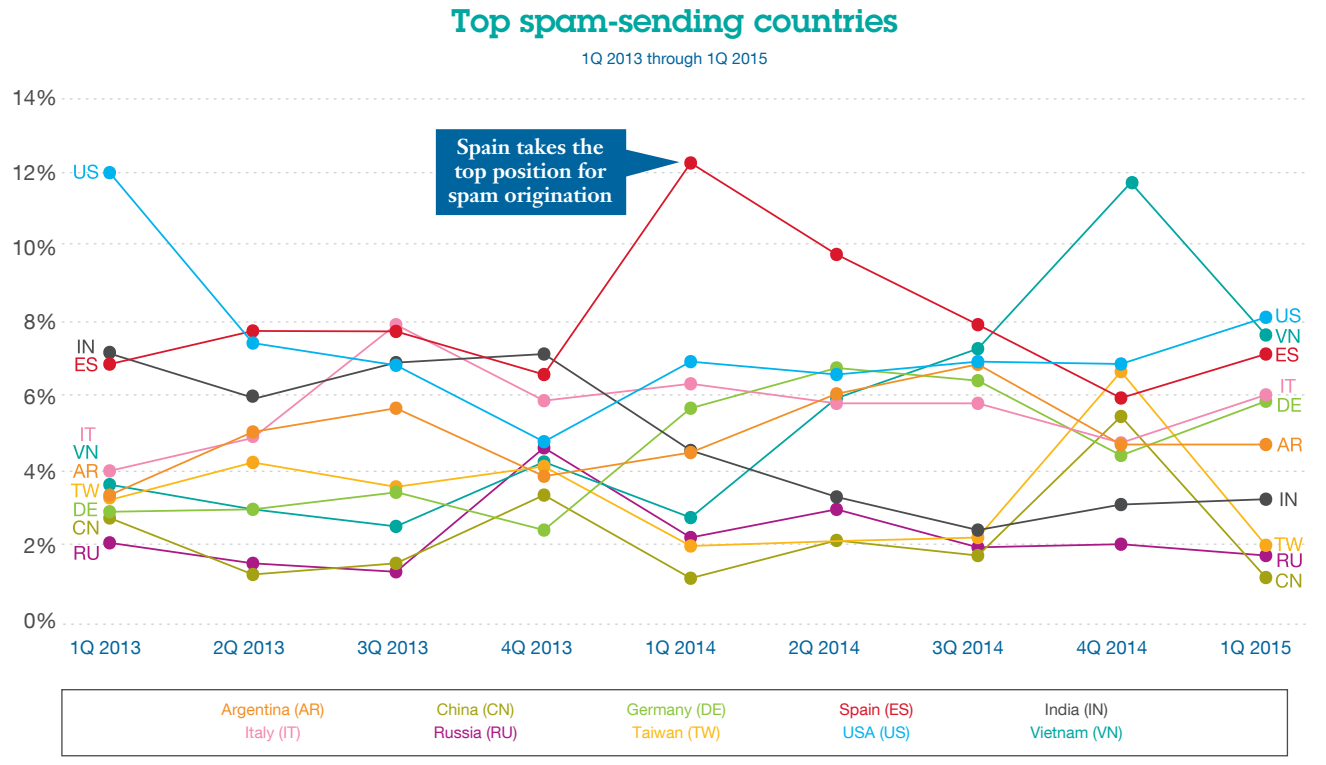


Figure 1. Top spam-sending countries, 1Q 2013 through 1Q 2015

Looking at these numbers, one might get the impression that there is nothing new. The same impression might occur when looking at the spam volume of the last two years, as shown in Figure 2.

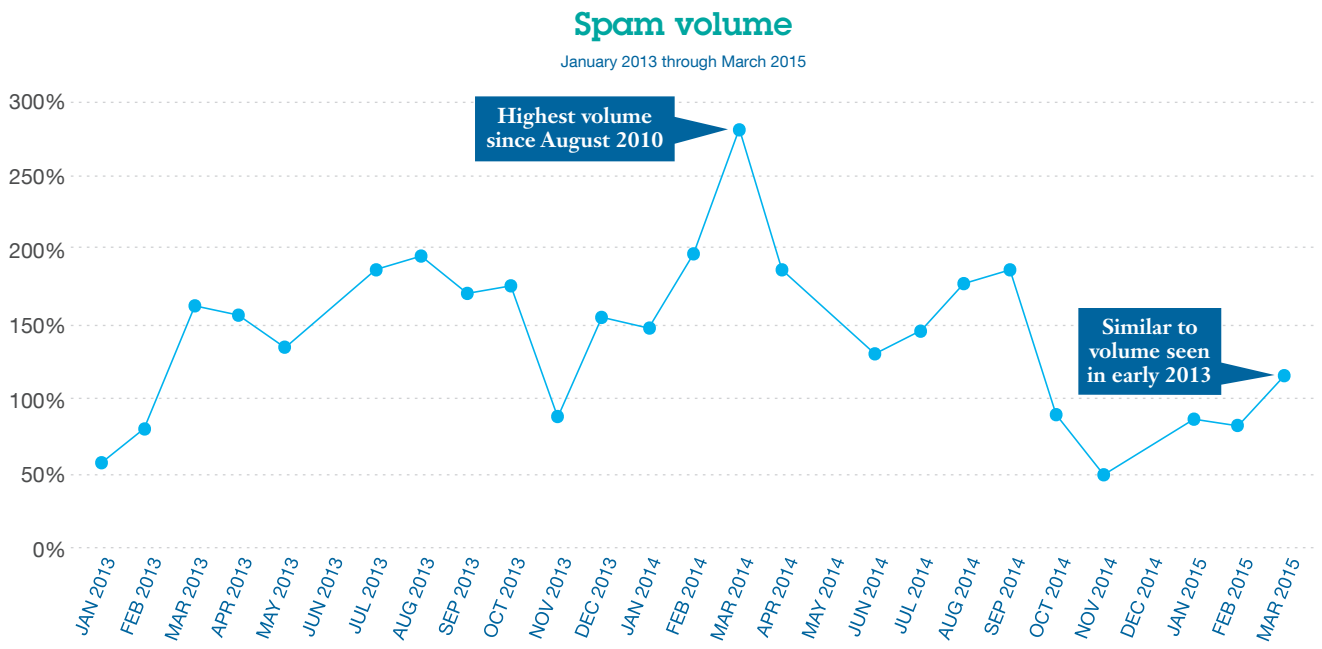


Figure 2. Spam volume, January 2013 through March 2015

Although we have seen major ups and downs of the overall spam volume during the last two years, the current volume is comparable to that of two years ago. However, we should not conclude that nothing has happened in the area of spam. Figure 3—the percentage of spam transporting malicious attachments—shows major changes.

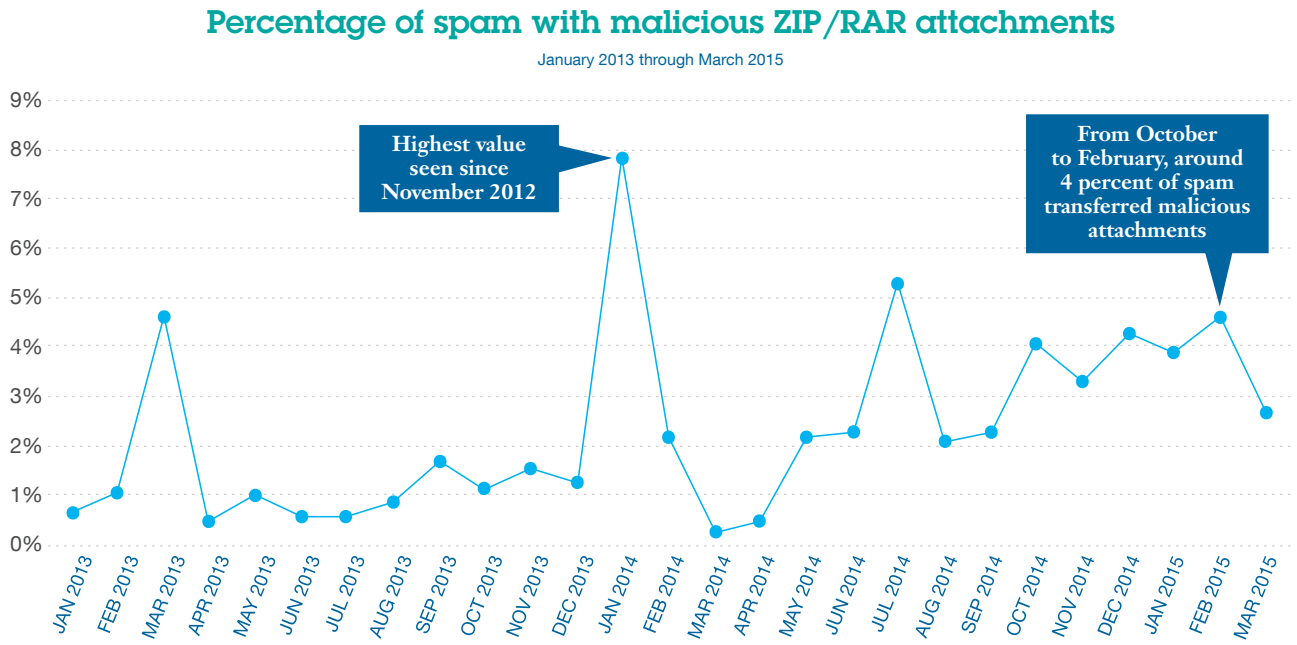


Figure 3. Percentage of spam with malicious ZIP/RAR attachments, January 2013 through March 2015

Until the summer of 2013, the percentage of spam carrying malware rarely exceeded one percent. Then, in the autumn of that year, there was a significant increase. During the first few months of 2015, the percentage of spam with malicious attachments has been around four percent. Thus, although the overall spam volume has not changed over the last two years, spammers are now using this channel to spread malware more than before.

This current trend corresponds with a trend reported in our IBM X-Force Threat Intelligence Quarterly – 1Q 2015 report. At that time, we saw that malware ranks as one of the most common attack types, and spam with malicious attachments provides one way to get malware into company networks and onto users' computers.

Any sort of malware might be attached to spam email messages, just as the links in them might go anywhere. Many spammers operate as for-profit ventures in which the buyer determines the payloads rather than the spam system operators. The spam operation can be hired by any sort of adversary, with any sort of motivation, from criminal intent to financial gain. As difficult as the repercussions for individual users can be, the invasion of your corporate network by ransomware can pose a significant risk to your business. In addition, an adversary more interested in your intellectual property and business secrets can use spam to infiltrate your network with keyloggers and password theft tools.

From these observations, we can draw several conclusions. Most important, spam grows more risky every day. In the past, spam operations focused on convincing victims to buy something or participate in a scam. As time passes, spam increasingly attempts to infect machines with malware. This trend pushes reliable spam filtering higher in your network security priorities. And, because no technology can guarantee perfect effectiveness, we must educate users and make them tougher to convince.

Recommendations

Here are recommendations to network administrators to help fend off malicious spam attachments.

- Keep your spam and virus filters up to date.
- Block executable attachments. In regular business environments it is unusual to send executable attachments. Most spam filters can be configured to block executable files even when they are within zip attachments.
- Use mail client software that allows disabling automatic rendering of attachments and graphics, and preloading of links—and then disable them.

Improving the defense posture of your users presents trickier problems. It's up to them to be aware of the danger—and to apply common sense at all times. Before opening that email and clicking on that link or opening the attachment it contains, users should ask some simple questions:

- Do I know the sender?
- Did I expect this email and this attachment?
- Does it make sense that the attachment is zipped, and is the format appropriate for this type of message and attachment type?
- Which file type is in the zip file? If it is an executable, a screensaver or a file type unknown to me, I should not open it!

Spammers often try to make their emails look like standard messages from online shops, banks or financial institutions, or the network's internal systems such as fax and copy machines. Users must be skeptical about these emails as well.

Every breach requires a plan of action

Learn how forensic analytics can provide the insight you need to understand what is happening in your network and what steps are necessary to prevent threats.

Securing a network from potential compromises is akin to being an airplane pilot; months of boredom and moments of panic. Just as an airplane pilot is trained to react methodically to any malfunction of the airplane, so too are security specialists required to have the training and tools to react methodically to any compromise of their network assets.

A *secured* system has been defined as one in which the work required to breach the system is far greater than any potential benefit that can be gained. However, both the *work* and the *benefit* represent moving targets. The work necessary to breach an organization decreases as adversaries socialize their hacker tools, share their techniques and collaborate on attacking defined targets. The rewards are typically great enough that legions of hackers are at work developing sophisticated software for testing and penetrating networks based on newly published vulnerabilities. Security specialists at target companies can watch their network "light up" as a new vulnerability is announced and these specialized dark applications test and probe services.

The point, then, is not whether your network is going to be compromised but whether you will be prepared and how you will respond to an attack. Imagine a pilot with no malfunction training. That situation is not likely to turn out well. Now imagine a network with no forensic capabilities. The prospects aren't promising there, either.

For example, today's consumers regularly receive messages from their health, banking and e-commerce providers that the network has been compromised, but the companies cannot provide a clear description of the compromise. In many cases, the only answer is for customers to change their credit card and login identities, and reset their passwords. A more serious consequence, however, is that users will never be able to retrieve their Social Security numbers, addresses, phone numbers and other personal identification. That's because while the loss of a single piece of personal identification may not be serious, when cybercriminals have the relationships or connections contained in all of an individual's personal identity, they have about 95 percent of the data needed to electronically carry out financial theft and fraud—regardless of whether or not the victim has changed credit card numbers. And going forward, if the provider cannot clearly identify how the compromise was conducted, it is unlikely that they can make sure the compromise will not happen again.

The ability to precisely identify the compromise is a fundamental tenet for any company that retains information beneficial for an e-crime.

Network and Asset Forensics

Forensics is the ability to clearly re-create and articulate any compromise of your systems. The basic functions include packet capture, search, filtering reconstruction and micro-inspection.

Packet Capture

"Capture" is the ability to gather and store every transaction that takes place on the network. It provides the visibility to conduct forensics, and it requires significant storage capabilities. For example, to store the network traffic of a 10 gigabit link running at 60 percent capacity requires approximately 7 terabytes of daily storage. A typical 2-rack unit (2U) capture appliance with a capacity of 56 terabytes would provide 8 days of historical network data. This time period is referred to as the forensic *window of visibility*. The larger the window, the greater the visibility available for use in forensic analytics.

Because many compromises take place over longer periods of time, providing the largest window at the lowest cost takes on great importance. The greatest expense for enabling packet capture is the cost of storage, so obtaining storage at a lower price is paramount in providing larger windows of visibility. Leading storage vendors implement compression technology in their products to increase the capacity of a system by as much as four times. Figure 4 represents the cost to capture a 10 gigabit network with and without compression technology. In this scenario, using compression technology reduces the cost by a factor of four, which would allow for nearly 45 more days of packet capture at relatively the same cost of uncompressed storage.

Search

A forensic investigation typically consists of searching for the unknown. That's where search engine technology can help, by providing:

- An easy and familiar interface for searching
- 100 percent instantaneous visibility to all forensic data

Anyone searching the Internet for a document containing *support@corporatebank.syzexperts.com*, for example, would receive immediate results. Search engine technology applied to forensics delivers the same capacity for captured network traffic. The sample email address above is a typical example of one that might be used in a phishing attempt, where the name brand of the company (*corporatebank*) is embedded within the attacker's domain (*syzexperts.com*). Properly indexed search engine technology instantly reveals the network transactions using that address.

One hundred percent visibility requires that the entire contents of the captured packets be indexed. In the indexing process, search engines categorize data into fields that enable high-fidelity queries. For example, network traffic is indexed by web domains, email addresses, URLs, HTTP error codes and hundreds of other fields to enable specific inquiries. Consider the following query:

IPAddress:192.72.68.121 AND Port:880 AND URL:*$^% AND HTTPError:404

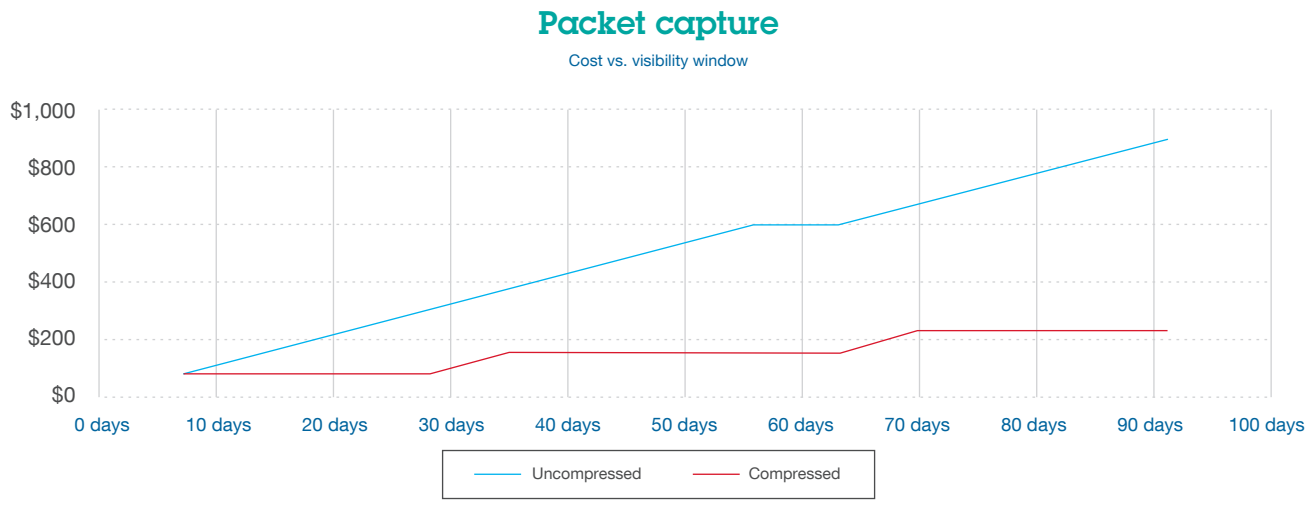


Figure 4. Packet capture, Cost vs. visibility window

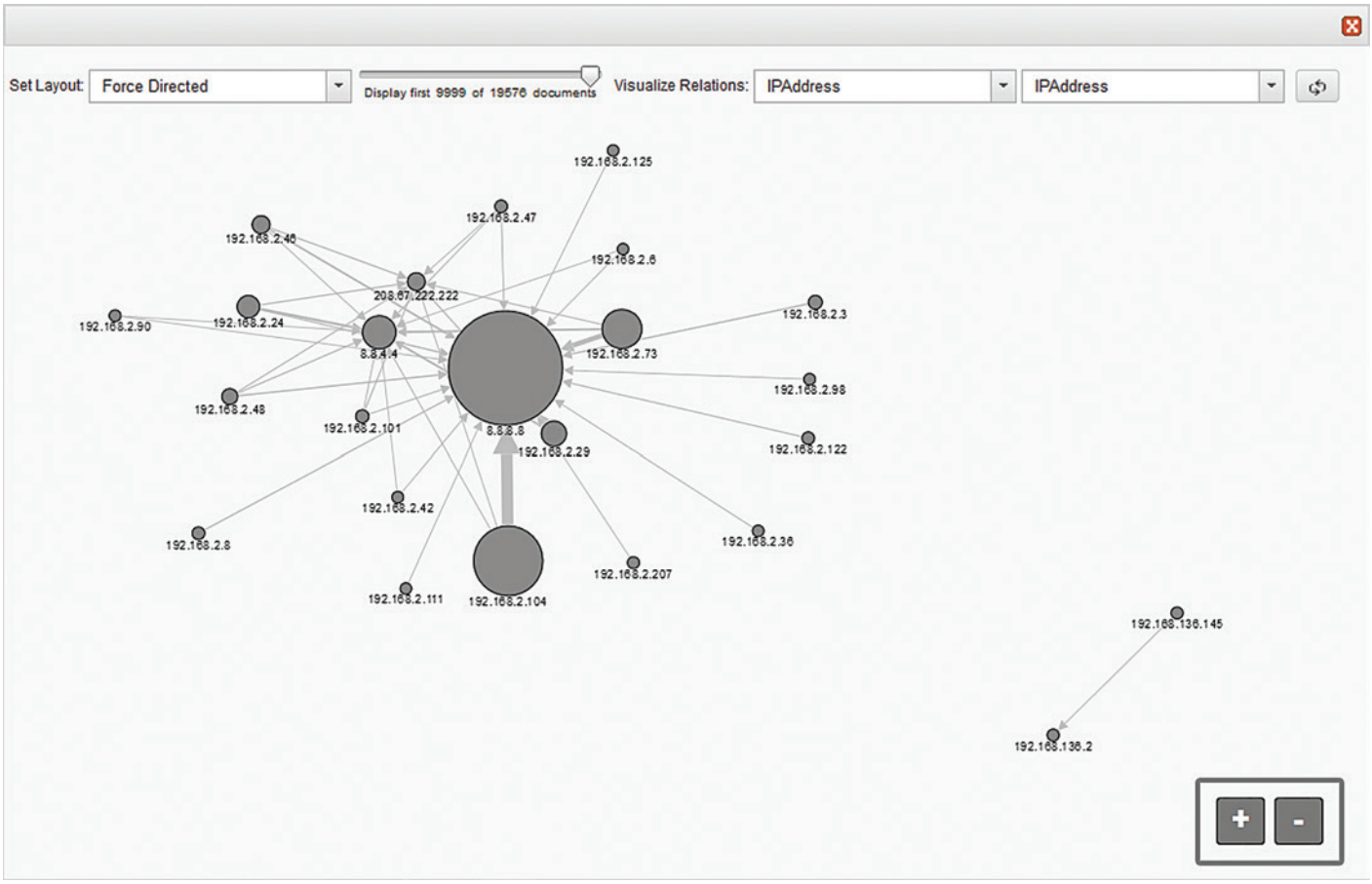
This query enables a forensic investigator to search for any attempt to obfuscate an HTTP application service by fuzzing the representation state transfer (REST) interface using strange characters. A forensic investigator may want to refine a search for a phishing attempt.

From:*syzexperts* AND password

This search would find any email traffic that contained *syzexperts* in the email name and the text *password* in the contents of the message body.

Filtering

When searching for the unknown, it's as necessary to determine what is not important as what is important. Forensic capabilities should include the ability to easily filter and visualize data in a fashion that differentiates the important from the inconsequential. For example, a researcher may find out that some strange behavior with domains is taking place within the network. A simple search on DNS traffic and visualizing the endpoint relationships can quickly reveal "outliers" in a manner not readily available in reports. For example, Graphic 1 shows all DNS traffic for a particular query. This visualization makes very apparent the two outlier domains that resolved outside the normal operations. This visual depiction provides a clear starting point for the investigator to further examine those outliers, otherwise unobtainable in standard reports.



Graphic 1. DNS network entity relationships

Reconstruction

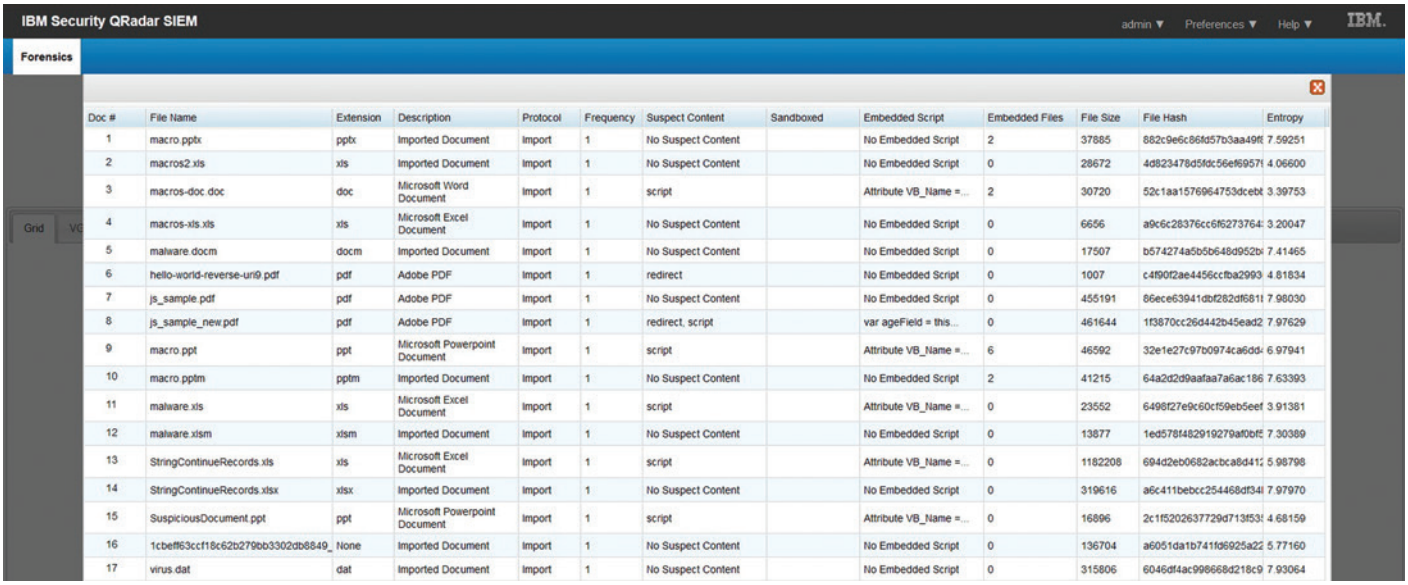
Reconstruction enables organizations to view recorded network transactions in formats tailored for human consumption. Storage systems contain the raw, unintelligible blocks of traffic data captured from the network. This raw data must be dissected and analyzed before it can be reconstructed. Examples of reconstruction include displaying a web page accessed by an adversary, a complete email message (or thread) involved, a file stolen in an attack, or even an entire IM conversation.

In the reconstruction process, software modules known as inspectors break down network data into the intermediate representations for search and reconstruction. An inspector identifies the network traffic through bit patterns from electronic flows. It is important to identify the traffic based upon data patterns—not the port number—as an attacker may try to disguise the protocol. Inspectors are written by engineers who analyze the protocols and services extracting key field metadata. The metadata is fed to the search engine in a structured format that enables detailed reconstruction of network events. When assessing the capabilities of a forensic solution, it is important to understand the difference between protocol identification and protocol inspection. Many vendors claim thousands of protocol identifiers. An identifier only labels the protocol used; an inspector breaks down the protocol for search and reconstruction. The following are differing types of reconstruction:

- Web page
- Chat
- Social networking
- Webmail
- Blogging
- File transfers
- File attachments
- File metadata (geo-location, last modified, and other similar attributes)
- File flows (attached executables, JavaScript, macros, redirects)

Micro inspection

Search and reconstruction refine the network transactions of interest from perhaps billions of flows down to a manageable set. Micro-inspection breaks down the final analytics (such as reporting on embedded files, file entropy, file obfuscation, file sandboxing and file flows, macros, executables, etc.) by identifying suspect content or data that pinpoint strategic forensic information. Premiere inspection environments include the ability to extract detailed file information in an automated fashion. Embedding information and files within files and obfuscating the file type are important methodologies for attackers.



Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Sandboxed	Embedded Script	Embedded Files	File Size	File Hash	Entropy
1	macro.pptx	pptx	Imported Document	import	1	No Suspect Content		No Embedded Script	2	37885	882c9e6c86fd57b3aa49ff	7.59251
2	macros2.xls	xls	Imported Document	import	1	No Suspect Content		No Embedded Script	0	28672	4d823478d5fdc56ef6957	4.06600
3	macros-doc.doc	doc	Microsoft Word Document	import	1	script		Attribute VB_Name =...	2	30720	52c1aa1576964753dcebt	3.39753
4	macros-xls.xls	xls	Microsoft Excel Document	import	1	No Suspect Content		No Embedded Script	0	6656	a9c6c28376cc6f6273764	3.20047
5	malware.docm	docm	Imported Document	import	1	No Suspect Content		No Embedded Script	0	17507	b574274a5b5b648d952b	7.41465
6	hello-world-reverse-uri9.pdf	pdf	Adobe PDF	import	1	redirect		No Embedded Script	0	1007	c4f90f2ae4456ccfba2993	4.81834
7	js_sample.pdf	pdf	Adobe PDF	import	1	No Suspect Content		No Embedded Script	0	455191	86ece63941dbf282df681	7.98030
8	js_sample_new.pdf	pdf	Adobe PDF	import	1	redirect, script		var ageField = this...	0	461644	1f3870cc26d442b45ead2	7.97629
9	macro.ppt	ppt	Microsoft Powerpoint Document	import	1	script		Attribute VB_Name =...	6	46592	32e1e27c97b0974ca6dd	6.97941
10	macro.pptm	pptm	Imported Document	import	1	No Suspect Content		No Embedded Script	2	41215	64a2d2d9aafaa7a6ac186	7.63393
11	malware.xls	xls	Microsoft Excel Document	import	1	script		Attribute VB_Name =...	0	23552	6498f27e9c60cf59eb5eef	3.91381
12	malware.xlsm	xlsm	Imported Document	import	1	No Suspect Content		No Embedded Script	0	13877	1ed578f482919279af0bf7	7.30389
13	StringContinueRecords.xls	xls	Microsoft Excel Document	import	1	script		Attribute VB_Name =...	0	1182208	694d2eb0682acbca8d412	5.98798
14	StringContinueRecords.xlsx	xlsx	Imported Document	import	1	No Suspect Content		No Embedded Script	0	319616	a6c411bebcc254468df34	7.97970
15	SuspiciousDocument.ppt	ppt	Microsoft Powerpoint Document	import	1	script		Attribute VB_Name =...	0	16896	2c1f5202637729d713f53	4.68159
16	1cbeff63ccf18c62b279bb3302db8849_	None	Imported Document	import	1	No Suspect Content		No Embedded Script	0	136704	a6051da1b741fd6925a22	5.77160
17	virus.dat	dat	Imported Document	import	1	No Suspect Content		No Embedded Script	0	315806	6046df4ac998668d218c9	7.93064

Graphic 2. Micro-inspection of all files within a network incident

Forensic systems detect embedded files using a variety of methods, including "magic numbers" and statistical analysis. Magic numbers are file identity attributes, and detecting multiple magic numbers within a file alerts investigators to suspicious content. Statistical analysis measures the "normalcy" of a data flow or file contents and can potentially detect when data has been injected into files or data flows.

Other file micro-inspection techniques include file deobfuscation where the file extension is compared to both the MIME and content type. For example, attackers often disguise executable files as image files. File flows attached to documents are also an attacker methodology for executing malware embedded within the file (macros, JavaScript, executables, URL re-directs, etc.)

Sandboxing provides the ultimate tool for forensic analysts to determine how an attack infects a host. Graphic 2 shows the micro-inspection capabilities of files found within refined search of network flows.

Summary

The ability to reconstruct the activities that took place during a network compromise is essential to securing the network and preventing further harm. In many cases, the compromises are difficult to accurately detect and a premiere forensic environment will have search capabilities as its fundamental offering. The ability to provide 100 percent visibility into the network traffic by capturing and indexing all data delivers pinpoint clarity to the investigative process. Supplemental tools that provide visualization, derived intelligence and micro-inspection capabilities drastically reduce the time to assess the compromise and can accurately depict the scope of the damage and the security adaptations and enhancement needed to prevent further damage.

Identity management helps control risk

Your entire staff—especially privileged users—can threaten your systems. Learn how the right tools can help manage the risk.

Threats to your business resources—including the "crown jewels" of your business data—can come from virtually anywhere and anyone in your organization. So you need a comprehensive set of tools to control risk. You need tools that can reach every corner of the enterprise, provide insight into every action that occurs, and help you manage everyone who has access to your environment.

Your people can be your weakest link

In many organizations today, the most serious security threat isn't external attacks, but the insider who can compromise or leak sensitive data. Modern trends in enterprise computing—the rise of social media, the cloud, mobility and the era of big data—make threats from employees, contractors, partners and others with trusted access harder to identify, and give insiders more ways to pass protected information with less chance of discovery.

Insider threats are caused by a wide range of offenders who can put an organization and its assets at risk. While malicious employees are an obvious source of threats, so are users who inadvertently leave their systems open to attack or who make mistakes that open the door to malware. Even companies with strong security practices are still vulnerable to acts of social engineering that enable cybercriminals to steal access credentials. For example, in one case, attackers sent malware-laced emails to unsuspecting employees to gain access to the vendor's customer data.[5]

Educating employees about suspicious communications and potential risks clearly is important. However, these efforts must be backed with other, more powerful automated threat protection tools and comprehensive security policies.

Use IAM solutions to mitigate insider threats

Identity and access management (IAM) solutions can play a key role in combating insider threats, helping relieve the threat of security breaches and noncompliance that results when users have outdated or inappropriate levels of access privileges. The potential for insider threat activity, in fact, is considerably higher when a user's profile grants access to resources that does not reflect current needs and actual use patterns. Insiders waging an attack also may take advantage of poorly controlled administrative privileges to escalate an attack or alter systems to enable eavesdropping. Poorly controlled and monitored user access privileges, coupled with a lack of visibility into the misuse or abuse of those privileges, often play a role in the success of these insider attacks. As a result, it's always important to make sure access privileges align with established security policies and that auditing and reporting tools are in place to monitor user behavior and enforce those policies.

In the face of insider threats, protecting valuable data and resources demands more than requiring each user to have a simple user ID and password. You need strong authentication that relies on sound policy for identity assurance. This not only helps protect against the bad guys who would attack the organization from outside, it also helps reduce opportunities for negligent insiders to unintentionally leak data. It also helps prevent malicious insiders from taking advantage of lax deprovisioning of expired or orphan accounts to attack your valuable resources.

The organization also should use identity governance solutions to help classify users by roles and access requirements—and to set and enforce role-based policies for automated user lifecycle and password management. It is not enough to allow or deny access to applications; you must know who is requesting access and why, and what an individual is doing with access rights once they are granted. IAM solutions should also perform monitoring and enforcement to help identify policy violations and identify abuse that could signal an insider threat.

Privileged users are often the biggest threat

The trends toward data-center consolidation, cloud computing, virtualization and outsourcing are generating more privileged IDs in today's IT infrastructures. This creates an even greater need to centrally manage and secure privileged IDs—and to pay attention to who you grant privileged ID status. The overarching access of these privileged users gives them extraordinary abilities to control and exploit an organization's data, applications and endpoints. If privileged-user IDs are not properly managed, they can cause accountability and compliance issues in addition to increasing the risk of data theft. At the same time, insider access controls for other groups, less privileged but still high risk, should not be ignored. System administrators and other IT staffers, who may have the skills to instigate an insider attack, should not be overlooked. As Figure 5 shows, decision makers surveyed in a recent IBM study already recognize the security threat posed by administrators and privileged users.

Fortunately, there are a number of approaches organizations can take to help mitigate the insider threat. Stricter policy controls and improved user education are a good start. This means ensuring that staff members across the organization are aware of their responsibilities and accountability for particular activities, as well as how to avoid attacks and inappropriate access. Firms also need to ensure employees are kept up to date on regulatory and compliance requirements.

These measures need to be bolstered by effective security tools. Security intelligence solutions that monitor behavior and provide anomaly detection are invaluable, as are privileged identity management (PIM) solutions that control and monitor access of "super users." Identity governance tools can help ensure user access entitlements map to users' job responsibilities. Intelligence and governance solutions, when integrated, can go a long way toward combating malicious insiders.

Top security threats, as reported in an IBM Institute for Business Value survey

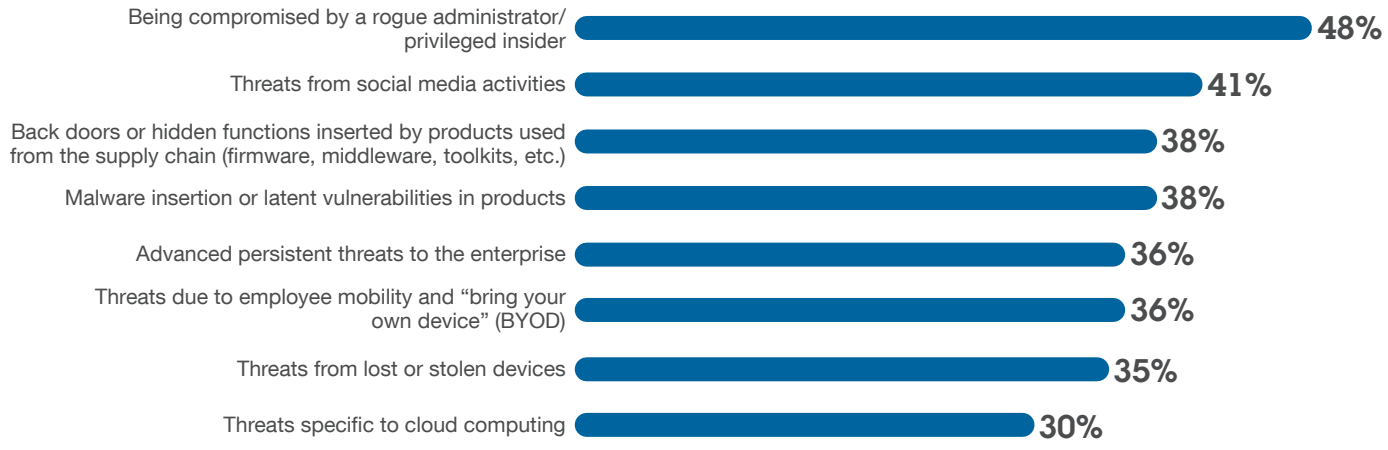


Figure 5. Top security threats, as reported in an IBM Institute for Business Value survey

Source: IBM Institute for Business Value, IT Infrastructure Study; Q7: How concerned are you about the following security threats?

Make operational intelligence your secret weapon

To effectively combat insider threats, it's important to establish and maintain access controls and monitoring over senior managers and executives who often have unfettered access to the organization's most sensitive data. Without the proper oversight, a senior person who left the organization months ago—or even an attacker who has penetrated your system—could use an executive's privileged access to your servers, appliances networks and data. Better oversight of these users and their activities can raise a red flag if/when confidential information is being inappropriately accessed, distributed and downloaded.

To help ensure user accountability and mitigate insider threats, organizations should consider an enterprise-wide IAM approach bolstered with analytics and security intelligence. Such an approach can enable organizations to quickly and accurately identify anomalies in user behavior, understand user roles and group memberships, protect against insider fraud and demonstrate compliance with burgeoning security regulations.

Integrated identity intelligence systems can also monitor user activity, a critical part of an active defense against insider threats. Using security intelligence analytics and reporting tools together, for example, can provide critical capabilities for auditing user activities and unearthing suspicious behavior. Based on security intelligence, user activity monitoring solutions provide comprehensive visibility into user activity and its impact.

Security intelligence also helps detect insider threats occurring over an extended time. Some solutions focus on specific events, assets or transaction types in order to store and analyze a much smaller and more manageable amount of data. This makes it possible to identify even a "low and slow" attack from the inside. Best of all, security intelligence can help the enterprises migrate from answering the question "What has happened?" to predicting "What will occur?"—helping the organization block potential breaches.

Recommendations

So what are some best practices to help you better mitigate insider threats and strengthen compliance?

Privileged IDs are growing, so control the associated risk. Organizations often delegate specific administrative tasks to a large pool of staff or contractors whose membership changes frequently. Additionally, employees such as application owners and developers might require occasional or one-time privileged access to specific resources to perform maintenance tasks. Both these practices can cause a surge in the number of IDs provided within the organization. But while it may be expeditious to control ID growth by allowing multiple privileged users to share one or more common user IDs on each resource, it's not a good idea. This practice circumvents the need to continually add and delete accounts as users come and go, but it also destroys user accountability. In addition to destroying user accountability, it can interfere with regulatory compliance. The preferred solution is to deploy an identity management system that can provide a secure and convenient way for IT staff to share privileged IDs while also providing audit trails of individual users' behavior.

Grant user entitlements appropriately and keep them updated. User entitlements should be updated to adapt to changes, especially when workers change roles or leave the organization. A relatively simple best practice that every organization can adopt is to authorize users based on the least access privilege they require—and then conduct regular audits of user entitlements. Because the potential for harm is so great as entitlements grow, the number of privileged accounts should be kept to a minimum. Granting privileged ID entitlements should be scrutinized and limited to only those who truly need the privileged access and who have the necessary credentials and clearances.

Manage and monitor users for both security and compliance. Once user accounts are established, organizations should carefully monitor and audit the activities associated with the IDs to highlight anomalies or misuse of the account's privileges. By combining user and application monitoring with application-layer network visibility, organizations can better detect meaningful deviations from normal activity, helping to stop an attack before it completes.

About X-Force

Advanced threats are everywhere. Help minimize your risk with insights from the experts at IBM.

The IBM X-Force research and development team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats.

IBM Security collaboration

IBM Security represents several brands that provide a broad spectrum of security competency:

- The IBM X-Force research and development team discovers, analyzes, monitors and records a broad range of computer security threats, vulnerabilities, and the latest trends and methods used by attackers. Other groups within IBM use this rich data to develop protection techniques for our customers.
- IBM X-Force Exchange is a robust, global threat-intelligence sharing platform designed to consume, share, and act on threat intelligence—all backed by the scale and reputation of IBM X-Force. Users can search for various threat indicators pulled from machine-generated intelligence, and add context via human intelligence for a collaborative way to research and help stop threats.
- The IBM Security Trusteer® product family delivers a holistic endpoint cybercrime prevention platform that helps protect organizations against financial fraud and data breaches. Hundreds of organizations and tens of millions of end users rely on these products from IBM Security to protect their web applications, computers and mobile devices from online threats (such as advanced malware and phishing attacks).
- The IBM X-Force content security team independently scours and categorizes the web by crawling, independent discoveries, and through the feeds provided by IBM Managed Security Services.
- IBM Managed Security Services is responsible for monitoring exploits related to endpoints, servers (including web servers) and general network infrastructure. This team tracks exploits delivered over the web as well as via other vectors such as email and instant messaging.
- IBM Professional Security Services delivers enterprise-wide security assessment, design and deployment services to help build effective information security solutions.
- IBM QRadar® Security Intelligence Platform offers an integrated solution for security intelligence and event management (SIEM), log management, configuration management, vulnerability assessment and anomaly detection. It provides a unified dashboard and real-time insight into security and compliance risks across people, data, applications and infrastructure.
- IBM Security QRadar Incident Forensics is designed to give enterprise security teams visibility into network activities and clarity around user actions. It can index both metadata and payload content within packet-capture (PCAP) files to fully reconstruct sessions, build digital impressions, highlight suspect content, and facilitate search-driven data explorations aided by visualizations. QRadar Incident Forensics easily integrates with QRadar Security Intelligence Platform and can be accessed using the QRadar one-console management interface.
- IBM Security AppScan® enables organizations to assess the security of web and mobile applications, strengthen application security program management and achieve regulatory compliance by identifying vulnerabilities and generating reports with intelligent fix recommendations to ease remediation. IBM Hosted Application Security Management service is a cloud-based solution for dynamic testing of web applications using AppScan in both pre-production and production environments.
- IBM Security identity and access management solutions help strengthen compliance and reduce risk by protecting and monitoring user access in today's multi-perimeter environments. They help safeguard valuable data and applications with context-based access control, security policy enforcement and business-driven identity governance.

Contributors

Producing the IBM X-Force Threat Intelligence Quarterly report is a dedicated collaboration across all of IBM. We would like to thank the following individuals for their attention and contribution to the publication of this report.

Contributor	Title
Ben Wuest	Senior Technical Staff Member, IBM Security Intelligence
Doug Franklin	Research Technologist, IBM X-Force Advanced Research
Leslie Horacek	Manager, IBM X-Force Threat Response
Michael Campbell	Senior Security Specialist, IBM Security Systems Sales Enablement
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force and Threat Portfolio
Ralf Iffert	Manager, IBM X-Force Content Security
Robin Cohan	Product Manager, IBM Security Identity Management
Roger J. Hellman	Worldwide Market Segment Manager, IBM Security Intelligence
Russell Couturier	Chief Technology Officer, IBM Network Forensics
Tim Kroupa	Engagement Lead, IBM Emergency Response Services
Veronica A. Shelley	Worldwide Market Segment Manager, IBM Identity and Access Management

For more information

To learn more about IBM X-Force, please visit:
ibm.com/security/xforce/

[1] "IBM Security Services 2015 Cyber Security Intelligence Index," http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home

[2] Sean Michael Kerner, "AT&T Insider Data Breach More Dangerous Than External Hacking," *eWEEK*, 16 June 2014. http://www.eweek.com/mobile/att-insider-data-breach-more-dangerous-than-external-hacking.html

[3] Darlene Storm, "Remotely listen in via hacked VoIP phones: Cisco working on eavesdropping patch," *Computerworld*, 8 January 2013. http://www.computerworld.com/article/2474060/cybercrime-hacking/remotely-listen-in-via-hacked-voip-phones--cisco-working-on-eavesdropping-patch.html

[4] Chris Poulin, "What Retailers Need to Learn from the Target Breach to Protect against Similar Attacks," *IBM Security Intelligence Blog*, 31 January 2014. http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.VUtHXPmqjRY

[5] Adam Greenberg, "Home Depot announces 53M email addresses stolen in breach," *SC Magazine*, 07 November 2014. http://www.scmagazine.com/home-depot-announces-53m-email-addresses-stolen-in-breach/article/382144/

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
June 2015

Please Recycle

WGL03076-USEN-00