IBM Security Systems

June 2014

IBM X-Force Threat Intelligence Quarterly 2Q 2014

Discover how application vulnerabilities, spam threats and incident response are evolving—based on the latest data and ongoing analysis

Contents

Executive overview

The IBM® X-Force® research and development team, along with colleagues from the IBM Global Technology Services® division, has been busy analyzing the latest round of security threats, and we're excited to share our latest findings. We began 2014 discussing the many breaches and security incidents that continue to challenge organizations. In this second quarterly report for 2014, we turn our attention toward methods resurfacing that achieved success in the past and toward slightly new issues to consider in today's security landscape.

First, let's look at the old threats. Over time, we have seen many threats come to replace the ones before them. Famous virus emails such as ILOVEYOU have evolved into insidious drive-by-download malware installations that silently collect sensitive user data. The defacement of websites just for bragging rights has moved into being a distraction for more malicious activity against servers and databases. In addition, worms such as Blaster and St0rm laid the framework for the latest distributed-denial-of-service (DDoS) attacks.

What can we glean from a history of Internet threats and how things have changed? Since the beginning of writing software applications, there have been vulnerable applications. When programmers write software and make mistakes, applications become vulnerable. In this report, we take a closer look at vulnerable website applications and how they continue to pose a serious threat vector for attackers who want to do harm to organizations or steal sensitive data.

Application scanning can help protect the most critical user-facing components of web services and applications, addressing both custom application code as well as third-party components. Still, customers need to be mindful of the security of the web server itself. Vulnerable technology that comprises the backbone of a web application stack can put the whole environment at risk.

In April 2014, a vulnerability (CVE-2014-0160) in the popular and widely used OpenSSL software put a huge percentage of websites at risk for data leakage of private and critical information. The patch itself was not difficult to apply, but mitigating potential damages of breached user credentials, SSL certificates and other sensitive information made cleanup a challenge. When critical vulnerabilities are announced or incidents occur, we should learn to "expect the unexpected." If your incident response is built around planning for the known situations, you're at a loss. Contents of random access memory (RAM) are now just as fair game as data stored on the disk. We'll provide some recommendations for organizations who want to improve in this important area of security.

For more information about Heartbleed, the OpenSSL transport-layer security (TLS) heartbeat vulnerability, refer to the recent IBM Security Intelligence blog post.[1]

In the next section of the report, we'll look at how spam—one of the oldest and longest lasting security threats—is alive and well. Most organizations have the proper controls in place to fight the onslaught of spam, but attackers still use it to clog email servers and sometimes to deliver malicious payloads to unsuspecting users. The IBM X-Force content security team continues to monitor how spam has evolved over time and how it remains a primary channel to insert malware into company networks. In March 2014, we saw a return of the highest levels of spam measured during the past two and a half years. We also analyzed the tracking data for spam bot infections and how it correlates to the (now) end of support for Microsoft Windows XP.

Finally, we'll close the report with a slightly new category of security threats. With help from the IBM Global Technology Services - Emergency Response Services (ERS) team, we'll share lessons learned when remote incident response becomes extremely remote. As worldwide organizations expand their reach into developing countries and nascent infrastructures, what happens when a security incident occurs in an area with limited bandwidth and communications? How can responders quickly transfer their critical data? We'll explain how incident response in remote countries or infrastructure-deficient areas requires a unique game plan.

Vulnerable applications as a serious threat vector

From injection vulnerabilities to broken authentication, find out what threats may be lurking in your dynamic web applications.

Attackers look for any path to exploit sensitive and valuable corporate data. Often the fastest way into a company's internal systems is through vulnerabilities, such as SQL injection (SQLi) and broken authentication. If companies are not testing their websites and the applications that access them, they are at risk of exposing valuable assets.

In the mobile application world, for example, IBM researchers recently found a series of vulnerabilities in Mozilla Firefox for Google Android that allowed malicious applications to leak sensitive information about user profiles.[2] A threat actor can exploit these vulnerabilities to extract information such as cookies and cached data such as browser history and user IDs.

Another mobile vulnerability discovered by IBM researchers is fragment injection in the Android framework that impacted a number of popular applications including Google Now, Gmail, Dropbox and Evernote.[3] Attackers exploiting this vulnerability were able to access sensitive information pertaining to the vulnerable application by breaking the Android sandbox.

Web applications are another attractive target for threat actors because they often have access to internally stored, high-value corporate data. Exploiting an injection vulnerability, such as SQLi, can lead to manipulation of protected back-end databases. And failure to protect data in transit to and from a web application can result in data leaks of user credentials, credit card data and private communications.

What are the top 10 web application threats?

In 2013, the Open Web Application Security Project (OWASP) Top 10 identified a list of the 10 most critical web application security risks. As shown in Figure 1, injection attacks, broken authentication and session management, and cross-site scripting were at the top of this list.[4]

In the next sections we take a deeper look at the web application threat research from the IBM team that manages hosted application testing.

Web application threat data

The IBM Hosted Application Security Management (HASM) service is a cloud-based solution for dynamic testing of web applications using IBM Security AppScan® in both pre-production and production environments. HASM services include a dedicated security analyst to configure and manage the testing.

For this report, the HASM team collected threat data from more than 900 dynamic web application scans conducted in 2013. Some key points about this data are that:

- The data set comprises applications from a wide variety of industry sectors, including government, financial services, industrial, pharmaceutical, retail and telecommunications.
- Most of the scans are from organizations that have been using the HASM service for more than five years. They have mature and established security practices, which means the scanned applications typically have a lower number of vulnerabilities than an organization that is new to web application security.
- Although regular scanning is performed on these organizations' web applications, vulnerabilities are found on an ongoing basis, often introduced by code changes or deployment of new applications. This is why applications should be rescanned after new functionality is deployed as well as after code updates and patches.
- The majority of the issues found relate to the lack of proper input validation and sanitization.

2013: The year of the broken authentication threat

Figure 1 shows that cross-site scripting (XSS) and cross-site request forgery (CSRF) threats are still quite prevalent in web applications. Injection attacks, while less frequent in this customer sample set, are still quite common and dangerous because they lead directly to threat actors accessing sensitive, internal data. However, since these vulnerabilities are well known, we're going to take a closer look at another prevalent issue—broken authentication.

Broken authentication can result from the failure to protect user ID and password credentials as well as the failure to properly manage session IDs. Without proper protection of authentication information, an attacker can hijack a user session and impersonate that user. For example, a threat actor can exploit this vulnerability to take over a banking session and transfer funds as if the attacker were the legitimate user.

HASM data highlights that one of the most common broken authentication issues found in authenticated scans is the issue type, "Session ID not updated during login." This particular test checks to make sure that the value of the session cookie is updated during the login sequence, that is, after a user clicks the submit button on a login page. If the session ID (SID) is not updated at login, the web application may be vulnerable to session-fixation attacks. In a session-fixation attack, if attackers can gain access to a valid SID, they can use that ID to bypass the login process and access the victim's account. This attack can work with both user- and server-generated SIDs.

Microsoft ASP.NET applications are often at risk for session-fixation attacks because, typically, the JSESSION cookie value is generated on the login page before the user signs in and, by default, it isn't updated during the login process.

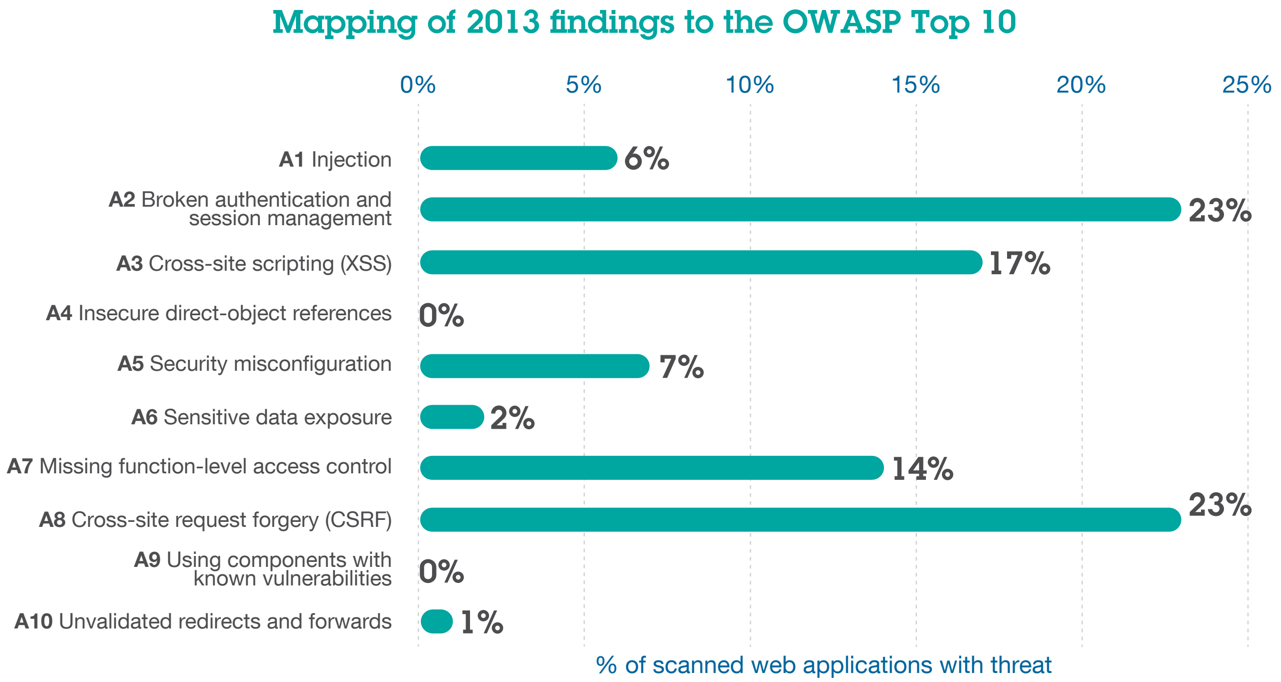


Figure 1. Common vulnerabilities found occurring in web applications tested by the IBM Hosted Application Security Management (HASM) service, compared to the OWASP Top 10 for 2013

Session fixation, and misuse of SIDs, is a common vulnerability. We've also found that this particular issue isn't well understood and typically takes a few iterations before developers understand the problem and the exploit can be remediated properly.

To help improve application testing for the early detection and remediation of session-based authentication vulnerabilities, IBM recommends:

1. Updating the SID on login
2. Enforcing a timeout on the SID after logout or a period of inactivity
3. Providing application programming interfaces (APIs) or libraries for authentication functions

Trends in application security testing

As web application security awareness grows, so does the trend toward organizations investing in web application scanning. Organizations develop a baseline of their web application risk by adding regular web application scanning in either pre-production or production environments.

Traditionally, HASM clients have been most interested in scanning their applications before deployment. But in the past year, we've seen a distinct uptick in organizations that want to perform large-scale, ongoing scanning of their live sites.

To facilitate these bulk-scanning initiatives of live applications, organizations need to build an inventory of all web applications using an automated method of application discovery. It's becoming increasingly difficult for IT security staff to keep track of, or find, all of the web applications that they own. It's not uncommon for organizations to underestimate the number of web applications they have by up to 50 percent. And if you don't know you have an application running, it's a pretty safe bet that you're not scanning it for security vulnerabilities. However, the attackers are scanning for vulnerabilities. This is why performing regular scanning and updating application inventory information is so crucial.

Because web application scanning requires a specific skill set, a significant investment in software, and perhaps additional infrastructure, many organizations are using an outsourced model. It can be costly and time-consuming to build internal teams with deep application security testing skills. Thus, outsourcing the work allows organizations to get up and running quickly at a low price point. Besides the quick start-up time, testing vendors have extensive security knowledge and experience. They can also provide ongoing maintenance of the scanning software and required infrastructure.

Tips for safe production scanning

When using outsourced scanning, it is important to understand the nature of the scanning that's being performed. Talk to the testing team to understand how the scans are being configured, what is being tested, if anything isn't being tested and what coverage is being achieved. Then, ask if there are any risks or pitfalls. This last point is particularly important because testing applications that are in production can lead to service outages. When you evaluate vendors, make sure that you understand their production-scanning approach and test coverage.

Production scanning

If a vendor is recommending production scanning, there are some key points to consider. For a website with static content, there is less to worry about, but for applications that collect data and save that data to back-end databases or feed that data to other back-end systems, it's important to understand how the vendor is going to test those areas. There are two main approaches for production scanning:

1. **Full-form testing**—In this approach, all of the forms in your application are tested. While this approach can provide good coverage and pick up the majority of issues, there are numerous risks:
   - When data is submitted into a database using forms, testing can cause a lot of test data to be inserted into the back-end database and systems. For example, a form with 10 form fields can be submitted more than 1,000 times.

- Some forms are used either to directly send email or to link to other back-end systems that generate email. Again, if these forms are tested, thousands of emails can be generated.
- Although rare, it is possible for scans to cause the complete failure of applications or back-end systems. Even if they don't fail, the test data that gets inserted may cause failures in back-end processing.
- Web application security scanning can generate large quantities of http(s) traffic and cause bandwidth or performance problems for some applications that might directly impact your users.

2. **No form filling or selective form filling**—in this approach, there is no or minimal form filling, which can help prevent the issues that can occur during full-form testing. However, this type of testing is less thorough and can result in security gaps. Forms are typically the areas in an application where many critical issues are found—mostly due to inadequate input validation. By not testing all forms, organizations run the risk of missing these important issues.

Figure 2 illustrates the point that when production scanning is done in such a way to reduce the potential problems of full-form testing, fewer vulnerabilities are found.

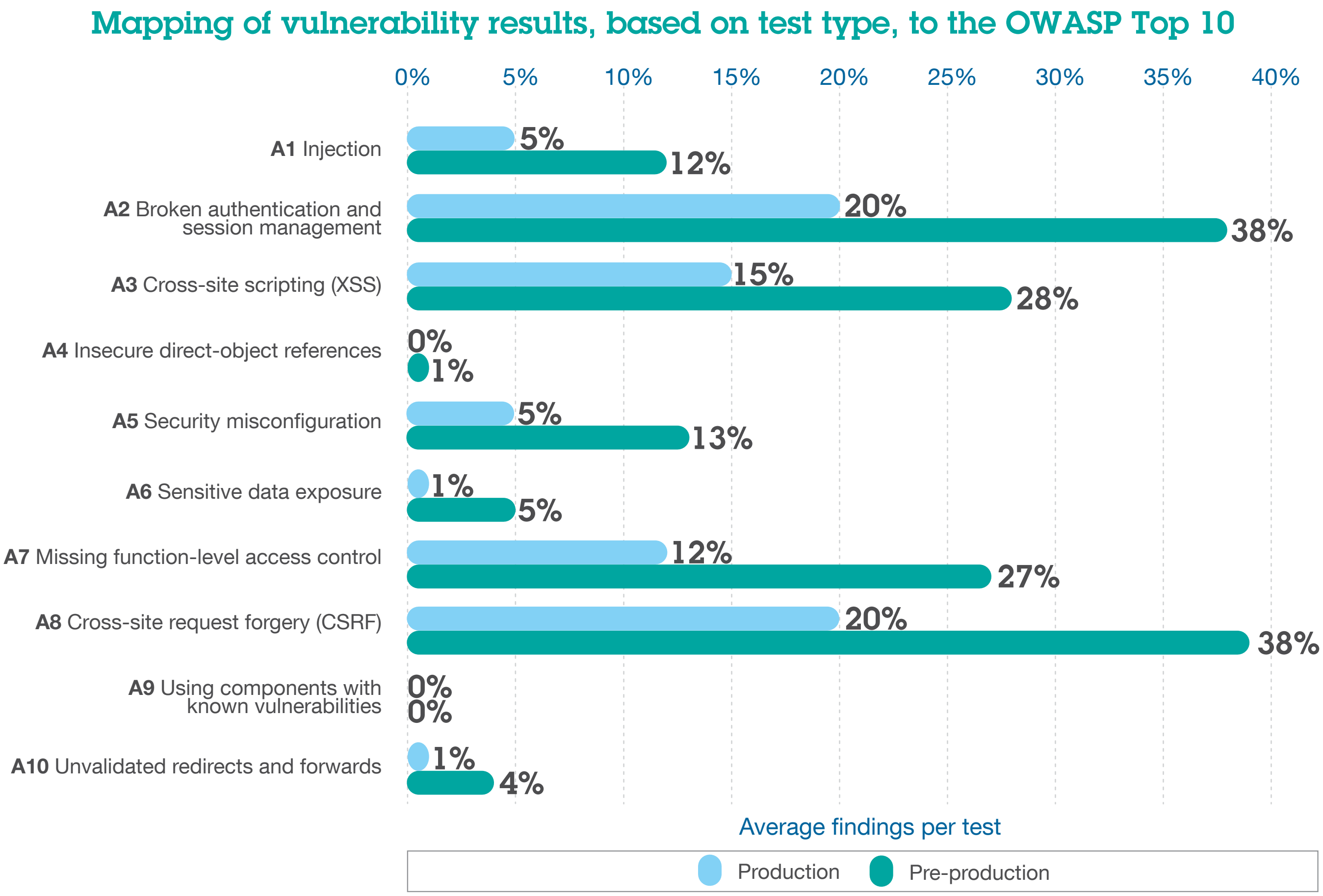


Figure 2. Results from production scanning and pre-production scanning by the IBM Hosted Application Security Management (HASM) service, compared to the OWASP Top 10 for 2013

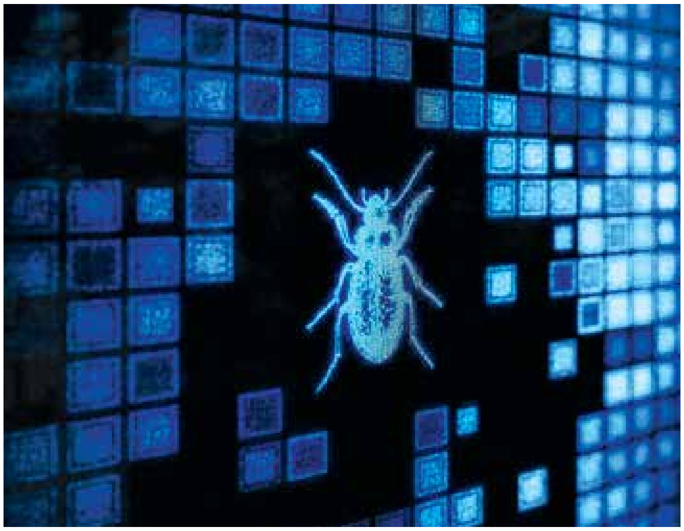
Due to the issues with full-form testing, it is often advantageous to run scans in a staging or quality-assurance (QA) environment before deployment. Pre-production scanning can be complemented with regular unobtrusive (that is, no form-filling) scans on production applications. This approach allows full testing of applications without the risk of data corruption or disruption to production systems. Plus, it also supports ongoing testing and monitoring.

Coverage

Another item to consider is the actual coverage area for testing—for example, does the testing cover just web pages or does it also include dynamic areas? Don't assume that scans will cover 100 percent of your applications. There are many ways to approach the scanning of applications and, if it isn't done correctly, your scans could have significant blind spots and you could be leaving yourself exposed.

As previously mentioned, scans can be performed in both production and pre-production environments. Given the need to protect live environments, production scans are often designed to be limited in coverage. However, pre-production scans should be performed in a more intrusive manner, especially when it comes to form filling. You can help ensure proper coverage by understanding the scan configuration being used in pre-production and production scans.

When it comes to form filling for dynamic web applications, using an auto-crawl mechanism for testing is typically insufficient. Highly dynamic applications require specific form data and the user interface (UI) is often too sophisticated for an auto-crawl mechanism to navigate it successfully to test all functionality. This means that, to get full testing coverage of these applications, you should augment the auto-crawling mechanism with manual crawling completed by a knowledgeable security testing professional.



Finally, from a page-coverage perspective, it is important to understand what filtering is being applied to the scan. Settings within scan configurations can filter pages on page similarity and other URL redundancy. Although filtering is a good tool for helping ensure that scans are optimized to run faster, it can also limit coverage. These settings can usually be manually adjusted and may need to be applied differently depending on the website.

Final recommendations

Applications are a key target for attackers. If applications aren't tested for security vulnerabilities and fixed, attackers can find and enter through any threat window. IBM researchers recently found vulnerabilities in both the Android framework and the Firefox browser that put corporate data on mobile devices at risk. Similarly, the IBM HASM services team, using AppScan for testing, found that injection vulnerabilities and broken authentication are active in many web applications in production environments. The best way to help prevent threats—and help protect data accessible on mobile devices and through web applications—is to test your applications for security vulnerabilities and fix the ones you find.

Spam and its persistence through time

What are the latest trends in spam? Learn how attackers are reinventing ways to exploit the email inbox and evade detection.

Since its origins in the late 1970s, the battle between email spam creators and spam-detection systems has persisted. Looking toward more recent developments in the last decade, the IBM X-Force 2011 Trend and Risk Report had an extensive analysis of the evolution of spam, including long-term trends, techniques and fluctuations in overall volume.

Now, some years later, we continue to see some of the same trends come and go. Plain-text spam and spam with infected zip attachments still reign strong, with attackers finding new ways of evading detection. Other techniques, such as sending MP3 files or PDF attachments, have not been as effective. Image-based spam, which first emerged in 2005, has been coming around again in new ways. Whether promoting penny stocks in a pump-and-dump scheme, or linking to malicious content, we continue to see attackers explore new ways to exploit the email inbox for maximum effectiveness.

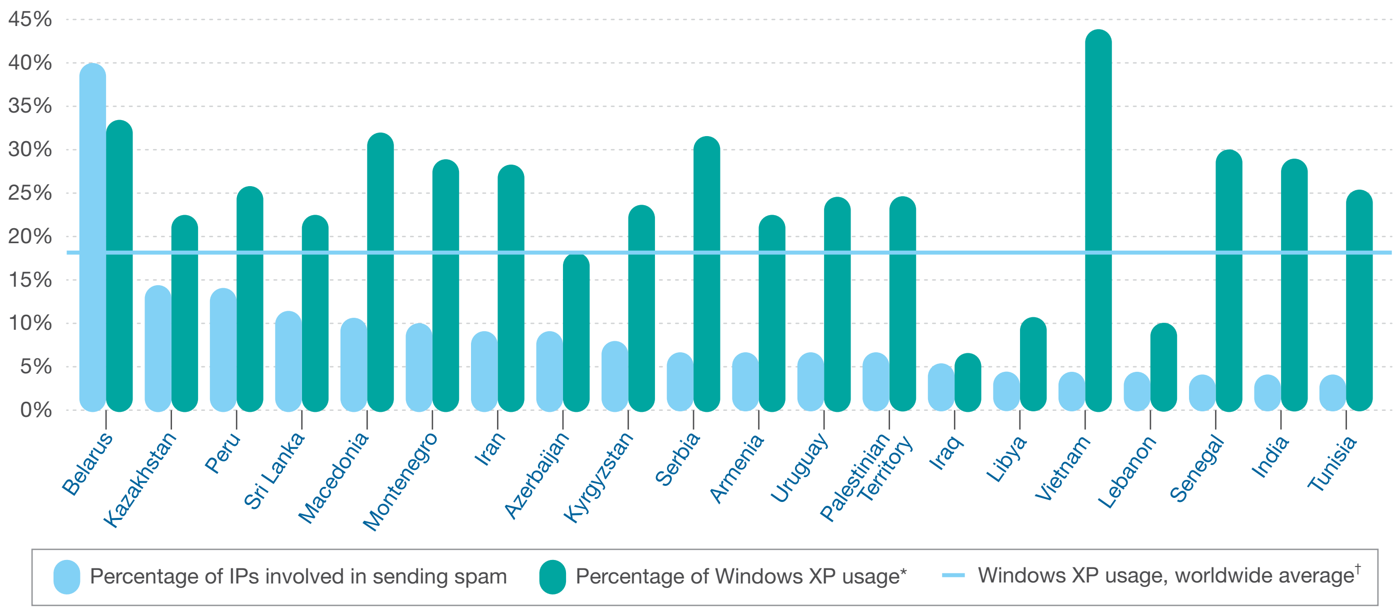
Another view on the origins of spam

Spam has been, and still is, a serious issue, as it continues to be a main channel of malware into company networks. In March 2014, we saw the highest levels of spam measured during the last two and a half years. Figure 3 shows the top countries where spam originated in the last six months, and many countries that have been listed in the past continue to be the top offenders today (for more information on countries where spam originates, see the IBM X-Force 2013 Mid-Year Trend and Risk Report).

Top 10 countries where spam originates, 4Q 2013 through 1Q 2014

10.1%	Spain
6.2%	Italy
6.2%	United States
5.7%	India
4.5%	Germany
4.4%	Romania
4.3%	Argentina
3.4%	Vietnam
3.1%	Russia
3.0%	United Kingdom
49.1%	Other

Figure 3. The top 10 countries where spam originates, 4Q 2013 through 1Q 2014



The top 20 countries with spam bot infections, compared to Windows XP usage

4Q 2013 through 1Q 2014

Figure 4. Comparing the top 20 countries with spam bot infections and their Windows XP usage, 4Q 2013 through 1Q 2014

* Data compiled from "StatCounter Global Stats: Top Desktop, Tablet and Console OSs Per Country from Oct to Dec 2013" and "StatCounter Global Stats: Top Desktop, Tablet and Console OSs Per Country from Jan to Mar 2014," *StatCounter*, Accessed 14 May 2014.

† "StatCounter Global Stats: Top 7 Desktop, Tablet and Console OSs from Oct 2013 to Mar 2014," *StatCounter*, Accessed 17 April 2014.

Spam bot infections and the end of support for Windows XP

Another interesting insight into this data comes from calculating the percentage of how many computers (or IP addresses) are involved in sending spam. When we compare the number of IPs seen in spam attacks during the last six months with the total number of IPs per country, we get the results shown in Figure 4.

Although each of the countries listed in Figure 4 is the source for less than three percent of the worldwide spam (with the exception of India and Vietnam), the spam bot infection ratio of computers in these countries is alarmingly high. One reason might be that many computers do not use the latest patches or even operating systems. Currently, approximately 18.4 percent of computers worldwide still use Windows XP.[5] But in 16 out of the 20 countries listed in Figure 4, the usage of Windows XP is significantly higher than the worldwide average. In some cases, the usage is more than 30 percent, with Vietnam even higher at 42.4 percent.

On 8 April 2014, Microsoft announced the end of support for the Windows XP operating system.[6] The end-of-support date has been common knowledge for some time and many organizations migrated large user bases to newer versions. However, there are many organizations that are still struggling—or that, by choice, have simply not taken actions—to move off of Windows XP. In addition, certain industries, such as banking, industrial software and healthcare, are struggling with the Windows XP end-of-life announcement. For example, 95 percent of US-based ATMs use Windows XP and could become hot targets for attackers.[7] These organizations may now face challenges in the post-Windows XP-supported world.

From a different perspective, Windows XP usage in many cases can also be correlated with the countries where the highest volume of spam originates. These statistics show that:

- There is widespread evidence of viral spam bot infections.
- Using the most current operating systems and applications, while maintaining and applying the latest security updates and patches, remains the most effective way to protect both end recipients and vulnerable servers against spam.

The return of image spam

Image spam had its heyday in 2006 and 2007. During October 2006 through March 2007, more than 40 percent of all spam contained an image attachment. However, by the summer of 2007, image-spam threats stopped almost completely. There were only two short comebacks:

- In the autumn of 2008, the percentage of spam containing image attachments reached 13.5 percent at the beginning of October (measured on a weekly basis).
- By the end of April 2009, image-based spam accounted for 13 percent of all spam (again, when measured on a weekly basis).

Since April 2009, the percentage of image spam has not exceeded 10 percent. From time to time we have seen image-spam threats, but they have been less than 10 percent (when measured on a weekly basis).

However, in December 2013, image spam made a comeback. As shown in Figure 5, on 5 December, spammers surprised us with a large amount of image spam. This new attack of image-based spam continued until 16 December, with these image-based attacks occurring nearly every day. After a short break, spammers started a massive image-spam attack on 23 December. This attack ran for one month—with another short break between 8 January and 13 January—and stopped on 22 January 2014.

Figure 5 also shows that one month later, on 24 February, another image-spam threat began. But this threat lasted only three days. On these days the volume was only half of the volume we had seen in December and January.

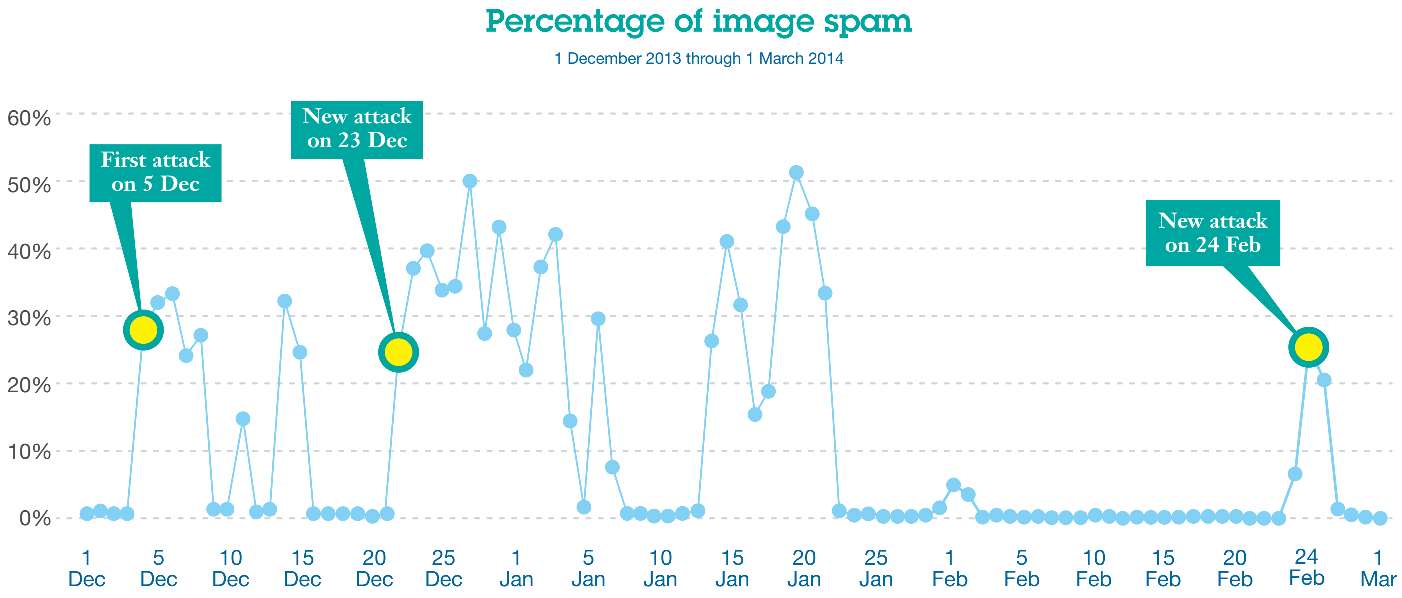


Figure 5. Percentage of image spam, 1 December 2013 through 1 March 2014

Feature	December 2013 through January 2014 attack	February 2014 attack
Advertised products	**Medical products**	**Stocks**
Image features used in both attacks	We observed some differences in how attackers currently use image spam from when the technique first gained popularity in the 2006 through 2007 time period. Originally, attackers seemed to be more careful about avoiding spam-filter detection by slightly modifying the images. Since many spam filters used a file hash to determine if an attachment was associated with spam activity, attackers at that time made a base image seem like a different file by using slight variations such as changing the colors or a few pixels. But in recent attacks, images do not change very often. Spammers use the identical image again and again.	
Image features	Medical products were shown on the images.	Screenshot of text was shown that advertises a particular stock. Within this threat, only two different images were used.
URL features	When clicking on the images within the email, recipients were directed to a website, most often to a website such as [...]doctor[...].ru or [...]medic[...].ru. These URLs did not change that often.	No URLs were used. The spammers provided the stock symbol and expected the recipients to search for this symbol to buy the corresponding stocks.
Random text used in both attacks	Below the image within the email, attackers placed a lot of random text, in many cases from Wikipedia articles. Typically, this text was used to obfuscate spam-content filters such as Bayesian filters.	
Random text	The text was hard to read because it was very faint with white background. It was placed directly below the image.	The text was shown in the email without any obfuscation. But below the image there were many empty lines inserted so that a user had to scroll down to see the random text.

Table 1. Technical details found during image-spam attacks in December 2013 through January 2014 versus February 2014

Table 1 summarizes some of the technical details discerned during these recent attacks.

By comparing these attacks, we have concluded:

- Technically, these recent spam threats are not using any new techniques. The usage of image variations and time span for maintaining spam URLs is actually "old-fashioned." We are not sure why spammers use these older techniques but, perhaps after a five-year absence, they are assuming that spam filters are not prepared for large attacks of image-based spam.
- There are many similarities between these two attacks, suggesting that both attacks may have been initiated by the same spam toolkit.
- Image spam remains an interesting and important issue, as spammers can transport their message exclusively within the image, where content-analysis modules typically cannot extract any information from the text content. This might impact the spam-detection capabilities of spam filters working with text-content detection. Spammers might even ask users to enter a URL from an image (as seen in the past), and this URL could infect the user's computer via a drive-by-download. In this context, these new image-spam threats might be some kind of a test for future image-related spam attacks.

It will be interesting to see whether 2014 is the comeback year for image-based spam.

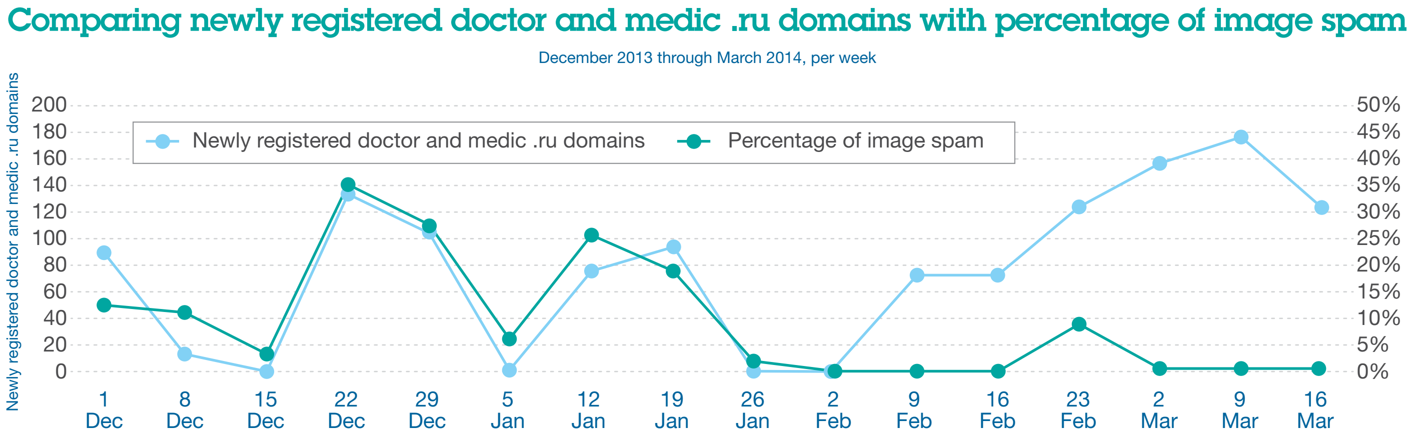


Figure 6. Comparing newly registered doctor and medic .ru domains with the percentage of image spam per week, December 2013 through March 2014

As shown in Figure 6, attackers are using doctor and medic .ru domains in these attacks, which brings up the question of whether spammers are still using the mechanism to register [...] doctor[...].ru or [...]medic[...].ru domains. The answer is yes.

From the beginning of December 2013 through the end of January 2014, the number of newly registered [...]doctor[...].ru or [...]medic[...].ru domains correlated with the percentage of image-based spam. But since the beginning of February 2014, spammers have used these domains for other, non-image based types of spam.

Interestingly, spammers using image-based spam still use these domains for relatively long periods of time—sometimes for several hours and other times for up to a day or more. This life span did not change within the last four months observed. This is considered a long period for URLs used in spam. In contrast, most spammers use their domains only for a few hours or even for a few minutes, because many spam filters check for the URLs used within emails and block them if they were seen in spam previously. Because the spammers own these domains, they can easily measure how long users click on these URLs. Thus, even if a domain is in use for one day or more, there still seem to be spam filters that do not catch this spam or there still remain users without a spam filter in use.

Top five considerations when remote incident response becomes extremely remote

Security breaches can happen almost anywhere. Discover how to prepare your IT staff for remote incident response.

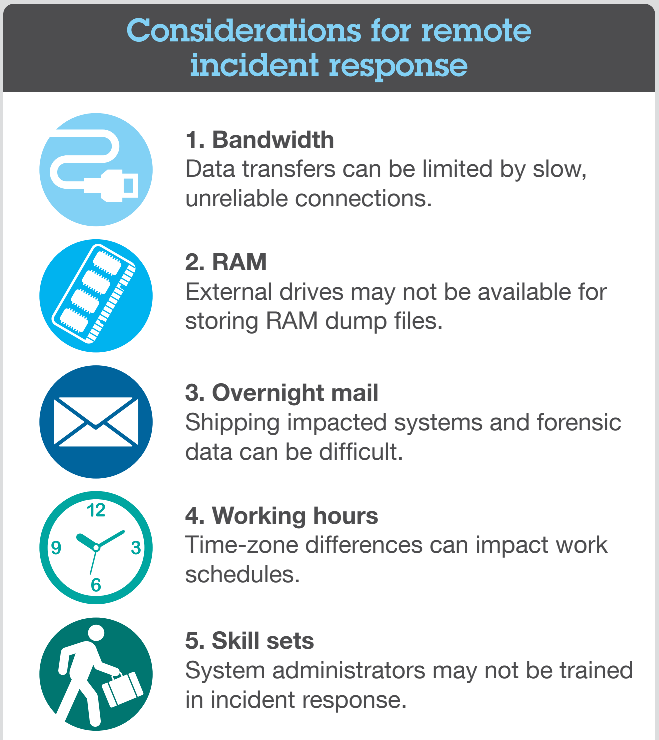
Incident response used to entail flying to a client site for each and every engagement. And incident responders would be overjoyed when a call was received from a client site located on a warm tropical island.

Recently, the paradigm has shifted. Driven by stiffer regulations on personal data and the importance placed on security breaches, many organizations need answers faster and more efficiently than ever before. In some states, organizations must notify regulatory agencies in mere days after a breach is not just confirmed but only suspected. As a result, incident responders, such as members of the IBM Global Technology Services - Emergency Response Services (ERS) team, have developed methodologies and use triage tools to help accelerate incident response. They use these tools and methodologies to quickly pull relevant artifacts such as RAM and event logs from compromised systems and send the artifacts to remote analysts who can quickly start the analysis.

But what happens when the information system suspected to be part of a breach is located in an area of the world that lacks the infrastructure to support incident response efforts? For example, what if there's not enough Internet bandwidth to transfer key artifacts to incident response analysts (a common technique to enable a quick assessment)? The information system may also be located in a remote underdeveloped country that causes travel to be impractical and, furthermore, may also lack skilled IT professionals.

This is exactly the situation increasingly faced by the IBM ERS team. As more and more companies expand operations outside of traditional markets, extremely remote incident response engagements occur on a more frequent basis. Responding to incidents in remote countries or infrastructure-deficient areas requires a unique game plan.

This section of the report looks at the top five considerations when confronting incident response situations where the impacted information systems are extremely remote. Some of the considerations are technical while others are managerial in nature. All are equally valuable.



Considerations for remote incident response

1. Bandwidth
Data transfers can be limited by slow, unreliable connections.

2. RAM
External drives may not be available for storing RAM dump files.

3. Overnight mail
Shipping impacted systems and forensic data can be difficult.

4. Working hours
Time-zone differences can impact work schedules.

5. Skill sets
System administrators may not be trained in incident response.

Figure 7. The top five considerations for remote incident response by the IBM Global Technology Services - Emergency Response Services (ERS) team

1. Bandwidth is king

Because not all security incidents occur with information systems located in high-bandwidth areas such as a data center or an industrialized country, incident responders may be working with slow and unreliable network connections. This situation may be detrimental to incident response efforts. Typically, when the ERS team becomes involved in a security incident, ERS analysts begin work as soon as select files—such as logs, malware samples, RAM and other artifacts—are transferred. Although transferring several gigabytes of files is potentially slow, it is perfectly feasible and allows ERS to start analysis faster than flying analysts to a remote information system location or shipping hard drives.

When bandwidth becomes an issue, incident responders are forced to eliminate several larger and potentially valuable information system artifacts in favor of smaller artifacts. Eliminating a set of information system artifacts can increase the time to provide findings, cause less certainty in these findings and increase the overall cost of the response. Bandwidth restrictions also limit the ability to use a jumpbox or bastion host, a tried-and-true method of conducting analysis, to connect to extremely remote systems.

What is a bastion server?

A bastion host[9] is a special-purpose computer that is fully exposed to attacks. The computer sits on the public side of the demilitarized zone (DMZ), unprotected by a firewall or filtering router. Due to this exposure, bastion hosts are typically configured to fulfill a specific role—such as, acting as a proxy server—and all unnecessary services, protocols, programs and network ports are disabled or removed. Bastion hosts are also hardened to help control access from intruders and limit potential methods of attack.

2. RAM may be off limits

Undoubtedly, one of the most valuable artifacts to an incident responder is the RAM on a compromised system. The RAM of a modern PC system is considered the most useful place to find comprehensive, evidentiary data, and there is little else that matches or surpasses its value in that respect. RAM can contain a treasure trove of information, including details about open ports, network connections, running processes and so on.

Why is RAM potentially off limits? In the IBM ERS team's experience, extremely remote engagements present two main challenges. During several extremely remote engagements, ERS has had a multitude of problems collecting RAM. First, the RAM file size, especially on high-end servers, may be very large—often in excess of 8 GB, even after compression. Internet bandwidth and reliability issues are likely to cause large-file transfers to be unacceptably slow or to fail. Second, when collecting RAM, it's necessary to dump it to an external location such as a USB device. ERS has encountered several incidents in which USB devices were not available for storing a RAM dump file. If a USB device is not immediately available, it will almost certainly be difficult to find an electronics retailer nearby—for example, when the compromised system resides on an oil platform off the coast of Nigeria or in rural Uganda.

While it may not be possible to access the entire RAM dump file, it may be possible to access (or have a system administrator access) data held within the RAM. Logged-in users, open files, scheduled tasks and other information may still be gathered, albeit using rudimentary and less than efficient techniques. Regardless of whether RAM is completely off limits or the incident responder is using less than efficient techniques, the organization should be prepared for challenges when gathering volatile data.

Working within the constraints of minimal bandwidth and an inability to gain access to a RAM dump doesn’t make incident response impossible. However, incident response teams unaccustomed to working within such boundaries must be prepared. Developing methodologies and training to expect these hurdles must be standard for organizations with information systems located in bandwidth-deficient locations or where a RAM dump may not be possible. Otherwise, these challenges may become crippling obstacles.

3. Overnight mail may not exist

The IBM ERS team’s domestic clients frequently choose to send impacted systems or collected data via overnight mail to ERS incident response analysts. Sending forensic images, collected RAM, log files or even entire systems may take as few as 12 hours via an overnight carrier. In addition, when contemplating transfers of data between countries—whether physically or “over the wire”—it is important to understand any regulations that may impede data transfer. Obviously, when there is an urgent need to provide findings as soon as possible, overnight mail may be a good option.

But what if your information systems and data are in a location that does not have overnight mail? Continuing with the oil platform example, it may not be logistically feasible to ship a system or select files from such a location. Alternatively, even if the information system resides in a country with service via UPS or FedEx, it’s not uncommon for shipments of potentially high-value items such as computers to be held in customs for days. When answers are needed and time is short, delays like this can interfere with a swift and effective response effort.

4. Working hours may impact schedules

Typically, during incident response engagements, ERS provides requests to points of contact (such as system administrators) during the work day as analysis progresses. It’s a fluid process and requests are usually fulfilled with urgency due to the severity of most security compromises.

This may not be the case when analyzing potential security compromises for organizations located in extremely remote areas. Time zone differences may cause your points of contact to have working hours several hours before or after your local working hours, with little overlap. This constraint may require the incident response team to either adjust their work schedules or provide aggregate requests. Your analysts will need to carefully consider what items are needed to progress with the analysis, since a follow-up request may not be addressed for another 24 hours.

5. Skill sets may be lacking

The incident responders at ERS are usually fortunate to work with highly skilled system administrators when responding to a security compromise. In some cases, this may be the difference between an incident that lasts a few days and an incident that takes weeks to resolve.

In most of the engagements ERS has worked on in extremely remote areas, however, skilled system administrators or even points of contact with basic technical skill sets are often lacking. When working in extremely remote settings, incident response experts must be aware of this limitation and help ensure that all instructions, questions and other communications are extremely specific, not open to interpretation and not dependent on a high degree of skill.

One way to help minimize the problems posed by zone differences and a lack of technical skill sets is to ensure that the organization has incident response subject matter experts (SMEs) in various geographies. The SMEs don't have to be incident response gurus. Rather, having a minimally trained system administrator knowledgeable with a baseline incident response skill set can help ensure that SME support is at least somewhat available where your incident is occurring. Having a local SME knowledgeable in basic first-responder, data-preservation and investigatory methodologies may mean the difference between an incident that lingers for weeks and one that is resolved in days.

To recap, performing incident response in extremely remote areas is possible; however, the incident responders must be prepared to adjust their operational procedures, develop different tactics and work with a limited set of data. Understanding limitations and making adjustments at the onset of the engagement can help ensure a successful response despite unwelcome obstacles.

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.
- Trusteer,[8] an IBM company, 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 Trusteer to protect their web applications, computers and mobile devices from online threats (such as advanced malware and phishing attacks). With a dedicated, advanced research team, Trusteer's unique and real-time intelligence enables its cloud-based platform to rapidly adapt to emerging threats.
- 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 operates 10 security operations centers that provide managed security services, tools and expertise to clients around the world, on a 24x7 basis. It is responsible for monitoring exploits related to endpoints, servers (including web servers), applications and general network infrastructure. Its security experts track exploits, attacks and incidents for thousands of clients.
- IBM Professional Security Services delivers enterprise-wide security assessment, design and deployment services to help create an effective security intelligence strategy and 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 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.

Contributors

Producing the IBM X-Force Threat Intelligence Quarterly 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.

For more information

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

Contributor	Title
Andrew Cranke	Senior Application Security Consultant, IBM Hosted Application Security Management
Anik Campeau	Application Security Consultant, IBM Hosted Application Security Management
Diana Kelley	Application Security Strategist, IBM Security AppScan
Dr. Jens Thamm	Database Manager, IBM X-Force Content Security
John Adams	Senior Incident Response Analyst, IBM Global Technology Services - Emergency Response Services
Leslie Horacek	Manager, IBM X-Force Threat Response
Marc Noske	Database Administrator, IBM X-Force Content Security
Mark Wallis	Senior Information Developer, IBM Security Systems
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force and Security Intelligence
Ralf Iffert	Manager, IBM X-Force Content Security
Rob Lelewski	Engagement Lead, IBM Global Technology Services - Emergency Response Services
Robert Freeman	Manager, IBM X-Force Advanced Research
Thomas Millar	Senior Incident Response Analyst, IBM Global Technology Services - Emergency Response Services

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2014

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

[1] Chris Poulin, "What to Do to Protect against Heartbleed OpenSSL Vulnerability," *IBM Security Intelligence Blog*, 10 April 2014. http://securityintelligence.com/heartbleed-openssl-vulnerability-what-to-do-protect/

[2] Roee Hay, "New Vulnerabilities in Firefrox for Android: Overtaking Firefox Profiles," *IBM Security Intelligence Blog*, 26 March 2014. http://securityintelligence.com/vulnerabilities-firefox-android-overtaking-firefox-profiles/

[3] Roee Hay, "A New Vulnerability in the Android Framework: Fragment Injection," *IBM Security Intelligence Blog*, 10 December 2013. http://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/

[4] "OWASP Top 10 for 2013," *OWASP*, 12 June 2013. https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

[5] "StatCounter Global Stats: Top 7 Desktop, Tablet and Console OSs from Oct 2013 to Mar 2014," *StatCounter*, Accessed 17 April 2014. http://gs.statcounter.com/#os-ww-monthly-201310-201403-bar

[6] Enterprise Customers: Support for Windows XP has ended," *Microsoft*, April 2014. https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

[7] Jose Pagliery, "95% of bank ATMs face end of security support," *CNNMoney*, 4 March 2014. http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/?iid=EL

[8] Trusteer, Ltd. was acquired by IBM in September of 2013.

[9] Kurt Dillard, "Intrusion Detection FAQ: What is a bastion host?" *The SANS Institute*, Accessed 13 May 2014. http://www.sans.org/security-resources/idfaq/bastion.php

Please Recycle