

IBM X-Force Threat Intelligence Quarterly 1Q 2014

Explore the latest security trends—from malware delivery to mobile device risks—based on 2013 year-end data and ongoing research



Contents

- 2 What's new
- 3 Executive overview
- 4 Roundup of 2013 security incidents
- 9 Malware: Delivered via application exploits
- 12 Mobile threats: Perception versus reality
- 14 Vulnerability and exploit disclosures in 2013
- 18 About IBM X-Force
- 18 IBM Security collaboration
- 19 Contributors
- 19 For more information

What's new

It's time again for the latest news from the IBM® X-Force® research and development team, and we would like to note some exciting changes we've made to the [IBM X-Force Trend and Risk Report](#) for 2014.

Quarterly format

IBM previously issued the report twice yearly in a long-form format. Starting with the first quarter of 2014, and going forward, IBM will issue the report in a shorter, more nimble quarterly format. With the new publication schedule comes a new name, "IBM X-Force Threat Intelligence Quarterly," as well as updates to style and format.

Team expansion: Introducing Trusteer

With this edition of the report, we are introducing data collected from our new colleagues at Trusteer,¹ an IBM company since September, 2013.

As a leading provider of software that helps protect organizations against fraud and advanced security threats, Trusteer offers products that are currently used by more than 100 million users across more than 350 financial institutions worldwide. Trusteer technology and research focuses on preventing the root cause of most fraud: malware and phishing attacks that compromise customers' computers and mobile devices.

We are pleased to welcome the Trusteer team to IBM. The combined knowledge and expertise of researchers between X-Force and Trusteer will continue to enhance future reports.

Executive overview

Since late 2010, X-Force has been reporting the yearly increases of security breaches across all industries. In the second half of 2013, the advancement of these attacks continued to rise. Within this report, we'll explain how more than half a billion records of personally identifiable information (PII) such as names, emails, credit card numbers and passwords were leaked in 2013—and how these security incidents show no signs of stopping.

We asked the new X-Force malware researchers (Trusteer) to report their most significant finding at the end of 2013, and they responded with an update on how attackers continue to weaponize content with the objective of injecting malware onto a user's computer. They also reported that Oracle Java vulnerabilities continue to be a top point of entry for many of these malware attacks.

Mobile security continues to be a dynamic area of change for many organizations. We will discuss how the actual risks associated with the increasing use of mobile devices in the workplace are not as straightforward as many perceive—and as the media may have you believe—and provide insight and recommendations on how organizations can better protect their mobile environments.

Finally, we'll close the report by discussing how 2013 ended with public vulnerabilities inching just above the year-end final numbers for 2012. And even though overall vulnerabilities increased during the past year, we have also seen some declining trends across important reporting areas.



Roundup of 2013 security incidents

With privacy concerns at an all-time high—thanks in part to heavy media coverage of several large consumer attacks—security incidents have become a mainstream conversation, from the boardroom to the living room.

Over the years that the X-Force team has been tracking security incidents, the overall attack tactics and techniques have not changed significantly. However, there has been a marked increase in volume across all areas. The number of overall incidents has increased, the amount of traffic used in distributed-denial-of-service (DDoS) attacks has multiplied and the number of leaked records has been steadily rising. As you can see in Figure 1, of security incidents analyzed by X-Force, the rate of growth, frequency and size of possible financial impact have been steadily on the rise since 2011.

In 2013, attackers continued to use tried and true methods of extracting data. As shown in Figure 2, they successfully exploited vulnerable web applications with attacks such as SQL

injection (SQLi) and cross-site scripting (XSS), as well as utilized a mix of sophisticated and generally accessible toolkits to gain critical points of entry. These tools—which target endpoints through employee social engineering, spear phishing and other forms of malware installation—have created a major challenge for organizations tasked with protecting sensitive data.

Figure 2 illustrates a sampling of security incidents from 2013. The larger circles in the second half of the end of the year represent several major breaches with more than half a billion pieces of PII and credit card numbers leaked. The figure also illustrates the possible financial impact of a data breach in terms of fines, loss of intellectual property, loss of customer trust and loss of capital that an organization of any size might face.

A historical look at security incidents by attack type, time and impact, 2011 to 2013

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

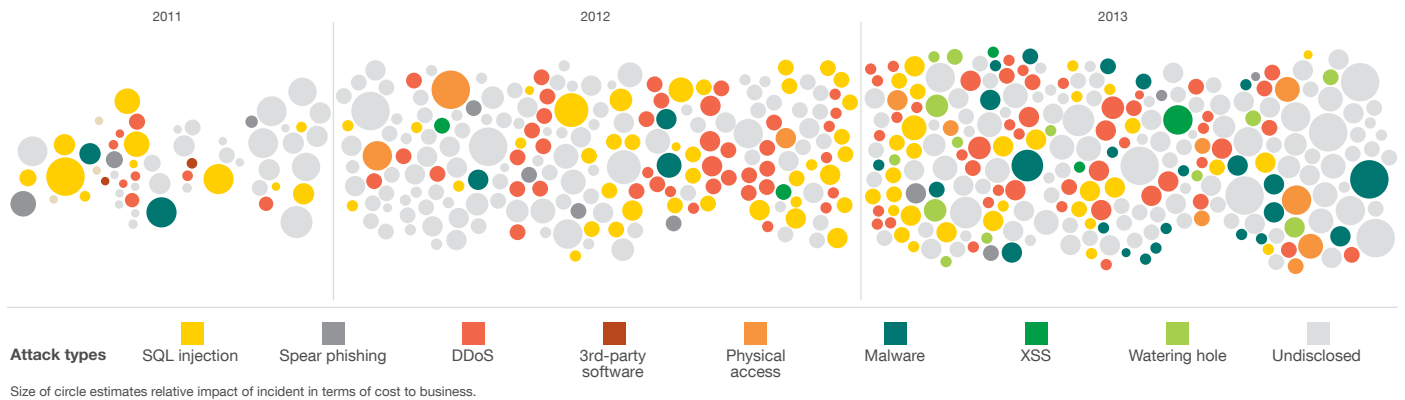
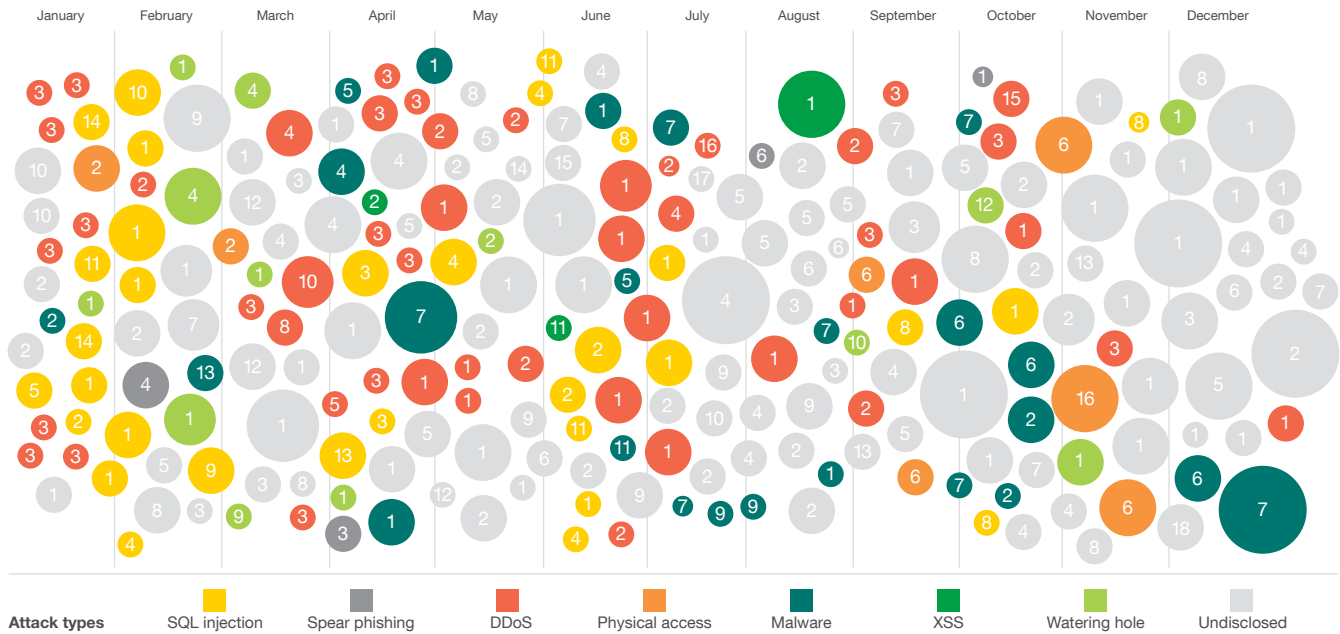


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Sampling of 2013 security incidents by attack type, time and impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

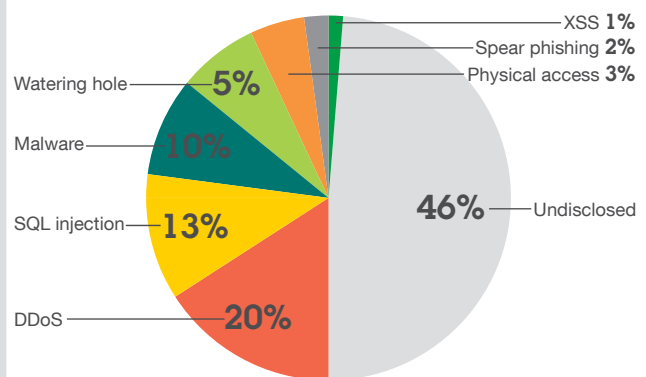


Size of circle estimates relative impact of incident in terms of cost to business.

Most-commonly attacked industries

- 28%** Computer Services (1)
- 15%** Government (2)
- 12%** Financial Markets (3)
- 9%** Media & Entertainment (4)
- 7%** Education (5)
- 5%** Healthcare (6), Retail (7), Telecommunications (8)
- 3%** Consumer Products (9)
- 2%** Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
- 1%** Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
- <1%** Aerospace & Defense (17), Insurance (18)

Most-common attack types



What is the cost of a data breach?

Data breaches have financial impact in terms of

finances, loss of intellectual property, loss of customer trust, loss of capital

In 2013, [the Ponemon Institute estimated](#) \$136 per lost record of data based on real-world data.*

* "2013 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, May 2013.

For example:

- A major retailer with millions of leaked credit cards could be looking at more than \$1 billion in fines and other associated costs.
- A university that leaked 40,000 records could be looking at up to \$544,000 in losses.

Figure 2. Sampling of 2013 security incidents by attack type, time and impact

As a notable example, much attention has been given to the retail industry's use of credit card-processing systems deployed on e-commerce websites and point-of-sale (POS) devices, many of which run embedded or older versions of Microsoft Windows, making them susceptible to exploitation. These credit card-processing systems are a lucrative data-gathering target for attackers who utilize optimized malware to archive credit card numbers, magnetic stripe data and other sensitive information.

Tools targeting these endpoints generally work via some type of "RAM scraper" technology, which can be used to read information directly from memory during the split second between the encrypted data arriving on the system and clear text validation of the card information. Once data has been gathered it can be sent to a compromised server within the enterprise, at which point attackers can manually exfiltrate this data outside of the network. Several retail industry incidents in 2013 were disclosed as being perpetrated by this optimized malware.

Additionally, of the sampling of security incidents reported by X-Force in 2013, in terms of the country where the attack target was located, more than three quarters of them occurred in the United States.

Central strategic targets

In the [2013 first-half report](#), X-Force identified that attackers are increasingly going after central strategic targets as a means to optimize their efforts and increase their return on exploit. This trend continued into the second half of the year. Notable examples include vulnerabilities in web frameworks, such as Ruby on Rails and Apache Struts, which provided attackers a way to compromise thousands of websites. A vulnerability in the popular forum software vBulletin led to a breach of more than 35,000 websites.² In addition, some of those affected sites had very large user bases with more than one million leaked records.³



Sampling of 2013 security incidents by country








77.7%		United States
4.5%		Australia
3.9%		United Kingdom
3.9%		Taiwan
3.9%		Japan
3.4%		Netherlands
2.8%		Germany

Figure 3. Sampling of 2013 security incidents by country

DNS providers

DNS providers were targeted throughout 2013 in several ways. Attackers seeking to shut down access were able to carry out DDoS attacks on DNS providers, which in turn caused downtime for customers using those services for their DNS infrastructure. In some cases, attackers were able to target companies with otherwise strong security in place by hijacking



DNS requests at the DNS provider. This allowed them to redirect traffic going to the legitimate site. From there, the attackers had several options: they could do something fairly benign such as display a defaced version of the website; they could do something more insidious like detect user cookies as a man-in-the-middle-type attack;⁴ or they could expose endpoints to malware before they reached the host site. These types of attacks affected several high-profile social media and news sites.

Social media

Social media accounts with a large number of followers provided another type of central strategic target. Throughout 2013, attackers successfully gained access to accounts of prominent celebrities, media outlets, tech companies and individual persons of interest. Web services that interact with social media to schedule posts and carry out other tasks also proved to be worthwhile targets because of the model of trust under which they operate. Usually these services are authenticated to the user's profile via an application programming interface (API), giving attackers the ability to post feed updates from thousands of compromised accounts. This was the case with a popular social-media management service,⁵ in which attackers leveraged its user base of more than one million accounts to send out weight-loss spam to its followers.

Virtual currency

Bitcoin technology was a hot topic in 2013, given the exponential increase in valuation of its virtual currency. As expected, this motivated attackers to find new opportunities to benefit. There were several types of attacks targeted against Bitcoin websites, including denial of service (DoS) against exchanges in which users buy and sell Bitcoins. These types of attacks can destabilize the currency and can also be used as a cover to steal from digital wallets. Virtual currency stored in digital wallets is at risk not only from theft, but from corruption of digital media (hard drive crashes) and lost credentials such as encryption passwords. In August, it was reported that bitcoins were stolen by attackers who crafted custom malware that exploited a vulnerability in the operating system (OS) random number generator used by certain Bitcoin wallet applications running on the Google Android platform.⁶

Evolution of attack types

Another way in which attackers have been successful throughout 2013 has been through the use of watering hole attacks. These types of attacks involve an attacker compromising special interest websites and injecting visitors with malware through the exploitation of browser or browser plug-in vulnerabilities. Watering hole attacks have proven effective at reaching groups of users who frequent certain types of websites. Notable examples include PHP.net⁷—a website that provides reference information for web developers using the PHP open-source website scripting language—and a series of compromised websites in the Energy & Utilities and Chemicals & Petroleum industries.⁸

Similar to watering hole attacks, *malvertising* is gaining traction.⁹ Malvertising occurs when attackers target advertising networks by injecting ads with malicious exploits that lead to drive-by downloads. These malicious ads can then expose

vulnerable users across the many websites displaying the content arriving from the advertising networks. The Trusteer research team recently blogged an in-depth article about malvertising¹⁰ whereby a recent Java zero-day vulnerability (CVE-2013-0422) was being exploited in the wild. That specific campaign was leveraging Blackhole exploit toolkits that utilize this vulnerability to compromise user endpoints.

All of these efforts enable attackers to focus on a smaller number of critical targets, which can then provide access to thousands more.

Despite the hype and mass media coverage of the volume and scope of today's security breaches, businesses and users alike can still go a long way toward protecting themselves by applying basic security best practices around passwords, network segmentation and secure software development.



Malware: Delivered via application exploits

It has long been known that attackers exploit application vulnerabilities to download malware onto endpoints of unsuspecting users. An analysis of X-Force threat intelligence data during the month of December, 2013 reveals that out of a survey of more than one million Trusteer banking and enterprise customers, the most targeted applications were Oracle Java, Adobe Reader and popular browsers.

Exploitation of application vulnerabilities

from survey of 1 million Trusteer customers, December 2013

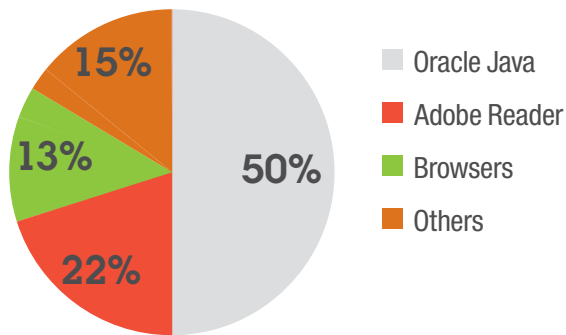


Figure 4. Exploitation of application vulnerabilities

It's not surprising that these are the most targeted user applications. After all, these are all applications found on most user endpoints; they all have vulnerabilities that can be exploited to deliver malware to users' machines; and all of these applications can receive and process external content. This means that attackers can create "weaponized" content: files or documents that contain exploits that take advantage of vulnerabilities in the application. Attackers use spear-phishing messages to draw users to websites that contain hidden malicious Java applets (exploit sites). Weaponized content is typically delivered to users via spear-phishing messages or exploit sites. Once the user opens the file or document using a vulnerable application, the exploit causes a chain of events that ends with the delivery of malware to the user's machine and subsequent infection—all without the user's awareness.

Java: A powerful yet vulnerable application

Java is a widely deployed high-risk application that exposes organizations to advanced attacks. The number of Java vulnerabilities has continued to rise over the years, and 2013 was no exception. The number of reported Java vulnerabilities jumped significantly between 2012 and 2013, more than tripling.

Research has indicated that with this increase in vulnerabilities, there has been a significant increase in Java exploits as well, as evidenced by half of the observed sample customers affected. This was a result of the discoveries of new zero-day vulnerabilities and the introduction of exploits into popular exploit toolkits. In past [X-Force Trend and Risk reports](#), we discussed how exploit toolkits such as *Blackhole* and *Cool* were found to be using unpatched Java vulnerabilities to escape the Java sandbox and install malware on victims' machines. Through the end of 2013, this popular trend continued.

Java vulnerability disclosures growth by year, 2010 to 2013

originating in either the core Oracle Java or in IBM Java SDKs

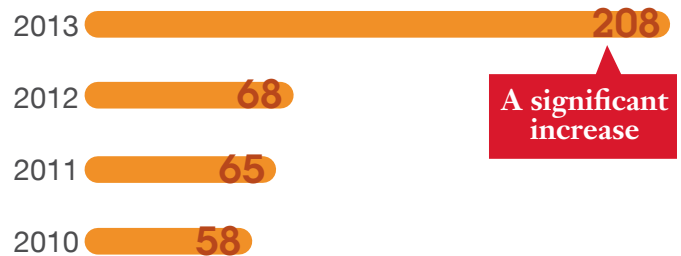


Figure 5. Java vulnerability disclosures growth by year, 2010 to 2013

Use of Java may expose organizations to advanced attacks due to numerous vulnerabilities in the application that can be exploited to deliver malware and compromise user machines. Once on an endpoint, it is extremely difficult to prevent the malicious execution of Java malware. Nevertheless, Java's powerful capabilities continue to make it a popular platform for developing enterprise applications. Today, it can be found in nearly every enterprise environment, and because organizations are highly dependent on Java applications, it is not practical to remove it from these environments (as some recommend). Since organizations can't eliminate Java from their environments, it's not surprising that attackers use malicious Java code to infiltrate them.

Native versus applicative Java exploits: With applicative exploits in the lead

Java vulnerabilities can allow two different types of exploits: native and applicative. Most of the exploits that target vulnerabilities in end-user applications, like browsers or Microsoft Office applications, execute natively. A native exploit results in running native shell code. This type of exploit is accomplished by techniques that include buffer overflow, use-after-free and more.

A number of native OS-level protections help protect organizations from native exploits. These protections include ASLR (address space layout randomization) and DEP (Data Execution Prevention), as well as general security protections that include SEHOP (Structured Exception Handler Overwrite Protection), heap-spraying protection (such as NOZZLE), Stack Pivoting protection, and Export Address Table Access Filtering (EAF).

However, taking a closer look at Java exploits reveals that the more common type of Java exploit is an applicative exploit (in this example, Java Layer Exploits). Unlike native exploits, which target the application memory, the applicative exploits aim to break the Java security manager affecting Java applications that run within a virtual machine (JVM).

Total Oracle Java exploits

2012 to 2013

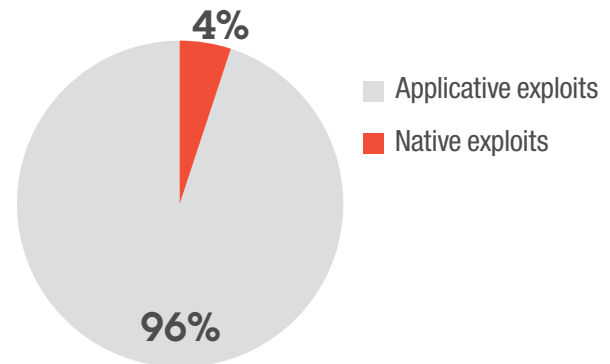


Figure 6. Total Oracle Java exploits, 2012 to 2013

The Java security manager is a class that manages the external boundary of the JVM, controlling how Java applet code executing within the JVM can interact with resources outside the JVM. Applicative exploits abuse vulnerabilities that break the Java security model. Once the security model is broken, nothing prevents the Java applet from running critical operations that should not be performed.

Java applicative exploits are more difficult to defend against because they allow the applet to gain unrestricted privileges—which makes malicious activities seem legitimate at the OS level. This means that, unlike native exploits, Java applicative exploits completely bypass native OS-level protections. Plus, Java applicative exploits don't generate buffer overflow, and hence are not prevented by methods such as DEP, ASLR, SEHOP and others.

Recommendations

Because organizations can't eliminate Java from their environments, it is important they secure Java applications to avoid the execution of malicious Java code. However, the native Java protections available today are very limited in their capabilities, especially against zero-day threats.

To help prevent Java exploits and malware-based infiltrations, it is important to restrict execution to only known and trusted Java files. Organizations that struggle to manage and maintain

a complete list of all known and trusted files should, at a minimum, restrict execution to files that have been signed by trusted vendors or downloaded from trusted domains. Otherwise, untrusted Java files should not be allowed to freely execute within the enterprise environment. Restricting untrusted Java files allows organizations to more safely run their businesses by decreasing their risk of exposure to high-risk files.



Mobile threats: Perception versus reality

Despite executive worries that bring-your-own-device (BYOD) programs risk exposing enterprise data through loss or theft of mobile devices,¹¹ we haven't seen significant incidents in public disclosures to corroborate this concern. While internet searches yield many articles and blogs portending the dangers of BYOD programs, the actual incidents used to back up these dire warnings typically involve laptops, USB drives or secure digital (SD) cards—not smartphones or tablet computers.

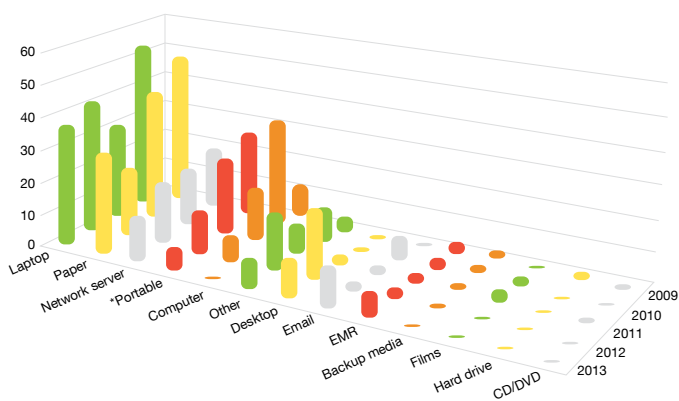
Although many of us treat our smartphones and tablets like digital appendages (some surveys find that almost half of users keep smartphones at their bedsides for fear of missing calls, text messages or social networking updates while they sleep¹²), we still sometimes forget them at restaurants, leave them in cabs, or have them stolen (sometimes called *apple picking*). These orphaned devices, if used for business, may contain electronic protected health information (ePHI), PII and/or intellectual property belonging to the organization, and this data could be compromised.

To clarify, for the purposes of this report, when we refer to mobile devices and the new threats they pose, we have limited our scope to smartphones and tablets. We have excluded company-owned laptops because they have been staple business tools for decades and, because they're based on general-purpose OSs like Windows, Apple OS X and Linux, they pose different challenges to security than embedded OSs like Apple iOS and Android. We also exclude USB drives, SD cards, external disks, backup tapes and the like, because while they're technically mobile, they're simply storage media. As with laptops, they're not a new technology or threat; organizations have had to manage data exfiltration on mobile storage devices for years.

The facts

In order to validate the lack of incidents involving exposure of sensitive data on mobile devices, we chose a sample data set to analyze: public disclosures tracked by the Office for Civil Rights (OCR) at the US Department of Health and Human Services.¹³ X-Force research uncovered no reported incidents of ePHI being lost or stolen from mobile devices. We found that laptops and paper are most often involved in such incidents, with USB drives and theft from servers (in some cases, the server itself was stolen) tied for third place.¹³

Public disclosures of ePHI by media type 2009 to 2013



* All storage media, no smartphones or tablets

Figure 7. Public disclosures of ePHI by media type, 2009 to 2013

Generally, our research shows that enterprise applications that enable access to organizational data via mobile devices don't store significant amounts of records on mobile devices. Because of the need for ubiquitous access, mobile devices are untethered from the enterprise and provide the user interface—but most data is stored in the cloud. Mobile apps generally connect to data stores through publicly accessible portals and work by transaction, interacting with one record at a time, or small batches cached for performance.

That's not to say that sensitive enterprise data doesn't find its way onto mobile devices. One notable repository is email, which many users treat as an alternate file system for sharing and storing anything and everything, from correspondence with family members to negotiations for corporate mergers. Also, some mobile devices can be used as mass storage devices, similar to USB drives.

Yet, the lack of publicly disclosed evidence of a large-scale breach involving mobile devices is not proof that the threat is not real. Let's not forget that many enterprises have been resistant to moving enterprise data onto mobile devices out of fear.

So what is the actual threat, and how wide is the exposed aperture?

The real threat

The bottom line is that while some organizational information may be present on mobile devices, we found that the biggest risk to the enterprise isn't the data contained on these devices—it's the credentials.

It's more efficient for attackers to directly attack the portal that the mobile application connects to and gain access to the entire enterprise data repository, rather than "pick the pockets" of a multitude of mobile devices. Often all that's needed is a user name and password, which can be stolen from a single mobile device using a keystroke logger, redirecting access to the portal through an intermediate site where credentials are captured, or seizing a digital wallet and cracking it offline.

Mobile devices also contain a trove of personal information, which can allow for further social engineering to mount new or deeper attacks into the enterprise.

The other major threat on mobile devices is applications that have been cracked and redistributed through rogue app stores. Arxan, an IBM Business Partner, found that of the top 100 paid applications on Android, 100 percent of them have hacked variants in the wild. The story on iOS is slightly better, with just over 50 percent having rogue variants.¹⁴ And as we pointed out in the [X-Force 2013 Mid-Year Trend & Risk Report](#), mobile

now comprises four percent of all vulnerabilities. The threats are out there and already resident on hundreds of thousands of mobile devices; just because we haven't seen significant breaches of enterprise data from smartphones and tablets until now, doesn't mean that the future will remain as bucolic.

Recommendations

While mobile devices can certainly pose new threats to enterprise data, these threats may be different than what you expected. It's important to understand the likely avenues of attack and protect against them, instead of viewing the whole mobility issue as a general threat. Specificity counts in security.

Mobile has caused a renaissance of new thinking in security: sandboxing, containerization and trusted transactions are all emerging technologies that promise to provide enhanced protection and open up the willingness of security and IT executives to further enable mobile applications in the workforce.

A viable strategy for protecting mobile devices has three key components:

- Protect the device—Use technologies such as Mobile Device Management (MDM) and Enterprise Mobility Management (EMM)
- Protect the application—Separate personal and employee data with containerization, sandboxing and application-level security
- Protect transactions—Not all mobile interactions are with applications, and not everyone in your ecosystem will be part of your MDM or EMM framework, so it is important to ensure that transactions with customers, partners and temporary workers can also be protected from rooted and jailbroken devices, fraudsters, and mobile malware

In the final analysis, the X-Force team believes these findings support our prediction in the [2012 X-Force Trend and Risk Report](#) that mobile computing devices should be more secure than traditional computing devices by the end of 2014.

Vulnerability and exploit disclosures in 2013

X-Force has been documenting public disclosures of security vulnerabilities since 1997. Seventeen years later, we house a database of information on more than 78,000 vulnerabilities. Countless hours are put into researching application vulnerabilities and threats as well as scouring the internet, researching the data for the X-Force vulnerability database.

Since 2006, and our first decline in vulnerability disclosures in 2007, we have seen the total number of vulnerabilities go up and down every other year. However, at the end of 2013 we

observe the first year in which these cyclical totals do not alternate between the higher and lower annual sequence seen over the past seven years.

As a percentage of overall disclosures, the number of web application vulnerabilities fell sharply compared to what we observed in 2012.

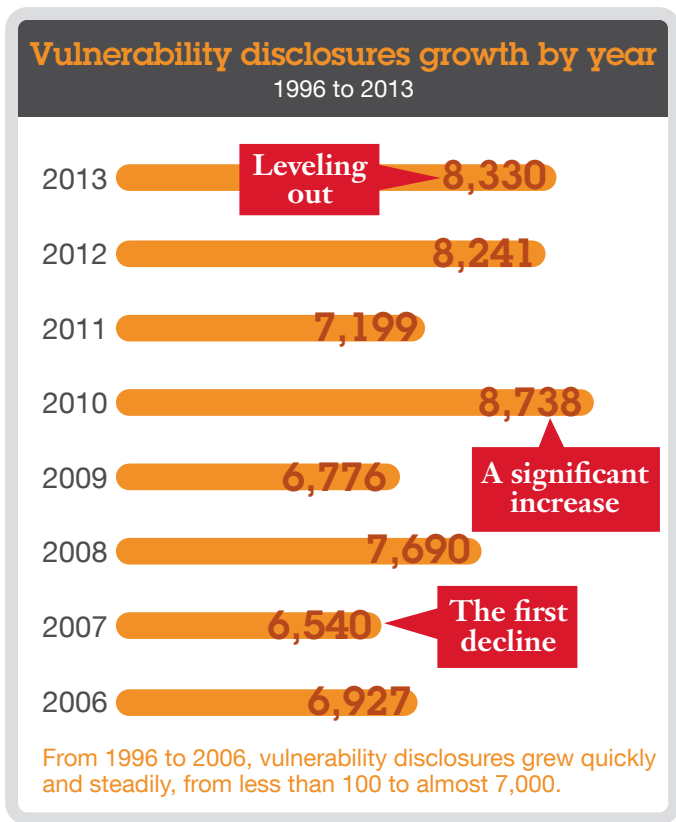


Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

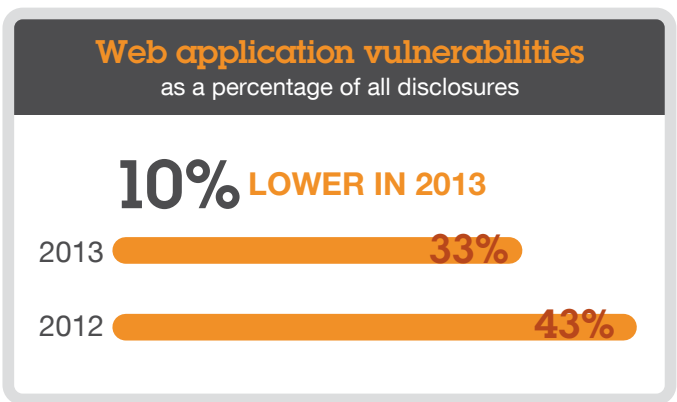


Figure 9. Web application vulnerabilities as a percentage of all disclosures, 2012 to 2013

Unpatched vulnerabilities

The total amount of unpatched vulnerabilities recorded **dropped by 15%** in 2013.

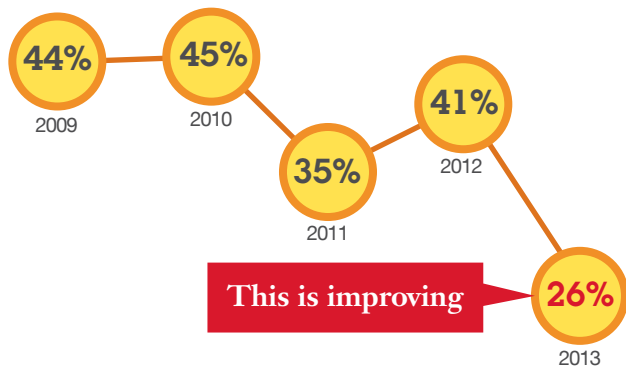


Figure 10. Vendor patch rates of publicly disclosed vulnerabilities, 2009 to 2013

In addition, vendor patch rates of publicly disclosed vulnerabilities have reached some of the highest rates we've seen since X-Force began tracking this data. In 2013, we found that only 26 percent of publicly disclosed vulnerabilities remain unpatched—this shows improvement!

When looking across web application vulnerabilities by attack technique, we found significant drops in both XSS and SQL injection.

The declines in vulnerabilities demonstrated at the end of 2013 in both XSS and SQL injection, shown in Figure 11, could indicate that developers are doing a better job at writing secure web applications, or possibly that traditional targets like content management systems (CMSs) and plug-ins are maturing as older vulnerabilities have been patched. As noted, XSS and SQL injection exploitation continue to be observed in high numbers, indicating there are still legacy systems or other unpatched web applications that remain vulnerable. This is expected, considering there are many thousands of blogs and other websites run by individuals who may not have the skills or awareness to update to later versions of their platform or framework.

Web application vulnerabilities by attack technique

as percentage of total disclosures, 2009 to 2013

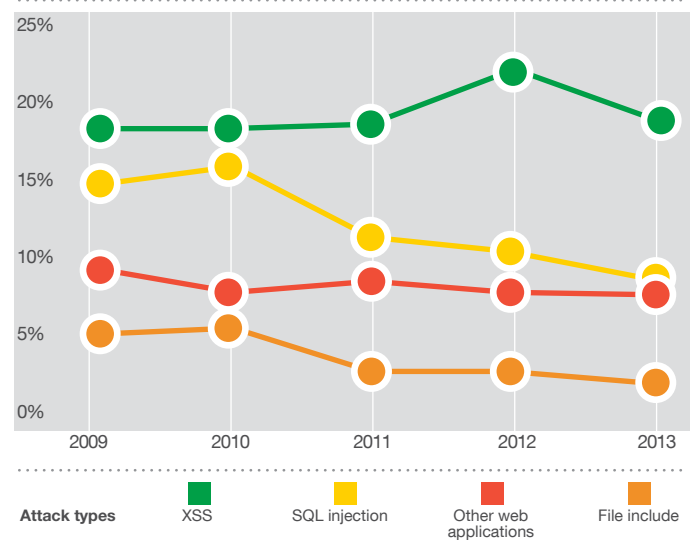


Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013

Consequences of exploitation

X-Force categorizes vulnerabilities by the consequence of exploitation. A consequence is essentially the benefit that the

attacker gains by exploiting the vulnerability. Table 1 describes each consequence.

Consequence	Definition
Gain access	Obtaining local and remote access to an application or system; also includes vulnerabilities by which attackers can execute code or commands, because these usually allow attackers to gain access to the underlying service or system OS
Cross-site scripting	Varying impact depending on the targeted application or user, but could include such consequences as sensitive information disclosure, session hijacking, spoofing, site redirection or website defacement
Denial of service	Crashing or disrupting a service or system
Obtain information	Obtaining information such as file and path names, source code, passwords, or server configuration details
Bypass security	Circumventing security restrictions such as authentication, firewall or proxy, and intrusion detection system (IDS)/intrusion prevention system (IPS) or virus scanners
Gain privileges	Obtaining elevated privileges on an application or system via valid credentials
Data manipulation	Manipulating data used or stored by the host associated with the service or application
Unknown	The consequence cannot be determined based on insufficient information
Other	Refers to anything not covered by the other categories
File manipulation	Creating, deleting, reading, modifying or overwriting files

Table 1. Definitions for vulnerability consequences

The most prevalent consequence of vulnerability exploitation for the first half of 2013 was *Gain access*, at 26 percent of all vulnerabilities reported. In most cases, gaining access to a system or application provides attackers complete control over the affected system, which would allow them to steal data, manipulate the system or launch other attacks from that system. *Cross-site scripting* was the second most prevalent consequence at 18 percent, and typically involves attacks against web applications.

A complete breakdown of all vulnerability consequences reported during 2013 is shown in Figure 12.

Consequences of exploitation 2013

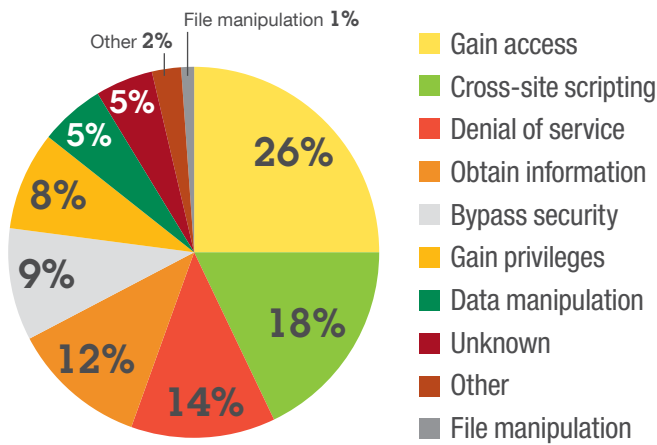


Figure 12. Consequences of exploitation 2013

Exploits

X-Force catalogs two categories of exploit: exploit and true exploit. Simple snippets with proof-of-concept code are counted as *exploits*, while fully functional programs capable of standalone attacks are categorized separately as *true exploits*.

Publicly available and disclosed true exploits have continued to decrease over the past five years to the lowest levels we've seen since 2006. At the end of 2012 we reported that total true exploits were still down overall and at the end of 2013, we see this trend continue.

True exploit disclosures

The number continues to drop steadily from 2009 to 2013.

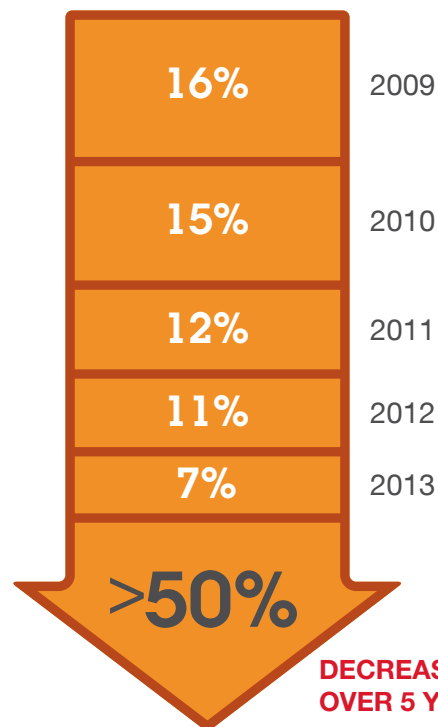


Figure 13. True exploit disclosures, 2009 to 2013

About X-Force

The X-Force research and development team studies and monitors the latest threat trends including vulnerabilities, exploits and 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, 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 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 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 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 identity 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.

Contributors

Producing the 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
Avner Gideoni	Vice President, Security, Trusteer
Brad Sherrill	Manager, IBM X-Force Threat Intelligence Database
Chris Poulin	Research Strategist, IBM X-Force
Dana Tamir	Director, Enterprise Security Product Marketing, Trusteer
Jason Kravitz	Techline Specialist, IBM Security Systems
Leslie Horacek	Manager, IBM X-Force Threat Response
Pamela Cobb	Worldwide Market Segment Manager, Security Intelligence
Perry Swenson	IBM X-Force Product Marketing
Robert Freeman	Manager, IBM X-Force Advanced Research
Scott Moore	Software Developer, Team Lead, IBM X-Force Threat Intelligence Database



- ¹ Trusteer, Ltd. was acquired by IBM in September of 2013.
- ² David Gilbert, "35,000 Websites Hacked Using Vulnerability in vBulletin Forum Software," *International Business Times*, October 15, 2013. <http://www.ibtimes.co.uk/35000-websites-hacked-vbulletin-vulnerability-cms-software-514034>
- ³ Arnold Kim, "MacRumors Forums: Security Leak," *MacRumors*, November 12, 2013. <http://www.macrumors.com/2013/11/12/macrumors-forums-security-leak/>
- ⁴ John Koetsier, "LinkedIn DNS hijacked, traffic rerouted for an hour, and users' cookies read in plain text," *VentureBeat*, June 19, 2013. <http://venturebeat.com/2013/06/19/linkedin-dns-hijacked-traffic-rerouted-for-an-hour-and-users-cookies-read-in-plain-text/>
- ⁵ Christina Warren, "Buffer Users' Facebook and Twitter Feeds Spammed After Hacking," *Mashable*, October 26, 2013. <http://mashable.com/2013/10/26/buffer-hacked/>
- ⁶ Elad Shapira, "The Android BitCoin vulnerability explained," *AVG Technologies*, August 20, 2013. <http://blogs.avg.com/mobile/android-bitcoin-vulnerability-explained/>
- ⁷ Larry Seltzer, "PHP project site hacked, served malware," *ZDNet*, October 28, 2013. <http://www.zdnet.com/php-project-site-hacked-served-malware-7000022513/>
- ⁸ Emmanuel Tacheau, "Watering-Hole Attacks Target Energy Sector," *Cisco Systems*, September 18, 2013. <http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/>
- ⁹ Jeremy Kirk, "Yahoo's malware-pushing ads linked to larger malware scheme," *PCWorld*, Jan 10, 2014. <http://www.pcworld.com/article/2086700/yahoo-malvertising-attack-linked-to-larger-malware-scheme.html>
- ¹⁰ George Tubin, "Malvertising Campaigns Get a Boost from Unpatched Java Zero-Day Exploits," *Trusteer Blogs*, January 30, 2013. <http://www.trusteer.com/blog/malvertising-campaigns-get-a-boost-from-unpatched-java-zero-day-exploits>
- ¹¹ IBM Center for Applied Insights, "A new standard for security leaders: Insights from the 2013 IBM Chief Information Security Officer Assessment," *IBM Corp.*, October 2013. <http://public.dhe.ibm.com/common/ssi/ecm/en/ciw03087usen/CIW03087USEN.PDF>
- ¹² Aaron Smith, "Smartphone Ownership 2013," *Pew Internet & American Life Project*, June 5, 2013. <http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx>
- ¹³ Chris Poulin, "A Fresh Look at Healthcare Data Breach Numbers," *IBM Security Intelligence Blog*, November 25, 2013. <http://securityintelligence.com/healthcare-data-breach-numbers/#>
- ¹⁴ "State of Security in the App Economy: Mobile Apps Under Attack," *Arxan Technologies, Inc.*, 2013. https://www.arxan.com/assets/1/7/State_of_Security_in_the_App_Economy_Report_Vol._2.pdf

© Copyright IBM Corporation 2014

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2014

IBM, the IBM logo, ibm.com, QRadar and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.



Please Recycle