IBM Security Systems

March 2015

IBM X-Force Threat Intelligence Quarterly, 1Q 2015

Explore the latest security trends—from “designer vulns” to mutations in malware—based on 2014 year-end data and ongoing research

Contents

Executive overview

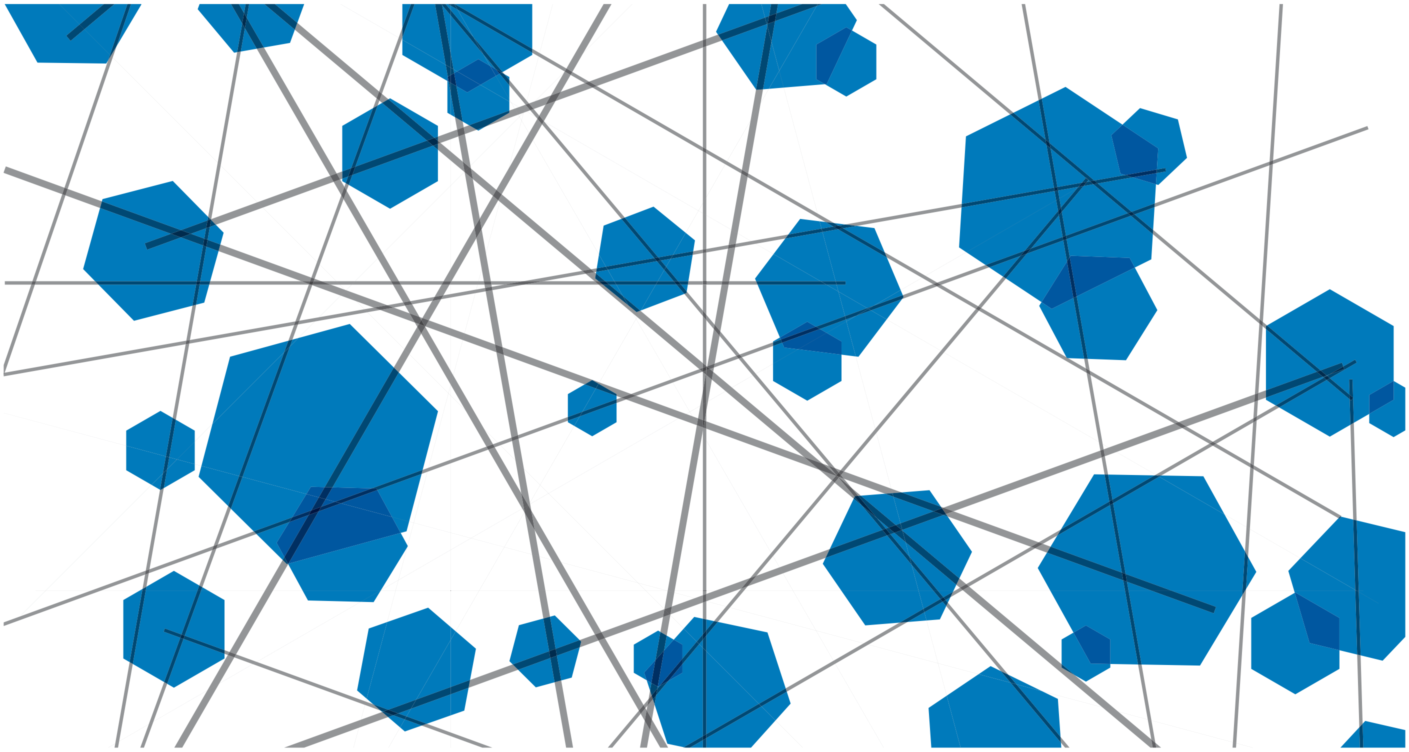
When we look back in history to review and understand the past year, you can be assured it will be remembered as a year of significant change.

In early January 2014, companies large and small scrambled to better understand and analyze a major retail breach that left them asking whether or not their own security measures would survive the next storm. Before spring was barely in motion, we had our first taste of the "designer vuln"—a critical vulnerability that not only proved lethal for targeted attacks, but also had a cleverly branded logo, website and call-name (or handle) that would forever identify the disclosure.

These designer vulns appeared within long-held foundational frameworks used by the majority of websites, and they continued throughout 2014, garnering catchy name after catchy name—Heartbleed, Shellshock, POODLE, and into 2015, Ghost and FREAK. This in and of itself raises the question of what it takes for a vulnerability to merit a marketing push, PR and logo design, while the other thousands discovered throughout the year do not.

Breaches and security incidents were being announced so rapidly in 2014 that many struggled to keep up. By the end of the year, we began to see that this digital storm of attacks would not cease, but instead would likely become larger, grow more encompassing, and raise increasingly important personal privacy concerns, as evidenced by the breach at Sony.

However, data breaches and security incidents did not take all the limelight in 2014. We also continued to see new usage of familiar, "old" malware, which quickly became the tool of choice for cybercriminals. Citadel financial malware—historically a spawn of Zeus configurations—took a less noisy route by slowly and stealthily morphing into new variants that now target petrochemical sellers and suppliers, as well as password management software.



In addition to breaches, security incidents and malware, disclosures on mobile devices were still a key concern. In fact, researchers dug into the mobile frameworks to find flaws and help mobile application software developers do a better job of updating their tools and applications. To this day, critical disclosures for Apache Cordova—reported and fixed in July—are still affecting exploitable Android applications that have yet to be patched or updated. Many of these are banking applications, which are considered to be in a high-risk category.

Surprisingly, by mid-year 2014, IBM® X-Force® was prepared to declare a drop in the total number of reported vulnerability disclosures. However, everything changed in September when a Computer Emergency Readiness Team-Coordination Center (CERT/CC) researcher created and announced an automated tool to test the security of Android applications. Using this tool, he discovered security issues in thousands of Android applications. These vulnerabilities can allow an attacker to perform man-in-the-middle (MitM) attacks against affected mobile applications. This announcement not only changed the 2014 year-end count but also the disclosure landscape.

We ended the year in a white-knuckle rollercoaster ride of continued analysis of the state of Internet security, and preparing for a potential ground shift in how we measure vulnerabilities in the years to come.

Roundup of security incidents in 2014

From data breaches to ransomware, learn about the overarching themes that emerged in our year-end analysis of security incidents.

From exploitation of critical vulnerabilities in widely used Internet-facing open-source libraries, to international privacy concerns, to a deluge of highly publicized data breaches, few would argue that 2014 had the makings of a perfect storm of security incidents. Looking deeper into the data, was it hype or a harbinger of things to come?

With some estimates indicating there were more than a billion leaked emails, credit card numbers, passwords and other types of personally identifiable information (PII), it would seem that the chances of being affected by a security incident over the last year were quite high. From Hollywood to the local home repair store, the impact of security incidents on our everyday lives has become increasingly more pervasive.

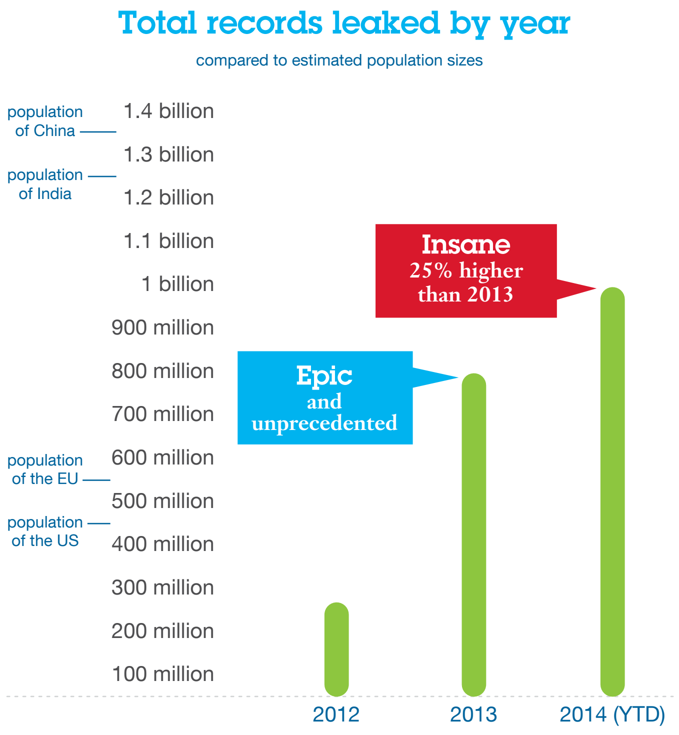


Figure 1. Total records leaked by year, compared to estimated population sizes

Figure 1 provides some perspective on what a billion or more records might look like when compared with population sizes. While each breached record doesn't necessarily denote an individual user, it is still likely that a significant percentage of the Internet-connected population experienced some form of loss as a result of security incidents in 2014.

Based on pure volume, the total number of records breached in 2014 was nearly 25 percent higher than in 2013 (when 800 million records were leaked). In August 2014, a security firm announced that it had uncovered a very large trove of leaked credentials.[1] However, the details of this announcement have not yet been fully confirmed, so we did not include those additional records in our calculations.

Key themes across security incidents in 2014

While there were many noteworthy events throughout the year, much of the security incident activity can be viewed through three overarching themes: privacy in a digital world, cracks in the foundation, and the lack of security fundamentals.

Privacy in a digital world

Since 2013, concerns over government monitoring of digital communications and the issue of maintaining privacy in the age of the Internet have intensified. We place a certain amount of trust that the vendors of communications and data storage services employ adequate security to keep our personal information private. However, as events throughout 2014 repeatedly demonstrated, even when primary points of entry are well secured, attackers will seek alternative means of access.

A prime example was the public disclosure of sensitive photos stored on a cloud service.[2] The security of the cloud service itself was not fundamentally flawed, but users' weak passwords and easy-to-guess security questions, coupled with lax policies on brute-force authentication, resulted in stolen data. While technology makes it simple to store backups in the cloud, it also adds a layer of detachment for everyday users who do not consider where their data resides and how it may be at risk.

A similar incident occurred when private photos of users of a social media application were leaked by a third-party service.[3] While the core application was used to send transient images, which were deleted several seconds after they were viewed, additional third-party services used the application programming interface (API) to save content for later viewing. When attackers were able to compromise the third-party service, they had access to content that users had thought was deleted.

In one of the most significant privacy breaches of the year, private email communications at a major Hollywood studio (Sony) were released as part of a larger leak of data.[4] Offering a behind-the-scenes view into the world of celebrities and movie producers, many media sites discussed intellectual property and private conversations as casually as any other kind of daily gossip.

The impact of security incidents was not just limited to online interactions. Retail customers, particularly in the United States, were subject to repeated thefts of credit card numbers across a variety of different restaurants, stores and e-commerce websites. From fast-food chains to clothing stores, the convenience of paying by credit card—and vulnerabilities in the systems that process those payments—put many people at risk.

Cracks in the foundation

There are more than a billion unique websites on the Internet, and this number continues to increase every day. A large percentage of these sites are dependent on the same operating systems, open-source libraries and content management system (CMS) software.

2014 proved to be a unique year, since vulnerability disclosures affected not just one, but several of these foundational systems, resulting in a huge number of exploited websites.

This concept of going after widely used platforms and popular services has been at play in the past few years, for example, when vulnerabilities in CMS software resulted in the exploitation of millions of sites. In 2014, several of the most popular CMS platforms—such as WordPress, Joomla! and Drupal—had major vulnerabilities in both the core platform and widely used plug-ins. There were also critical vulnerabilities in web-forum software, such as phpBB and vBulletin, which allowed attackers to take over web servers.

These data breaches are concerning, even for sites that do not contain sensitive user data. From within almost any website, attackers can still use breaches to serve malware or as bots under command and control for large-scale distributed-denial-of-service (DDoS) attacks. Companies are also at risk for compromised servers that are used to exfiltrate sensitive data or to attack their business partners, customers and supply chain.

2014 was also unique in that the underlying libraries that handle cryptographic functionality on nearly every common web platform—including Microsoft Windows, Mac OS X and Linux—were found to be vulnerable to fairly trivial remote exploitations capable of stealing critical data.

The first disclosure of these remote cryptographic vulnerabilities came in April when a two-year-old bug in the OpenSSL library was publicly disclosed as CVE-2014-0160 or "Heartbleed."[5] This vulnerability was discovered to be remotely exploitable, allowing attackers to obtain data residing in server memory, including user login records, private security certificates and other sensitive data. Not only were HTTPS web servers affected, but also any devices or applications that used SSL for encryption were potentially vulnerable.

While the OpenSSL vulnerability primarily affected UNIX-based web servers, Microsoft servers were also at risk for remote execution from a crypto library. In November, a patch was released for CVE-2014-6321, which is a vulnerability in the Microsoft security channel package that affects all desktop and server versions of the operating system and can allow attackers to execute remote code.

In addition to requiring a patch for the UNIX SSL vulnerabilities, OS X was also susceptible to a man-in-the-middle (MitM) attack, dubbed "Goto Fail" (CVE-2015-1266), in which attackers could eavesdrop or hijack SSL-encrypted web traffic from public wireless access points.[6]

All three of these taking place in a single year is significant, but there were also several other high-impact vulnerabilities throughout the year that affected a large number of web servers and endpoints. For example, the Shellshock family of bugs in the UNIX bash shell (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186 and CVE-2014-7187) can be exploited to remotely run shell commands on a vulnerable server.[7]

Another family of vulnerabilities affecting cryptographic systems was named Padding Oracle on Downgraded Legacy Encryption, or POODLE (CVE-2014-3566 and CVE-2014-8730). While not as detrimental as Heartbleed or Shellshock, POODLE can, when exploited, allow attackers to perform a MitM attack to silently intercept a secure session.

Besides igniting a trend of labeling high-profile designer vulnerabilities with a catchy name and logo, these types of vulnerabilities affected a large percentage of websites and, in many cases, were fairly easy to exploit by using scripts and automated tools.

The lack of security fundamentals

For several years, X-Force has advised on the importance of adherence to basic security fundamentals as an effective way to protect against or mitigate the impact of a security breach. This was just as true in 2014 as in past years.

One of the best examples of the importance of basic security fundamentals was with password security, which continues to be a major factor in data breaches. Whether users have predictable or weak passwords, or they reuse passwords across the Internet and the enterprise, the ability for attackers to gain access as a result of poorly managed authentication policies is concerning.

There are millions of known email addresses and plain-text passwords culled from years of previous data breaches, which can be used to attempt to gain access to other sites. This data helps attackers enumerate common passwords, and it puts people who reuse passwords across multiple sites at risk for brute-force account takeover. In one notable example, more than six million accounts at a popular cloud storage provider[8] were compromised. While the cloud storage provider itself was not breached, login data from other breaches, as well as malware, keyloggers and phishing tactics allowed attackers to access accounts.

Use of default passwords continues to be a problem as well. Several retail breaches in the last year were perpetrated by attackers who remotely accessed point-of-sale (POS) servers[9] by using default or known logins to screen-sharing software used for legitimate technical support troubleshooting. These breaches demonstrate that fundamental security practices, such as changing default account passwords, are still not being implemented adequately.

Attack types and industries

Year to year, X-Force has been tracking a sampling of security incidents by attack type and industry. As with previous years, it is interesting to look across this data to uncover trends. Figure 2 represents the latest iteration, showing a number of incidents that were publicly disclosed in 2014.

Sampling of 2014 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

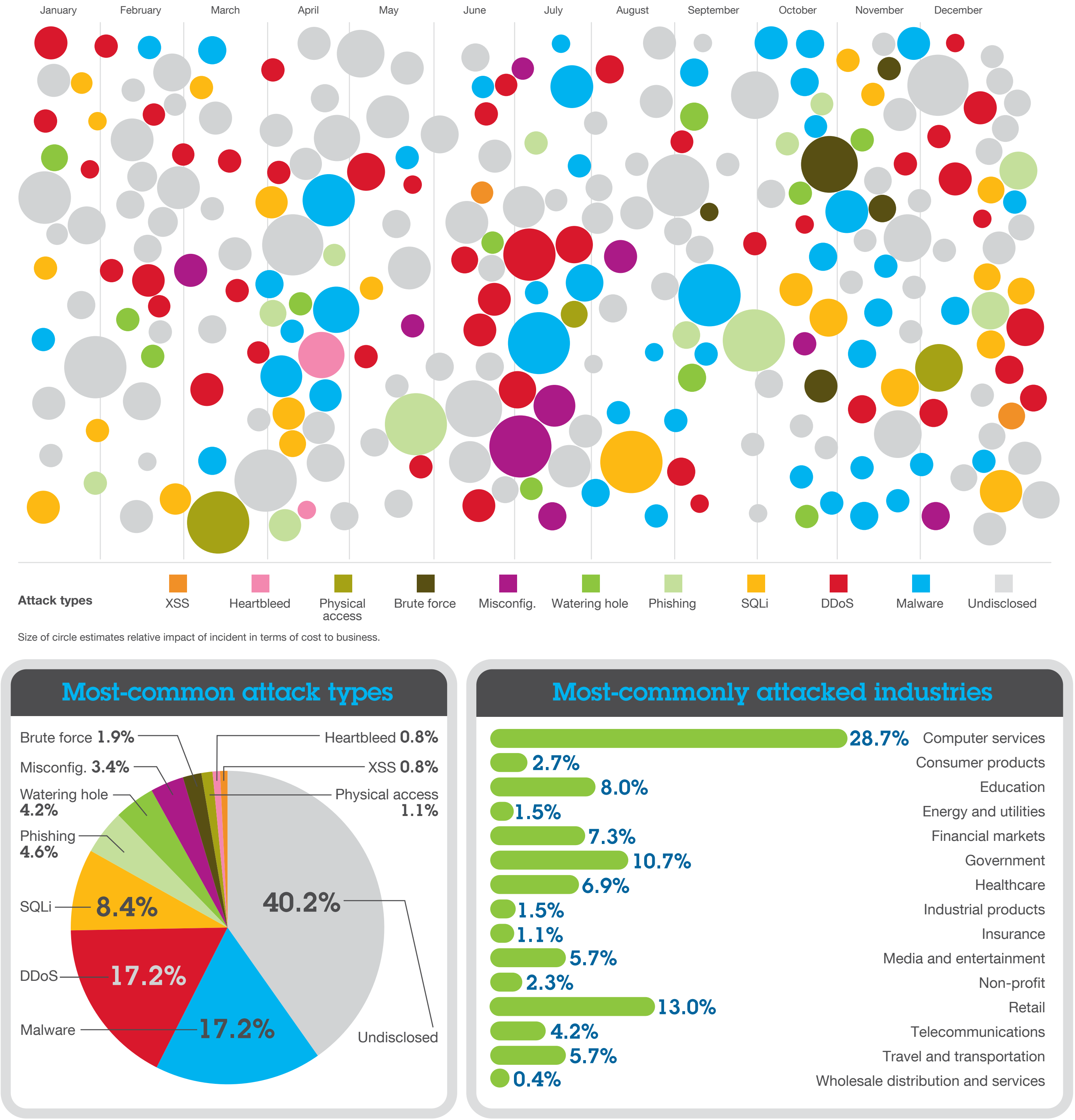
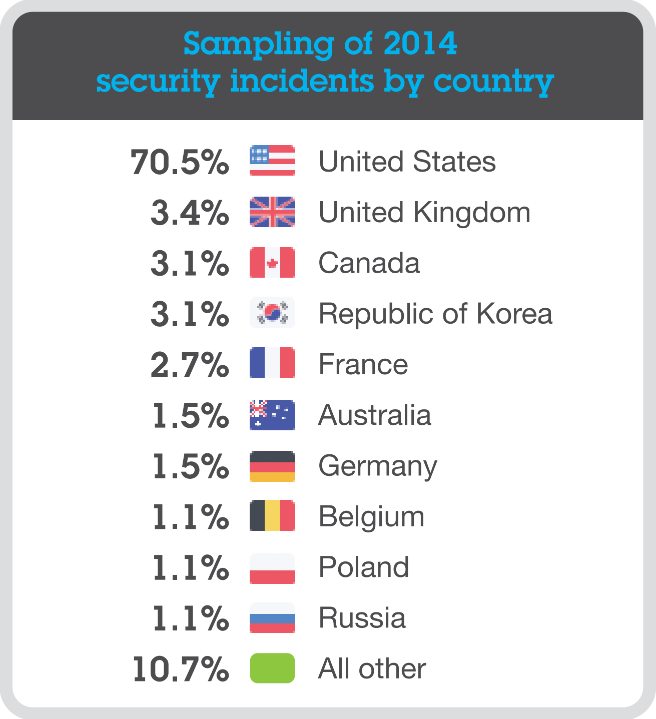


Figure 2. Sampling of 2014 security incidents by attack type, time and impact



Sampling of 2014 security incidents by country

70.5%	United States
3.4%	United Kingdom
3.1%	Canada
3.1%	Republic of Korea
2.7%	France
1.5%	Australia
1.5%	Germany
1.1%	Belgium
1.1%	Poland
1.1%	Russia
10.7%	🟩 All other

Figure 3. Sampling of 2014 security incidents by country

Similar to previous years, the number of incidents in the United States is far higher than in other countries. This is likely due to disclosure laws in the United States being more stringent than those in other countries, resulting in more publicly disclosed incidents. In addition, more high-profile websites are hosted in the United States than in other countries. Republic of Korea had a number of severe incidents in 2014 affecting large percentages of the population.

As mentioned, the retail industry, particularly in the United States, was heavily impacted. The tone was set at the end of 2013 from a high-profile breach at Target stores, which affected more than 70 million shoppers,[10] and continued in 2014 with breaches affecting a number of national restaurant chains and retail shops. Employing a similar methodology throughout the year, attackers successfully gained entry into these enterprises through techniques like spear phishing. After gaining access, they could install RAM-scraping malware on card processing systems, capable of logging encrypted card data as it passed in plain text in server memory. The stolen credit card data could then be exfiltrated and sold on the black market.

Some businesses, which audited their own systems as a result of this widespread attack pattern, discovered malware that had been running undetected for periods ranging from a few weeks up to several years.

Malware attacks outpace SQLi

The near-weekly disclosure of retail POS malware was only one of several high-profile attack vectors that unfolded throughout 2014. In past years, X-Force has reported on the effectiveness of SQL injection (SQLi) attacks as a means of extracting data from web servers and applications. Historically, SQLi once reigned as a leading cause of security incidents. In 2014, however, with regard to the incidents tracked by X-Force, malware and DDoS attacks took the lead in terms of the volume of security-incident attack types.

2014 still saw widespread SQLi vulnerabilities leading to large-scale exploitation and loss of data. Most notably, vulnerabilities in CMS platforms provided attackers with a means to reach many targets using a minimal amount of effort. For example, a stock exchange in Poland[11] was believed to have been breached via a known SQLi vulnerability in the Joomla! CMS platform, while a major SQLi vulnerability in Drupal CMS put hundreds of thousands, if not millions, of servers at risk for exploitation.[12] At year end, a SQLi vulnerability on an Australian travel insurance website led to a leak of more than 750,000 records, one of the largest breaches in Australia to date.[13]

CMS platforms were also affected by insecure plug-ins. Previous X-Force reports have addressed how CMS plug-ins are often created by small, third-party development groups, who are trying to solve a niche problem and may not employ adequate security protection. This was the case when a vulnerability in a popular WordPress slider plug-in enabled attackers to inject malicious JavaScript onto more than 100,000 websites.[14]

DDoS attacks have also made headlines in recent years as the volume of traffic targeting a single server and data center has increased significantly. It is not uncommon to hear about DDoS attacks consuming more than 100 Gbps of bandwidth with others taking as much as 400 or 500 Gbps. Large attacks like this can not only take out a single website, but potentially other sites within the same data center as traffic spills over, saturating available bandwidth.

DDoS attacks have also been used as a distraction in recent years as a cover for breaching a target. In one unfortunate case in the United States, severe intellectual property and financial damages from a crippling DDoS attack and concurrent data breach resulted in the shutdown of a source-code hosting provider.[15] Another web-based email provider in Ireland had to shut down operations for a period of time to mitigate a high-volume DDoS and breach attempt, leaving customers without access to their webmail.[16]

In past years, shutting down a website with a DDoS attack has been used as a form of political "hacktivism" to protest government entities. These kinds of attacks continued throughout 2014, although the impact of shutting down a city's or a political party's public website is not always clear from a business or operational standpoint. One type of significant impact can come in the form of interrupted communications, as was the case in Arizona when a DDoS protest shut down a public-facing website[17] that police officers use remotely from their vehicles to get critical information while on patrol.

Ransomware increases in 2014

DDoS attacks were also used as a form of "ransomware" or extortion throughout the year. A number of well-established websites[18] were notified that they would be targeted by a DDoS attack unless they paid a ransom ranging from a few hundred dollars to several thousand. The majority of these businesses opted not to pay, and while they did endure downtime as a result of the DDoS threats, they were able to regain service without giving in to the attackers' demands.

What is a crypto ransom?

Ransomware holds a system hostage by encrypting data and requiring users to pay a "ransom" to get the keys they need to recover the data. Payment instructions are typically displayed in a message to the user; payments often have a deadline, and the amount can escalate beyond the specified date. Ransomware typically demands payment using a "micro currency" such as Bitcoin to reduce the attacker's risk. Security software can detect a crypto-ransom attack in its early stages, since the encryption can take some time to complete. Immediate removal of the malware can help limit the damage it can do, but may prevent recovery of the data it has already processed.

What can you do to keep yourself protected? Simple steps such as performing regular backups and maintaining up-to-date anti-virus software and patches for your operating system are just a few tips. To learn more ways to protect yourself, please refer to the US-CERT alert on crypto ransomware.

Whether targeting individuals or enterprises, ransomware appeared to be on the rise in 2014. These types of attacks fell into several categories. One type, described previously, involves extorting businesses to pay a fee to avoid a DDoS attack or public leak of data. A second type of attack comes in the form of a crypto-ransom scheme, in which criminals target businesses and home users. Crypto-ransom attackers encrypt and lock out users from their own data, computers or mobile devices; then, they demand a payment, usually in Bitcoin, in return for the unlock key. The success of crypto-ransom campaigns has led to an increase in these types of attacks, with newer versions of the ransomware toolkits getting more advanced and more difficult to disable.

The city of Detroit[19] was targeted by such a scheme in which the attackers demanded the Bitcoin equivalent of USD800,000 to release a city database that they had encrypted. Fortunately, the database was no longer required and the extortion attempt was not successful.

Security incidents that result in systems going offline temporarily—or result in the theft of personal data and financial information—often leave the underlying systems intact. In contrast, some attacks are meant to do permanent damage, either by erasing hard drives and overwriting the Master Boot Record (making them unusable) or by destroying physical systems, such as those used by industrial and manufacturing companies.

Several incidents throughout the last year resulted in such damages, the most notable being the Sony attack[20] in which wiper malware was used to disable endpoint systems. In Germany,[21] a spear phishing attack led to extensive damage to a blast furnace at a steel mill. Microsoft Active Directory servers at a casino enterprise were also targeted by wiper malware,[22] although in this case, it actually impeded the attacker's ability to gain a foothold into international sites and limited the attack to US properties only.

In 2012, the term "watering hole" was introduced to describe attacks that target specific groups of users by injecting malicious code on the websites where such users congregate. Several new watering-hole attacks occurred in 2014, such as an attack targeting readers of defense and military news websites.[23] In another case, researchers discovered malicious code[24] on an industrial website catering to automotive, aerospace and manufacturing companies.

Malvertising is an attack type similar to a watering-hole attack. Malvertising is an exploit vector consisting of a compromised ad network, which serves malicious code that has been injected into ads displayed on legitimate sites. This allows attackers to reach a much larger audience than compromising a single website. And it provides a way to target companies that may have tighter security around their own servers, but unknowingly are serving malicious ads that are embedded in their content.

In both watering-hole and malvertising attacks, attackers are able to deploy exploit kits to vulnerable endpoints by leveraging a number of browser-based vulnerabilities as well as by targeting plug-ins, such as Java and Adobe Flash.

Conclusion

While general attack types remain consistent year to year, creative applications of these fundamental building blocks can vary greatly. A review of the breaches in 2014 shows a mix of attackers targeting low-hanging fruit (for example, by running scripts against known vulnerabilities) as well as using sophisticated, custom exploits to reach high-profile targets with surgical precision.

In response to the high capacity, volume and nature of attacks that have continually increased over time, X-Force is launching the Interactive Security Incident (ISI) website to help users gain an in-depth understanding of security events in the current year, as well as a historical perspective of how security events have evolved year to year. We encourage you to visit this site often to stay up to date on the latest breaches and security incidents as they are confirmed by public sources.

For a three-year view of security incidents, please download the X-Force 1Q 2015 Graphics package.

To explore the X-Force Interactive Security Incident website now, please visit:

***ibm.com**/security/xforce/xfisi/*

Citadel, the financial malware that continues to adapt

How can you protect against constantly mutating malware? Learn about the latest variants of Citadel and how the targets have shifted beyond the financial industry.

Over the past eight years, financial malware has undergone a wide range of significant changes. These include evolving methods of stealing data (from using simple keylogging capabilities to deploying fully automatic crimeware capable of taking over devices and capturing data and credentials), distribution and delivery of malware to targeted devices, the introduction of new "security updates" that allow malware to evade detection, and many more.

One such recent change in malware is the type of target. In the past, several variants of financial malware have targeted non-financial institutions, including e-commerce sites, airlines, hotels, healthcare organizations and online gaming companies. Now, the list has expanded even further. A variant of Citadel,[25] a popular financial malware, now targets petrochemical sellers and suppliers, as well as password management software—with the apparent goal of giving attackers access to sensitive corporate intellectual property rather than financial data.

In addition, while most targeted attacks use remote access tools (RATs) and specially designed malware, going forward, we may see increasing use of "battle-proven" malware like Citadel to gain a foot in the door of different types of organizations.

The evolution of Zeus, from pioneer to mass usage

When financial malware emerged, there was one malware that stood above all others in terms of capabilities and usability—Zeus. It quickly became the tool of choice for cybercriminals, allowing easy configuration without the need to code, as well as multiple ways to extract credentials from its victims. Zeus v2 was introduced in late 2009, but 18 months later, the Zeus source code was leaked in an underground forum. The leak allowed cybercriminals to develop their own variants and essentially eliminated the need to buy the malware from the selling group.

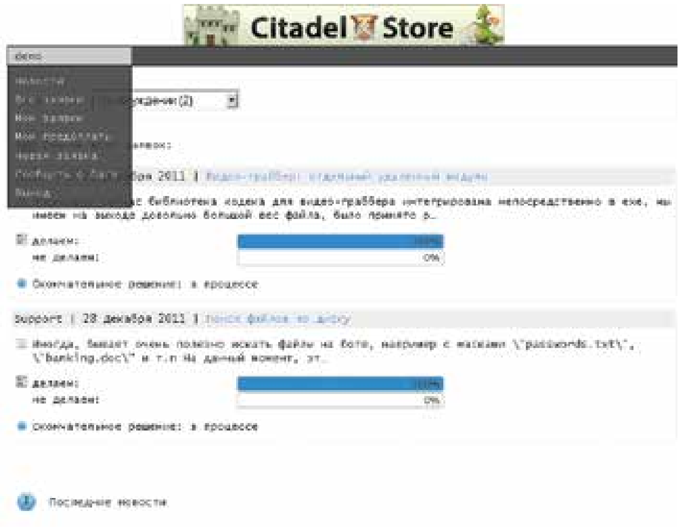
Many underground forum discussions theorized why the source code was leaked. One rumor was that Slavik,[26] the alias of the Zeus coder, had a quarrel with people in the team and decided to move to his own private venture and destroy the gang's business. In any case, the effect of the source-code leak did not take long to materialize—and shortly thereafter, new Zeus variants appeared. These variants ranged from simple malware, such as Ice IX, to very complex variants, such as GameOver Zeus. In addition, other malware families stole pieces of the code to implement specific modules, such as Ramnit stealing the virtual network connection (VNC) module. One of these variants was Citadel, which was introduced to the market in late 2011 and offered some unique features.

Citadel evolving over time

Citadel was introduced in a Russian underground forum and offered cybercriminals a new advanced tool encompassing "classic" Zeus capabilities as well as new features. The original post in the forum indicated that the malware is "Zeus compatible," meaning that configuration files and HTML injections that were used with older versions of Zeus would work with Citadel. The advertisement highlighted that Citadel enabled the attacker to run shell commands off the infected device (which would allow an attacker to, among other things, map the network in which the device was infected—obviously aiming at more than just financial data). The advertisement also indicated that the malware would not work on devices using a Cyrillic keyboard layout, since the authors did not wish to target Russian or Ukrainian systems.

In addition to these capabilities, purchasers of Citadel were able to influence future versions by participating in polls that the Citadel team initiated. These polls asked users to choose between features they would want to see in upcoming versions. Once a feature received a majority vote and a minimal amount of money, the Citadel team committed to developing the feature.[27]

New variants of Citadel started targeting financial institutions worldwide with the user-requested features, new at that time. For example, the VNC module allowed attackers to take control of infected devices—overcoming device ID and IP reputation systems. Other variants included video-capturing features, which allowed attackers to monitor users' desktops to learn their behavior and click patterns when accessing online banking applications.



…бря 2011 | Видео-граббер: отдельный удаленный модуль

…с библиотека кодека для видео-граббера интегрирована непосредственно в exe, мы имеем на выходе довольно большой вес файла, было принято р…

делаем: 100%
не делаем: 0%

Окончательное решение: в процессе

Support | 28 декабря 2011 | поиск файлов по диску

Иногда, бывает очень полезно искать файлы на боте, например с масками \"passwords.txt\", \"banking.doc\" и т.п На данный момент, эт…

делаем: 100%
не делаем: 0%

Окончательное решение: в процессе

Последние новости

Graphic 1. Voting for features on the "Citadel Store"
(source: Brian Krebs)

Over time, Citadel has continued to evolve, releasing new versions such as v1.3.4.x and v1.3.5.x, and features such as automatic localization of fraud content.[28] One interesting variant expanded on the malware's persistency—or to be more precise, its operator's ability to take control of an infected device. Citadel's built-in VNC (the VNCfox) has also proven to be a valuable tool in the hands of cybercriminals.

However, as the Citadel malware has gained popularity, more and more anti-virus and anti-malware software developers have included detection and removal tools for this threat. One Citadel variant had a solution to this problem. An attacker could use this Citadel variant's "AutoCMD" functionality to run shell commands on an infected device. Upon infection, this variant created a new user on the infected device and added it to the native Microsoft Windows remote desktop protocol (RDP) group. By doing so, even if the malware was removed from the infected device, the operator still had a back door into it using Windows RDP.

In addition, IBM Security Trusteer® researchers recently discovered[29] that Citadel may also be used to target new entities and software. "Classic" Citadel targets were financial in nature, be it banks, credit unions or e-commerce. However, new variants discovered are now targeting petrochemical sellers and suppliers as well as password management software. In light of Citadel's successful track record in infecting and stealing data—as well as its abilities to traverse the network of an infected device, run commands, and take control of infected devices and new targets—it seems this malware is moving from facilitating fraud to becoming a cybercrime tool for targeted attacks.

What can you do to protect from Citadel?

As Citadel evolves and changes its targets and attack methods, end users and enterprises must change and adapt as well. To better protect against such threats, a combination of endpoint protection and cloud-based malware and criminal detection are needed for financial institutions. Advanced malware protection is also required for the enterprise.

Endpoint protection can help users immunize their devices against malware infection and remove existing threats. Cloud-based detection can help detect malware on unprotected devices and criminal detection can identify account takeover attacks coming from a criminal device or even those using the victim's device as a proxy. Enterprises should protect employees' devices with advanced malware protection to identify infection attempts and targeted attacks that utilize popular software such as products from Java, Adobe, Microsoft and more. In addition, large organizations should use advanced malware protection systems to identify data exfiltration attempts, which are the final step in most targeted attacks.

Are mobile application developers for Android putting their users at risk?

The vulnerabilities in mobile applications are higher than ever. Learn how the industry is responding and what developers can do to be more proactive.

The mobile development landscape continues to fragment due to the many devices and multiple platforms available—each with its own programming language and development framework. As such, it is increasingly challenging for developers to target these various platforms.

Frameworks that allow for cross-platform development from a single code-base are therefore desirable and are becoming increasingly popular within the application development community.

Apache Cordova (previously known as PhoneGap) is one such platform that allows developers to use HTML5 as a single, cross-platform development technology. According to AppBrain,[30] Cordova is used in approximately six percent of all Android applications. Furthermore, Cordova is prevalent in categories that may be of high interest to attackers such as the business, medical and finance categories where more than 12 percent of all applications in each respective category are based on Cordova.

In July 2014, IBM X-Force discovered a series of vulnerabilities in the Android version of Cordova, which we disclosed privately to the Apache Foundation. Fixes or mitigations for these vulnerabilities were provided by the Cordova development team in August[31] and a technical security advisory was published with the public disclosure of the vulnerabilities. In order to highlight the severity of the vulnerabilities in respect to real-world exploitability, we also demonstrated a proof of concept[32] showing how a complete, remote, end-to-end attack could be constructed and provided accompanying technical details.

What are the vulnerability disclosures for the Android version of Cordova?

Apache Cordova cross-application scripting (CVE-2014-3500)

This vulnerability allows an attacker to execute JavaScript code within the context of the Android application, breaking the platform sandbox protection mechanism. The attacker could exploit this vulnerability to steal sensitive information, such as the application's cookies file. Furthermore, this vulnerability could be triggered via malware residing on the victim device (local context) or, in certain circumstances, could even be triggered remotely (such as via a drive-by download attack).

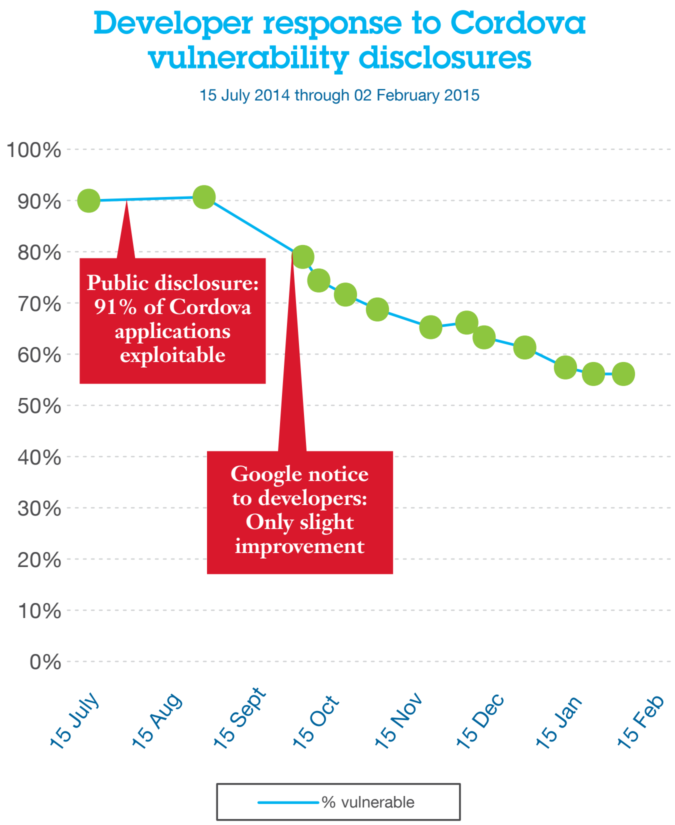
Cordova whitelist bypass for non-HTTP URLs (CVE-2014-3501) and data leaks to other applications via Android intent URIs (CVE-2014-3502)

Android provides a whitelisting mechanism which, when correctly configured, should theoretically stop an attacker from making requests to arbitrary endpoints under the control of the attacker. These two vulnerabilities provide a bypass mechanism to the whitelisting security feature which can be exploited by an attacker to exfiltrate data (for example, attackers can combine the bypass mechanism with an exploit of the cross-application scripting vulnerability described previously to exfiltrate data).

At the time of public disclosure, we started tracking Android applications from various categories that are based on Cordova. Of these applications, 91 percent were initially discovered to be exploitable.

We continued tracking these applications over a six-month period to see how quickly developers would apply the fix to their applications. The results of this tracking can be seen in Figure 4.

In October 2014, we started tracking 17 additional banking applications to discern developer response in this high-risk category.


Developer response to Cordova vulnerability disclosures

15 July 2014 through 02 February 2015

Public disclosure: 91% of Cordova applications exploitable

Google notice to developers: Only slight improvement

Figure 4. Developer response to vulnerabilities after disclosures, 15 July 2014 through 02 February 2015

What is interesting is the apparent developer apathy in making the necessary effort to keep users safe. While this reaction may be expected from developers of applications in the general app category (especially those applications that do not hold any information attractive to an attacker), such apparent apathy is surprising from banking application developers. These applications could be considered high-value targets for an attacker (for example, because some banking applications allow for online money transfers) and, further driven by the low complexity of such an attack, one would expect an immediate response on the part of the banks to protect their customers. However, as of January 2015, 10 of the 17 banking applications we tracked (59 percent) were still vulnerable—exactly the same number of vulnerable applications as when we started tracking in October!

At the beginning of October 2014, Google sent a message[33] to application developers using a vulnerable version of Cordova asking them to update to a non-vulnerable version as soon as possible or risk sanctions against their applications on Google Play.

Google's message to Cordova developers

"Please note, applications with vulnerabilities that expose users to risk of compromise may be considered 'dangerous products' and subject to removal from Google Play."

After this communique to developers from Google, we noticed some improvement in application updates in the general application category; however, banking application developers seemingly continue to be unresponsive to these vulnerabilities as updates have plateaued.

We find the failure-to-update trend identified in this case to be worrying. It is difficult to find justification for not taking immediate action to protect end users—especially in cases of potential financial harm. It is clear that more effort needs to be made on the part of—and more responsibility taken by—the application developers who are ultimately entrusted with keeping user data safe from harm.

Recommendations

Developers should be proactive in the measures taken to keep their users safe. This includes being aware of any security updates that may be available for all third-party software that may be used. Many third-party projects provide mailing lists or blogs that can be used for this purpose. Developers should also have processes in place that allow for the rapid implementation and deployment of security fixes.

Large companies should consider establishing product security incident response teams (PSIRTs) responsible for tracking vulnerabilities across in-house products, and ensuring that developers are notified and take all necessary actions.

The industry should provide better mechanisms for ensuring that applications are kept up to date with respect to third-party software. Developers are often aware of security patches; but it may be difficult for developers to respond quickly due to various factors, such as changing APIs, fixed-version build processes and other issues that could cause significant development work or introduce risk of new software bugs. Each of these factors potentially tips the cost-benefit in favor of not updating. Frameworks should therefore maintain backward-compatibility and, when possible, provide streamlined updates within the build process.

Furthermore, the industry should investigate the possibility of completely separating frameworks from the application code, thereby allowing third-party software updates to be deployed independently from the developer updates. For this to be feasible, these projects again need to provide stable, backward-compatible APIs and assure a high level of confidence that pushed updates will not break application code.

Shaking the foundation: Vulnerability disclosures in 2014

In our year-end review of vulnerabilities, learn how one automated testing tool may transform the disclosure landscape.

IBM X-Force has been documenting public disclosures of security vulnerabilities since 1997. Our X-Force researchers collect software advisories from vendors, read security-related mailing lists, and analyze hundreds of vulnerability web pages where remedy data, exploits and vulnerabilities are disclosed. This research is cataloged in the X-Force database, which now has more than 88,000 unique vulnerabilities and provides the foundation for the IBM Security Network Protection platform.

Each one of the vulnerabilities cataloged in the X-Force database is identified by a unique X-Force ID (XFID). New XFIDs are assigned following the same content decisions that CVE Numbering Authorities (CNAs) must follow when creating new CVE identifiers.[34] X-Force continuously monitors the official CVE list and includes all vulnerabilities in the X-Force database that have been assigned an official CVE identifier. However, a CVE identifier is not required for a vulnerability to be included in the X-Force database. At the time of this writing, X-Force has documented close to 20,000 vulnerabilities throughout its history that do not yet have an official CVE identifier assigned, and recent developments may drastically increase this catalog.

Examples of vulnerabilities without an official CVE identifier

Many times, official CVEs are assigned to vulnerabilities several weeks, months or years after the vulnerabilities have been publicly disclosed. This typically occurs when vulnerability disclosures are made by non-enterprise level vendors or security researchers who do not follow standard disclosure practices. It can also occur when a new CVE is not formally requested by the researcher.

Following are some examples of vulnerabilities in the X-Force database that do not yet have assigned CVEs. It is possible that at a later date, MITRE could issue a CVE to any of these vulnerabilities. What is important to the X-Force database team—and factors into the ahead-of-the-threat protection of the IBM Security Network Protection platform—is that the vulnerability is recorded and, where possible, advanced signature protection is provided.

WinRAR filename spoofing
- XFID disclosure reported: **23 March 2014**
- IBM Security Network Protection coverage provided: **13 May 2014**

MicroSCADA Wserver CreateProcess remote code execution
- XFID disclosure reported: **05 April 2013**
- IBM Security Network Protection coverage provided: **07 July 2014**

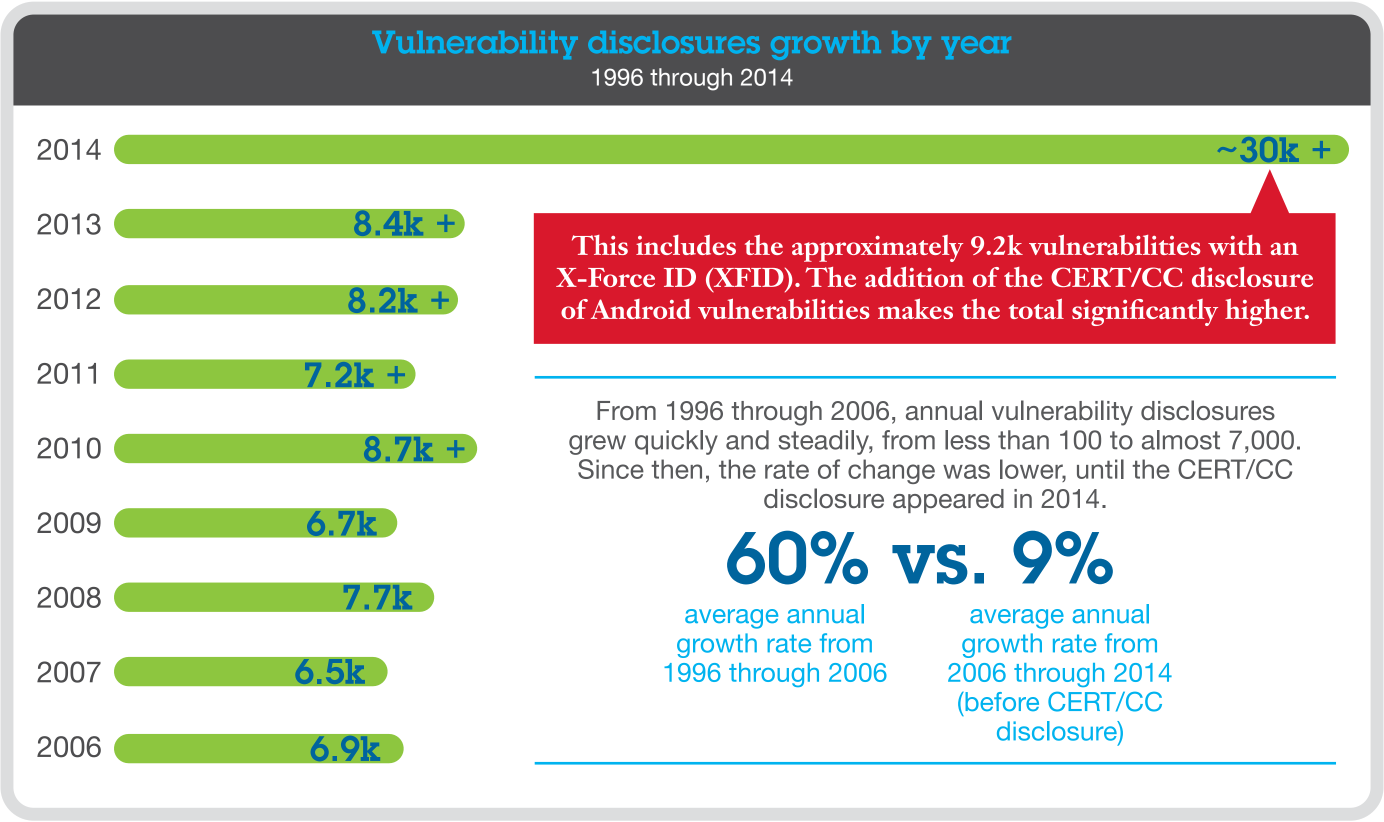
MicroSCADA Wserver remote code execution
- XFID disclosure reported: **05 April 2013**
- IBM Security Network Protection coverage provided: **07 July 2014**

NTP denial of service
- XFID disclosure reported: **25 August 2014**
- IBM Security Network Protection coverage provided: **13 October 2014**

Vulnerability disclosures in 2014

2014 was a record year for X-Force. We cataloged more than 9,200 new security vulnerabilities affecting over 2,600 unique vendors. This represents a 9.8 percent increase over 2013 and is the highest single year total in the 18-year history of X-Force. In the IBM X-Force Threat Intelligence Quarterly - 3Q 2014, we reported a potential downturn in the number of vulnerability disclosures that could result in the total yearly vulnerabilities dropping below 8,000 for the first time since 2011. However, the forecast drastically shifted in September—when a CERT/CC researcher made a landmark disclosure about Android vulnerabilities.[35]

As outlined in CERT/CC Vulnerability Note VU#582497, the CERT/CC researcher identified a class of vulnerabilities affecting thousands of Android applications regarding the improper validation of SSL certificates. These vulnerabilities could allow an attacker to perform man-in-the-middle (MitM) attacks against affected mobile applications. Depending on the type of application targeted, the attacker could execute code or obtain sensitive information (personal, financial or other information) that could be used to leverage additional attacks.



This includes the approximately 9.2k vulnerabilities with an X-Force ID (XFID). The addition of the CERT/CC disclosure of Android vulnerabilities makes the total significantly higher.

From 1996 through 2006, annual vulnerability disclosures grew quickly and steadily, from less than 100 to almost 7,000. Since then, the rate of change was lower, until the CERT/CC disclosure appeared in 2014.

60% vs. 9%

average annual growth rate from 1996 through 2006

average annual growth rate from 2006 through 2014 (before CERT/CC disclosure)

Figure 5. Vulnerability disclosures growth by year, 1996 through 2014

X-Force continues to analyze this disclosure and the vulnerable applications, and we expect to create XFIDs for these vulnerable applications as this research progresses. Once this analysis is complete, the total vulnerabilities for 2014 could increase to more than 30,000 reported for the year. The question here is whether this total will turn out to be a one-year spike or become the new normal as more vulnerabilities are discovered and disclosed through the use of automated tools, such as the case in the CERT/CC disclosure.

In Figure 6, we compare the quantity of Android application disclosures associated with VU#582497 to those of other disclosures announced by vendors, including the top 10 enterprise-level software vendors. The CERT/CC disclosure provides nearly 15 percent of the total for the year, inching the final count to a new historical peak. As a side note, these percentages only include the roughly 1,400 Android SSL issues that have CVE IDs, and do not contain the potential 20,000+ that are still being tracked in the CERT/CC vulnerability note that we discussed previously.

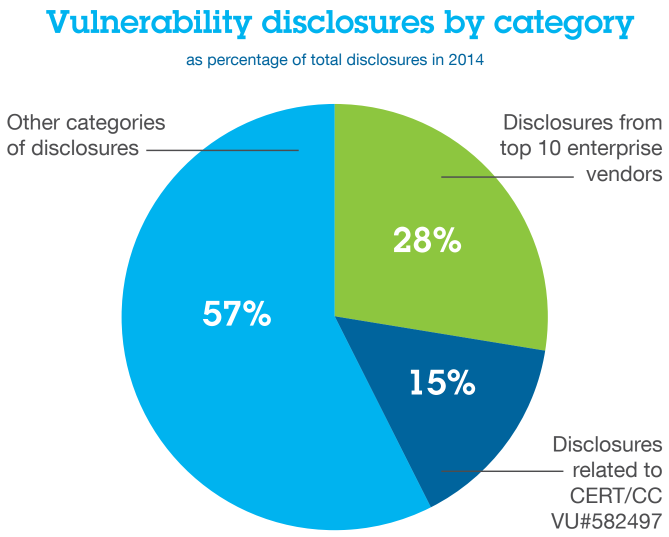


Figure 6. Vulnerability disclosures by category, as percentage of total disclosures in 2014

The impact of one automated testing tool

Will Dormann's CERT/CC article, "Announcing CERT/CC Tapioca for MITM Analysis,"[36] describes the methods used by one researcher at CERT/CC to test the security of Android applications. In the process, he created a tool to help automate such testing. CERT/CC makes the Tapioca tool freely available on the website as a virtual machine appliance preconfigured to perform MitM testing and analysis. The tools in the Tapioca package allow developers and researchers to inspect Android applications for vulnerability to MitM attacks, and analyze the results, with no operator input.

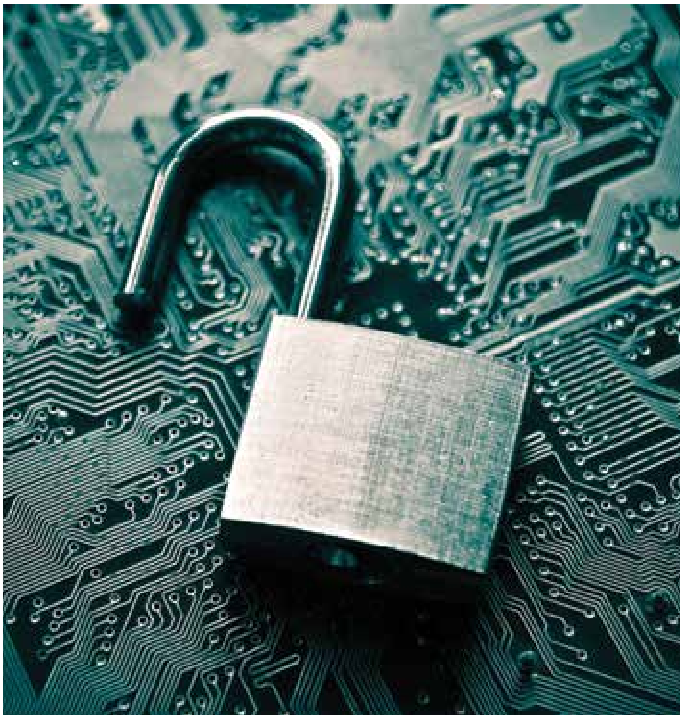
The CERT/CC research began by systematically scanning and dynamically testing the applications in the Google Play Store to determine which applications failed to properly validate SSL certificates. This effort has (so far) produced literally thousands of disclosures of individual applications vulnerable to MitM attacks. In other words, these reports represent the same fundamental vulnerability affecting a wide variety of individual applications. They do not represent thousands of unique methods of attacking different applications; they represent one way of attacking thousands of applications. Multitudes of developers need to update their applications, but they all need to make the same logical changes, rather than each of them having to figure things out from the ground up. Additionally, how to track these types of issues will be a matter of debate by the CVE editorial board and discussions will likely continue as new choices are determined.

Conclusion

In essence, CERT/CC created a tool that can help the industry start to systematize and automate security testing long done manually, when done at all. Thus far, testing focused on SSL/TLS issues that can render a supposedly secure connection insecure. The tool offers additional capabilities. The question remains: will others pick up the gauntlet and follow CERT/CC's lead?

If they do, we will likely see a huge increase in the volume of disclosed vulnerabilities as those efforts produce results. Some reports will pertain to problems with specific applications. Others will reflect widespread poor development practices (such as not validating SSL certificate chains). And some will identify errors in system services and frameworks used by many applications. With thousands of applications in the various "stores," though, each system or framework issue will potentially result in thousands of individual disclosures under current practice.

As users and as an industry, we can hope that others will pick up the gauntlet. We can hope that the publicity resulting from these disclosures will cause at least the more reputable and better funded vendors to implement more complete testing of their applications, prior to release. This result could end up being the best thing for the industry if it leads to significantly better overall security through identifying the problems, publicizing the required corrections, and applying pressure to application developers to pay better attention.



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.
- The IBM Security Trusteer product family delivers a holistic endpoint cybercrime prevention platform that helps protect organizations against financial fraud and data breaches. Hundreds of organizations and tens of millions of end users rely on these products from IBM Security to protect their web applications, computers and mobile devices from online threats (such as advanced malware and phishing attacks).
- The IBM X-Force content security team independently scours and categorizes the web by crawling, independent discoveries, and through the feeds provided by IBM Managed Security Services.
- IBM Managed Security Services is responsible for monitoring exploits related to endpoints, servers (including web servers) and general network infrastructure. This team tracks exploits delivered over the web as well as via other vectors such as email and instant messaging.
- IBM Professional Security Services delivers enterprise-wide security assessment, design and deployment services to help build effective information security solutions.
- IBM QRadar® Security Intelligence Platform offers an integrated solution for security intelligence and event management (SIEM), log management, configuration management, vulnerability assessment and anomaly detection. It provides a unified dashboard and real-time insight into security and compliance risks across people, data, applications and infrastructure.
- IBM Security QRadar Incident Forensics is designed to give enterprise security teams visibility into network activities and clarity around user actions. It can index both metadata and payload content within packet-capture (PCAP) files to fully reconstruct sessions, build digital impressions, highlight suspect content, and facilitate search-driven data explorations aided by visualizations. QRadar Incident Forensics easily integrates with QRadar Security Intelligence Platform and can be accessed using the QRadar one-console management interface.
- IBM Security AppScan® enables organizations to assess the security of web and mobile applications, strengthen application security program management and achieve regulatory compliance by identifying vulnerabilities and generating reports with intelligent fix recommendations to ease remediation. IBM Hosted Application Security Management service is a cloud-based solution for dynamic testing of web applications using AppScan in both pre-production and production environments.

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
Brad Sherrill	Engineering Manager, IBM X-Force Exchange and IBM X-Force Database
Chris Poulin	Research Strategist, IBM X-Force
David Kaplan	Application Security Research Strategist, IBM X-Force Advanced Research
Doug Franklin	Research Technologist, IBM X-Force Advanced Research
Etay Maor	Senior Fraud Prevention Strategist, IBM Security
Jason Kravitz	Techline Specialist, IBM Security
Leslie Horacek	Manager, IBM X-Force Threat Response
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force and Threat Portfolio
Roee Hay	Application Security Group Lead, IBM X-Force Advanced Research
Scott Moore	Software Developer, IBM X-Force

[1] "Russia gang hacks 1.2 billion usernames and passwords," *BBC News Technology*, 6 August 2014. http://www.bbc.com/news/technology-28654613

[2] Natalie Kerris and Trudy Muller, "Apple Media Advisory: Update to Celebrity Photo Investigation," *Apple Press Info*, Accessed 16 February 2015. http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html

[3] "Third-Party Applications and the Snapchat API," *Snapchat*, 14 October 2014. http://blog.snapchat.com/post/99998266095/third-party-applications-and-the-snapchat-api/

[4] Dana Tamir, "Who Hacked Sony? New Report Raises More Questions About Scandalous Breach," *IBM Security Intelligence Blog*, 5 February 2015. http://securityintelligence.com/who-hacked-sony-new-report-raises-more-questions-about-scandalous-breach

[5] 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

[6] Paul Ducklin, "Anatomy of a 'goto fail' - Apple's SSL bug explained, plus an unofficial patch for OS X," *Naked Security*, 24 February 2014. https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/

[7] Michelle Alvarez, "Revelations in data protection in the aftermath of shellshock," *Security Intelligence*, 28 October 2014. http://securityintelligence.com/revelations-in-data-protection-in-the-aftermath-of-shellshock/#.VNjLpGNTcog

[8] Rose Troup Buchanan, "Dropbox passwords leak: Hundreds of accounts hacked after third-party security breach," *The Independent*, 14 October 2014. http://www.independent.co.uk/life-style/gadgets-and-tech/nearly-seven-million-dropbox-passwords-hacked-pictures-and-videos-leaked-in-latest-thirdparty-security-breach-9792690.html

[9] Lisa Vaas, "Carwash POS systems hacked, credit card data drained," *Naked Security*, 25 June 2014. https://nakedsecurity.sophos.com/2014/06/25/carwash-pos-systems-hacked-credit-card-data-drained

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

[11] "Exchange hacked - stolen passwords and documents," *Niebezpiecznik*, 23 October 2014. http://niebezpiecznik.pl/post/gielda-papierow-wartosciowych-zhackowana/

[12] Mark Stockley, "Millions of Drupal websites at risk from failure to patch," *Naked Security*, 30 October 2014. https://nakedsecurity.sophos.com/2014/10/30/millions-of-drupal-websites-at-risk-from-failure-to-patch/

[13] Claire Reilly, "Aussie Travel Cover hack exposes details of 770,000 customers," *CNET*, 20 January 2015. http://www.cnet.com/au/news/aussie-travel-cover-hack-exposes-customer-details/

[14] Kate Knibbs, "Report: Mysterious Russian Malware Is Infecting 100,000+ Wordpress Sites," *Gizmodo*, 15 December 2015. http://gizmodo.com/mysterious-russian-malware-is-infecting-over-100-000-wo-1671419522

[15] Stephanie Mlot, "DDoS Attack Puts Code Spaces Out of Business," *PCMag*, 19 June 2014. http://www.pcmag.com/article2/0,2817,2459765,00.asp

[16] Adrian Weckler, "Eircom forced to shut email services after hacking breach," *Indpendent.ie*, 5 January 2015. http://www.independent.ie/business/technology/eircom-forced-to-shut-email-services-after-hacking-breach-30234537.html

[17] Ionut Ilascu, "City of Phoenix Computers Under DDoS Attack," *Softpedia*, 28 October 2014. http://news.softpedia.com/news/City-of-Phoenix-Computers-Under-DDoS-Attack-463286.shtml

[18] Lily Hay Newman, "Evernote and Feedly Are Recovering After Sustained Hacker Attacks," *Future Tense*, 11 June 2014. http://www.slate.com/blogs/future_tense/2014/06/11/evernote_and_feedly_were_down_because_of_a_ddos_attack.html

[19] Ms. Smith, "Ransomware: City of Detroit didn't pay, TN sheriff's office did pay to decrypt," *Network World*, 19 November 2014. http://www.networkworld.com/article/2850052/microsoft-subnet/ransomware-city-of-detroit-didnt-pay-tn-sheriffs-office-did-pay-to-decrypt.html

[20] Rick M. Robinson, "Wiper Malware Poses Destructive Threat," *Security Intelligence*, 21 January 2015. http://securityintelligence.com/wiper-malware-poses-destructive-threat/#.VNDlQmPVuhM

[21] Pamela Cobb, "German Steel Mill Meltdown: Rising Stakes in the Internet of Things," *IBM Security Intelligence Blog*, 14 January 2015. http://securityintelligence.com/german-steel-mill-meltdown-rising-stakes-in-the-internet-of-things

[22] Benjamin Elgin and Michael A. Riley, "Nuke Remark Stirred Hack on Sands Casinos That Foreshadowed Sony," *Bloomberg Business*, 11 December 2014. http://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony

[23] Eset Research, "Sednit espionage group now using custom exploit kit," *welivesecurity*, 8 October 2014. http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/

[24] Jaime Blasco, "Scanbox: A Reconnaissance Framework Used with Watering Hole Attacks," *AlienVault*, 28 August 2015. https://www.alienvault.com/open-threat-exchange/blog/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks

[25] Dana Tamir, "Massively Distributed Citadel Malware Targets Middle Eastern Petrochemical Organizations," *IBM Security Intelligence Blog*, 15 September 2014. http://securityintelligence.com/massively-distributed-citadel-malware-targets-middle-eastern-petrochemical-organizations

[26] Brian Krebs, "ZeuS Source Code for Sale. Got $100,000?" *Krebs on Security*, February 2011. http://krebsonsecurity.com/2011/02/zeus-source-code-for-sale-got-100000/

[27] Brian Krebs, "'Citadel' Trojan Touts Trouble-Ticket System," *Krebs on Security*, 23 January 2012. http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/

[28] Etay Maor, "Going Global: New Citadel Trojan Automatically Localizes Fraud Content," *IBM Security Intelligence Blog*, 30 June 2014. http://securityintelligence.com/new-citadel-trojan-automatically-localizes-fraud-content-global

[29] Dana Tamir, "Cybercriminals Use Citadel to Compromise Password Management and Authentication Solutions," *IBM Security Intelligence Blog*, 19 November 2014. http://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions

[30] "PhoneGap / Apache Cordova," *AppBrain: Stats*, Accessed 16 February 2015. http://www.appbrain.com/stats/libraries/details/phonegap/phonegap-apache-cordova

[31] Marcel Kinard, "Apache Cordova Android 3.5.1," *Cordova*, 4 August 2014. http://cordova.apache.org/announcements/2014/08/04/android-351.html

[32] Roee Hay, "Apache Cordova Vulnerability Discovered: 10% of Android Banking Apps Potentially Vulnerable," *IBM Security Intelligence Blog*, 5 August 2014. http://securityintelligence.com/apache-cordova-phonegap-vulnerability-android-banking-apps

[33] "Cordova vulnerability," *Google Groups*, October 2014. https://groups.google.com/forum/#!topic/android-security-discuss/FC3bMzY83dc

[34] "CVE Content Decisions Overview," *CVE*, 27 October 2011. https://cve.mitre.org/cve/editorial_policies/cd_overview.html

[35] Will Dormann, "Vulnerability Note VU#582497: Multiple Android applications fail to properly validate SSL certificates," *CERT*, 8 December 2014. https://www.kb.cert.org/vuls/id/582497

[36] Will Dormann, "Announcing CERT Tapioca for MITM Analysis," *CERT*, 21 August 2014. http://www.cert.org/blogs/certcc/post.cfm?EntryID=203

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2015

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

WGL03073-USEN-00