IBM X-Force 2013
Mid-Year Trend and Risk Report

September 2013

Contributors

Producing the IBM X-Force Trend and Risk Report is a dedication in collaboration across all of IBM. We would like to thank the following individuals for their attention and contribution to the publication of this report.

Contributor	Title
Brad Sherrill	Manager, X-Force Data Intelligence
Carsten Hagemann	X-Force Software Engineer, Content Security
Chris Meenan	Product Manager QRadar Vulnerability Manager
Chris Poulin	Security Strategist - Critical Infrastructure
Cynthia Schneider	Technical Editor, IBM Security Systems
Dr. Jens Thamm	Database Management Content Security
Jason Kravitz	Techline Specialist for IBM Security Systems
Leslie Horacek	X-Force Threat Response Manager
Marc Noske	Database Administration, Content Security
Mark E. Wallis	Senior Information Developer, IBM Security Systems
Mark Yason	X-Force Advanced Research
Michael Hamelin	X-Force Security Architect
Paul Sabanal	X-Force Advanced Research
Perry Swenson	X-Force Marketing Manager
Ralf Iffert	Manager X-Force Content Security
Robert Freeman	Manager, X-Force Advanced Research
Scott Moore	X-Force Software Developer and X-Force Data Intelligence Team Lead
Yong-Chuan Koh	X-Force Advanced Research

About this report
This X-Force® report provides insights into some of the most significant challenges facing security professionals today. Read this report for an in-depth analysis of the latest security threats and trends.

About IBM X-Force
IBM X-Force® research and development teams study and monitor 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 X-Force Report Contributors

The X-Force trend and risk report contributors represent a broad spectrum of security competency, including:

- 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 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 (MSS).
- The IBM security software development team offers one of the most advanced and integrated portfolios of enterprise security products. The portfolio provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more.

Contents

Contents

Executive overview

As we look back at the first half of 2013, it is clear that successful tactics implemented by attackers continue to challenge enterprises to keep up with security basics.

Social media has become a top target for attacks and mobile devices are expanding that target. We witnessed continued efforts to reach security savvy companies and saw how relatively new techniques take advantage of trusting users by compromising websites they frequent. Distributed denial-of-service (DDoS) attacks are being used as a distraction; allowing attackers to breach other systems in the enterprise while IT staff are forced to make difficult risk-based decisions, possibly without visibility of the full scope of what is occurring.

IBM X-Force continues to see operationally sophisticated attacks as the primary point of entry. Some of these were attacks of opportunity, where unpatched and untested web applications were vulnerable to basic SQL injection (SQLi) or cross-site scripting (XSS) exploitation. Others were successful because they violated the basic trust between end user and sites or social media personalities thought to be safe and legitimate.

Many of the breaches reported in the last year were a result of poorly applied security fundamentals and policies and could have been mitigated by putting some basic security hygiene into practice. Attackers seem to be capitalizing on this "lack of security basics" by using a model of operational sophistication that allows them to increase their return on exploit. The idea that even basic security hygiene is not upheld in organizations, leads us to believe that, for a variety of reasons, companies are struggling with a commitment to apply basic security fundamentals.

Watering hole attacks, which have continued, are a great example of how operational sophistication is being used to reach targets not previously susceptible. This type of campaign involves a form of targeted attack in which the attacker identifies a website that a select group is known to visit. By compromising the central site and using it to serve malware, attackers are able to reach more technically savvy victims who may not be fooled in phishing attempts, but who do not suspect that the sites they trust could be malicious. Several high tech companies, as well as government agencies have been successfully breached in past months.

Additional operational sophistication was seen in the attack of major global corporations by breaching franchises or local language sites in countries outside of corporate headquarters. Often these satellite sites are not secured with the same standard as the home office. By going after a weaker point of entry into larger enterprises, attackers were able to reach and tarnish well-known brands. This can damage a brand's reputation and create legal issues if sensitive customer data is leaked. These types of leaks affected the food industry, consumer electronics, automotive, and entertainment industries in particular.

Attackers have demonstrated enhanced technical sophistication in the area of distributed-denial-of-service (DDoS) attacks. DDoS methods per se are not advanced, but the method for increasing the amounts of capable bandwidth is a new and powerful way to halt business by interrupting online service. The banking industry was hit particularly hard in the first half of 2013. Attackers in June 2013 began to focus their attention on domain name system (DNS) providers. Attacks on the DNS providers are another example of compromising central strategic targets. There are several ways these attacks can be disruptive and we explore those in the breach section of this report.

Another growing trend this year is the takeover of social media profiles that have a large number of followers. This trend continues to play a pivotal role in the way attackers are reaching their targets. Social media introduces sociological challenges that open the door to security exploitation and we see the same abuses of trust that were effective three years ago are still relevant today, begging the question, have we learned anything about trust and social media?

Social media exploits affect more than individuals; they can negatively impact enterprise brand reputation and cause financial losses. We take a look at some different ways social influence can be used to catch people unaware and even cause damage in the offline world.

Mobile devices are still a lucrative target for malware authors. Although mobile vulnerabilities continue to grow at a rapid pace, we still see them as a small percentage of overall vulnerabilities reported in the year. One significant development for mobile vulnerabilities is that fewer than 30 percent of all mobile disclosures have public exploits or proof-of-concept code available. Most of these exploits are targeted specifically towards mobile applications and are primarily disclosed on popular public exploit repositories.

Android devices are enjoying a rapid growth, and with that growing market, there is a renewed interest by malware authors to capitalize on this increase of possible victims. 2013 witnessed the release of a trojan named Obad which demonstrated new technically sophisticated features that made it stand out. X-Force believes this release is significant in that it shows how malware authors are investing more effort into creating Android malware that are more resilient and dangerous.

In the first half of 2013, publicly reported security vulnerabilities are tracking to be on par with what was disclosed in 2012. Again in the first half of the

year, more than half of all web application vulnerabilities that were reported publicly were cross-site scripting (XSS) vulnerabilities. The X-Force database team reports that content management system (CMS) vendors continue to improve their patching rates. However, the third-party vendors creating plug-ins for CMS platforms have not shown improvement. With over 46 percent of vulnerabilities left unpatched, third-party plug-ins attract many opportunities for attacks to occur and in fact were known entry points into various breaches in the last year.

With respect to the exploitation of vulnerabilities, we watched in the first six months of the year as several zero-day vulnerabilities affecting widely deployed software were exploited in the wild. Most of the zero-day exploits were initially found in targeted attacks, and we witnessed how much attackers are willing to invest in these attacks when sophisticated zero-day exploits bypassed modern security mechanisms in software. Microsoft Internet Explorer and Oracle Java were hit particularly hard.

Later in our report we provide an update on web trends, spam and phishing, which all remained comparatively flat in the last six months. The country of Belarus became the top distributing country for spam in the first part of the year, pushing the U.S. out of the top spot.

Finally, in an effort to continue the renewed focus on security practices, we discuss the challenges so many enterprises face when it comes to vulnerability management. Despite vulnerability management having long been a core requirement of every organization's security practices, the primary reason for this struggle is the sheer number and rate of new vulnerabilities being introduced into environments. We discuss some ways to help system administrators do a better job to help them with securing the enterprise.

Let's review how the first part of this year came about.

2013 mid-year highlights

Targeted attacks and data breaches

- Based on the incidents we have covered, SQL injection (SQLi) remains the most common breach paradigm and in the first half of 2013, security incidents have already passed the total number reported in 2011 and are on track to surpass 2012 by the end of year. (page 12)
- The Watering Hole attack category has been used by attackers to successfully breach several high tech companies and government groups by injecting browser exploits on websites frequently visited by targeted employees. These exploits which can lead to trojan malware installation are successful because they break a certain layer of trust between the target and what they believe to be a legitimate and safe website.(page 15)
- The takeover of notable social media accounts with a large number of followers is another growing trend this year. If a Twitter user with millions of followers is able to send a link to an infected site, it greatly increases the odds that some percentage of people will click on it, unaware that it is malicious. Aside from surprising end users and infecting computers, breaking the trust of online profiles can also be used to cause damage offline. (page 16)
- A wave of data breaches which target international branches of large businesses, corporations and franchises takes advantage of the fact that satellite and local language websites representing their brand are not always secured to the same standard as the home office. These types of incidents affected the food, automotive, entertainment and consumer electronics industries, and can result in a reputation hit as well as legal implications from the loss of sensitive customer data. (page 17)
- Recapping some of the other security incident highlights, high volume distributed denial-of-service (DDoS) attacks against prominent targets persisted from 2012 into the first half of 2013. The banking industry has been heavily attacked, causing downtime and business interruptions for online banking customers. (page 17)
- Domain name system (DNS) amplification attacks are turning legitimate DNS Providers into unwilling accomplices as high bandwidth assaults leveraging open DNS resolvers exhaust resources and affect thousands of customers. (page 18)

Social and mobile

Social media

- Social media exploits affect more than individuals; they can negatively impact enterprise brand reputation and cause financial losses (page 19)
- Because attackers have learned to monetize social media vulnerabilities, a black market has cropped up to trade compromised and fabricated accounts on social media sites (page 22)
- Technology controls are in place, but are often either not enabled or are circumvented by the user's extended network. The only effective defense is education and to engender suspicion (page 22)

Mobile—Android malware

- With the growth of Android, more attention has been generated by malware authors hoping to capitalize on that growth. One example is Chuli malware, discovered in March 2013. This malware was considered a highly targeted attack and only intended for specific individuals, but the existence indicates that Android users are increasingly becoming viable targets for these types of sophisticated attacks with strong intent related to specific organizations. (page 24)

- Obad, a trojan that was mostly spread through short message service (SMS) spam, gained attention in June 2013 when it was dubbed "The most sophisticated Android trojan." Some features that made it stand-out were anti-analysis techniques, code obfuscation, device administration and the ability to spread through Bluetooth. We believe it is significant in that it shows how malware authors are investing more effort into creating Android malware that are more resilient and dangerous. (page 25)
- Even though new security enhancements are being developed to combat against Android malware, X-Force still believes that OS fragmentation (older versions that are being used as much as newer ones) will remain a problem. (page 27)

Vulnerabilities and exploitation

Vulnerability statistics

- In the first half of 2013, X-Force reported the addition of just over 4,100 new publicly reported security vulnerabilities into the database. If the trend continues, the total projected year end count looks to be nearly the same number of 8,200 vulnerabilities reported in 2012. (page 34)
- Again in the first half of 2013, more than half of all web application vulnerabilities reported publicly were cross-site scripting (XSS) vulnerabilities. However, the web application vulnerabilities category only represented 31 percent of overall vulnerabilities. This number is down significantly from 2012 when we saw levels at 42 percent. (page 35)
- Content Management Systems (CMS) are some of the most popular software applications used on the World Wide Web. Year over year we see vendors doing a better job of keeping their products patched as 78 percent of all vulnerabilities in CMS software have been patched in the first half of 2013 versus only 71 percent patched in 2012. (page 36)
- Third-party creators of CMS plug-ins did not fare as well in patching as core vendors with only 54 percent of plug-in vulnerabilities patched—leaving 46 percent of those vulnerabilities unpatched and an attractive target for attackers. (page 36)
- **MOBILE:** Although vulnerabilities affecting mobile applications and operating systems represent a relatively small percentage of total disclosures (projected at just over 4 percent in 2013), we have seen the total number of disclosures increase significantly since 2009 when mobile vulnerabilities represented less than 1 percent of the total disclosures. (page 37)
- **MOBILE:** One significant development of note regarding mobile vulnerabilities in 2013 had to do with the number of public exploits available. In 2013, fewer than 30 percent of all mobile disclosures have public exploits or proof-of-concept code available. In comparison, only 9 percent of mobile vulnerabilities disclosed between 2009 and 2012 had public exploits. Most of these exploits are specifically targeted toward mobile applications and are primarily disclosed on popular public exploit repositories. (page 37)
- X-Force categorizes vulnerabilities by the consequence of exploitation. This consequence is essentially the benefit that exploiting the vulnerability provides to the attacker. The most prevalent consequence of vulnerability exploitation for the first half of 2013 was "gain access" at 28 percent of all vulnerabilities reported. Cross-site scripting (XSS) was the second most prevalent consequence at 18 percent and typically involves attacks against web applications. (page 38)

Exploitation

- In the first half of 2013, X-Force issued 14 alerts and advisories on disclosures that deserved close attention. We placed seven of these alerts and advisories, coincidentally comprised entirely of Internet Explorer (IE) and Java, in the top-right quadrant of the matrix—which indicates vulnerabilities that have a high rate of return for attackers who develop ways to exploit them. The seven listed vulnerabilities can all be used in drive-by exploitation, reaching as many victims as possible. (page 41)
- In the first six months of the year, several zero-day vulnerabilities affecting widely deployed software were found to be exploited in the wild. Most of the zero-day exploits were initially found in targeted attacks, and we witnessed how much attackers are willing to invest in these attacks when sophisticated zero-day exploits bypassed modern security mechanisms in software. (page 28)
- As highlighted in the breach section, watering hole attacks using zero-day exploits are on the increase. This type of campaign involves a form of targeted attack in which an attacker identifies the websites a targeted group usually visits or will most likely visit and then compromises those websites so they become the launch pads of the attack. IBM X-Force provides some recommendations for website administrators to help lower the risk of compromise. (page 28)

Web trends, spam and phishing

- Twenty-three percent of all malicious links hosted on the Internet are located on pornography sites. However, blogs which provide dynamic websites with the ability to add content also allow bad actors to place malicious links on the sites 16.5 percent of the time. (page 45)
- The top malware hosting country is the United States, with over 42 percent of all malicious links hosted there. Following the U.S. we see Germany hosting nearly 10 percent and then China, Russia, the Netherlands, the United Kingdom and France hosting the remainder of malware between 5.9 and 3.4 percent. (page 46)
- Nearly one third of all botnet command and control (C&C) servers are hosted within the United States. In second place is Russia at nearly 10 percent. (page 47)
- Within the top 100 most used websites, IPv6 deployments continue to increase, and in the last six months they have already grown by 10 percent as compared to the 2012 year-end numbers. (page 48)

Spam and phishing

- Belarus becomes the top country for distributing spam, by sending out more than 10 percent in the second quarter of 2013. Earlier in the year, the first position was held by the United States, which sent out 12 percent but then dropped below Belarus to eight percent in the second quarter. Rounding out the top five spam sending countries of origin were Spain, India, and Argentina. (page 49)
- The top three areas enticing users to click on bad links and attachments are: emails that look like they are coming from Internet payment companies, social networks, and internal scanners or fax devices. Together these three focus areas represent more than 55 percent of all scam and phishing incidents. (page 50)

Security practices

- Many security teams continue to struggle with vulnerability management despite it having long been a core requirement of every organization's security practices. The primary reason for this struggle is the sheer number and rate of new of vulnerabilities being introduced into environments by operating system software and third-party applications, and the relatively manual and slow process of mitigating and/or patching these weaknesses. Typical networks can expect to see on average anywhere between 10 and 30 vulnerabilities per IP address in their environment; some will have none, and some will have hundreds, with the numbers changing daily. (page 52)

For more information

To learn more about IBM X-Force, please visit:
http://www-03.ibm.com/security/xforce/

Targeted attacks and data breaches

State of security incidents in 2013

Browsing through mainstream media, we find articles about data breaches and security incidents on a regular basis. While the media coverage has greatly expanded in recent years, the number of total incidents is also measurably rising. 2012 was a record year for reported data breaches and security incidents, with a 40 percent increase in total volume over 2011.[1] In the first half of 2013, security incidents have already surpassed the total number reported in 2011 and are on track to surpass 2012.

This year kicked off with a number of high profile sophisticated attacks on major websites, media, and tech companies. In the IBM X-Force 2012 Trend and Risk Report, we discussed the idea of operational sophistication versus technical sophistication. Throughout the first half of 2013, we observed a continuation of this trend in both the type of breaches that have occurred and the motivations behind them.

Operational sophistication versus technical sophistication

The attraction of operational sophistication is that attackers can use a path of least resistance to gain a maximum return on exploits. This translates to the use of tried and true techniques like SQL injection (SQLi), cross site scripting (XSS) and spear phishing, as well as exploiting platforms that reach a larger number of cross-browser and cross-operating system targets such as Adobe Flash and the Java browser plugin. Target reconnaissance continues to greatly benefit from publicly available information located within social media profiles or other confidential documents that have been unintentionally indexed on public facing websites and discoverable through common search engines. Figure 1 shows several examples of how attackers are using operational sophistication to breach targets.

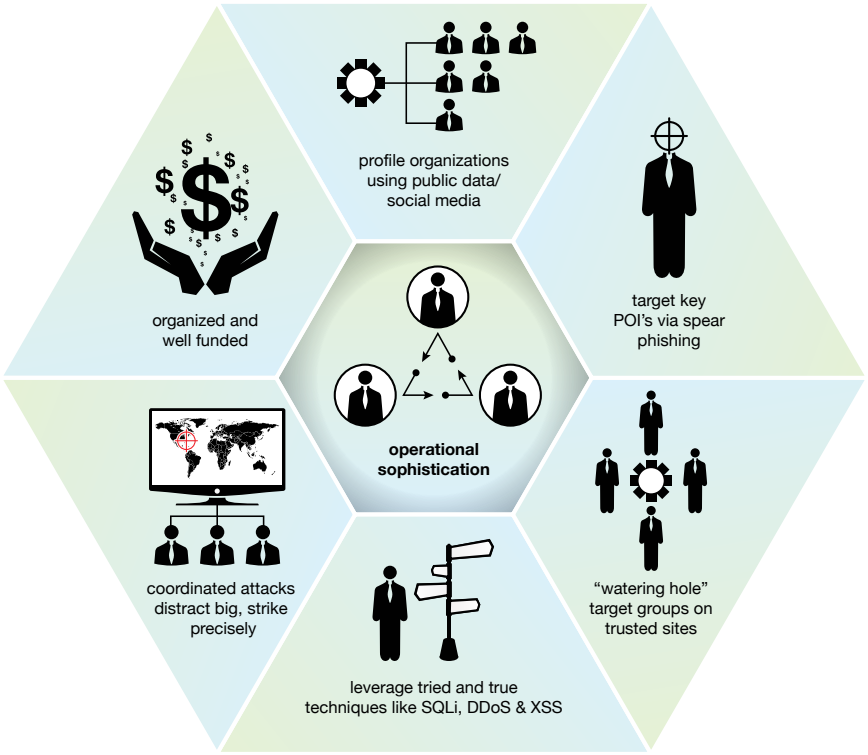


Figure 1: 2013 Methods of Operational Sophistication

1 http://datalossdb.org/statistics

In contrast, technical sophistication relies on using advanced attacks such as zero-day vulnerabilities and in some cases, custom exploitation techniques. While technical sophistication exists, it is atypical.

Figure 2 illustrates a sampling of data breaches from the first half of 2013. When tracking publicly disclosed breaches, we determine the attack type by one of two primary ways. The first is through a notice from the company, usually in an official letter or statement to customers explaining the situation, and the second is through a data dump, in which the attacker discloses the vulnerability used to gain entry.

One positive development is that companies have been more proactive in 2013[2] about alerting their customers when an incident has occurred. In several cases, with large online companies, all user account passwords were automatically reset or invalidated. This honesty in disclosure and prompt action is helpful in mitigating the impact of breaches, both in terms of technical damage and brand reputation.

Based on the incidents we have covered, SQL Injection (SQLi) remains the most common breach paradigm. We have not been surprised by this as SQLi is the most direct way to gain access to records in the database. In terms of return on exploit, SQLi is an effective attack of opportunity, where automated scripts can scan wide ranges of potential targets that run common web application software with known SQLi vulnerabilities. Several of the incidents displayed in Figure 2 were the result of unpatched or vulnerable web forums or other widely used third party products.

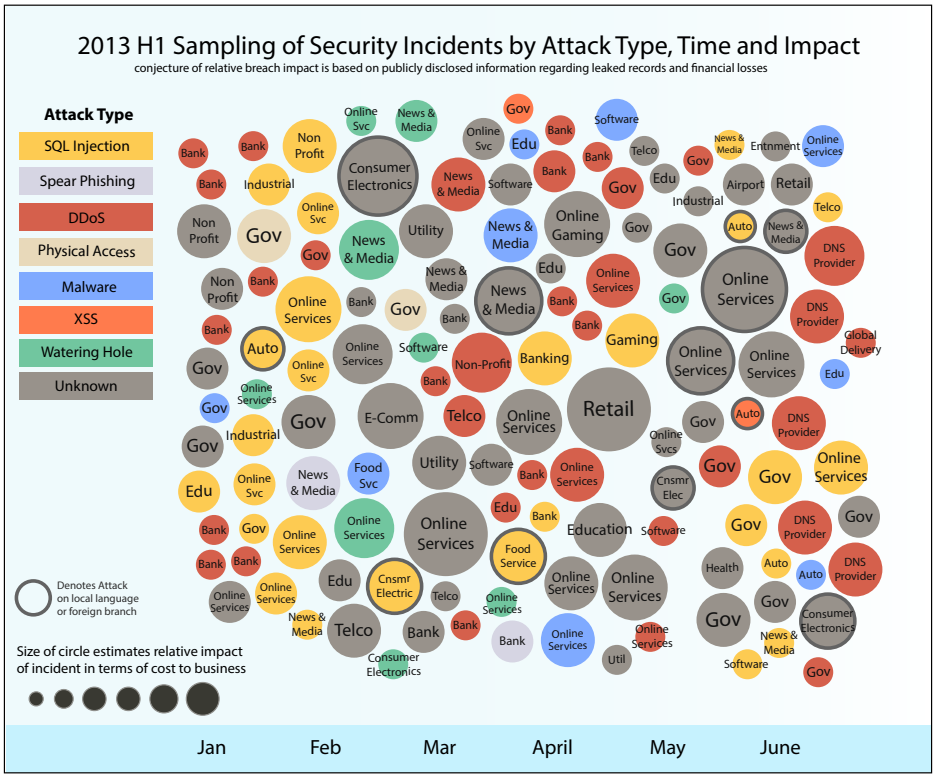


Figure 2: 2013-H1 Sampling of Security Incidents by Attack Type, Time and Impact

2 http://www.wired.co.uk/news/archive/2013-03/04/evernote-hacked

Incidents that involved attack-type malware were at times the result of companies discovering malicious software on one or more critical servers. These in turn resulted in the disclosure[3] of a possible breach, in some cases proactively, even if further impact was not immediately discernible.

Distribution of malware to consumer and corporate users is still highly effective due to vulnerabilities in browsers and browser plugins. A troubling development, first reported in April, is the proliferation of a rogue Apache web server module dubbed Darkleech,[4] which to date has compromised over 40,000 websites, turning them into malware hosts capable of infecting end-user systems with exploit kits such as Blackhole. There is no definitive correlation between all the infected web servers. It seems that in some, though not all cases, vulnerabilities in Plesk cPanel were used to gain entry.

Darkleech, as well as another similar (possibly the same), backdoor called Linux/CdorkedA,[5] are a new class of threat which use technical sophistication in how they are deployed, and in how they are able to run stealthily. For example, one advanced feature is how the malware behaves when an end user visits an infected website. Rather than blindly redirect to the exploit kit for every visitor, as was the case in older drive-by-download scenarios, the software uses advanced IP address tracking to selectively target visitors. There is a whitelist and blacklist feature which provides the ability to hide itself from security researchers and scanners, making detection more difficult.

While providing remote access and snooping through sensitive data are common objectives, malware can also be used for more destructive purposes. In March, in what appears to have been a coordinated effort against several South Korean[6] television stations and banks, a malicious program called Jokra disabled end-user systems, causing permanent damage by wiping the master boot record on affected hard drives.

While remote malware is prevalent, physical access is still a factor in several noted breaches. This could be the result of insiders stealing data, or of the loss of unencrypted assets like old drives, laptops, or mobile devices. These types of incidents are not always maliciously motivated. A mistake in printing retirement information led to U.S. social security numbers[7] being visible in the clear window of the mailing envelope, putting sensitive data at risk. Inadvertent loss of data from human error is not uncommon.

3 http://www.salemnews.com/local/x1533629707/SSU-data-breach-affects-25-000
4 http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/
5 http://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
6 http://www.infoworld.com/d/security/symantec-finds-linux-wiper-malware-used-in-s-korean-attacks-214965
7 http://blogs.newsobserver.com/business/26000-nc-retirees-warned-of-security-breach

As illustrated in Figure 3, in the breaches tracked by IBM X-Force and in terms of the country where the attack target was located, the United States is the country with the most disclosed breaches by a large margin. This could be based on the fact that many websites are operated from the United States, or possibly that it is more common that U.S. companies and websites are disclosing publicly.

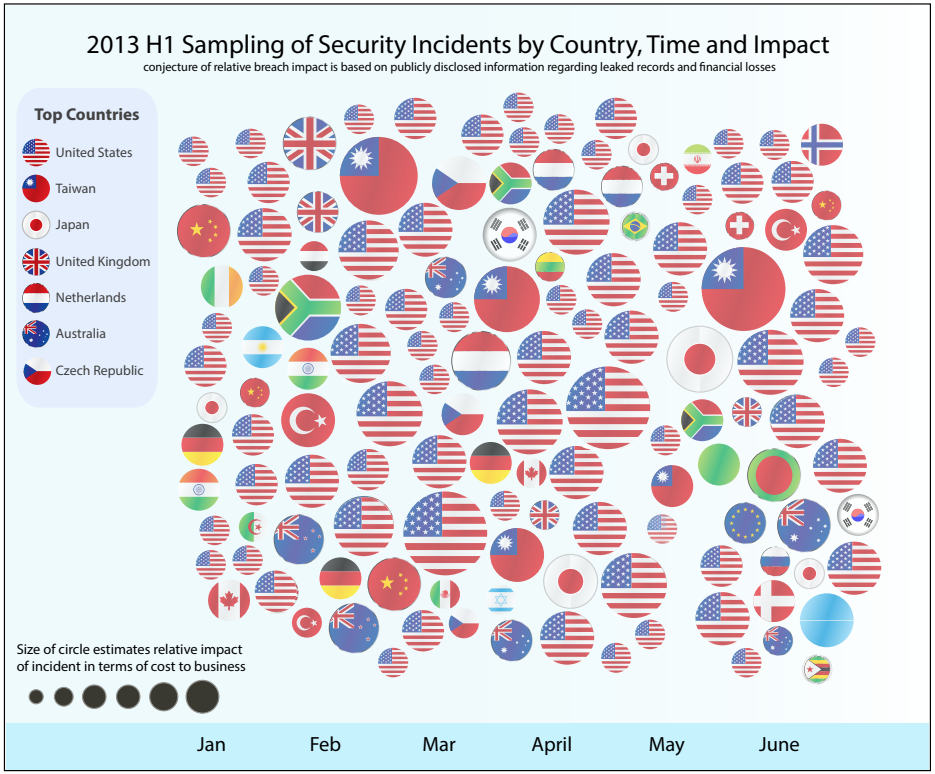


Figure 3: 2013-H1 Sampling of Security Incidents by Country, Time and Impact

Watering hole attacks continue to increase

A relatively recent attack type—and newly debuting on our charts this time—is the watering hole attack. Attackers have successfully breached several high tech companies[8] by injecting browser exploits on websites frequently visited by targeted employees. These exploits lead to trojan malware installation. This same type of attack has also been used this year to target government employees.[9] For a more detailed explanation of watering hole attacks, see the topic titled "Zero-Day Attacks in 2013 H1."

Watering hole attacks are good examples of operational sophistication because they reach a large number of select targets by compromising a single centralized location. In contrast, with spear phishing for example, an attacker has to individually connect with a larger group of people and only a small percentage might be successfully compromised. Often these attacks are successful because there is enough traffic from target organizations, and by nature they break through a certain layer of trust between the target and what the target believes is a legitimate and safe website.

8 http://threatpost.com/why-watering-hole-attacks-work-032013/77647
9 http://news.softpedia.com/news/Cybercriminals-Behind-DOL-Watering-Hole-Attack-Target-USAID-Employees-353138.shtml

This pattern of compromising centralized strategic targets, which then in turn can be used to reach a broader base of targets, is repeated in a variety of different attack vectors. IBM X-Force has highlighted some of these types of attacks in previous reports. For example, attacking a known security vendor with the aim of comprising two-factor authentication tokens, compromising code signing certificates from software vendors, and attacking SSL certificate providers in order to intercept encrypted traffic.

Additionally, there have been a few other notable incidents in which attackers have compromised centralized strategic targets. Malicious content serving malware was injected into the pages of several prominent, highly trafficked websites such as the LA Times, National Journal, Toyota Japan, and MSI Electronics. In June, the makers of the Opera web browser[10] reported that they were targeted in an attack that resulted in at least one of their code certificates being compromised. This meant that for a small window of time, people who thought they were downloading a legitimate, signed version of the browser might have downloaded malware.

Another growing trend this year is the takeover of notable social media accounts with a large number of followers. If a Twitter user with millions of followers is able to send a link to an infected site, it greatly increases the odds that some percentage of people will click on it, unaware that it is malicious.

Aside from infecting computers or end users, breaking the trust of online profiles can also be used to cause damage offline. In April, when a compromised Associated Press[11] account sent out false information about explosions at the White House, the stock market was impacted, resulting in a temporary drop of 143 points. The ability of a single attack to influence the actions of millions of people in real time is alarming. We discuss the psychology of **Social Media** attacks in the next section of this report.

10 http://www.scmagazine.com/maker-of-opera-browser-said-its-network-was-hacked-to-steal-code-signing-certificate/article/300580/
11 http://mashable.com/2013/04/23/ap-hacked-white-house/

Disenfranchised—compromised websites far from home

Last year X-Force reported on data breaches at international branches of large businesses and corporations, and in 2013 there was a new round of similar targeted attacks. Companies often have local language websites representing their brand, but these sites are not always secured with the same standard as the sites at the home office. Such was the case with several well-known brands that suffered damage to their reputation as well as legal implications for leaking large amounts of customer data. These types of leaks affected the food, consumer electronics, automotive, and entertainment industries in particular. Several circles in the chart in Figure 2 have a dark gray border around them. These are indicative of companies who experienced a security incident at a foreign branch or localized language site.

In many cases, including several of the customer data leaks in the food industry last year, the same group has claimed credit, indicating a specialty in this type of target.[12, 13, 14, 15, 16]

Often times, the point of entry was a sub-site setup for promotional purposes where customers sign-up to win something by providing personal information in the process. These types of temporary pages are a lucrative target considering that a major food or entertainment brand might reach many millions of customers in local regions. When these sub-sites are quickly deployed without proper security controls, such as secure web forms and encrypted passwords, the result of a data leak can be damaging.

Overall, as in previous years, a large percentage of all breaches tracked by X-Force were due to a lapse in basic security fundamentals. In a previous report, X-Force discussed how to properly secure encrypted passwords before storing them in a database. While many of the breaches in 2013 reported that their passwords were securely stored, it is disconcerting that several targets were still storing passwords in clear text. These were not unsophisticated businesses, but rather universities, government groups including police departments, banks, web host providers, and even self-proclaimed security and privacy based companies. The result of this lapse in fundamental web security is that when a database is leaked with an email address and clear text password, anyone who is reusing passwords on multiple sites is at risk. It is also worth noting that when large batches of real-world password data is uncovered, they are added to password lists which can then be used to brute force and crack users accounts against future targets.

Distributed denial of service (DDoS) targeted at banking industry continues

Recapping other security incident highlights, high volume distributed denial-of-service (DDoS) attacks against prominent targets persisted from 2012 into the first half of this year. The banking industry has been heavily attacked, causing downtime and business interruptions for online banking customers. Spamhaus,[17] a non-profit organization dedicated to tracking spam abuse, was hit with what some consider to be the largest DDoS attack in the world, with traffic rates reported as high as 300 Gbps. These high bandwidth DDoS attacks escalated last year and continue to present a challenge in terms of successful attack mitigation. DDoS incidents also continue to provide an excellent distraction technique where the true motivation is to breach systems under the cover of the DDoS attack.

12 http://www.cyberwarnews.info/2013/07/13/sony-italy-hacked-over-40k-personal-details-leaked/
13 http://www.cyberwarnews.info/2013/06/20/samsung-kazakhstan-social-hub-domain-hacked-62235-accounts-leaked/
14 http://www.cyberwarnews.info/2013/08/22/fast-food-giant-pizza-hut-spain-and-malta-hacked-data-leaked-site-redirected/
15 http://www.cyberwarnews.info/2013/03/31/official-mtv-taiwan-hacked-607286-account-credentials-leaked/
16 http://www.cyberwarnews.info/2013/03/28/official-mcdonalds-austria-taiwan-korea-hacked-over-200k-credentials-leaked/
17 http://www.informationweek.com/security/attacks/spamhaus-ddos-suspect-arrested/240153788

Domain Name System (DNS) amplification attacks

An interesting emerging trend in DDoS targets has been unfolding since June where many DNS providers have reported service interruptions and downtime.[18] Targeting the DNS provider is another example of the pattern of attacking a centralized strategic target to reach a larger group of potential victims. There are several ways this can be disruptive. The first and most obvious is that if the DNS provider is unreachable,[19] due to a successful DDoS, any site relying on that DNS for its domain will be impacted as well. The second is that if attackers can breach the DNS provider by DNS Hijacking,[20] then they can redirect web addresses to alternate servers that can then be used for phishing or to distribute malware. DNS providers were also targeted simply to use the DNS as a stepping stone to attack other targets. By abusing open DNS Resolvers, attackers are able to carry out DNS Amplification attacks against other targets. These types of attacks are effective because the attacker is able to send out a smaller amount of traffic, which results in a larger response packet getting sent to the spoofed source or to the target of the DDoS attack. The DNS providers become unwilling accomplices in this process by responding to what seem like legitimate requests until their bandwidth is exceeded.

As the scope and frequency of data breaches continue in an upward trajectory, it is more important than ever to get back to basic security fundamentals. Throughout this report we look at many facets of secure computing from both the IT and network administrative perspectives, and for end users. While technical mitigation is a necessity, educating users within the enterprise that security is a mindset, not an exception, can also reduce these incidents.

One of the more interesting topics we will discuss is how social media has expanded as a platform for exploitation, and how employees and companies can be more alert against potential threats.

18 http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-outages.html
19 http://www.theregister.co.uk/2013/07/18/netsol_ddos/
20 http://www.zdnet.com/linkedin-just-one-of-thousands-of-sites-hit-by-dns-issue-cisco-7000017124/

Social and mobile

Social media—targeting users and abusing trust

The psychology of risky social media behavior

Social media is a relatively new sociological construct, and yet it's been incorporated at a phenomenal pace as an extension of our real world presence; an additional sense used to communicate our thoughts, activities, locations and even feelings.

The risk of this rapid integration, which is also fueled by the expansion of mobile devices into our lives, is that we don't fully understand how to interpret the subtleties of interaction online in the same way our brains have adapted to analyzing non-verbal communication, such as body language, micro expressions,[21] and how we respond to cultural and paralinguistic elements. Despite these critical nuances in communications we grant trust to online personalities we've never met—and who may be deceased[22] or completely fictitious. Users ignore their better judgment in favor of building a large network, with the status that comes with it, and the promise of gaining access to opportunities that are obviously too good to be true.

Attackers understand these weaknesses and are starting to learn how to exploit them effectively. Social attacks, which are more human and personal, can be crafted to reference relevant topics of interest and current events. Attackers are taking a page from marketing organizations in professional enterprises and leveraging metrics such as return on investment (ROI) and search engine optimization (SEO) to gain higher click through rates with maximum reach, and ultimately optimize their capital gain.

We expect to see the skill in psychological manipulation become more sophisticated as attackers create complex internetworks of identities and refine the art of deceiving victims.

Economic and reputational impact

The widespread adoption of social media, both in personal and business circles, makes it much more pervasive in the enterprise and necessary to attract new talent as well as promote the business. Instead of trying to block access to social media, businesses must think about how to monitor and mitigate abuses of these platforms.

In April of 2013, sixty characters cost the U.S. stock market $200,000,000,000. Yes, that's two hundred billion. From a single tweet!

That should put to rest the argument that social networks are solely useful for teens to broadcast pictures of themselves and for your aunt to share motivational weight loss quotes.

21 http://www.paulekman.com/micro-expressions/
22 http://www.businessinsider.com/deceased-liking-stuff-on-facebook-2012-12

The "flash crash" was instigated when the main news wire Twitter account of the Associated Press[23] (AP) was hacked and the perpetrators tweeted, "*Breaking: Two Explosions in the White House and Barack Obama is injured*." The incident underscores the trust that the general public puts in the information shared on social networks.

The AP was not the only large organization that lost control of their social media channel. Reuters Twitter account[24] was hacked by the Syrian Electronic Army (SEA) and used to post political cartoons in support of Syrian president, Bashar al-Assad. The SEA also compromised the New York Post's Facebook page[25] as well as well as the Twitter accounts of some of its reporters, followed by the satirical news site, The Onion,[26] posting tweets denouncing Israel and the U.S.

One of the original hacktivists, Anonymous, compromised Burger King's Twitter account[27] and used it to promote the competitor, McDonalds. The following day, Jeep's Twitter account was hacked and tweets were sent bearing a similarity to those from Burger King, claiming Jeep had been sold to Cadillac with a picture of a McDonalds branded car as the background image.[28]

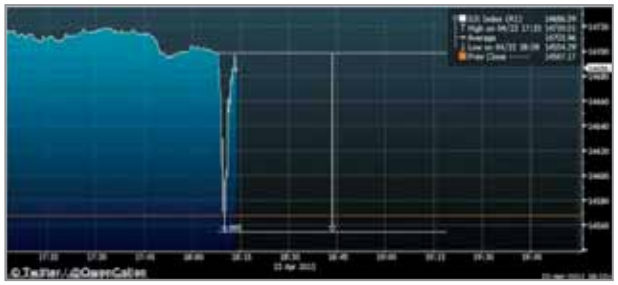


Image credit: http://www.dailymail.co.uk/news/article-2313652/AP-Twitter-hackers-break-news-White-House-explosions-injured-Obama.html

These compromises have a few things in common:

- They were motivated by hacktivism, the drive to make a political statement;
- Rather than create a financial opportunity for the attackers, the incidents caused reputation damage with potential economic impact, however transient and negligible, to the victim organizations;
- The attacks were conducted against humans instead of the social media sites, using phishing to take over user and organizational accounts.

Social media continues to serve as a key communication platform for the enterprise, providing news, promotions, business updates, and other types of announcements and alerts. It is more important than ever to ensure the integrity and safety of these accounts and profiles, and to ensure users entrusted with accounts associated with the enterprise understand strong security practices. Any organization is only as secure as its weakest link.

23 http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
24 http://www.theguardian.com/technology/2013/jul/30/reuters-twitter-hacked-syrian-electronic-army
25 http://www.thedailybeast.com/articles/2013/08/13/syrian-electronic-army-strikes-again-hits-socialflow-new-york- post.html
26 http://arstechnica.com/security/2013/05/no-joke-the-onion-tells-how-syrian-electronic-army-hacked-its-twitter/
27 http://www.telegraph.co.uk/technology/twitter/9878724/Burger-Kings-Twitter-account-hacked.html
28 http://www.huffingtonpost.com/2013/02/19/jeep-twitter-hack_n_2718653.html

Pre-Attack Intelligence gathering

Social media is fertile ground for pre-attack intelligence gathering, as we've covered in previous IBM X-Force Trend and Risk Reports. The attack itself has then typically been conducted through email spear phishing and enticing the target to open a malware infected attachment.

As we discuss earlier in the section "*Watering hole attacks continue to increase*", all an attacker has to do is lure a victim to a website—often a legitimate website that's been compromised—to infect the intended target. A simple link within a tweet or a wall post will do, as with the recent exploit attempt targeting a group of Chinese political activists and affiliates.[29] It's interesting to note that social media may be used both to gather information about the targets, such as their topics of interest, news sites they frequent, and language, as well as for more direct exploitation with direct messages, for example. These attacks can be rendered more effective by including commonly used URL-shorteners, which give no indication of the true destination URL and provide yet another form of link obfuscation.

Social media provides more than just reconnaissance and direct exploitation opportunities; it can be used to actively create trusted networks. For example, in the Robin Sage experiment[30] a security consultant created a fictional persona, Robin Sage, who was purportedly a cyber-threat analyst for the U.S. Department of Defense. Robin had accounts on LinkedIn, Twitter, and Facebook, and those were used to create a network of professional "targets". Most of the contacts worked for the U.S. military, government, or affiliated organizations. Despite the lack of hard evidence to corroborate Robin's clearance, credentials, or even existence, the contacts shared information that revealed their email addresses, bank accounts, and even the location of secret military units. Robin was sent documents to review and offered speaking slots at conferences. A similar experiment was recently conducted and presented at Defcon.[31]

29 https://www.cybersquared.com/apt_targetedattacks_within_socialmedia/
30 http://www.robinsageexperiment.com/
31 http://www.csoonline.com/article/737662/dating-guru-resurrects-robin-sage-by-social-engineering-ts-sci-holders-on-linkedin?source=rss_security_awareness

The rise of the social media black market

The value of having access to social media accounts has created a black market.[32] Criminals are selling accounts, some of which belong to actual people whose credentials were compromised, others fabricated and designed to be credible through realistic profiles and a web of connections.

One use is to manipulate interest around brands by faking "Likes",[33] called "likejacking", planting contrived product reviews, or by helping content go viral. To gain a sense of the scale of the problem, consider that Facebook's own page lost 125,000 likes and Lady Gaga lost 65,000 fans after Facebook undertook a campaign to purge fake accounts.[34] The more insidious uses of account trading include hiding one's identity to conduct criminal activities, the online equivalent of a fake ID but with testimonial friends, or to seed a new network of trusted connections, as in the Robin Sage experiment.

And size counts. The bogus identity's reputation is reinforced by the size of its social network, and the opportunity for exploitation expands in proportion. More connections equal more victims, victims to likejack, to infect with malware, and to extract personal information for deeper exploitation.

Engender suspicion to protect users and assets

We're taught at an early age to be helpful, and many social media users carry this ethical lesson into their behavior online. In the real world there are social controls that deter criminal conduct; online activity is often either not monitored or there's so much data that threats hide amidst the noise. Ultimately, Pandora's boxes are delivered in many forms into the hands of end users, and they make the decision whether to peek under the lid or summon the enterprise cyber hazmat crew.

Dodging attempts to exploit the trust that you, your employees, and your family and friends put in social networks requires a combination of behavioral modification and technology. No, we're not advocating electroshock therapy; and yet, the evasive measures may feel as excruciating.

We've discussed technology controls in previous X-Force Trend and Risk Reports, and those recommendations are still relevant. In addition, users must adopt a mindset of guilty until proven innocent when it comes to social media.

- Only accept invitations to connect from people you know. If the request comes from out of the blue, confirm the intent of the requestor through another channel, such as direct email or by phone.
- Don't click on links—any links, even from close friends—without verifying them by at least hovering over and examining the status bar. On tablets, smartphones, and any touch device, touch and hold the link to view the destination. For the truly paranoid, type the URL manually in a new tab or window or examine the page source.
- If you are concerned about suspicious looking short URL's, there are browser plug-ins and web services which can reverse the link so you can see the actual destination URL first before clicking.
- Don't post anything sensitive; treat social media like you're yelling across an airport terminal where everyone can hear you. Even bits of data that by themselves aren't sensitive can be combined and complete a story. The U.S. Department of Defense calls this OPSEC, or operations security.[35]

Remember, even if you post something sensitive to your best friends, they may repost it in their network, and their security and privacy controls may still be at the default, weak settings.

32 http://blog.webroot.com/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/
33 http://www.ibtimes.co.uk/articles/499985/20130819/instagram-zeus-malware-virus-create-likes-followers.htm
34 http://www.businessinsider.com/facebook-targets-76-million-fake-users-in-war-on-bogus-accounts-2013-2
35 http://en.wikipedia.org/wiki/Operations_security

Conclusion

One of the lessons from our still prototypical foray into social media is that we are interacting with accounts, not people. Accounts can be compromised, they can be fabricated. The only kinetic universe analogs come from science fiction: a compromised human is a pod being; a fabricated human is an android. Even in movies, though, the good guys can recognize the slightly odd behavior of the alien parasites and cyborgs.

We have not yet achieved the same capacity to vet the virtuous from the villainous, the sublime from the suspect, in social media. As with all human interaction, the core issue is trust. And because social networks can expand exponentially broader and faster than even the most well connected politician's network in real life, we simply can't keep track of who's who, no less to whom we should extend our confidence.

As such, the danger of social media is one of transitive trust: we tend to extend trust to friends of friends. Fake friends infiltrate social groups quickly once they convince the first target to accept their connection request.

As the expression goes, "just because I'm paranoid, it doesn't mean they're not watching me." While it's rarely good to imbue fear in our charges, a healthy dose of skepticism that falls just short of fear or paranoia is appropriate as we learn the skills to accurately substantiate the quality of relationships in social media.

Recent advances in Android malware

Introduction

In the past few years, there has been an explosive growth in Android devices. According to reports,[36] Android currently has 59 percent of all smart mobile devices. There were 470 million Android devices shipped in 2012 alone, and if the forecasts[37] are accurate, by 2017 there will be more than 1 billion Android devices in use. Unfortunately, the increase in Android devices has also generated more attention from malware authors. According to additional industry reports,[38] there was a 600 percent increase in the number of Android malware discovered compared to last year, which brings the total of known Android malware to around 276,000.

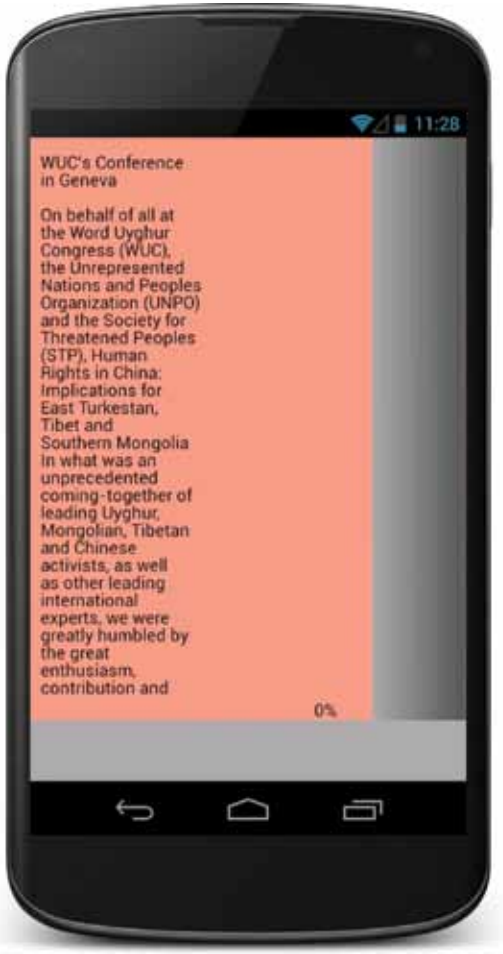
The first half of 2013 also saw the discovery of some malware that indicates that Android is steadily becoming a more attractive target platform for malware authors. Let's look at a couple of these.

Targeted attack

In the 2012 Mid-Year Trend and Risk Report, we discussed targeted attacks and mentioned that on the Mac OS platform there had been attacks against Tibetan Non-Government Organizations (NGOs). This year, malware authors set their sights on Android as well as toward the same types of victims.

Chuli, discovered in March 2013, was used to target contacts of a Tibetan hacktivist who was apparently hacked and had his address book compromised. Using the hacked account, emails were sent to the target contacts purporting to be about a conference run by the "World Uyghur Congress". The attached file is an Android APK file named "WC's Conference.apk". When opened, it (Chuli) displays a message about the conference.

In the background, Chuli sets up hooks into Android's SMS service so that it can intercept incoming SMS messages and send them to a remote Command and Control (C&C) server. It also sends the user's SMS history, call history, contacts, and geolocation to the C&C server. Chuli is a highly



Example of Android malware - Chuli

36 http://www.canalys.com/newsroom/smart-mobile-device-shipments-exceed-300-million-q1-2013
37 http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017
38 http://thenextweb.com/insider/2013/06/26/juniper-mobile-malware-is-an-increasingly-profit-driven-business-as-92-of-all-known-threats-target-android/

targeted attack and is only intended for specific individuals, thus the risk of infection to the common user is low. However, the existence of this malware indicates that Android users are increasingly becoming viable targets for these types of sophisticated attacks. Of course, in this case, the sophistication is related to the organization and intent of the attack—the raw technology in Chuli is not particularly novel.

The "most sophisticated" Android malware, Obad, a trojan that was mostly spread through SMS spam, gained attention in June 2013 when it was dubbed "The most sophisticated Android trojan".[39] We have seen the core functionality of Obad in other Android malware before, including information stealing and premium SMS sending, but here are the features that made it stand out:

1. Anti-analysis techniques and code obfuscation
Obad employs two exploits that make static and dynamic analysis more difficult both for the malware analyst and to malware-analysis sandbox systems. First, it modifies the Dalvik executable in the APK in a way that will cause an error in some reverse-engineering tools, leading to an erroneous output. Second, the AndroidManifest.xml provided in the APK is also modified so that it is incomplete, but Android's manifest checking code ignores it and allows the APK to be installed. Unfortunately, most dynamic analysis tools rely on the missing information to run and analyze the APK. This leads to an incomplete analysis report from these tools.

Obad also uses code and string obfuscation to make it harder to analyze. All strings, including class and method names, are encrypted, and some are encrypted multiple times. To make analysis even harder, it also employs techniques such as calling API methods via reflection and adding garbage code.

2. Device administration
When Obad is installed, it asks the user for Device Administrator privileges, which gives it certain privileges such as locking the device. It also prevents the app from being uninstalled in the normal manner. To uninstall a Device Administrator app, the user has to uninstall it through the Device Administrator's list in the Settings menu. However, Obad exploits a bug in Android that prevents an app from being listed in the Device Administrator's list, hence there is no way to uninstall it.

3. Spreading through Bluetooth
Another unique feature of Obad is its ability to spread itself and other malware through Bluetooth. It can receive a command from the C&C server that tells it to scan for discoverable Bluetooth enabled devices in the vicinity. It then attempts to send a possibly malicious file to them.

There were no reports of widespread infection of Obad when it first came out, but we believe it is significant in that it demonstrates how malware authors are now investing more effort into creating more resilient and dangerous Android malware.

So, to recap, there are some interesting technical attributes to the Obad trojan which are novel. Additionally, the intent behind Obad is dissimilar to Chuli and X-Force expects a greater variety of malware attacks on the Android platform with time. At the moment, one troubling aspect of Android security is how out-of-date much of the user-base is regarding Android firmware. For example, an out-of-date Android user with no upgrade plans and/or firmware upgrade available has no real chance of being immune to the bug Obad leverages to prevent uninstallation. Let's continue with a look at the current state of Android security as of July.

39 http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan

Android security enhancements

At the time of this writing, the most widely used version of Android is 2.3 at 34 percent[40] of all devices running Android. Meanwhile, the latest version of Android (as of July 2013), 4.2 is used on less than six percent of all Android devices, despite having been available since November 2012. This version offers several security enhancements that could reduce the likelihood of infection, or at the very least lessen the impact once infected. Here are some of the security enhancements that could help thwart malware:

1. Application verification

Android 4.2 includes an app verifier that checks whether an app about to be installed is potentially harmful or not, regardless or whether it is installed from the Google Play market or from somewhere else. This feature can be enabled by going to Settings > Security > Verify Apps. During app installation, information about the app that includes the app name, SHA1 sum of the APK, and associated URLs, among others, are sent to Google. Google then responds with the detection result. Apps are flagged as either potentially dangerous or dangerous. If an app is flagged as potentially dangerous, the app verifier displays a warning and gives the user the choice of continuing the installation or canceling it. Apps flagged as dangerous are blocked outright and won't be installed.

Security enhancements for Android 4.2

2. Improved permissions display

The permissions screen that is displayed during app installation has been improved to provide more details about the app permission requests. Whereas previous versions simply displayed a short description of the permissions to be requested, the new permissions screen also displays warnings about the dangers of allowing certain permissions.

3. Premium SMS send notification

Premium SMS scams (or Toll Fraud) constitute the most prevalent method in which Android malware authors earn money. To counter this, Android 4.2 adds a feature wherein it notifies the user whenever an app attempts to send an SMS message to a premium SMS short code number. The user then has the option to allow it.

40 http://developer.android.com/about/dashboards/index.html

These security enhancements, along with safe Android computing practices such as refraining from installing apps from third-party marketplaces and being aware of the permissions requested by the apps you install, should go a long way in preventing malware infection on Android devices.

Conclusion

For the rest of 2013, X-Force expects to see the number of Android malware apps continuing to rise. We also anticipate that the degree of sophistication for this malware will eventually rival those found in desktop malware. There could be more improvements to combat malware in future versions of Android, but we believe that OS fragmentation (older versions that are being used as much as newer ones) will remain a problem. Unfortunately, and more commonly the norm, new firmware is not available. However, we recommend that Android users check to see if a firmware update is available and to consider upgrading.

Vulnerabilities and exploits

Zero-day attacks in 2013 H1

The first half of 2013 has been very busy from a zero-day attack perspective. In the first six months of the year, several zero-day vulnerabilities affecting widely deployed software were found to be exploited in the wild. Most of the zero-day exploits were initially found in targeted attacks and we witnessed how much attackers are willing to invest in these attacks when sophisticated zero-day exploits bypassed modern security mechanisms in software. In this article, we'll look at these zero-day attacks and give suggestions that can lower your risk of becoming a victim.

Internet Explorer and dangerous watering holes

The year was greeted with a zero-day attack in Internet Explorer that exploited an unpatched Internet Explorer vulnerability (CVE-2012-4792) that had been seen in the wild during the last week of December 2012.[41] The attack involved attackers implanting the exploit code in the compromised website of the Council for Foreign Relations. A few months later, in May 2013, an exploit for another zero-day vulnerability (CVE-2013-1347) in Internet Explorer surfaced.[42] Similar to the first attack, the exploit code was also found in a compromised website—this time the U.S. Department of Labor website was used by the attackers to launch the zero-day exploit.

Common to both attacks was the use of a compromised website to launch the zero-day exploit. Both are believed to be part of a watering hole campaign—a form of targeted attack in which an attacker identifies the websites a targeted group usually visits or will most likely visit and then compromises those websites to become the launch pad of the attack.

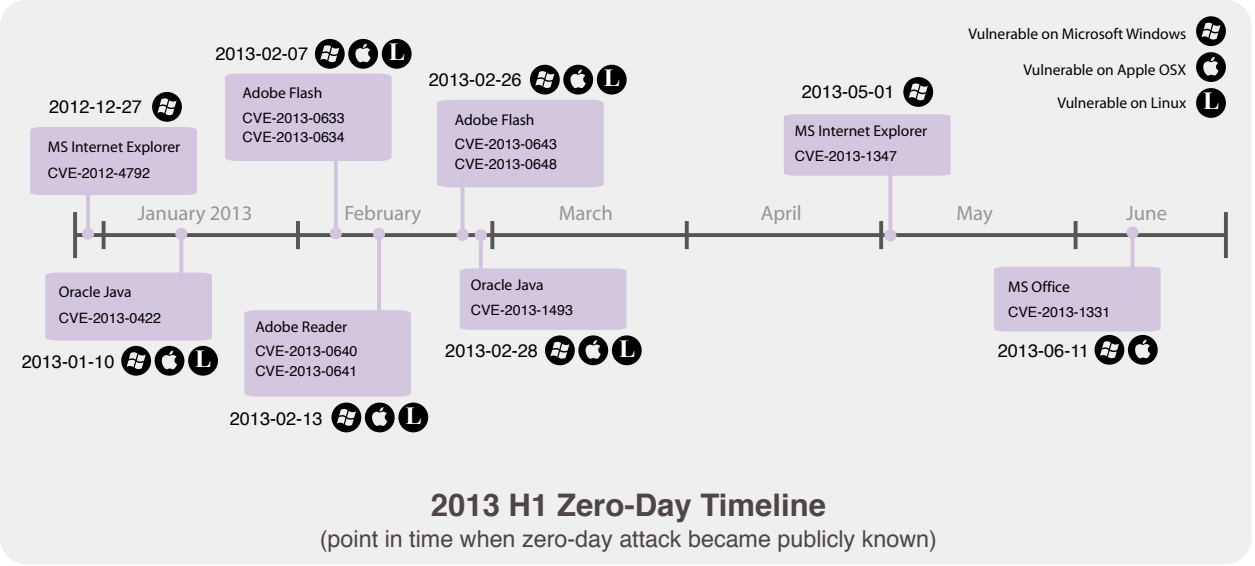


Figure 4: Zero-Day Timeline
(Point in time when the zero-day attack became publicly known)

41 http://www.fireeye.com/blog/technical/malware-research/2012/12/council-foreign-relations-water-hole-attack-details.html
42 http://labs.alienvault.com/labs/index.php/2013/new-internet-explorer-zeroday-was-used-in-the-dol-watering-hole-campaign/

How can you protect against these attacks

For website administrators, becoming a launch pad for watering hole campaigns damages their website's reputation and can result in the loss of customer trust. If you are a website administrator, below are some suggestions that can help lower the risk of your website from being compromised:

- Harden your servers. There are plenty of hardening guidelines available online for specific operating systems and software; for general guidelines, one reference is the "Guide to General Server Security"[43] published by NIST (National Institute of Standards and Technology).
- Make sure that the software and web applications installed on the server are always up to date. If you are developing the web application yourself, the OWASP (Open Web Application Security Project)[44] provides guidelines for securing web applications.
- Stolen server login credentials are also a cause of website compromises. One of the reasons for stolen login credentials is if the client machine used for logging into the server gets compromised. Therefore, make sure that the client machine you use for logging into the server is not compromised and that it is also hardened. Later in this article are some suggestions that apply to hardening client machines. Finally, using strong passwords and using different passwords for different accounts are best practices.

What is a water hole campaign?

Water holing was first coined by RSA in 2012.[45] Though similar form of attacks may have been observed in the past, RSA first used it in a campaign dubbed "VOHO".[46] In the VOHO campaign, several websites catering to specific groups related to political activism, defense industrial base, and specific geographical areas were compromised to load exploit code located in another compromised website. In early 2013, watering hole campaigns were further popularized when several high-profile companies such as Apple[47] and Facebook[48] reported that some of their employees were attacked via a compromised developer website.

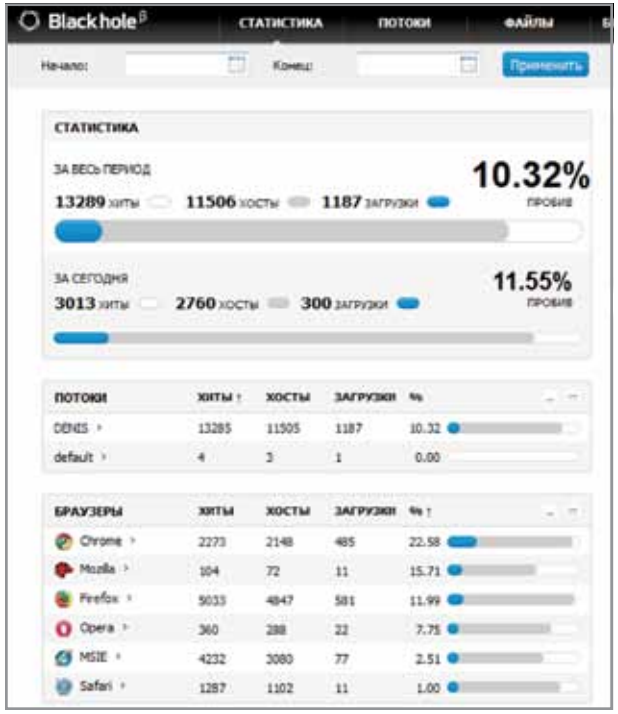
Watering hole campaigns are passive compared to spear-phishing campaigns as the potential victims are not directly enticed by an attacker to perform a particular action. Instead, the attacker waits for the victims to visit the compromised website and then launches the attack from there. This particular property of watering hole attacks makes even trained users a potential target since these types of users are less likely to be prey from spear-phishing attacks but most likely will visit the compromised sites as part of their normal routine.

43 http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
44 https://www.owasp.org/index.php/Main_Page
45 http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/
46 http://blogs.rsa.com/wp-content/uploads/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf
47 http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219
48 https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766

Java: continued interest from exploit kit authors

Even before the December Internet Explorer zero-day vulnerability was patched, two new Java zero-day vulnerabilities (both labeled as CVE-2013-0422) were found exploited in the wild. During the second week of January, exploit kits such as the Blackhole and Cool exploit kit were found to be using unpatched Java vulnerabilities to escape the Java sandbox in order to install malware on victims' machines. Continuing the trend that we reported on in the annual IBM X-Force 2012 Trend and Risk Report, other exploit kit authors showed interest in the Java zero-day vulnerabilities and soon followed by integrating the zero-day exploit into their exploit kits.[49]

A few weeks afterwards, a third Java zero-day vulnerability (CVE-2013-1493) was found exploited in the wild. Initial exploits for the zero-day were discovered during the last of week of February.[50] It is not clear how the initial attacks were conducted, but what came next was not a surprise: several exploit kit authors started integrating the exploit for the zero-day into their exploit kits.[51]



Blackhole Exploit Kit Control Panel

The first half of 2013 was not all bad news for Java as Oracle made two important security enhancements for running Java in the browser. The first was made in the Java 7u10 release which was the addition of a feature to easily disable Java in a browser. The second important change was made in the Java 7u11 release which was the change of the default security settings level to "High" which means that the user is prompted before running unsigned Java applications in the browser. This latter change makes it less attractive for attackers to use Java exploits since they would now need to use social engineering tactics to lure users to run their malicious Java application or exploit a secondary vulnerability that allows the attacker to bypass the Java security prompt.

49 http://malware.dontneedcoffee.com/2013/01/0-day-17u10-spotted-in-while-disable.html
50 http://www.fireeye.com/blog/technical/cyber-exploits/2013/02/yaj0-yet-another-java-zero-day-2.html
51 http://malware.dontneedcoffee.com/2013/03/cve-2013-1493-jre17u15-jre16u41.html

Flash Player: attacks via Office documents

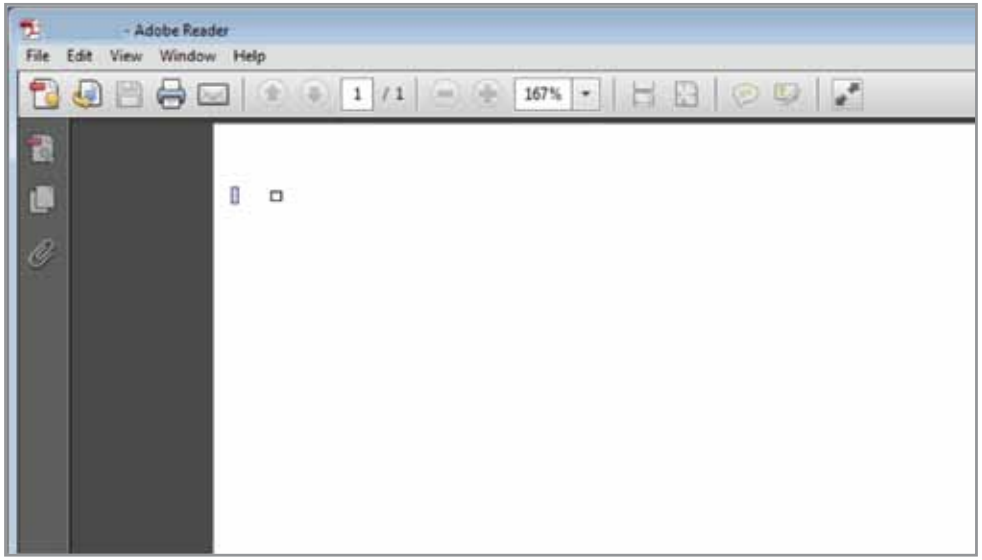
February was also a busy month as several zero-day attacks were discovered or reported. In addition to the third Java vulnerability previously discussed, two additional widely deployed applications were found targeted by zero-day exploits. The first of these is the Adobe Flash Player discussed here and the second is the Adobe Reader, discussed in the next section.

While users were still recovering from the Java zero-day attack in January, in early February, two Flash Player zero-day vulnerabilities (CVE-2013-0633 and CVE-2013-0634) were found being exploited in the wild. From the vendor's report,[52] a common trait in both attacks was that, for Windows users, the attack involved delivering the exploits via Flash files embedded in Word documents. Then, on February 26, Adobe published another security bulletin stating that two additional zero-day vulnerabilities (CVE-2012-0643 and CVE-2013-0648) were found exploited in the wild.

Adobe noted[53] that since the introduction of the Reader sandbox in 2010, the most common delivery method for Flash Player zero-day attacks had been Office documents. In addition to the first two Flash zero-day attacks discussed earlier, a notable example of this is the RSA breach in 2011 in which attackers embedded a Flash zero-day exploit in an Excel document.[54]

Adobe Reader: sophisticated exploits

Just a few days after the first set of Flash Player zero-day vulnerabilities were found exploited in the wild, a sophisticated zero-day exploit for Adobe Reader emerged. Interestingly, this particular zero-day exploit is the first in-the-wild exploit capable of escaping the Reader sandbox (which was first introduced in 2010).



Reader zero-day exploit – a seemingly blank PDF file is shown while a sophisticated attack that exploits two zero-day vulnerabilities executes in the background

52 http://www.adobe.com/support/security/bulletins/apsb13-04.html
53 http://blogs.adobe.com/asset/2013/02/raising-the-bar-for-attackers-targeting-flash-player-via-office-files.html
54 https://blogs.rsa.com/anatomy-of-an-attack/

The attack exploited two zero-day vulnerabilities (CVE-2013-0640 and CVE-2013-0641), one of which allowed the exploit to run arbitrary code inside the Reader sandbox when the user opened a PDF file. The other vulnerability is used by the first exploit to run code outside the restrictive Reader sandbox. Initial exploits were reported[55] to have been used in targeted attacks where the victims are sent an email with an attached PDF file containing the exploit.

Exploits such as the sophisticated Reader exploit demonstrate that attackers are willing to invest significant resources to infiltrate their targets. Developing an exploit that bypasses several modern security mechanisms—such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) and the Reader sandbox in this case—and that works in a modern version of an operating system, is not an easy feat. The development of this particular exploit required several weeks or months of research and development depending on the skills of the attackers involved. As application sandboxes grow in popularity, we can expect to see more of these kinds of attacks in the future.

Office: extremely targeted attack

In June, Microsoft reported and patched a zero-day vulnerability (CVE-2013-1331) in Microsoft Office. Microsoft describes[56] the initial attacks as extremely targeted. This is why not much was known about the attack before the Microsoft advisory was published. The vulnerability affected the latest version of Office for Mac (Office 2011) but only affected an older version of Office in Windows (Office 2003).

Lowering your risk: reduce, update, and educate

Zero-day vulnerabilities will continually be discovered and exploited as attackers continue to see them as vehicles for crimes and espionage. Even if the initial zero-day exploits are found in targeted attacks, the exploits eventually end up in automated attack tools such as exploits kits. This means that, eventually, every one using the affected software could become a potential target.

55 http://www.adobe.com/support/security/advisories/apsa13-02.html
56 http://blogs.technet.com/b/srd/archive/2013/06/11/ms13-051-get-out-of-my-office.aspx

Lowering your risk is one of the first steps you can do to avoid becoming a victim from zero-day attacks. Below are some suggestions you can follow:

1. **Reduce attack surface.**
   One of the most important steps in lowering your risk from becoming a victim of zero-day exploits—and exploits in general—is reducing the means of how you can be attacked. Take time to review your installed browser plug-ins and uninstall those you have not used for a while. If you really need to use a particular browser plugin, use the "Click-to-Play" feature if your browser supports it. Click-to-Play prevents silent or "drive-by" exploitation of browser plug-ins by requiring an additional user interaction before a plugin can be activated. Another example of reducing your attack surface is disabling ActiveX controls in Office[57] which can mitigate Flash exploits delivered via Office documents. Finally, if you are using Java to run desktop (standalone) applications but are not using Java to run applications in the browser, you can opt to disable Java in the browser.[58]
2. **Update installed software.**
   Newer or updated versions of applications introduce new security features which make them more costly or less attractive for an attacker to use as vectors for exploits. Examples of such security features include sandboxing capabilities and features which prevent automatic loading of potentially unsafe content. These include Click-to-Play in browsers and the security-level settings in Java, which prevents automatic execution of unsigned Java applications in the browser.
3. **Get educated on spear-phishing attacks.**
   In spear-phishing campaigns, the attacker sends personalized emails to a specific set of victims, the email usually entices the recipient to open an attached document or file, or click a link to a website which in turn may launch an exploit. By getting educated on how to spot these suspicious emails, you can avoid becoming prey by these spear-phishing campaigns.

As zero-day exploits continue to become more sophisticated and as attackers develop different ways to deliver these zero-day attacks, being prepared by lowering your risk is one of the best actions X-Force believes you can take.

57 http://office.microsoft.com/en-us/excel-help/enable-or-disable-activex-controls-in-office-documents-HA010031067.aspx
58 http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/client-security.html

Vulnerability disclosures in the first half of 2013

Since 1997, the X-Force has been tracking public disclosures of vulnerabilities in software products. The X-Force collects software advisories from vendors, reviews security related mailing lists, and analyzes hundreds of vulnerability web pages where remedy data, exploits, and vulnerabilities are disclosed.

In the first half of 2013, we entered just over 4,100 new publicly reported security vulnerabilities. If this trend continues throughout the rest of the year, the total projected vulnerabilities would approach 8200 total vulnerabilities, virtually the same number we saw in 2012.

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 if the numbers hold up, this could be our first year in which these totals do not alternate between the higher and lower annual sequence seen over the past seven years.

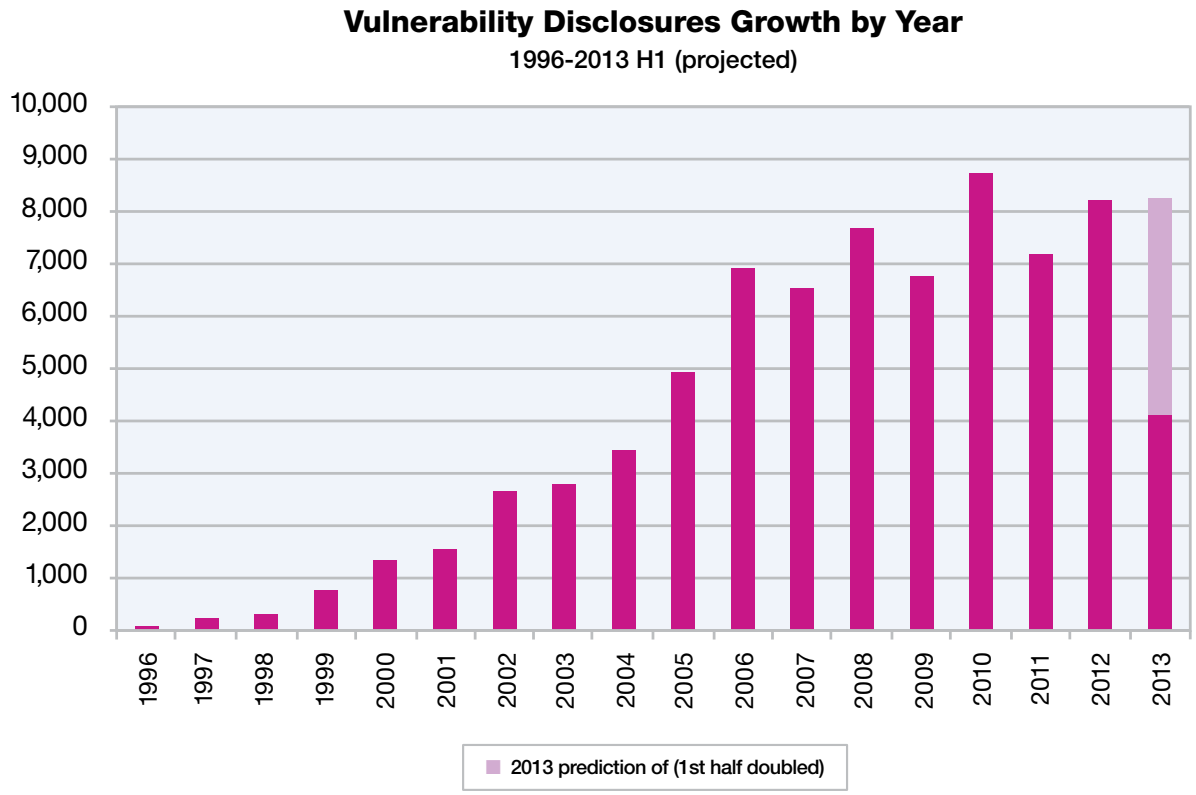


Figure 5: Vulnerability Disclosures Growth by Year - 1996-2013 H1 (projected)

Web application vulnerabilities

The majority of vulnerabilities that the X-Force team documents are those in web application programs, such as Content Management Systems (CMS). In the first half of 2013, 31 percent of vulnerabilities that were publicly reported are what we categorize as applications used on the World Wide Web. This number is down significantly from 2012 where we saw levels at 42 percent. More than half of all web application vulnerabilities are cross-site scripting.

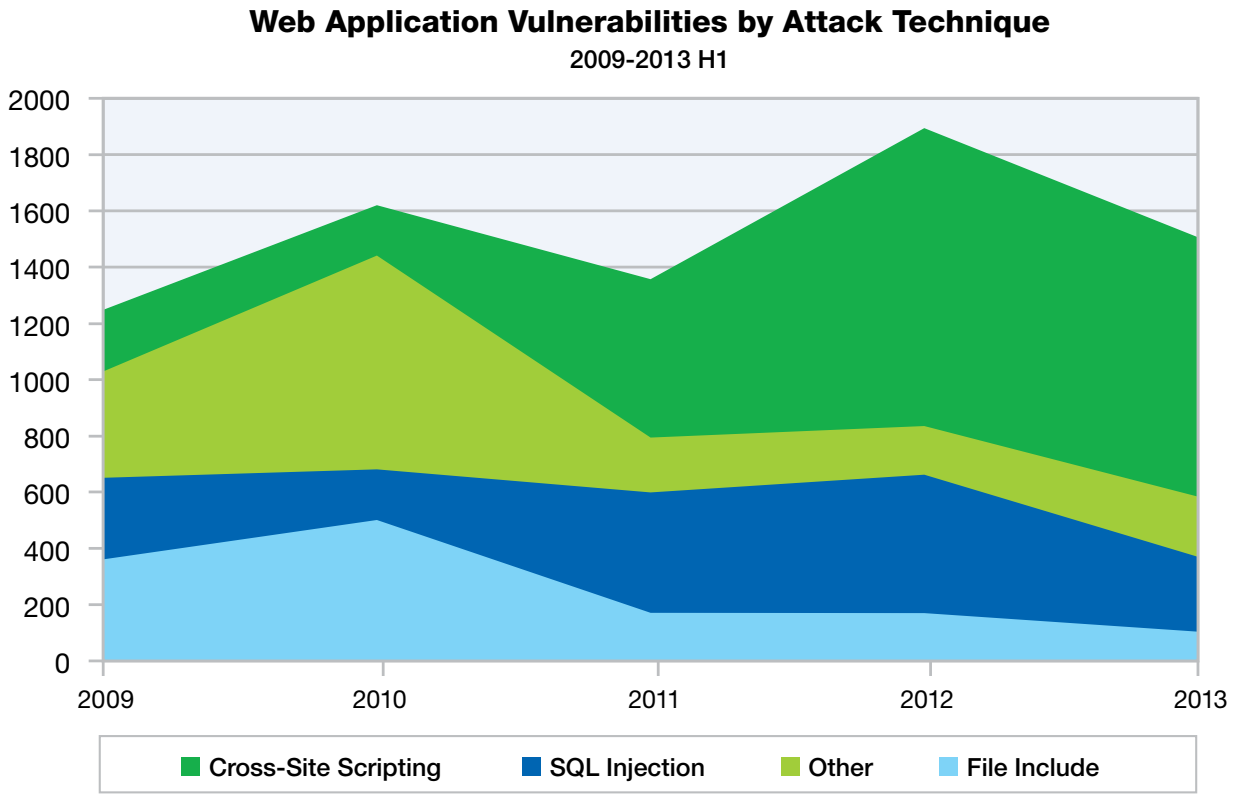


Figure 6: Web Application Vulnerabilities by Attack Technique - 2009-2013 H1

Content Management Systems are some of the most popular software used on the World Wide Web. Major CMS vendors have embraced security and do a good job of patching their core software when security vulnerabilities are reported to them. Seventy-eight percent of all vulnerabilities reported in CMS were patched in the first half of 2013, while in 2012 we saw that only 71 percent of vulnerabilities were patched. Year over year we see that these vendors are doing a better job of keeping their products up to date with the most recent security coverage.

However, third-party creators of plug-ins for CMS did not fare as well with only 54 percent of vulnerabilities having a patch supplied. With over 46 percent unpatched vulnerabilities, third-party plug-ins become attractive opportunities for attacks to occur.

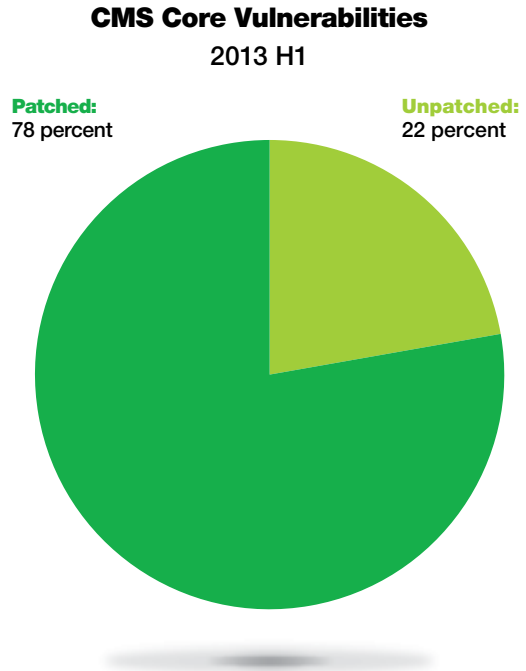


Figure 7 : Disclosed Vulnerabilities in Core Content Management Systems – Patched versus Unpatched 2013 H1

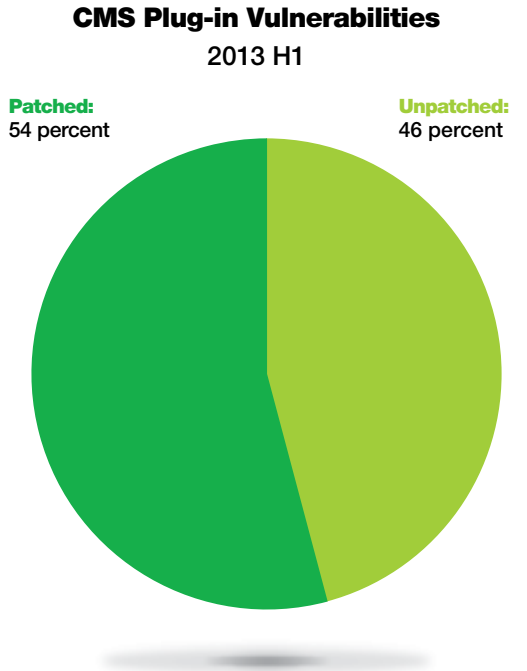


Figure 8 : Disclosed Vulnerabilities in Plugin Content Management Systems – Patched versus Unpatched 2013 H1

Mobile vulnerabilities

Although vulnerabilities affecting mobile applications and operating systems represent a relatively small percentage of total disclosures (projected at just over four percent in 2013), we have seen the total number of disclosures increase significantly since 2009 when mobile vulnerabilities represented less than one percent of total disclosures. After a substantial jump in 2009, the number decreased slightly from 2010 to 2011 before another substantial jump in 2012 (See Figure 9).

Many of the vulnerabilities affecting mobile platforms originate in components that are used in both mobile and desktop software. The remaining vulnerabilities are specific to mobile applications and represent a large portion of the increase in disclosures seen in 2012 and 2013.

One significant development of note regarding mobile vulnerabilities in 2013 has to do with the number of public exploits available. In 2013, fewer than 30 percent of all mobile disclosures had public exploits or proof-of-concept code available. In comparison, only nine percent of mobile vulnerabilities disclosed between 2009 and 2012 had public exploits. Most of these exploits are targeted specifically towards mobile applications and are primarily disclosed on popular public exploit repositories.

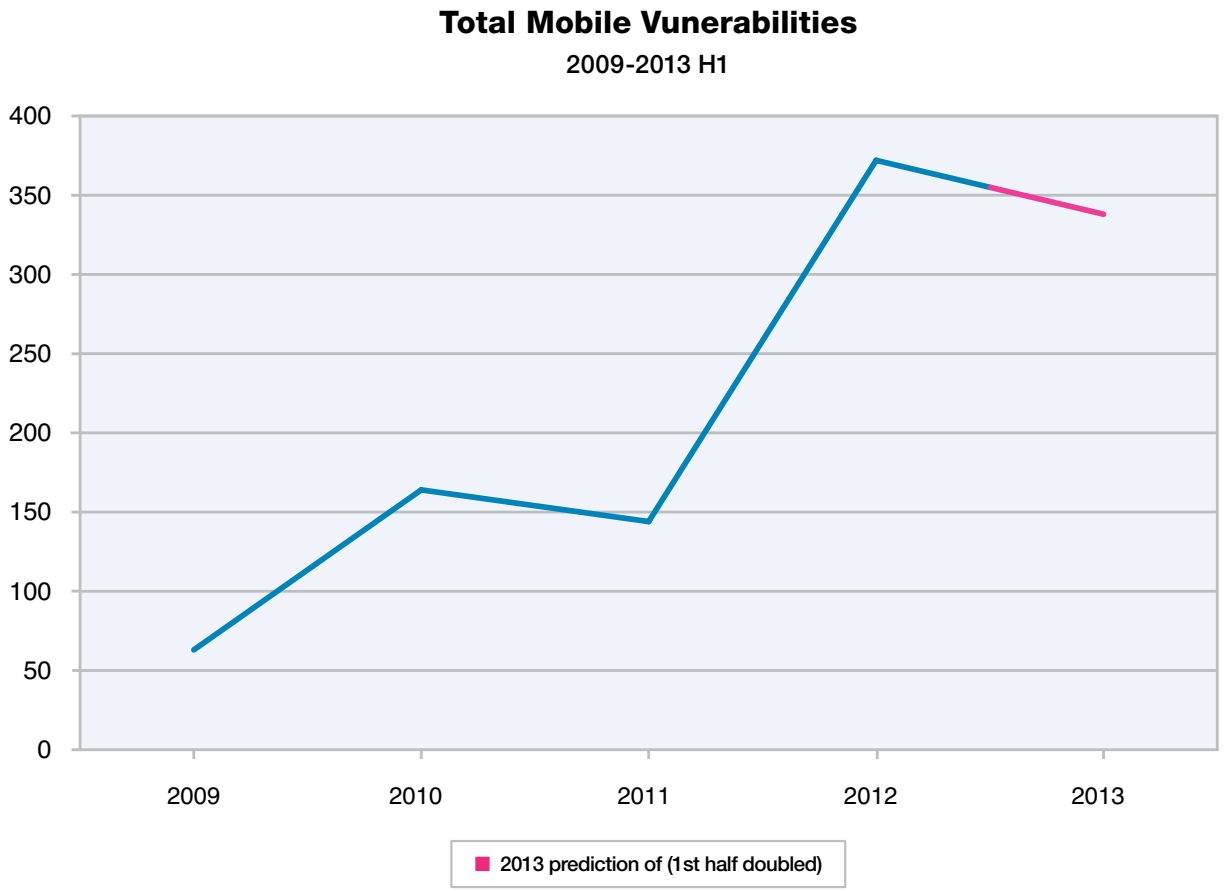


Figure 9: Total Mobile Vulnerabilities - 2009-2013 H1

Consequences of exploitation

X-Force categorizes vulnerabilities by the consequence of exploitation. This consequence is essentially the benefit that exploiting the vulnerability provides to the attacker. Table 1 describes each consequence.

Consequence	Definition
Bypass Security	Circumvent security restrictions such as authentication, firewall, proxy, IDS/IPS system, or virus scanner
Cross-Site Scripting	The impact of cross-site scripting varies depending on the targeted application or victim user, but can include such consequences as sensitive information disclosure, session hijacking, spoofing, site redirection, or website defacement
Data Manipulation	Manipulate data used or stored by the host associated with the service or application
Denial of Service	Crash or disrupt a service or system
File Manipulation	Create, delete, read, modify, or overwrite files
Gain Access	Obtain local and remote access to an application or system. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the underlying service or operating system
Gain Privileges	An attacker using valid credentials can obtain elevated privileges for an application or system
Obtain Information	Obtain information such as file and path names, source code, passwords, or server configuration details
Other	Anything not covered by the other categories
Unknown	The consequence cannot be determined based on insufficient information

Table 1: Definitions for Vulnerability Consequences

The most prevalent consequence of vulnerability exploitation for the 1st half of 2013 was "gain access" at 28 percent of all vulnerabilities reported. In most cases, gaining access to a system or application provides the attacker complete control over the affected system, which allows 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. For additional information on web application vulnerabilities in 2013, refer to page 35.

A complete breakdown of all vulnerability consequences reported during the 1st half of 2013 is shown in Figure 10.

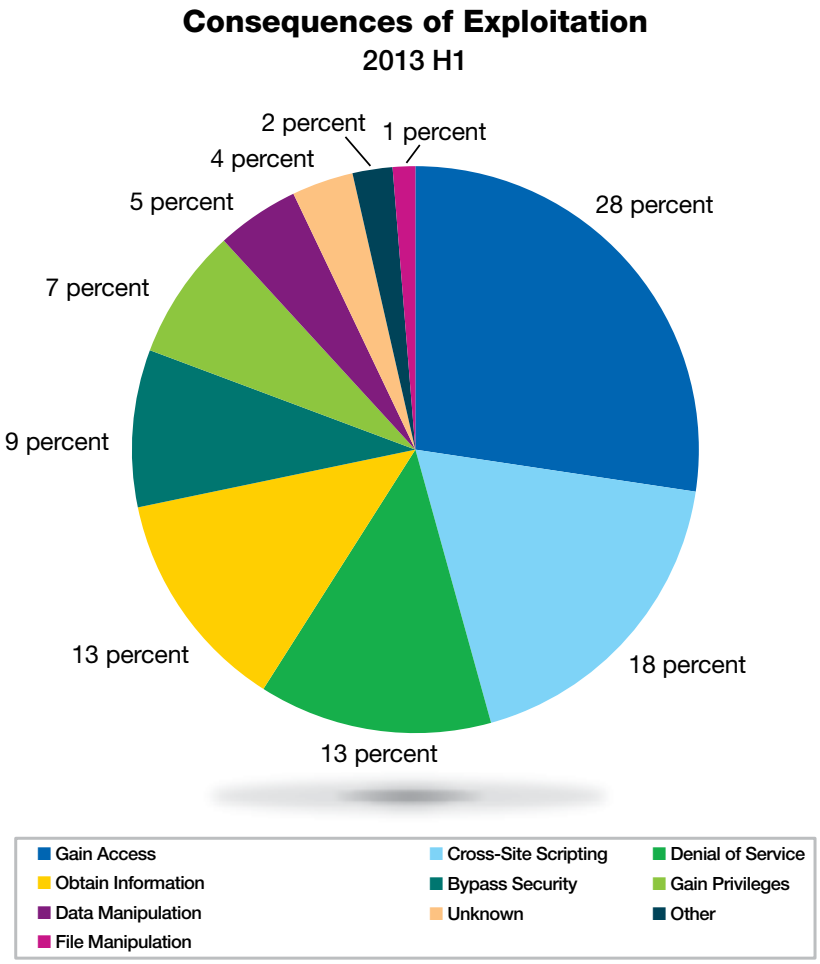


Figure 10: Consequences of Exploitation - 2013 H1

Exploit effort vs. potential reward

As cyber-attacks intensify, monitoring the numerous vulnerability disclosures every day becomes daunting. Within IBM X-Force, we track publicly issued vulnerabilities through a triage process to identify which ones are most likely to be used by an attack, and then determine which ones require deeper research. By performing this review, we recognize that all vulnerabilities are characterized by two factors; the exploit "potential reward" that entices the attacker and the "exploit effort to achieve" that deters the attacker from further development. The exploit-probability matrix is devised by charting the "exploit reward" and "exploit effort to achieve" along the axes. By assigning vulnerabilities to the appropriate quadrant, it becomes clear which are favored by attackers.

The exploit "potential reward" lies along the Y-axis, and indicates the value of data that is extracted from compromised machines. In the quantitative sense, vulnerabilities with wide product coverage on desktop machines, or vulnerabilities affecting corporate servers containing every employee's account are attractive to attackers. In the qualitative sense, confidential data has higher value and is more alluring. Financial gains from the data, and exploitation opportunities, are synonymous with this axis.

The "exploit effort to achieve" lies along the X-axis, and indicates the resources required to translate vulnerabilities into reliable exploits. These resources include the expertise, time, and effort an attacker spends to bypass the protection mechanisms, and/or manipulation of memory layout to achieve code execution. As more protection mechanisms are implemented in modern operating systems, the pool of skilled attackers inevitably shrinks. Clearly, this also means that compromised data increases in value, and implies the direct proportionality between the exploit "potential reward" and the "exploit effort to achieve".

In the exploit probability matrix, four categories of classification emerge. In the top-right quadrant, vulnerabilities with huge potential reward and low exploit cost fall into this "widespread exploitation" category. Because they yield the best investment returns, these vulnerabilities are expected to be widely exploited in the wild. In the top-left quadrant, vulnerabilities with huge potential reward and high exploit effort fall into this "sophisticated attack" category. Although attackers are equally motivated by the gains, only sophisticated attackers have the required skills to achieve code execution. Therefore, exploitation of these is likely to be contained. In the lower-left quadrant, vulnerabilities with low potential reward but high exploit effort fall into this "not targeted widely" category. These vulnerabilities are perhaps better suited for educational purpose rather than cyber-attacks. In the lower-right quadrant, vulnerabilities that also yield low potential reward with low exploit effort fall into the "occasional exploitation" category. Even though the returns are low, they are sufficiently easy to exploit. We expect to see these in the wild only when attackers have very specific objectives.

In the first half of 2013, X-Force issued 14 alerts and advisories on disclosures that deserve close attention. We place seven of these alerts and advisories, coincidentally entirely composed of Internet Explorer (IE) and Java, in the top-right quadrant—vulnerabilities with high reward and low cost. The seven vulnerabilities can all be used in drive-by exploitation, reaching as many victims possible. The IE use-after-free issues can be exploited with the browser scripting capabilities. These fit the criteria for "widespread exploitation."

CVE-2013-1347 was used in the watering hole attack involving the U.S. Department of Labor (as discussed in earlier sections). Although it only affected IE8, many other machines might still be affected for two reasons—IE8 is the highest browser version allowed in Windows XP/2003, and it is also the default browser in a freshly installed Windows 7.

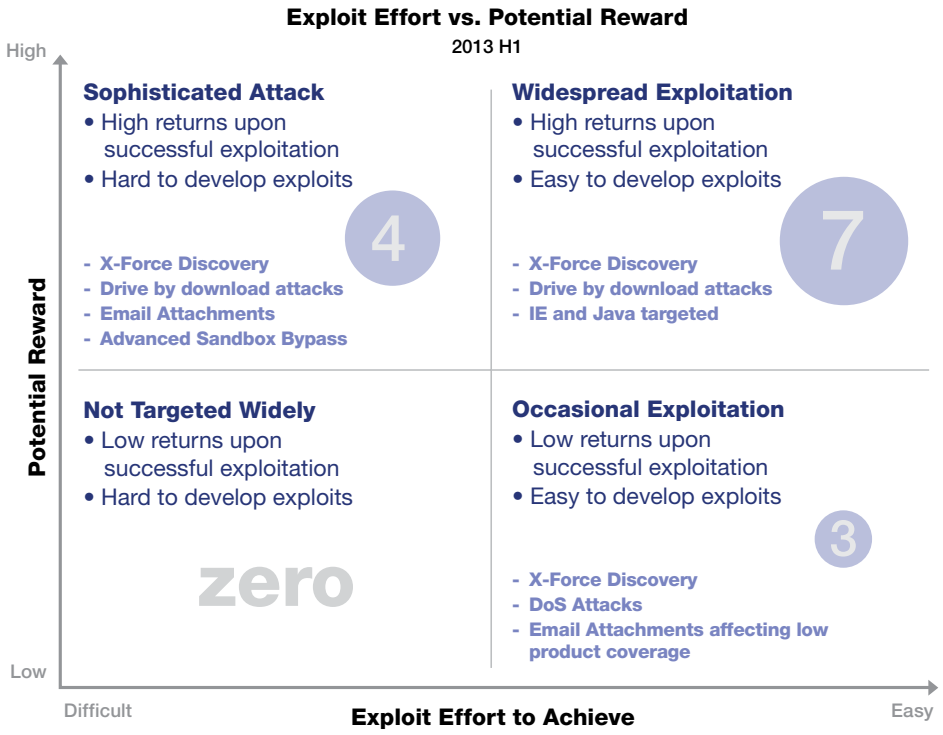


Figure 11: Exploit Effort vs. Potential Reward – 2013-H1

We place four other alerts and advisories in the top-left quadrant—vulnerabilities with high reward and high development effort. These vulnerabilities involve heap overflow issues which require attackers to manipulate the memory following the overflow with useful objects. Considering the amount of expertise required, we expect to see such vulnerabilities being used in more sophisticated attacks. Two of the alerts/advisories are for sandbox escape vulnerabilities. Achieving a full exploitation of sandboxed applications is typically a two-stage process—a vulnerability for code execution in the sandbox process before using another vulnerability to escape into the broker process. If either vulnerability is seen in the wild, it implies that the attacker has the capability for the other. Subsequently, X-Force does not treat sandbox escape vulnerabilities differently. The other two alerts and advisories, CVE-2013-0633 and CVE-2013-0634, are vulnerabilities involving the Adobe Flash Player. These vulnerabilities have varying attack vectors; they can be used in browser drive-by exploitation or by embedding the malformed files in email documents.

The remaining three alerts and advisories are placed within the lower-right quadrant—which are vulnerabilities with low reward and low development effort. CVE-2013-1331 is a classic stack overflow affecting Microsoft Office 2003 and Office for Mac 2011. We believe that the opportunity for exploitation is limited for different reasons; Microsoft Office 2003 is already a 10-year old product while Office for Mac 2011, though current, is less widely deployed than the Windows version. CVE-2013-0176 and CVE-2013-1305 are denial of service (DoS) vulnerabilities affecting server systems. Although less attractive than code execution, DoS attacks still serve their purpose, as evidenced by recent high-profile DoS attacks. With these vulnerabilities, attackers are able to DoS the systems with a single packet instead of having to grow a botnet. X-Force therefore deems it appropriate to issue alerts and advisories on them.

What's the difference between a Protection Alert and an Advisory?

Basically, it's the difference between whether the security issue was discovered by IBM X-Force, or whether IBM X-Force is providing additional information on an existing security issue discovered by someone else. Both provide protection information for the profiled threat.

IBM X-Force Protection Alerts are released when X-Force discovers significant additional information about an existing security issue.

IBM X-Force Protection Advisories contain information from original, internal X-Force research. Each advisory includes a detailed description of the security vulnerability, its impact, affected versions, and recommendations for managing and/or correcting the issue.

Widespread Exploitation	CVE-2013-1347	Alert	Microsoft Internet Explorer Use After Free Vulnerability
	CVE-2013-1486	Alert	Oracle Java Runtime Environment JMX code execution
	CVE-2013-0027	Advisory	Microsoft Internet Explorer CPasteCommand code execution
	CVE-2013-0029	Advisory	Microsoft Internet Explorer CHTML code execution
	CVE-2012-3342	Advisory	Oracle Java Runtime Environment Remote Code Execution
	CVE-2013-0422	Alert	Oracle Java Runtime Environment MBean code execution
	CVE-2012-4792	Alert	Microsoft Internet Explorer Could Allow Remote Code Execution
Sophisticated Attack	CVE-2013-0504	Advisory	Adobe Flash Player for Firefox Sandbox Bypass
	CVE-2013-0640	Alert	Adobe Reader and Acrobat XFA Remote Code Execution
	CVE-2013-0641	Alert	Adobe Reader and Acrobat XFA Remote Code Execution
	CVE-2013-0633	Alert	Adobe Flash Player buffer overflow
Occasional Exploitation	CVE-2013-1331	Alert	Microsoft Office vulnerability could allow Remote Code Execution
	CVE-2013-1305	Alert	Microsoft Vulnerability in HTTP.sys Could Allow Denial of Service
	CVE-2013-0176	Advisory	libsshpublickey_from_privatekey() function denial of service

Table 2: X-Force Alerts and Advisories 2013 H1

Web trends, spam, and phishing

Web threat trends

The IBM X-Force Content data center constantly reviews new web content data and analyzes 150 million new web pages and images each month.

The IBM X-Force Content data center has been crawling and indexing web pages continuously for 14 years and has to date, analyzed and classified 20 billion pages and images. The main result of this classification is the IBM web filter databases consisting of 81 million entries across 69 unique classification categories. The database currently gets around 150,000 new or updated entries every day as it keeps up with the dynamic nature of the Internet.

This topic provides a review of the following items:

- Analysis methodology
- Percentage of unwanted Internet content
- Website categories containing malicious links
- Geographic distribution of malware and C&C servers
- IPv6 deployment for websites

Analysis methodology

X-Force captures information about the distribution of content on the Internet by counting the hosts categorized in the IBM Security Systems web filter database. Counting hosts is an accepted method for determining content distribution and provides a realistic assessment of it. When using other methodologies—such as counting web pages and subpages—results may differ.

Percentage of unwanted Internet content

In our efforts to classify what percentage of websites provide unwanted content, we have focused on the top one million most popular and most used websites as ranked by Alexa.[59]

While nearly 93 percent of the web contains ordinary content, every 20th website shows pornography and 2.1 percent provides other salacious content, such as web proxies, gambling, malware, phishing, and so on.

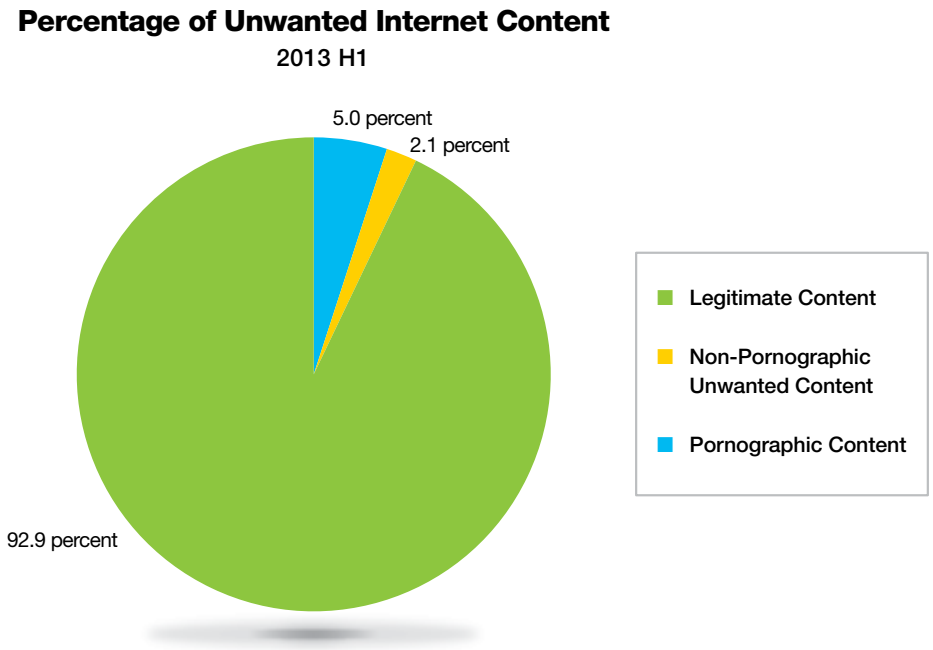


Figure 12: Percentage of Unwanted Internet Content – 2013 H1

59 According to the site ranking by Alexa: http://www.alexa.com/

Website categories containing malicious links

As malware is spread all over the Internet one might ask the question whether there are more or fewer dangerous areas. When looking at the content category of websites indeed we detect differences in the risks.

- The most risky single content area of the Internet is contained within sites hosting pornography. These sites were responsible for nearly 23 percent of all the malicious links found.
- Dynamic websites like blogs where users can contribute content through articles, comments, and messages are the second most dangerous area of the Internet. The bad guys are using these platforms to place the malware and 16.5 percent of all bad links are found on those sites.
- Even some sites in reasonably safe catagories of "traditional" websites, such as portals and personal homepages are found to be hosting 8 percent and 5.7 percent respectively.
- Another hot category is gambling sites that are found to host 7.9 percent of all the malicious links.
- Thirty-nine percent of the malicious links are widely spread over other content categories—we listed these as "other". You can safely conclude that the malicious links and malware are lurking everywhere on the Internet.

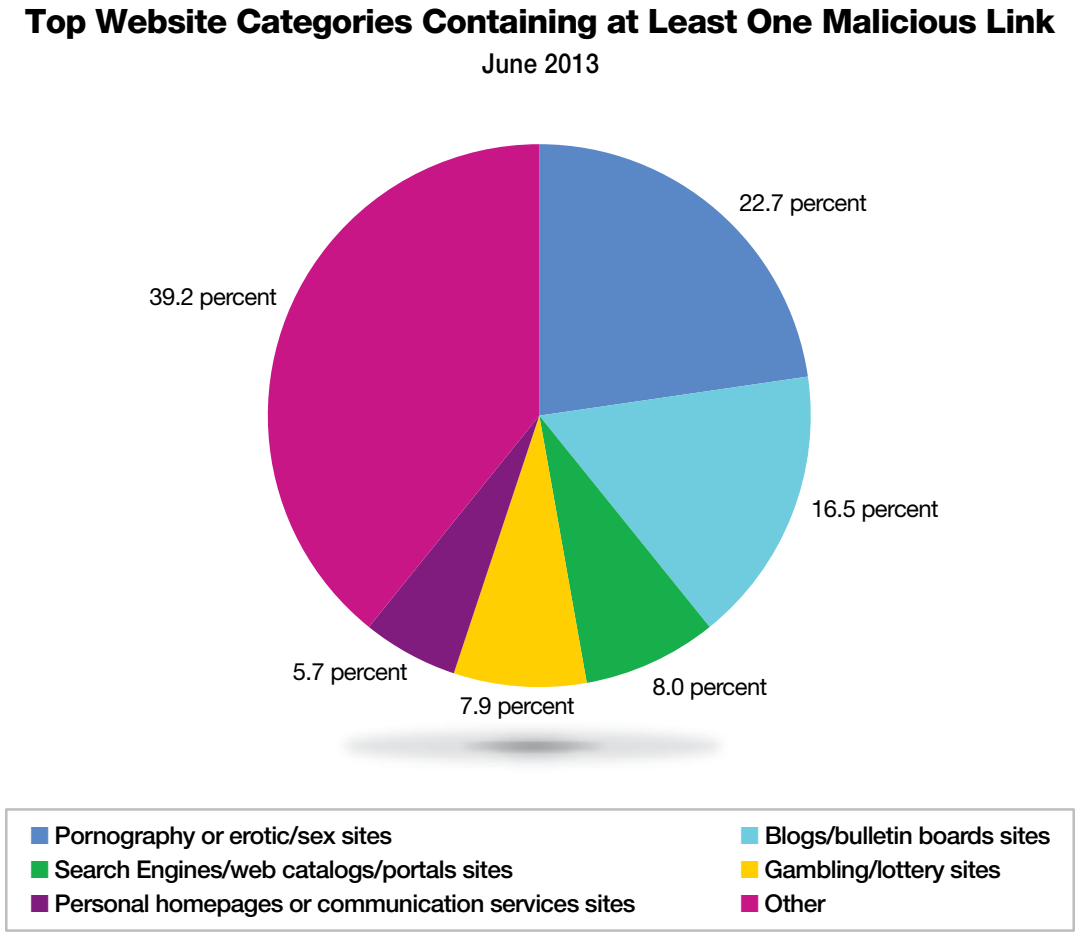


Figure 13: Top Website Categories containing at Least One Malicious Link –June 2013

Geographic distribution of malware and botnet C&C servers

This topic discusses the countries where malicious links are hosted and the geographic distribution of botnet command and control servers (C&C).

- The United States dominates the scene by hosting more than 42 percent of all malicious links.
- The geography with the second highest concentration of malicious links is Germany, with nearly 10 percent.
- The next five countries, positions 3-7, are all found to be hosting very similar amounts of malicious links: China, Russia, Netherlands, United Kingdom, and France host between 5.9 and 3.4 percent of the malware.

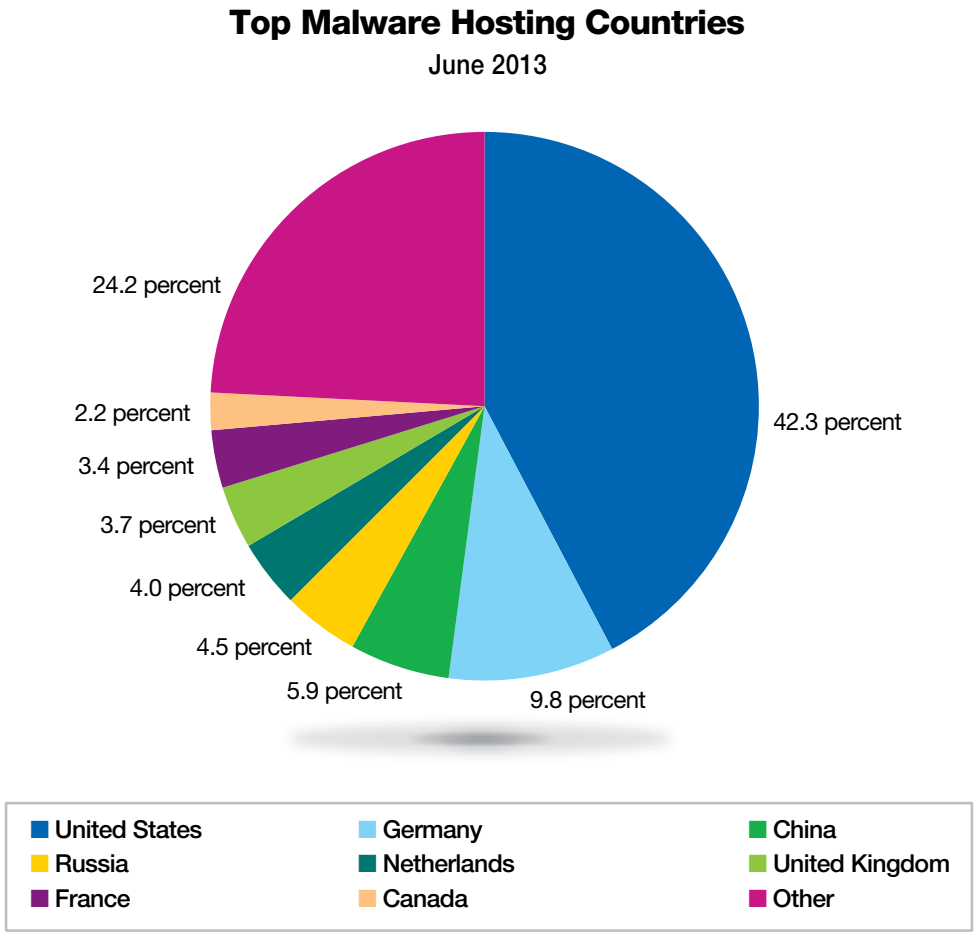


Figure 14: Top Malware Hosting Countries – June 2013

When looking at the geographic distribution of botnet command and control servers (C&C) the picture is similar.

- The country with the largest number of C&C servers with nearly one-third of all C&C Servers is the United States.
- The country with the second highest number of C&C servers is Russia with nearly 10 percent.
- Germany, South Korea, China, and United Kingdom are close together, hosting between 7.0 and 4.2 percent of the C&C Servers.

Botnet Command and Control server
Botnet command and control (C&C) servers are computers that send commands to and receive feedback from other computers that are part of the botnet (botnet drones). Botnets are used for different types of attacks, such as distributed denial-of-service attacks and email spam. To start such an attack, the C&C server sends special commands to its drones to perform the attack on a particular target (which crashes by not being able to cope with so many botnet drones) or to send out a new spam campaign.[60]

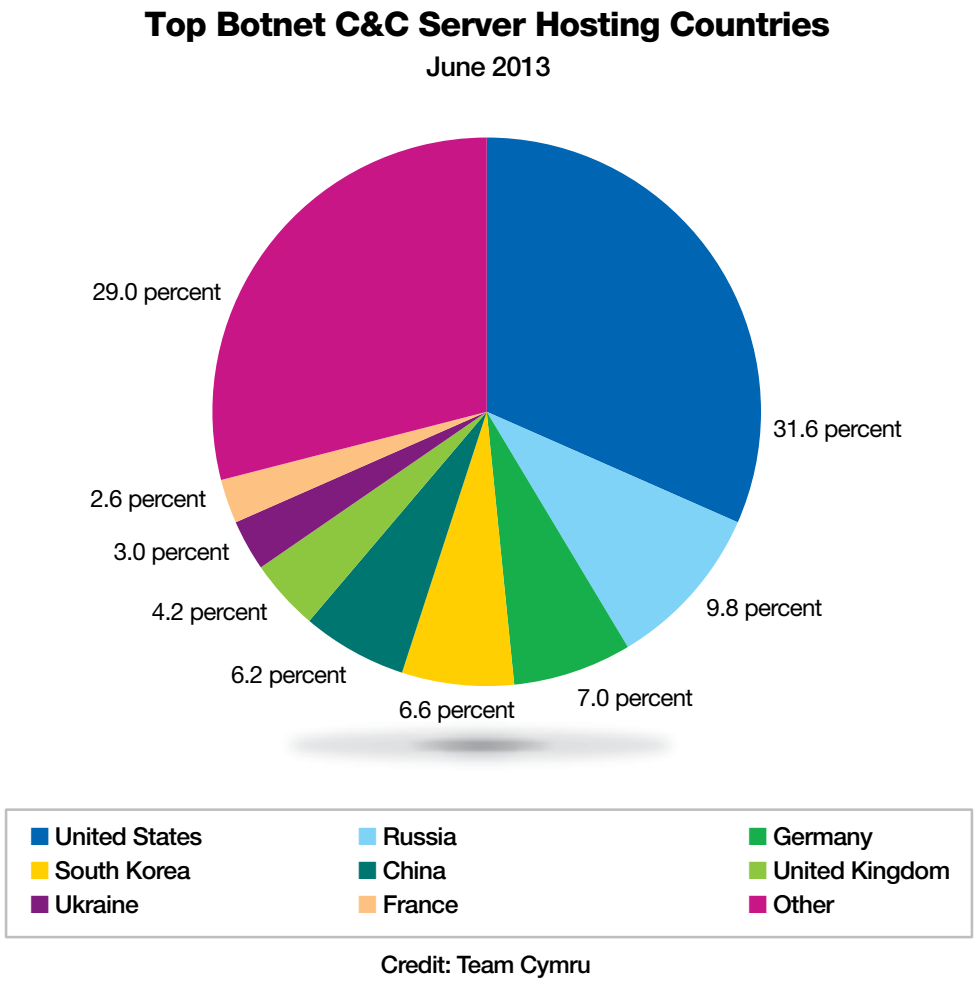


Figure 15: Top Botnet C&C Server Hosting Countries – June 2013 - Credit: Team Cymru

60 For more details see http://en.wikipedia.org/wiki/Botnet

IPv6 deployment for websites

To measure the IPv6 deployment for websites, we have done DNS requests (which check for an AAAA record in DNS) for millions of hosts every week. As IPv4 is running out of space, we expect that more and more Internet sites are switching to IPv6. We have focused our analysis on the 100,000 most popular and most used websites[61] to see how many of them have already stepped into the IPv6 world.

- Of the top 100 most used websites, 32 percent are IPv6 ready—10 percent more than six months ago.
- Nearly 14 percent of the top 1000 sites are IPv6 ready—4 percent more than half a year ago.
- Looking at the top 10,000 sites, almost 6 percent are providing IPv6—up 1.2 percent.

In comparison to the status six months ago, the most accessed Internet sites have already invested in IPv6 availability.

When reviewing the percentage of malware hosted on IPv6 addresses we found it to be only 2.8 percent, and for botnet C&C server IPs only 2 percent of them are hosted on IPv6 IPs. For now, the bad actors still seem to be focused on the IPv4 world which offers more connectivity from all networks using only a small percentage of IPv6 space (so far) for nefarious resources.

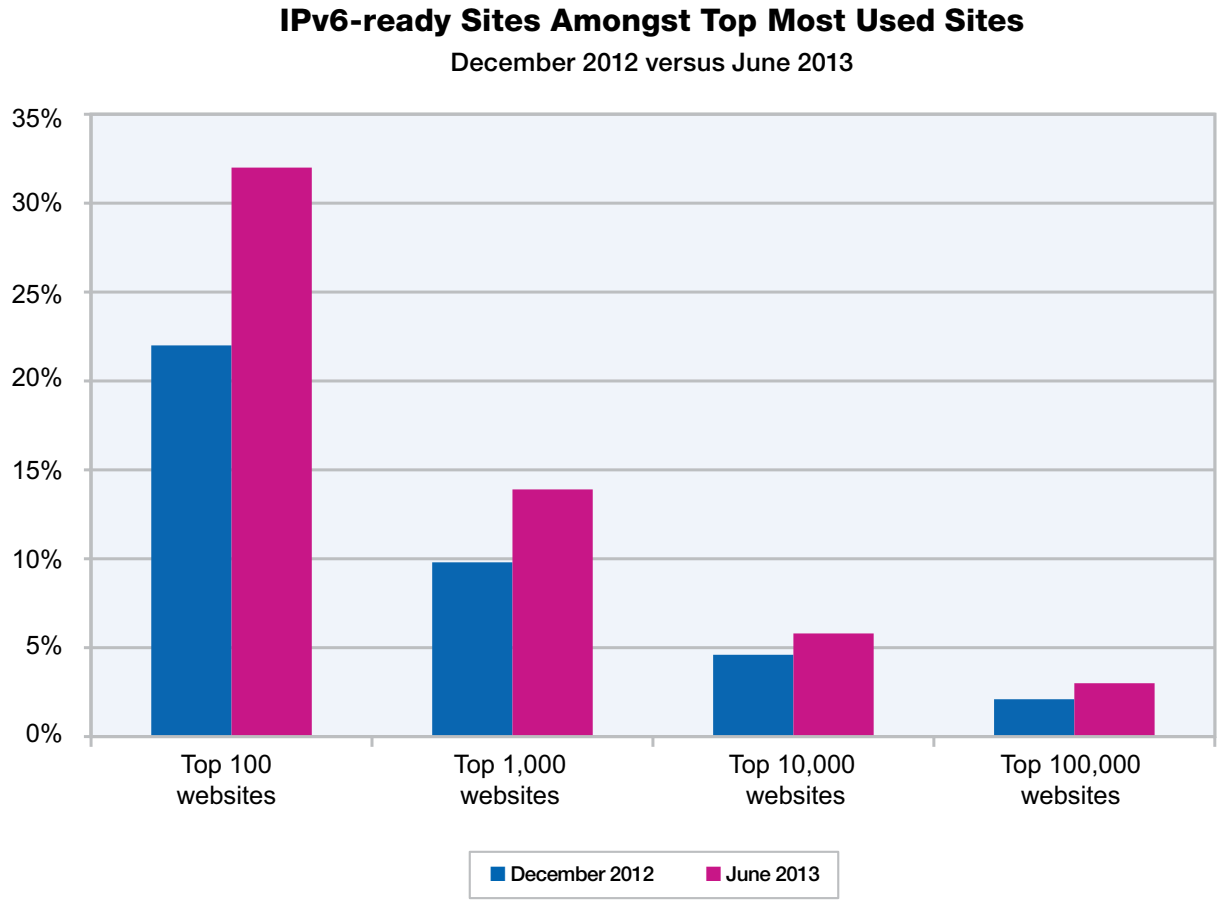


Figure 16: IPv6-ready sites amongst top most used sites – December 2012 versus June 2013

61 According to the site ranking by Alexa: http://www.alexa.com/

Spam and phishing

The IBM spam and URL filter database provides a world-encompassing view of spam and phishing attacks. With millions of email addresses being actively monitored, the content team has identified numerous advances in the spam and phishing technologies that attackers use.

Currently, the IBM spam filter database contains more than 40 million relevant spam signatures. Each piece of spam is broken into several logical parts (sentences, paragraphs, and so on). A unique, 128 bit signature is computed for each part and for millions of spam URLs. Each day there are approximately one million new, updated, or deleted signatures for the spam filter database. The updates are provided every five minutes.

This topic addresses the following topics:

- Spam—country[62] of origin trends
- Scam/Phishing targets by industry

Spam—country of origin trends

When looking at the countries that sent out the most spam over the last two and a half years, some interesting long-term trends become visible.

- Belarus is the new star with spam, sending out 10 percent in the second quarter of 2013.
- In the first quarter of 2013, and for the first time in two years, the USA took over the leadership position by sending out 12 percent, but then declined to about 8 percent in the second quarter.
- In the first half of 2013, Spain reached the top three for the first time in years.
- While India dominated the scene at the end of 2012, and sent out more than one-fifth of all spam in the third quarter of 2012, it was passed in the last six months by Belarus, the USA, and Spain.
- Argentina and Italy reached the top five and top six positions for the first time in years.
- Saudi Arabia did not repeat its performance of the third quarter of 2012 in sending out spam and remains flat at around 1 percent.

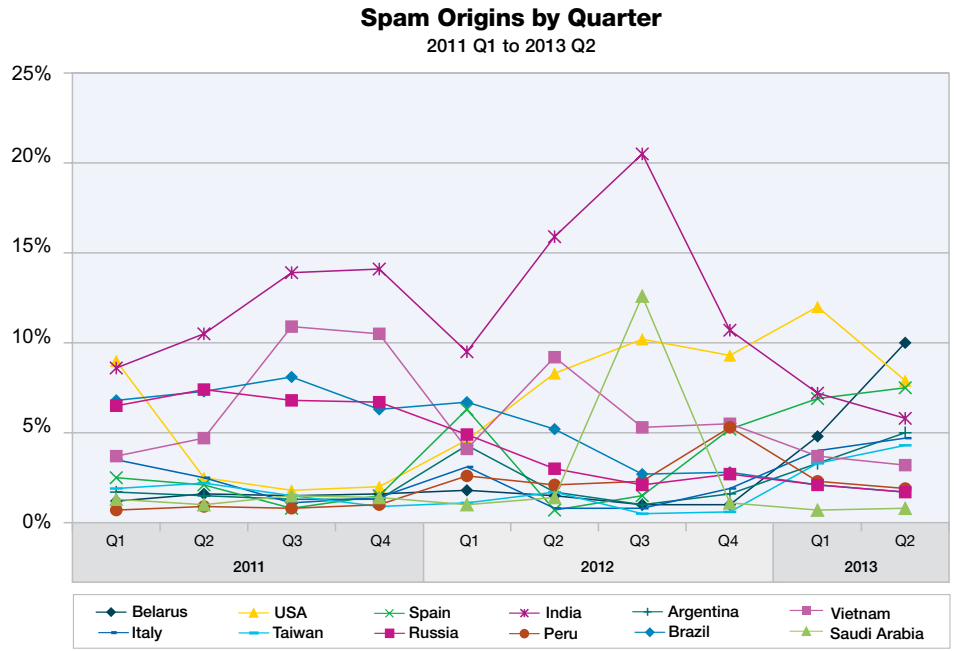


Figure 17: Spam Origins per Quarter – 2011 Q1 to 2013 Q2

62 The statistics in this report for spam, phishing, and URLs use the IP-to-Country information that comes directly from the five Internet Registries (ARIN, AfriNIC, APNIC, RipeNCC, LacNIC). The geographical distribution was determined by requesting the IP addresses of the hosts (in the case of the content distribution) or of the sending mail server (in the case of spam and phishing) into this IP-to-Country information.

Scam and phishing targets by area

In this section we review scam and phishing incidents related to specific areas. The statistics are calculated according to the following conditions:

- The statistics are exclusively based on scams and phishing campaigns deployed via email.
- The statistics include all emails that use the trusted name of well-known brands to make users click on a provided attachment or link, even if this attachment or link is not phishing-related. Hence, some of the included emails are only "phishing-like" emails.
- The statistics do not include any non-email related phishing attempts; such as keystrokes that record phishing malware that was provided through drive-by downloads.

Additional information about the methodology of the provided scam and phishing statistics can be found in the corresponding section of the IBM X-Force 2011 Trend and Risk Report.

- The top three campaigns observed enticing users to click on bad links and attachments in emails are Internet payment companies, social networks, and internal scanners or fax devices. Together these three focus areas account for more than 55 percent of all scam and phishing incidents.
- In positions four and five, there are emails pretending to be from parcel services and from financial institutions. These two focus areas account for 12.9 percent and 10.1 percent of these types of scams.

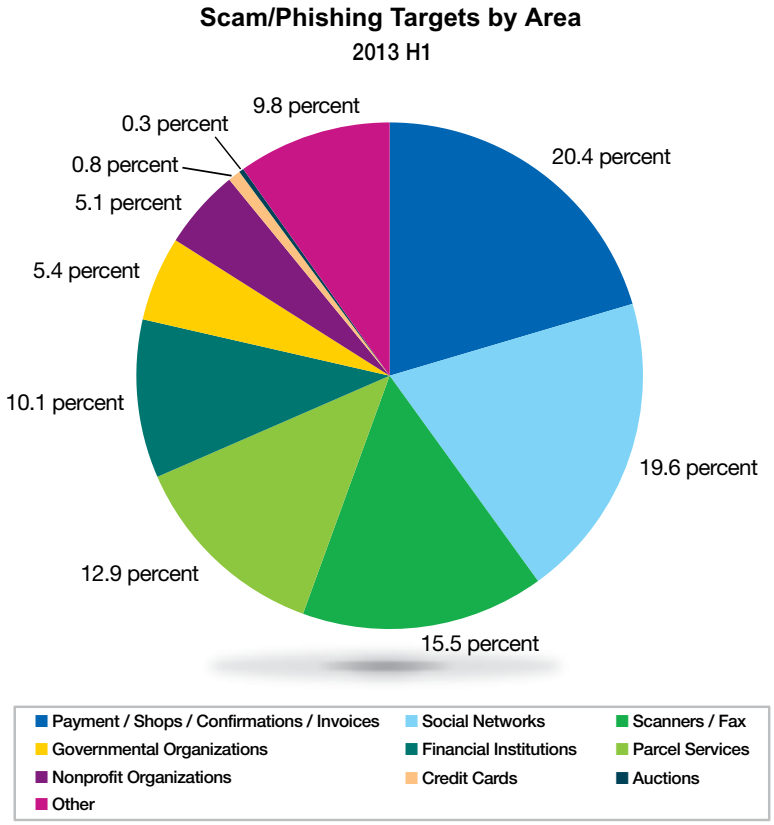


Figure 18: Scam/Phishing Targets by area – 2013 H1

- There are still a considerable amount of email scams that look as though they come from government organizations (such as the U.S. Federal Bureau of Investigations (FBI) or the tax authorities) or non-profit organizations; for example, the Better Business Bureau (BBB).

In comparison to last year, there are no major changes concerning these types of spam, neither in targeted brands nor technically within the emails. Obviously, from the scammers perspective, this is a well-established approach to get users—maybe new—to click on links and attachments. The following techniques work well for scammers:

- The initial amazement of a user when he receives an email that looks as if it came from the tax authorities and threatens with a high additional payment of taxes.
- Employees who are awaiting a fax, a scan, an order confirmation, or a message from the social network they have joined.

Security practices

The challenge of addressing vulnerabilities—reducing the attack surface

Many security teams struggle with vulnerability management, despite it having long been a core requirement of an organization's security practices. Vulnerability management helps organizations fully understand the extent of their exposures as well as the overall security state of their networks. The primary reason for this challenge is the sheer number and arrival rate of new vulnerabilities introduced into their environments by operating system software and third-party applications. This is exacerbated by the relatively manual and slow process of mitigating and patching these weaknesses. Typical networks might, on average, expect to see anywhere between 10-30 vulnerabilities per IP address in their environment. Some will have none and some will have hundreds, with the numbers changing daily.

These numbers simply overwhelm many enterprises so they focus on patching and protecting critical business servers and those that are more likely to be attacked. These servers include those that control or maintain business critical processes and data, are reachable from the Internet or from untrusted networks, or those that potentially harbor unknown threats. Yet in today's environment where the perimeter is much more porous, this isn't adequate because it does not guard against internal threats, Trojan horses, or other threats brought in from the outside due to the behavior of users on their networks.

To reduce the probability of being exploited, the focus needs to shift onto reducing the potential attack surface.[63] The attack surface is represented by those vulnerabilities that are most accessible to potential attackers. The accessibility of vulnerability to attack is defined primarily by the context of the network in which it resides. To make vulnerability management more effective, techniques that incorporate network context into the process need to be applied. Some effective techniques are listed below.

Understanding what is active and what is not

The majority of vulnerabilities are detected by scanners using a process called authenticated scanning. This involves logging into an endpoint, scanning for the installed software, retrieving its specific version and patch level, and then examining vulnerabilities known to be in that version. The key issue with this process is that the vulnerability scanner doesn't know whether or not that vulnerable application is active on that host. Clearly, active applications offer far greater potential to a would-be attacker than those that are dormant. Examples of inactive software that a vulnerability scanner will detect include:

1. Internet Explorer installed on servers where it is never used
2. Web application and server software installed that are not active
3. Embedded application databases that are not accessible remotely

In the current climate of auto-installed software and quick downloading to test software by end users, network administrators can expect that up to 60 percent of vulnerable applications on their networks are inactive. This presents a powerful tool to help focus on the vulnerabilities and hosts that should be remediated first.

Threat awareness and usage knowledge

It may seem obvious, but vulnerabilities are not an issue until someone or something attempts to exploit them. In many networks, the majority of end points do not communicate with malicious hosts or those that potentially could be malicious. Yet, there is a subset of endpoints that do. For example, take two endpoints that have Internet Explorer installed, both vulnerable. One browses the Internet day in and day out; the other is used on occasion to access the local intranet site. It is clear that the former, because it is in regular communication with a potential threat, has a much greater attack surface than the latter. Of course there are more specific threats on the Internet, and there can also be threats, or potential threats, within an enterprise. Examples of potential threats include assets that have been communicating with:

1. Known malicious IPs and websites on the Internet
2. Untrusted partner networks and wireless networks
3. Assets that have been potentially compromised or that are behaving abnormally
4. Assets that have been used by a potentially compromised user account
5. Assets that have a specific vulnerability or other weak security configuration

Applying threat intelligence of this dynamic environment to the vulnerability management process, is an effective tool that enterprises can use to ensure that vulnerabilities most likely to be exploited are mitigated or remediated first.

63 Controlling The Big 7 http://www.darkreading.com/vulnerability/controlling-the-big-7/240157835

Mitigations and remediation

Many enterprises invest significantly in perimeter defenses such as firewalls, intrusion prevention system (IPS) devices, and endpoint management systems to automatically apply the latest approved patches on hundreds and thousands of endpoints. These perimeter investments can be leveraged significantly by integrating them more closely with the vulnerability management process by understanding which vulnerabilities are currently mitigated from exploitation by firewall and IPS rules, and which are still an open risk. This is an effective technique to narrow the focus to a subset of vulnerabilities that are most likely to be exploited.

Further, having a vulnerability management system which is able to provide clear reporting on which specific vulnerabilities are scheduled to be patched by an endpoint system, and which ones are not, helps ensure that remediation efforts are directed most efficiently.

In practice, enabling vulnerability management with additional contextual data will require it to be seamlessly integrated with a security intelligence system with both a real time and an historic view of network activity, including what the current threat environment looks like and what the status is of current security controls.

For more information
To learn more about IBM X-Force, please visit:
http://www-03.ibm.com/security/xforce/

Inactive: Network flow data can help identify if applications are active

Blocked: Firewall and IPS rules can identify what vulnerabilities are exposed

Patched: Integration with patch management will reveal what vulnerabilities will be patched

Exploited: Integration with threat platforms can alert when specific vulnerabilities are attacked

Critical: Vulnerability knowledge base, remediation flow and policies inform about business critical vulnerabilities

At Risk: Usage and threat data can be used to identify what vulnerabilities are at risk

Techniques to reduce the attack surface represented by vulnerabilities

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
September 2013

Please Recycle

WGL03036-USEN-01