IBM Security Solutions
January 2010

IBM X-Force Threat Insight Quarterly

Contents

About the report

The IBM X-Force® Threat Insight Quarterly is designed to highlight some of the most significant threats and challenges facing security professionals today. This report is a product of IBM Managed Security Services and the IBM X-Force research and development team. Each issue focuses on specific challenges and provides a recap of the most significant recent online threats.

IBM Managed Security Services are designed to help an organization improve its information security, by outsourcing security operations or supplementing your existing security teams. The IBM protection on-demand platform helps deliver Managed Security Services and the expertise, knowledge and infrastructure an organization needs to secure its information assets from Internet attacks.

The X-Force team provides the foundation for a preemptive approach to Internet security. The X-Force team is one of the best-known commercial security research groups in the world. This group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM security products, and educates the public about emerging Internet threats.

We welcome your feedback. Questions or comments regarding the content of this report should be addressed to XFTAS@us.ibm.com.

Why Can't We Be Friends? An Insight into the New Threat Landscape Introduced within Social Networking

By David MacKinnon

Over the last few years, social networking sites have become a part of people's daily routines. These sites enable people to reconnect with old friends, communicate and collaborate with others and share pictures with distant friends and relatives. At the same time, it also opens up a new arena for those with malicious intent.

Background

Social networking popularity continues to grow at an incredible rate. Earlier this year, one of the most popular sites—Facebook—announced that it broke the 300 million user mark. QZone, Twitter, MySpace, Vkontakte, LinkedIn and many others, also have a large number of visitors accessing their site daily. The current adoption rate of social networking sites is second to none. Facebook alone grew from 200 to 300 million users in just five months.[1] In comparison to the adoption rate of other technologies, this is unheard of. For example, it took 38 years for radio and 13 years for television to each reach an audience of 50 million.[2]

One of the more unique aspects to social networking is the trend away from the expectation that a computer is the only medium for contact. The growth of mobile technologies allows users to update their status from virtually anywhere. It is estimated that one quarter of Facebook users access the site via mobile devices, growing by 45 million users in just nine months.[3] While this drives the social aspect of the medium, it also introduces a new attack vector—one that can be propagated via these social networking sites.

So what does this mean for the average person? The answer varies based on whether you're a security professional, a system administrator, or an average user of social media. This article is intended merely to help educate readers on the various threats that currently exist, so they can be prepared to combat this activity in their environment.

Phishing

Phishing is not new to the Internet. It's been around since the 90s, and over time has become more sophisticated. Initially, email was the typical medium for phishing attacks. An email that appeared to originate from a financial institution would ask users to update their account information. When the user clicked the link, they would be directed to a malicious site that mirrored the site of their legitimate financial institution. These sites worked to extract victims' account information, usernames and passwords without the victims' knowledge.

This trend has moved into social networking through two main types of phishing schemes. The first is via malicious emails and Web sites. Users are presented a link to what appears to be their social networking site of choice. These sites are perfect replicas of the real sites, and once users attempt to log in, their credentials are stolen. The second method of exploitation is accomplished via messages received within the social networking site itself. Users receive a message instructing them to install an update tool for their account. What the user is installing is really malware, which also steals the user's password.

Once account credentials are obtained, a number of avenues are opened for attackers who now have the ability to send additional phishing messages, promote malware, attempt to extort money, and perform identify theft. In the sections below, we will cover some of the common ways that these various attacks are performed.

[1] **300 Million and On** http://blog.facebook.com/blog.php?post=136782277130

[2] **United Nations Cyberschoolbus** http://www0.un.org/cyberschoolbus/briefing/technology/tech.pdf

[3] **Growth of Facebook Mobile Site** http://techcrunchies.com/growth-of-facebook-mobile-site-2/

Malware/Spyware

In the past, malware has traditionally been distributed via email, compromised Web sites, and more recently, compromised PDF and flash files. Over time, these exploitation methods have proven to be effective and rapidly propagated, and fortunately, they have also been very quickly mitigated. With the rapid adoption of social networking sites, an entirely new arena has opened up for malware developers, and they have wasted no time producing code.

Previously, the most common malware propagation technique was via malicious links in messages sent within the social networking application itself. These messages typically originated from users that were already infected with this malware. The links were portrayed as video clips, and when users clicked the links, they were prompted to update their systems Flash® player. More recently, these attacks are coming through fake malicious accounts, which have been created within the social networking sites. These accounts also have video links that prompt for an update, or appear to notify the user of a virus on the user's system.[4] In reality, the message, is installing malware, and the next time the user logs into a social networking Web site, the virus sends malicious messages to all of the infected user's contacts.

One of the first occurrences of spyware on Facebook propagated through a third-party application available to the system. Users received a message from the system that they have a "secret crush," and needed to install the application to find out from whom. Once installed, the application immediately asked a user for five friends to send links to, thus extending the potential number of infections. Finally, it popped-up an advertisement linking to additional software to install. In reality, any users who downloaded and installed this were installing Zango adware.[5]

In a more recent event, the CEO of Zynga, a very popular social gaming company, boasted about his efforts to exploit these creations for profit. The software company configured the games to allow players to advance through the game more rapidly. Leveraging credits, players were given the opportunity to receive credits by either purchasing them, or worse, installing various Adware/Spyware on their system in exchange for credits.[6]

A new vector for social network sites has been the usage of these sites as command and control channels for infected systems. Both Facebook and Twitter have recently had Trojans that utilized this medium. On Twitter, infected clients would receive tweets with base64 encoded strings providing the Trojan commands to perform on the system.[7] Clients infected with the Facebook variant would monitor the Notes section of Facebook user profiles for commands to perform on the client machine.[8]

[4] Facebook Shuts Down Fake Profiles Designed to Spread Malware http://www.enigmasoftware.com/facebook-shuts-down-fake-profiles-designed-to-spread-malware/

[5] Facebook Widget Installing Spyware http://www.fortiguard.com/advisory/FGA-2007-16.html

[6] Zynga CEO Mark Pincus: "I Did Every Horrible Thing In The Book Just To Get Revenues" http://www.techcrunch.com/2009/11/06/zynga-scamville-mark-pinkus-faceboo/

[7] Twitter-based Botnet Command Channel http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/

[8] Trojan pokes Facebook for zombie commands http://www.theregister.co.uk/2009/11/03/trojan_cnc_pokes_facebook/

Facebook has been proactive in its attempts to protect its user base. In addition to built-in security measures, they also use a third-party service to protect users from both phishing and malware.[9] Unfortunately, even with these added security measures, both application and malware developers continue to find unique ways to bypass these checks.

The new 419 Scam

In our Q2 '09 edition of the Threat Insight Quarterly, the article "Fraud Schemes; I love you. I will make you rich. Oh, and I need some money moved" covered romance schemes and how they attempt to take advantage of unsuspecting individuals with the intention of financial gains. This type of scam has extended to social networking sites, but they've added a new twist—the person asking for money is one of your friends.

As with other 419 scams, this too has proven quite successful. Earlier this year a woman in Cape Girardeau, MO sent multiple payments totaling $4,000 to help what she believed to be one of her friends.[10] Once the money is sent, there is little to no chance of recovering the funds.

The setup is really quite simple. Users receive either a message or a chat from one of their friends asking for help—they're on vacation in the United Kingdom, and they've been robbed. They have no money or credit cards, and they need your assistance to pay their outstanding hotel bill. They conveniently have a Western Union located only a few minutes away, and ask if you can wire them some money.

The user accounts that propagate this request are typically stolen accounts that are obtained by either users infected by malware or users who followed a phishing link. Once the account is taken over, the password is changed and any direct relationships (wife, girlfriend, etc.) are removed. The attacker then contacts all of their compromised accounts' contacts and makes the request.

Data gathering/Identity Theft

I think everyone has received one of those "get to know your friends" emails, where you learn about, among other things, your friends' first car, the schools they attended, and their pets' favorite colors. These types of emails have been circulating since the 90s, and they're making a comeback in social networking. What most people don't consider when filling out these surveys is how much information they're giving away. Have you ever looked at some of the security questions that your bank uses to verify your identity? Have you ever noticed the answers to some of those very same questions listed on your social networking account?

I know what you're thinking; it's no big deal, the only people who can see that information are my friends. To that, I ask you, what about the many third party applications that exist within social networking sites. These applications, by default, have the ability to see and gather information from not only the account that added the application, but also all of those users' contacts. Add to this, the risk of either your account or one of your friends' accounts becoming compromised, and think about how much of your personal data are readily available. Most online financial Web sites take advantage of two-factor verification for their customers. The first step is the typical username and password combination. The second step is for the user to answer personal questions to properly identify that user. If you use the same credentials for your social networking site as your financial institution, then it's fair to say that there's a high probability that your finances are at risk.

There are a few simple things that can be done to avoid this. First, ensure you use different passwords for your accounts. Second, when you are filling out anything that will be visible to other users, take note of the questions that match those of your financial institution and leave them blank.

9 Facebook Selects MarkMonitor Antifraud Solutions to Combat Malware http://www.circleid.com/posts/20090430_facebook_markmonitor_antifraud_malware

10 Cape Girardeau woman loses $4000 to hacker on Facebook http://www.kfvs12.com/Global/story.asp?S=11043673

Mobile threats

As mobile phone technology continues to evolve, manufacturers work to integrate as many new features as they can into their products. For the end user, this is usually viewed as a luxury, but it is also an opportunity for those with malicious intent. Currently, most social networking sites have an application that directly ties their site into mobile phones, and this extends the application's features beyond the computer and into users' phones. This also provides a medium for mobile malware to be distributed.

Earlier this year a very large malware outbreak hit Symbian based smartphones. This malware took advantage of a flaw in Symbian's signing code and provided very deep access to the device. Once infected, devices collected all of the personal information from the phone and broadcast it out to a pre-programmed set of servers. Additionally, the application can send text messages to all of the phone's contacts in an attempt to infect them as well.[11]

In another example, jailbroken iPhones were targeted. When iPhones are jailbroken, they use a default root password for the system. A worm was developed as a prank, which changed the wallpaper of the infected device.[12] While this prank was not overly malicious, within days, a new exploit with malicious intent was spotted on the internet.[13] Both of these exploits took advantage of users who had not changed the default password as a means to compromise the device, and once compromised, all of the data on the system was available.

At this time, no known mobile exploits have originated via social networking sites. Based on how rapidly the technology is advancing, and the tight integration between new mobile technology and social networking, I believe it's only a matter of time before this occurs.

Conclusion

A colleague of mine has a quote in his email signature, and I believe its use is quite fitting here. The quote reads, "Trust but verify." This truly is a great rule of thumb when using social networking sites. By default, a certain level of trust is extended to all of your friends, as they would never deliberately intend to harm you, but it never hurts to be sure. If your friend sends you a link that looks questionable, make sure it's legitimate prior to clicking on it. If they send you a message about being stuck in a foreign land and need money, ask them specific questions that only they would know to verify their identity. If you receive a software update from your favorite site, don't install it. Instead, in another browser window, visit the vendors' site directly and verify that an update is necessary. Ultimately, it's always good practice to ensure you keep your operating system, browser, and security software patches up to date when utilizing the internet, and especially when using social networking.

[11] Could Sexy Space be the Birth of the SMS Botnet? http://www.symantec.com/connect/blogs/could-sexy-space-be-birth-sms-botnet

[12] iPhone worm plays prank, but signals danger ahead http://www.scmagazineus.com/iPhone-worm-plays-prank-but-signals-danger-ahead/article/157452/

[13] Attack tool can hijack data off unlocked iPhones http://www.scmagazineus.com/Attack-tool-can-hijack-data-off-unlocked-iPhones/article/157587/

Advisory Monitoring in a Heterogeneous Enterprise Environment

By Troy Bollinger

A vulnerability[14] is a flaw or weakness that allows an attacker to gain unauthorized privileges or to impact the availability of a system. Vulnerabilities are a unique bug class that require a different approach to patching. This derives from the way the underlying bug is triggered. Vulnerabilities are subject to deliberate targeting, which means that administrators have less control over how the behavior affects their system. Because of the dynamic nature of vulnerabilities, customers don't have the luxury of scheduling the updates like they can with ordinary bug classes.

History has shown that vulnerabilities will be discovered in software and vendors have an obligation to their customers to provide notification when there are available fixes. System administrators in large organizations routinely support multiple products from multiple vendors. Keeping up to date with the latest security patches is challenging in such a large environment. Unlike consumer desktops, enterprise environments cannot take advantage of auto-updates pushed from the vendor. They must perform interoperability testing and then roll out patches according to business driven guidelines like change freezes.

In the past, many vendors chose to hide details about vulnerabilities—in part to prevent bad publicity. Conventional wisdom claimed this practice was designed to prevent attackers from using the details to attack customers. However, this also prevented customers from understanding the risks they faced in delaying, or even avoiding, patch installation. As time passed, vendors brought a more balanced approach to the way vulnerability patches were handled. It is has long been known that dedicated attackers could reverse engineer binary patches even in the absence of details provided by the vendor. The goal of responsible vulnerability disclosure is to provide customers with the necessary amount of information required for them to assess their risk and deploy patches before the attacker can develop and weaponize exploitation. It's a race that can only be won with complimenting processes by both vendor and customer.

There are three phases in the notification process whereby vendors can improve the ability of customers to assess their risk and protect against exploitation. The phases are monitoring, retrieving, and parsing vulnerability patch announcements.

Monitor notification channels

The first step for vendors is to provide a clear, consistent, and flexible mechanism for announcing critical fix availability. The mechanism can include a pre-announced schedule for releasing advisories, perhaps monthly or quarterly. This allows customers to allocate personnel and resources to treat each release in a "business as usual" fashion. However, there should also be a documented process for handling vulnerabilities that are too severe to wait for the next cycle. Customers must know that they will be aware of each announcement and not miss one in a sea of other vendor communications.

Vendors have a variety of options at their disposal. Examples include RSS feeds, Web archives, mailing lists, and knowledge bases. Each has its own set of advantages and disadvantages for the customer.

RSS feeds can be monitored with a multitude of readily available tools, making it one of the more popular options. RSS items typically contain only a subset of the announcement text, thereby requiring additional steps be performed to complete an analysis of the issue. Web archives are also popular, but vendors need to structure the HTML[15] so that it is easy to parse as part of the customer's automated monitoring process. Liberal use of "div" and other non-table tags should be used to delimit the advisory description, patches, and other sections of the advisory.

[14] CVE – Terminology http://cve.mitre.org/about/terminology.html
Definition of a Security Vulnerability http://technet.microsoft.com/en-us/library/cc751383.aspx

[15] What Beautiful HTML Code Looks Like http://css-tricks.com/what-beautiful-html-code-looks-like/

In general, mailing lists lack a context outside of a specific notification, making it difficult for customers to know whether a list has been abandoned or whether there just hasn't been any patched vulnerabilities lately. However, mailing lists provide a "push" capability that instantly notifies customers. Perhaps the best approach is a combination of vendor notification mechanisms that combines "push" notification along with an easy to parse Web archive to provide historical perspective.

If at all possible, vendors should store and announce their advisories separate from bug fixes. The vendor is in a unique position to identify vulnerability fixes, while customers often lack the expertise to make a judgment as to whether or not a particular bug can be triggered by an attacker in such a way as to gain unauthorized privileges. By separating announcements into different repositories or knowledge bases, it decreases the likelihood that customers will overlook critical fixes.

If a separate vulnerability patch repository is not available, vendors should use consistent tag identifiers so that the complete set of vulnerability announcements can be retrieved from their search engine.

Retrieve advisories

Vendors often place restrictions on how their advisories can be retrieved. Often, this is done by limiting the distribution of the information so as to prevent the appearance of poor quality control on the part of the vendor. Restricting access to this information is often enforced by limiting the access to customer support contract information, and by storing the advisories behind an access-controlled login. Even when login credentials are available to the public, there are often legal clauses in the fine print that prohibit or limit disclosure.

These restrictions can complicate the evaluation process. Customer security personnel are often required to assess the vulnerability severity in order to prioritize the administrator work load. Depending on the size of the organization, the security personnel may not have access to customer support numbers or other information required by the vendor to access the notifications.

Parse advisories

Once the notification has been received, it must be parsed into actionable items. Advisories typically contain a brief description of the vulnerability that includes the impact and any possible mitigation methods that can be employed if patches cannot be applied immediately. Descriptions should also include a mechanism for determining if the fix needs to be applied and how to tell if it has not been applied. This can include patch or package version numbers, as well as instructions on where to find and apply the patches. CVE numbers should be included so customers can cross-reference vulnerabilities across multiple vendors to ensure that other products in their environment are not left vulnerable. Vendor calculated CVSS scores should also be included to help provide some perspective on the impact of any possible exploitation attempts.

The overall format and content of the announcement will depend on many factors, such as the vendor's overall corporate culture and existing support infrastructure. The format of the advisory doesn't have to be based on an industry standard or have the same look or structure as other vendors. However, it should be a standard format across the company's product line so that customers can use a uniform process for interacting with that vendor.

In addition to providing advisory text that is clear and simply explained in a language recognized by the "human" customer, it is very helpful for vendors to provide a machine readable version of the advisory so that compliance checking processes can automatically determine whether a machine is up-to-date. The machine readable version typically includes patch numbers and package versions, along with an identifier that can be cross-referenced to the human-friendly version.

Conclusion

Managing a large environment that supports multiple vendor products while maintaining an overall security posture is a challenge. Vendors can help protect customers by providing critical notifications in an easy to process format. Customers can then use these notifications as part of a comprehensive compliance process. There have been some recent efforts to standardize[16] the vendor vulnerability notification process by an ISO working group for "Responsible Vulnerability Disclosure".[17] At the time of writing, there was no available public draft. The hope is that when it is finally published, it will provide additional direction and details for vendors looking to improve their advisory announcement process.

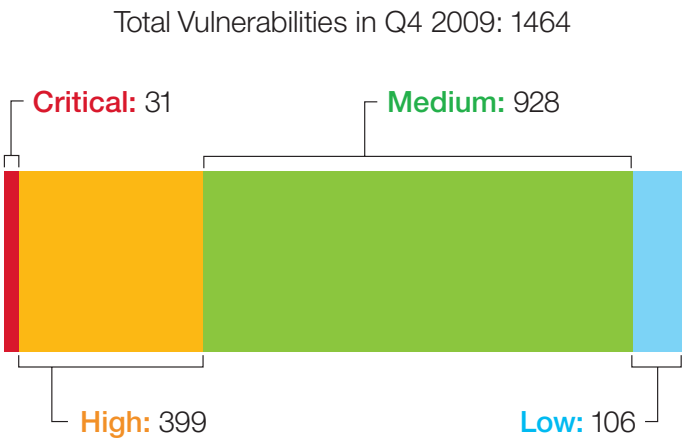
[16] Security, Equality, Fraternity: Behind the ISO Curtain http://blogs.msdn.com/katie_moussouris/archive/2009/11/14/behind-the-iso-curtain.aspx

[17] ISO/IEC NP 29147 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45170

Prolific and Impacting Issues of Q4 2009

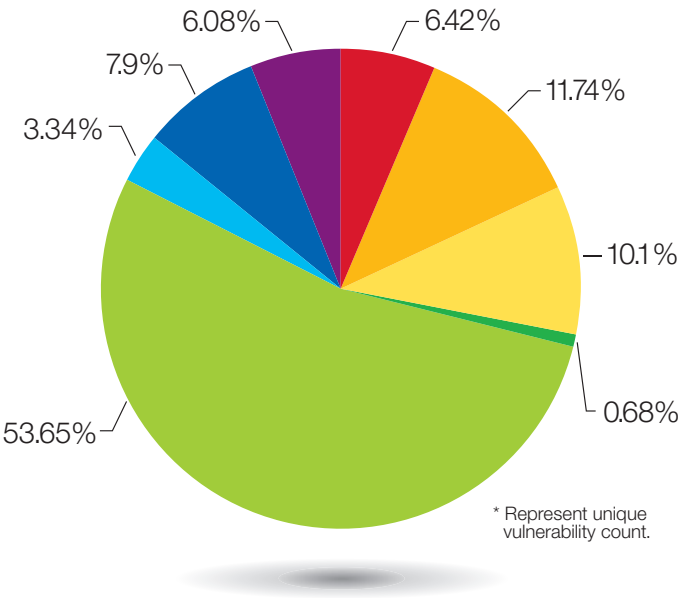
Significant disclosures

In Q4 2009, the X-Force team researched and assessed 1464 security related threats. A significant percentage of the vulnerabilities featured within the X-Force database became the focal point of malicious code writers whose productions include malware and targeted exploits.



Source: IBM X-Force

The chart below categorizes the vulnerabilities researched by X-Force analysts according to what they believe would be the greatest categories of security consequences resulting from exploitation of the vulnerability. The categories are: Bypass Security, Data Manipulation, Denial of Service, File Manipulation, Gain Access, Gain Privileges, Obtain Information, and Other. *



Source: IBM X-Force

Bypass Security	Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner.
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 to take down a network.
File Manipulation	Create, delete, read, modify, or overwrite files.
Gain Access	Obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system.
Gain Privileges	Privileges can be gained on the local system only.
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.

This quarter, the X-Force team produced a total of three protection advisories[18] and eight protection alerts[19] to address a variety of significant threats. Additionally, IBM raised its Internet Threat Level to AlertCon 2 on two different occasions.

In early October, X-Force analysts detected a 0-day Adobe Reader and Acrobat issue being actively exploited in the wild. This vulnerability could result in remote code execution caused by an error related to the handling of PDF files. Successful exploitation requires an attacker to persuade a victim to click a malicious Web page or open a malicious file. Links to these malicious documents can easily be sent through spam or through links on seemingly non-malicious Web sites.

- A protection alert provided by IBM X-Force: Adobe Acrobat and Acrobat Reader Remote Code Execution[20]
  - IBM X-Force Protection Signature: PDF_Javascript_exploit
- CVE-2009-3459
- Adobe Security Bulletin APSB09-15: Security Updates Available for Adobe Reader and Acrobat[21]

Microsoft's October 2009 Security Release addressed thirty-three vulnerabilities, of which, the X-Force team found nine to be most significant. The first issue is one discovered by the X-Force Research & Development team affecting Microsoft Internet Explorer that could allow an attacker to execute arbitrary code on a system by tricking them into visiting a malicious Web site. Web exploit toolkits are notorious for targeting browser and browser-related exploits like this vulnerability. Compromise of machines may lead to exposure of confidential information, loss of productivity, and further compromise.

- A protection advisory provided by IBM X-Force: Microsoft Internet Explorer Arguments Remote Code Execution[22]
  - IBM X-Force Protection Signatures: Various[23]
- CVE-009-2529
- Microsoft Security Bulletin MS09-054: Cumulative Security Update for Internet Explorer (974455)[24]

[18] Provides information about one or more critical vulnerabilities that were discovered by X-Force and for which X-Force has preemptive security content coverage.

[19] Provides information about one or more critical vulnerabilities for which X-Force has released or will be releasing security content coverage.

[20] A protection alert provided by IBM X-Force: Adobe Acrobat and Acrobat Reader Remote Code Execution http://iss.net/threats/348.html

[21] Adobe Security Bulletin APSB09-15: Security Updates Available for Adobe Reader and Acrobat http://www.adobe.com/support/security/bulletins/apsb09-15.html

[22] A protection advisory provided by IBM X-Force: Microsoft Internet Explorer Arguments Remote Code Execution http://www.iss.net/threats/351.html

[23] Refer to the following URL for associated signatures http://xforce.iss.net/CveSearch.do?p=CVE-2009-2529

[24] Microsoft Security Bulletin MS09-054: Cumulative Security Update for Internet Explorer (974455) http://www.microsoft.com/technet/security/bulletin/ms09-054.mspx

Seven of the vulnerabilities affect Microsoft Windows GDI+ and could allow remote code execution. Exploitation simply involves enticing a user to view an email or a URL that contains a specially-crafted image file. This technique of infecting end-user systems has been employed for many years and continues to be a means of infection today. Compromise means complete control of the end user's system.

- A protection alert provided by IBM X-Force: Multiple Microsoft Windows GDI+ Image Remote Code Execution Vulnerabilities[25]
  - IBM X-Force Protection Signatures: CompoundFile_Shellcode_Detected (CVE-2009-2528), Dot_NET_Shellcode_Detected (CVE-2009-2504), Image_WMF_GDI_Integer_Overflow (CVE-2009-2500), Image_PNG_GDI_Heap_Overflow (CVE-2009-2501), Image_TIFF_GDI_Buffer_Overflow (CVE-2009-2502), Image_BMP_Office_Code_Exec (CVE-2009-2518), Image_PNG_GDI_Integer_Overflow (CVE-2009-3126)
- CVE-2009-2500, CVE-2009-2501, CVE-2009-2502, CVE-2009-2504, CVE-2009-2518, CVE-2009-2528, CVE-2009-3126
- Microsoft Security Bulletin MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)[26]

The last vulnerability in Microsoft's October Security Release that warranted an X-Force Protection Alert affected the Microsoft Windows Indexing Service ActiveX control. By persuading a victim to visit a malicious Web page, a remote attacker could execute arbitrary code on a vulnerable system. Plug-ins, such as this ActiveX control, are one of the top targets of malicious Web exploit toolkit developers. These Web exploit toolkits now account for nearly all browser-related exploits seen in the wild.

- A protection alert provided by IBM X-Force: Microsoft Windows Indexing Service ActiveX Control Remote Code Execution
  - IBM X-Force Protection Signature: Script_Indexing_Service_Corruption[27]
- CVE-2009-2507
- Microsoft Security Bulletin MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)[28]

25 A protection alert provided by IBM X-Force: Multiple Microsoft Windows GDI+ Image Remote Code Execution Vulnerabilities
http://www.iss.net/threats/350.html

26 Microsoft Security Bulletin MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)
http://www.microsoft.com/technet/security/bulletin/ms09-062.mspx

27 A protection alert provided by IBM X-Force: Microsoft Windows Indexing Service ActiveX Control Remote Code Execution
http://www.iss.net/threats/349.html

28 Microsoft Security Bulletin MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)
http://www.microsoft.com/technet/security/bulletin/ms09-057.mspx

The Gumblar threat showed an increase in exploitation resulting in the elevation of the Internet Threat Level to AlertCon 2 on October 22nd. Gumblar first appeared in March 2009 and has been highlighted in previous Insight Threat editions. This growing automated botnet compromises traditionally non-malicious Web servers in order to exploit Personal Computers (PCs) that visit those Web sites. Malware that redirects Google searches is planted on the target PC, which provides the attackers with "pay-per-click" or possibly other types of income. Gumblar also looks for FTP credentials on the PC and uses them to infect new servers. In Q4 2009, the IBM Managed Security Services team observed an uptick in Gumblar attacks that were very effective at compromising the client side victim and propagating their malicious payload worldwide.[29]

In November, a vulnerability affecting the SSL/TLS protocol was disclosed. This vulnerability involves three attack scenarios. Two leverage server-initiated SSL ciphersuite renegotiations and one, the most dangerous of the three, involve a client-initiated SSL ciphersuite renegotiation that is induced by the attacker. The vulnerabilities allow the attacker to prepend data to the client's initial transmission or request. This attack could be used to compromise the security of Web sites that are expected to be protected through SSL/HTTPS. However most Web applications are unlikely to be configured in a way that is vulnerable to this kind of attack. Especially those that might have implemented some type of application-level protection against cross-site request forgery.

This issue does affect a large number of platforms including Web browsers, VPNs, smart cards, and any other application that uses SSL/TLS. The vulnerability could be exploited to cause man-in-the-middle type attacks and could be used to intercept encrypted data. Furthermore, if a Web application allows users to store or transmit arbitrary data from a post request to a location where the user can later retrieve it, an attacker can prefix the victim's entire HTTP request as a post. This post can then be read back out, allowing the attacker to gain access to sensitive information in the process such as cookies or other authentication credentials. This method was used to target Twitter and attackers were able to obtain usernames and passwords after they had been decrypted.

- A protection alert provided by IBM X-Force: Transport Layer Security (TLS) handshake renegotiation weak security[30]
  - IBM X-Force Protection Signatures: TLS_Client_Cipher_Renegotiation, TLS_Server_Cipher_Renegotiation, TLS_Cipher_Renegotiation (multiple)
- CVE-2009-3555

[29] Gumblar Reloaded http://blogs.iss.net/archive/GumblarReloaded.html

[30] A protection alert provided by IBM X-Force: Transport Layer Security (TLS) handshake renegotiation weak security http://www.iss.net/threats/352.html

Of the myriad Microsoft issues disclosed in November, X-Force analysts found two to be of most significance. The first is a remote code execution issue affecting Microsoft Windows Vista and 2008. The attack involves sending a specially-crafted WSDAPI (Service on Devices API) message to the WSD (Web Service Device) services. Although this vulnerability is in a core component of Microsoft Windows' operating systems, it only affects Windows Vista and 2008. Exploitation is remote (although the attacker has to be on the victim's local network) and does not require any user interaction. Successful exploitation provides the attacker with complete control of the end user's system.

- A protection alert provided by IBM X-Force: Microsoft Windows WSDAPI code execution[31]
  - IBM X-Force Protection Signature: HTTP_MS_WSDAPI_Code_Exec
- CVE-2009-2512
- Microsoft Security Bulletin MS09-063: Vulnerability in Web Services on Devices API Could Allow Remote Code Execution (973565)[32]

The second issue from the November Microsoft Security Release that caught our analysts' interests affects Microsoft Windows kernel-mode drivers. A remote attacker could execute arbitrary code on a vulnerable system by persuading a victim to open a specially-crafted file containing EOT font embedded in the document. This vulnerability is in a core component of prevalent Microsoft Windows operating systems: Windows 2000, XP and 2003. Successful exploitation provides the attacker with complete control of the end user's system.

- A protection alert provided by IBM X-Force: Microsoft Windows kernel font code execution[33]
  - IBM X-Force Protection Signature: Windows_Kernel_Font_Code_Execution
- CVE-2009-2514
- Microsoft Security Bulletin MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)[34]

In late November, a proof of concept exploit was made public for a 0-day remote code execution vulnerability in Microsoft Internet Explorer. By persuading a victim to visit a specially-crafted CSS page, a remote attacker could exploit a vulnerability in Microsoft Internet Explorer to execute arbitrary code on the system with the privileges of the victim.

- A protection alert provided by IBM X-Force: Microsoft Internet Explorer mshtml.dll RCE[35]
  - IBM X-Force Protection Signatures: JavaScript_NOOP_Sled, JavaScript_Shellcode_Detected
- CVE-2009-3672
- Microsoft Security Bulletin MS09-072: Cumulative Security Update for Internet Explorer (976325)[36]

31 A protection alert provided by IBM X-Force: Microsoft Windows WSDAPI code execution http://www.iss.net/threats/353.html

32 Microsoft Security Bulletin MS09-063: Vulnerability in Web Services on Devices API Could Allow Remote Code Execution (973565) http://www.microsoft.com/technet/security/bulletin/ms09-063.mspx

33 A protection alert provided by IBM X-Force: Microsoft Windows kernel font code execution http://www.iss.net/threats/354.html

34 Microsoft Security Bulletin MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947) http://www.microsoft.com/technet/security/bulletin/ms09-065.mspx

35 A protection alert provided by IBM X-Force: Microsoft Internet Explorer mshtml.dll RCE http://www.iss.net/threats/355.html

36 Microsoft Security Bulletin MS09-072: Cumulative Security Update for Internet Explorer (976325) http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx

December commenced with the release of an X-Force Protection Advisory to address a remote code execution vulnerability in Novell eDirectory discovered by X-Force analysts. A specially-crafted request can be constructed that a remote attacker could use to execute arbitrary code on the system. An attacker does not need to entice any kind of user interaction to trigger this vulnerability.

- A protection advisory provided by IBM X-Force: Novell eDirectory Remote Code Execution[37]
  - IBM X-Force Protection Signature: Application_Control_Request_Overflow
- CVE-2009-0895
- Novell Security Vulnerability: Novell eDirectory Heap-based Buffer Overflow[38]

The X-Force team also produced a Protection Advisory for a vulnerability they found in HP OpenView Network Node Manager. HP OpenView Network Node Manager permits unauthenticated users to send arbitrary HTTP requests. A malicious user can send a specifically-crafted HTTP message and overflow the vulnerable stack buffer.

- A protection advisory provided by IBM X-Force: HP OpenView Network Node Manager Remote Code Execution[39]
  - IBM X-Force Protection Signature: HTTP_Network_Management_Overflow
- CVE-2009-0898
- HPSBMA02483 SSRT090257 rev.2 - HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code[40]

On December 15, 2009, the Internet Threat Level was elevated to AlertCon 2 for the second time in the fourth quarter. This time, the Internet Threat Level was elevated to draw awareness to the active exploitation of a 0-day Adobe Reader and Acrobat issue. Successful exploitation of this issue, which requires a user to open a specially-crafted PDF file, could allow a remote attacker to execute arbitrary code on the system.

Vulnerabilities in Adobe products, and in particular Reader and Flash, have become the new "browser" for vulnerabilities. The X-Force team produced four alerts in 2009 to address Adobe Acrobat, Reader and Flash issues. In all four cases, the vulnerabilities were being exploited in the wild - either targeted exploitation or had been included in spam/exploit bots. In fact, according to the IBM X-Force 2009 Mid-Year Trend and Risk Report, one of the most popular exploits utilized in the first half of 2009 was an older Adobe Acrobat and Reader vulnerability (CVE-2007-5659). We foresee attackers continuing to use Adobe PDF files as a vector to conduct malicious activities in the future.

- A protection alert provided by IBM X-Force: Adobe Acrobat and Acrobat Reader Remote Code Execution[41]
  - IBM X-Force Protection Signatures: JavaScript_NOOP_Sled, PDF_Stream_Hiding, PDF_JavaScript_Detected, PDF_Encoded_JavaScript_Tag
- CVE-2009-4324
- Adobe Security Advisory for Adobe Reader and Acrobat[42]

37 A protection advisory provided by IBM X-Force: Novell eDirectory Remote Code Execution http://www.iss.net/threats/356.html

38 Security Vulnerability: Novell eDirectory Heap-based Buffer Overflow http://www.novell.com/support/viewContent.do?externalId=7004912&sliceId=1

39 A protection advisory provided by IBM X-Force: HP OpenView Network Node Manager Remote Code Execution http://www.iss.net/threats/357.html

40 HPSBMA02483 SSRT090257 rev.2 – HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877

41 A protection alert provided by IBM X-Force: Adobe Acrobat and Acrobat Reader Remote Code Execution http://www.iss.net/threats/358.html

42 Adobe Security Advisory for Adobe Reader and Acrobat http://www.adobe.com/support/security/advisories/apsa09-07.html

Additional Q4 2009 highlights

This section of the report briefly covers some of the additional threats facing security professionals during Q4 2009.

Major security breaches

A number of high-profile security breaches are reported every year drawing attention to the need to protect consumer and employee information from the risk of exposure to malicious individuals/identity (ID) theft rings. In addition to the loss or misplacement of information, corporations and individuals are at risk to exposure via malware, hacking, phishing attacks and various social engineering tactics. There are also non-cyber related methods such as stealing mail, "dumpster-diving" (rummaging through trash bins), or obtaining information from employees or stolen records. Below are some of the major security breaches that became public during the fourth quarter:

- **BlueCross BlueShield** – A laptop was stolen containing the personal information of 850,000 physicians in an unencrypted file.
- **Eastern Illinois University** – Viruses may have been the cause of a server compromise. Files containing personal information from about 9,000 current and former students may have been accessed by an attacker.
- **Microsoft** – Several thousand Windows Live Hotmail customers' credentials were exposed on pastebin.com, a third-party site. The vendor indicates this compromise was "due to a likely phishing scheme."
- **National Archives and Records Administration (NARA)** – The personal data of 70 million U.S. military veterans was compromised when a hard drive containing this information went missing.
- **Twitter** – DNS settings for the Twitter Web site were hijacked and, for a couple of hours, eighty percent of the traffic was redirected to other Web sites. It is unknown if any Twitter accounts were compromised during the incident.
- **Universal American Action Network** – 80,000 postcards containing the recipient's Social Security Number were sent to their clients.
- **Virginia Department of Education** – Sensitive information of more than 103,000 former adult education students in Virginia was compromised when a flash drive was misplaced.

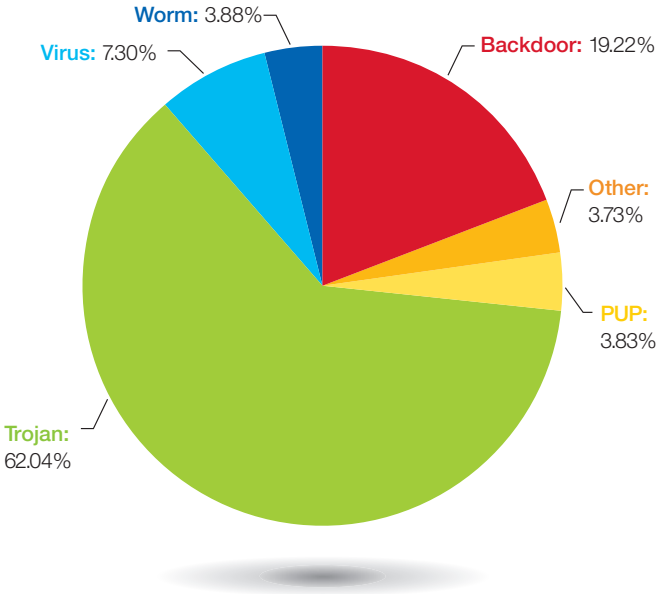
Malcode corner

The IBM X-Force Virus Prevention System (VPS) team's categorization of malcode is based on the most dominant features of the threat. The primary malcode categories are:

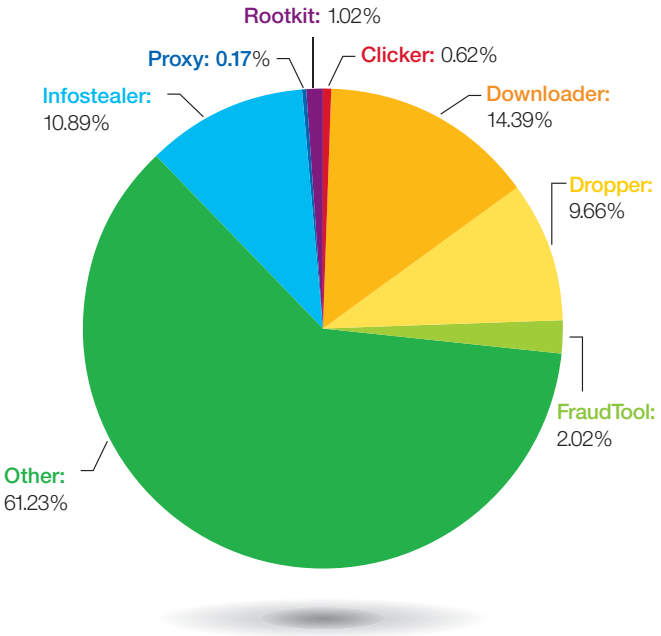
- **Backdoor** – Provides functionality for a remote attacker to log on and/or execute arbitrary commands on the affected system.
- **Other** – Unclassified malicious programs not falling within the other primary categories.
- **Potentially Unwanted Programs (PUP)** – Programs which the user may consent on being installed but may affect the security posture of the system or may be used for malicious purposes. Examples are Adwares, Dialers and Hacktools/"hacker tools" (which includes sniffers, port scanners, malware constructor kits, etc.)
- **Trojan** – Performs a variety of malicious functions such as spying, stealing information, logging key strokes and downloading additional malware.
- **Virus** – Propagates by infecting a host file.
- **Worm** – Self-propagates via e-mail, network shares, removable drives, file sharing or instant messaging applications.

The Trojan subcategories are as follows:

- **Clicker** – Generates website traffic, the purpose of which is to generate revenue or other malicious purposes.
- **Downloader** – Downloads one or more malware components from a remote site and then installs them on the affected system.
- **Dropper** – Drops and installs one or more malware components into an affected system.
- **FraudTool** – Malware used to commit fraud, an example of which are malware that displays fake error or infection messages which then incites the user to purchase fake tools or security software.
- **Other** – Trojans that do not fall within the other subcategories.
- **Infostealer** – Spies and/or steals information; this includes password stealers, keystroke loggers and spywares.
- **Proxy** – Allows a remote attacker to relay connection via the affected system in order to hide its real origin.
- **Rootkit** – Components used by other malware in order to have the capability to hide themselves from the user and security software.



Source: IBM X-Force



Source: IBM X-Force

List of Contributors for this paper include:

David MacKinnon – Security Intelligence Analyst
IBM MSS Intelligence Center

Troy Bollinger – Senior Researcher
IBM MSS Intelligence Center

Michelle Alvarez – Team Lead
IBM MSS Intelligence Center

IBM X-Force Database

IBM X-Force Virus Prevention System (VPS) team

References

Advisory Monitoring in a Heterogeneous Enterprise Environment

CERT/CC Vulnerability Disclosure Policy
http://www.cert.org/kb/vul_disclosure.html

Products & Services Security Vulnerability Policy
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Disclosure Policy – Secunia Research – Vulnerability Information
http://secunia.com/secunia_research/disclosure_policy/

wiretrip.net – rfpolicy – rain forest puppy
http://www.wiretrip.net/rfp/policy.html

Responsible Vulnerability Disclosure Process
http://www.wiretrip.net/rfp/txt/ietf-draft.txt

Symantec Product Vulnerability Management Process
http://www.symantec.com/security/Symantec-Product-Vulnerability-Response.pdf

How To Disclose Software Vulnerabilities Responsibly?*
http://infosecon.net/workshop/slides/weis_4_3.ppt

Zero Day Initiative - Disclosure Policy
http://www.zerodayinitiative.com/advisories/disclosure_policy/

Creating a Patch and Vulnerability Management Program (Section 2.3, Appendix C)
http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

Re: Status of draft-christey-wysopal-vuln-disclosure-00.txt
http://www.ietf.org/mail-archive/web/ietf/current/msg23995.html

Prolific and Impacting Issues of Q4 2009

BlueCross BlueShield data breach affects 850,000 doctors
http://www.id-theft-security.com/lifelock-blog/2009/10/bluecross-blueshield-data-breach-affects-850000-doctors/#ixzz0bl6hcOe2

EIU warns of student data security breach
http://archives.chicagotribune.com/2009/dec/04/news/chi-ap-il-eiu-computersecur

Issue closed: Phishing scheme affecting some Hotmail customers
http://windowslivewire.spaces.live.com/blog/cns%212F7EB29B42641D59%2141528.entry

Probe Targets Archives' Handling of Data on 70 Million Vets
http://www.wired.com/threatlevel/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/

Twitter hack linked to internal security breach
http://www.theregister.co.uk/2009/12/21/twitter_dns_hack_follow_up/

80,000 Mailers Sent Out With Recipients' Social Security Numbers In Plain View
http://www.wgal.com/news/21655737/detail.html

Data on 103,000 Students Misplaced
http://www.washingtonpost.com/wp-dyn/content/article/2009/10/14/AR2009101402118.html

*Information in this document concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2010

U.S. Patent No. 7,093,239

Please Recycle

TIL14000-USEN-00