IBM Security Solutions
April 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.

A New Job – the Continuing Saga of Fraud Schemes

By Lyndon J. Sutherland

The Q2 2009 X-Force Threat Insight Quarterly report featured an article titled “Fraud Schemes; I love you. I will make you rich. Oh, and I need some money moved”. In this article, we took a look at 419 (aka Nigerian) and Romance scams and we touched on the mechanics, social engineering and human cost aspects associated with those schemes. As Nigeria has become closely associated with online fraud schemes, we were a touch surprised to receive in one of our email inboxes an offer for a job in Nigeria. Surely one would think that receiving an unsolicited email regarding an offer that on the surface appeared to be too good to be true and involved Nigeria would be an immediate red flag. Yet, this scheme appears to have been operating in one form or another since at least 2005.

The offer

A job working for a company in Nigeria involved in the petroleum industry. The wages, not bad at all, around USD $21,000 per month (after taxes no less). The conditions, accommodations for the employee and his family while working 28 days on and 28 (paid) days off.

Credible?

How credible does it seem that we can receive in our email an unsolicited offer of well paid employment, apply with no prior experience, submit a fictitious resume, have it accepted without any references or background checks of any kind and be offered a position? Simply, it is not at all credible and this alone should be sufficient warning to anyone who receives such email. However, some people do fall victim to such schemes which is at least in part testimony to the social engineering skills of those running the scams. We suspect that many victims, who are successfully conned in these schemes, are likely to have had telephone contact with the scammers which is where the social engineering skills of the scammers come to the forefront.

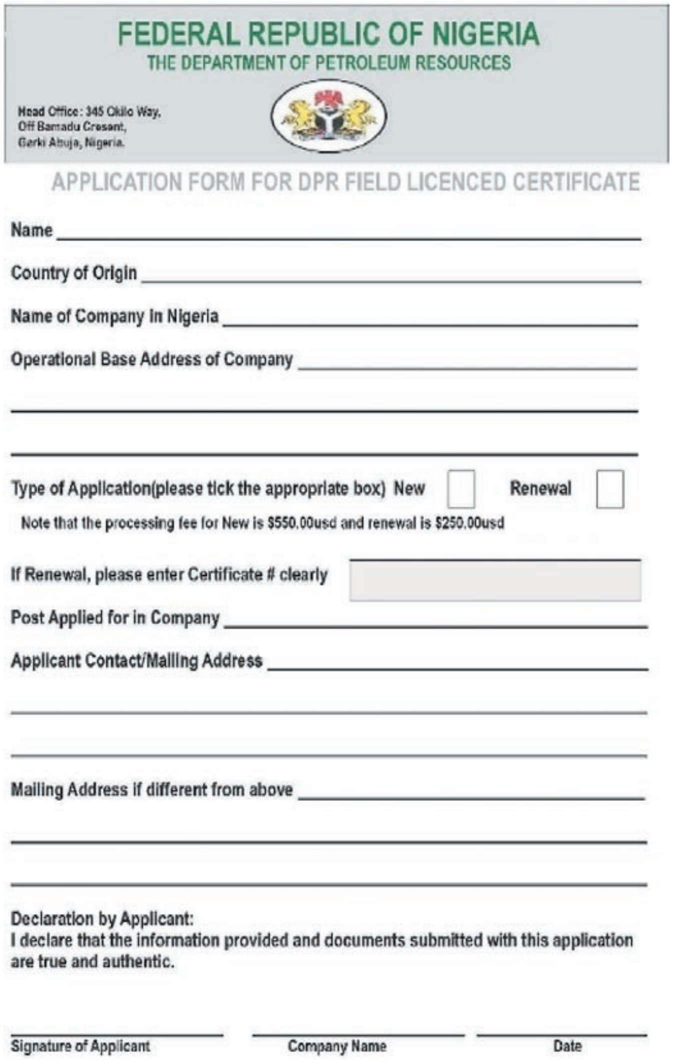
What did we do?

Well, of course we eagerly replied to the email quoting the reference number that was supplied with it. However, we stated in the response that our fictitious applicant had no prior experience in the oil industry but could we be considered for a position? The response came quickly which thanked us for our resume and notified us that it had been screened. So while it appeared we had managed to pass the screening process, we were now being directed to answer a set of questions within 48 hours. The questions apparently constituted an “brief online interview”. We replied, answering the 20 questions in the email and to our delight we received a response congratulating us on the offer of a position as a site supervisor. Isn’t this modern world so wonderful? Who ever thought that getting a well paying job could be so easy!

The sting

The sting comes in the form of our gracious new employer requiring a scanned copy of our “international” passport and a certificate issued by a Nigerian government department. Our new employer provided us the contact details for the department and instructions on how to proceed. We contacted the alleged government department and in turn received from them an email which stated our employer had mandated the agency to procure and process the required certificate.

The email contained an image of a form which we were to print, fill in and return. The form actually required very little information. However, we were required to send a specified amount of money via Western Union to a Nigerian destination. We were also instructed to scan and email a copy of the receipt for the transfer back to our scammer. There was no mention in this email or the form regarding a scanned copy of our applicant's passport.



FEDERAL REPUBLIC OF NIGERIA
THE DEPARTMENT OF PETROLEUM RESOURCES

Head Office: 345 Okilo Way,
Off Bamadu Cresent,
Garki Abuja, Nigeria.

APPLICATION FORM FOR DPR FIELD LICENCED CERTIFICATE

Name ______________________________

Country of Origin ______________________________

Name of Company in Nigeria ______________________________

Operational Base Address of Company ______________________________

____

____

Type of Application(please tick the appropriate box) New □ Renewal □

Note that the processing fee for New is $550.00usd and renewal is $250.00usd

If Renewal, please enter Certificate # clearly □

Post Applied for in Company ______________________________

Applicant Contact/Mailing Address ______________________________

____

____

Mailing Address if different from above ______________________________

____

____

Declaration by Applicant:
I declare that the information provided and documents submitted with this application are true and authentic.

Signature of Applicant ____________ Company Name ____________ Date ____________

The alleged government department does appear to exist and be a legitimate arm of the Nigerian government. The email address, form, and the person we were instructed to contact did not appear to be legitimate.

For a sum of USD $550.00 we would be provided the required certificate which would allow us to travel to and commence work in Nigeria. We know from past experience and our research into scams that the certificate would only be the beginning of the scam. There would be some form of difficulty or hiccup. Then we would be asked for more money to overcome whatever issue put forward by the scammers.

We did not proceed with obtaining the required certificate. We also did not present our applicant's passport details to our new employer. It is critical to use extreme caution when handing details or copies of one's passport. Any persons not justified in requesting such information should not have access to it. Passport information has value to criminal groups and can be used to facilitate identity theft among other issues.

A nice touch

We exchanged emails with the alleged government department to determine how greedy our scammer would become. We mentioned in an email we were concerned about the short time frame in taking up our employment in Nigeria. We were to start work less than a month after the position was offered to us. We asked if there was a way to expedite the certificate issuing process so we would not miss our start date. We explained we had just renewed our passport and had paid an extra fee to have the application processed quickly.

The answer that came back did not surprise us. The response was no. There was no way an extra fee could be paid to expedite the process. The reason provided was that, since the organization was government owned, there was no process for expediting the required certificate. Trying to expedite the process would only lead to problems. This seemed like a nice touch designed to convince the victim of the legitimacy of the scammer. We think our scammers had more in store than simply the certificate payment. Scammers are not known to turn down money unless they see greater long term gains.

Where were our scammers operating from?

Actually, they really were operating from Nigeria using dial up accounts from a Nigerian ISP in two different urban areas. Emails from the alleged employer and government department originated from both locations which suggest we were not handled by a single person. This indicates that we were dealing with an organized criminal group.

The history of this particular scam

The name of the company used in this scam is the name of a real company. Our scammers and their email addresses are not related to the real company in any way. The company name has been used by scammers to front their schemes since at least 2005. The actual (legitimate) company with this name has had a warning on their employment Web pages for many years warning of scams using their name and seeking money. The real company does not send unsolicited emails offering employment opportunities. They also do not ask people to send money.

While not directly related to this scam, we have anecdotal reports from law enforcement officials regarding other variations on employment scams where the victim actually goes to work in a foreign location. The scam in these cases operates on the principal of the worker agreeing to a contract for a fixed term and payment will be made to the victim on completion of the contract. When the settlement date arrives the sting takes place. Various payments and deductions are made from the victim's agreed payment which ultimately leaves the victim with no real way of obtaining the money they thought they would be paid.

How are people contacted by these employment scammers?

Similar to the 419 and romance scams email plays a large part in the distribution of the scam. Large volumes of email offering employment is sent out. It only takes a small number of potential victims to respond to the emails for the scam to be considered successful. In the case of employment scams, forums and job sites also provide vehicles for the scammers to promote their schemes. We have seen the scam we looked at in this article and another scam that uses another well known company name on many sites that cater to job seekers and employment opportunities. These sites range from the legitimate to what appears to be sites set up purely to promote scams.

In the scam we noted there were links to the alleged company offering the employment opportunity in the email. However the links returned "document not found" errors. The links also did not point to the Web site of the legitimate company with the name used by the scammers. Using search engines and specific criteria we noted several Web sites used or previously used by the scammers to serve their fake company Web pages.

An interview with a vampire?

During the process of background research and writing this article, we happened across a three part interview with an alleged former Nigerian scammer. There is a disclaimer from the editor that says there is no way to verify the identity or legitimacy of the person who provided the information or ability to verify the information itself. However, that aside, the interviews provide insight into how scams are operated and how the Nigerian gangs are involved in running scams. This information tends to gel with what we have learned and what law enforcement personnel have reported.

Back to the past

Also during the writing of this article, and perhaps somewhat ironically timed, we received an email from the scammers who were the subject of our last article. The email was to inform us that the alleged woman who needed our help to recover a sum of money from a bank account and who wanted to make us rich and start a new life with us, is now happily living in London with a new partner. According to the email, the new partner had financed the transaction of the funds and the transaction completed successfully. He has also proposed to her and they are busy with investment projects. We found that somewhat amusing.

Perhaps we judged our alleged scammer too harshly. While things didn't work out between us, she thinks we were very nice. To show her gratitude for our sincerity, courage and trust worthiness, she has set aside $250,000.00 just for us. All we have to do is collect it. We can do this by contacting a certain Reverend in Senegal with whom she's left a certified international bank draft. We are to provide him our phone number, mailing and email addresses.

It is interesting that, despite that she is allegedly now living in London, her emails are still being sent from somewhere in Senegal.

What have we learned?

Some very simple facts. Scammers are persistent. Even when their initial attempts fail they will probably have retained your contact details in order to try again in the future. Simply put, it is not a good idea to respond to spam. No matter how good (or bad) it might sound.

Broadly speaking, scammers are very good at social engineering. They are well organized and work in groups rather than alone. Groups may communicate, trade, sell or otherwise share information on victims and potential victims.

Few, if any, scammers have any conscience when it comes to taking money from their victims. It would not matter to them if their victim was bankrupted by their scheme. They only care that their goals are achieved, be they monetary or documentation to aid in identity theft for example.

While a scam's success rate may not seem high considering the number of victims versus the number of spam emails sent (see interview referenced above), their success rate is high enough to be considered profitable. The fact that scammers have operated schemes such as the employment scam for years, suggests the business of scamming people is profitable. And the number of scammers operating may well be increasing.

Very few victims of these fraud schemes recover any money even if the scammers are successfully prosecuted.

What to look out for?

It starts with the most basic thing, the thing that should alert any reader that what they have in front of them is a scam. In the case of our employment scam, one should ask a very simple question, "why would someone I do not know, send me an unsolicited email, offering me a well paying job, in a foreign country, when they do not know me and I do not know them?" Any unsolicited email that is offering riches or rewards is probably a scam.

Of course scammers don't always appear to be strangers. Social networking sites, for example, are rich with information on individuals, often including information on their friends and associates. Scammers have no hesitation in using such information to target victims. They may impersonate someone a victim knows, perhaps even trust, in an effort to fleece the victim. Even malware (viruses, Trojans, etc.) uses this trick by sending emails to people in the infected computer's email address book. The victims see these emails from friends and associates and may not be critical of them even if they appear a little suspect. Then they end up with their own computers infected by malware.

It is quite unlikely that any legitimate company or recruiting agency seeking to attract employees will operate in the manner our scammers have operated such as unsolicited contact by email and using email addresses from free email services. Scammers can achieve a veneer of credibility to the unwary by using real company and government department names and pointing to Web sites that may look legitimate. If you have not applied for the position, it is unlikely it will be offered to you via unsolicited email. Scammers often use the trick of their email appearing to be a reply to something you have sent them. While it might not seem likely some people do fall for such simple tricks.

What to do

Do not respond. While it may be tempting to see if an offer might be genuine, or it may be fun to play games with the scammer, it is unwise. Even using a free disposable email address, the scammers may learn more about you than you intended such as the IP address you use to send email from. Or perhaps a gifted social engineer may be able to slowly lure you in. And if they don't succeed, they may as our previous scammer did, send a follow-up email which is crafted to make it appear a golden opportunity was missed. Although the truth is the scammer is simply making another attempt to lure their potential victim into the trap.

If you or anyone you know has been a victim of advance fee, romance or employment frauds, report or encourage them to report the crime to your relevant local law enforcement agencies. The law enforcement agencies which deal with such frauds differ from country to country, for example, in the United States the local F.B.I. office is probably a good place to start. A helpful Web site that provides information and links on reporting fraud in several countries is here:
http://www.consumerfraudreporting.org/reporting.php

Getting Played

By Peter Q. Trinh

Video games have provided entertainment for people starting from childhood and often times lasting through adulthood. Whether the experience was from my PC, Atari® 2600, or the latest and greatest console, I recall the enjoyment I felt every time I was behind a mouse or controller. This form of entertainment aspires to provide stress free enjoyment, but the hacking community has intensified its aim on the industry and is leaving some gamers crying "Game Over".

Background

The video game industry has several factors that make it a favorable target for hackers. The popularity of video games provides a large audience and the continued growth of the industry makes it a stable mark. The largest segment within the industry is the PC (personal computer) gaming market. This market accounts for the largest user base and is one of the most financially lucrative, garnering about $11 billion annually.[1]

Exploits within video games are not a new trend. Games have always been plagued by exploits that make game play easier. First person shooter (FPS) games have their share of headaches with game cheats such as wall-hacks. Wall-hacks allow a player to see enemies behind solid objects. Another example is aim-bots which helps players pull off an automatic headshot against other opponents. These exploits undermine the enjoyment factor of the games but they primarily fall under the nuisance category, as they are targeted against the game client. The exploit trend that has been increasing against another popular genre, massively multiplayer online (MMO) games, are more focused attacks resulting in theft of user accounts.

Golden opportunity

Massively multiplayer online games are a top revenue generator and coupled with its huge following makes it a magnet for those with malicious intent.[2] The highest grossing MMO game is *World of Warcraft* (WoW), which hauls in more than one billion dollars a year.[3] MMO games are played over the Internet and support a large number of players simultaneously. They typically consist of a persistent virtual world that has their own form of virtual currency and virtual economy. The game centers on developing a character or avatar by interacting in this virtual world with one of the objectives being able to accumulate virtual currency. The accumulation of virtual wealth allows characters to purchase virtual items which aid in advancement within the game.

What is it about MMO games that have it wearing the bull's-eye? MMO games often require players to log many hours to develop their characters. Players who are pressed for time tend to take shortcuts to keep up with other gamers and to make game progression easier. This mentality is a contributing factor as it creates demand for a market selling virtual assets. Opportunities are often created at the intersection between people who have money but little time and people who have time but little money. One of those opportunities is the creation of a unique industry referred to as 'gold farming'.

[1] The PCGA Presents: The PC Gaming Industry in 2008 http://www.pcgamingalliance.org/imwp/download.asp?ContentID=15559

[2] Massively multiplayer online game http://en.wikipedia.org/wiki/MMOG

[3] The PCGA Presents: The PC Gaming Industry in 2008 http://www.pcgamingalliance.org/imwp/download.asp?ContentID=15559

Gold farming is the term used to describe the activity of accumulating items of virtual value, usually virtual currency such as gold or platinum. Players amass currency by repeating mundane tasks within the virtual world. The virtual currency is then sold for real world currency directly or indirectly via real money trading (RMT) brokers. This controversial practice is prevalent in developing countries such as China where the vast amount of players provides a cheap labor pool to drive the gold farming activities. The work takes place in cyber cafe type sweatshops with "farmers" engaging in 12 hour shifts seven days a week playing online games and collecting virtual gold. These workers are paid an average of $150 a month but the gold they accumulate can net their employers up to $60,000 per month.[4] It is estimated that there are anywhere between 400,000 to 1,000,000 people in China working in the gold farming trade with speculation that the industry serves five to ten million customers and yields $500 million to $1 billion a year.[5]

All your gear are belong to us

The market for virtual goods exists due in large part to the huge demand from the gaming population. Supply channels have been created such as the gold farming industry which has proven to be quite profitable. Hackers are motivated by monetary gain and can't resist taking advantage of the financial prospects within the online gaming arena.

The main objective of an attacker is the theft of online gaming account credentials. Hackers target MMO gaming accounts with the intention to loot them for anything of value. The virtual items would be sold on the underground black market for those interested in purchasing virtual assets. The activity occurs in such a rapid manner that it is extremely difficult for victims to detect and respond. The compromise could also result in account suspension which leaves victims unable to access their games while they attempt to reinstate their accounts. Virtual items serve as signs of achievement due to the time investment and effort required to obtain them. Losing these in-game assets could affect victims on an emotional level as it could be years of effort lost.

Hijacking of accounts to ransack virtual items is not the only use hackers have for gaming accounts. Compromised accounts are also used in gold farming activities. Blizzard Entertainment, the game development company that publishes popular titles such as *World of Warcraft* (WoW), claim that a high amount of gold sold from gold sellers are sourced from hacked accounts.[6]

Stolen gaming accounts themselves can also be sold on the black market. Some security experts asserted that the value of a WoW account is actually worth more than a stolen credit card. They estimate the value of a stolen credit card to be worth $6 while a WoW account could be sold for at least $10.[7] The value of a WoW account could fetch considerably more if the account had high level characters and rare items. The value of a stolen credit card is lower due to the aggressive security tied into the cards as well as the short time interval and high risks associated with using a stolen credit card. This is not the case with a stolen WoW account since the risks are minimal. A contributing factor to the continuing theft of WoW accounts is due to little interest from law enforcement agencies against such crimes.

[4] Wage Slaves http://www.1up.com/do/feature?cId=3141815

[5] MMORPG Gold Farming could be a $1 Billion Industry
http://pcgames.gwn.com/articles/article.php/id/996/title/MMORPG_Gold_Farming_could__be_a_1_Billion_Industry.html

[6] Gold Selling: Effects and Consequences http://www.wow-europe.com/en/info/faq/antigoldselling.html

[7] Cursor hackers target WoW players http://news.bbc.co.uk/2/hi/technology/6526851.stm

The usual suspects

Malicious users target gamers by employing a variety of methods including social engineering and installing keyloggers via malware. Attackers also take more imaginative methods like taking advantage of game functionality in carrying out the attack. They have shown a wide range of creativity in the ways they have carried out their exploits which adds to the difficulty of preventing attacks. This section will reveal some common attack scenarios with the goal of spreading awareness.

Social engineering

Social engineering is the act of manipulating people to perform actions through the use of deception. Phishing is one form of social engineering technique used to trick gamers into revealing their login credentials. The typical delivery methods include email or game related forum posts. The intent is to deceive the user with some urgent notice relating to their gaming account. These notifications lead the user to some mirrored site that closely duplicates the authenticity of the legitimate game site. A victim who falls for the phishing scam unknowingly sends their login credentials to the hacker.

An example of a phishing scam was conducted against players of a MMO game called *Runescape*. *Runescape* is a medieval style MMO game that boasts to have over 100 million players worldwide.[8] A man was arrested in the U.K. back in late 2009 for breaking into 284 *Runescape* accounts. The hacker used phishing techniques to gain access to the accounts in order to steal virtual items to boost his standing in the game.[9]

This discussion has been focused on PC MMO games but gaming system console users are not immune either. Microsoft® Xbox Live online gaming service accounts have also been targeted. Hackers use social engineering techniques to gain access to Xbox Live accounts. The perpetrator typically will engage in conversation with the victim via the in-game chat feature trying to illicit information about the gamer. The information they gather can be used to ascertain the account password reset questions. Hackers also use phishing scams luring users to enter their account info into Web forms promising false rewards such as offers for free Microsoft Points.[10] Xbox Live accounts pose a serious threat as they potentially can have a saved credit card number tied to the account. Phishing techniques have better odds of success against new users but lose their effectiveness against advanced or savvier gamers. The success rates in general are lower as the game developers notify and warn their customers of this type of activity in hopes of preventing such attacks.

[8] MMO developer Jagex outlines 'MechScape' http://www.techradar.com/news/gaming/mmo-developers-jagex-outline-mechscape--617551?artc_pg=1

[9] Hacker Arrested For Stealing Virtual Assets In Online Game http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=222000115

[10] Reports Of Hacked Xbox Live Accounts Stir Concerns Over Gamers' Security http://www.mtv.com/news/articles/1593637/20080827/id_0.jhtml

Malware

Malicious software is an effective method used by hackers to steal login credentials. There is an alarming increase in the amount of malware targeted towards online gaming accounts. Lavasoft the company that produces Ad-Aware touts on their Web site that in 2009 the number of online gaming virus infections has increased by 600 percent.[11] Microsoft noted that their Malicious Software Removal Tool (MSRT) removed nearly 1 million samples of the password stealing worm Win32/Taterf back in February of 2009. The company further indicated that they had seen more than 4.9 million infections caused by Taterf in the first six months of 2009, an increase of 156 percent over the last six months of 2008.[12] Based on January 2010 data Taterf infections have decreased activity but still rank as number three on Microsoft's MSRT tracker.[13]

There is a gamer mentality that usually drives them to optimize their gaming environment. This is done by utilizing game patches, add-ons, bots, and cheat programs to make game play easier. Malware creators exploit this mentality and embed 'Trojans' into known game tweaks.[14] It becomes a situation where the cheater gets cheated by using infected cheats. Social engineering techniques also come into play with malware propagation. Game related posts informing of a new game patch or game utility are posted in Internet forums which help to introduce the malware to victim's machines.

The Trojan-PSW.Win32 family and its variants are one of the most common types of online gaming malware. This type of malware monitors game executables and when the targeted games are launched, the Trojan captures keyboard strokes which then send the data to the attacker. A large number of registered hard-coded IP addresses that the data is sent to are registered addresses in China.[15] China is one of the larger sources of malware and there is correlation to suggest that it is tied to the popularity of online gaming in the country, which is predicted to reach 65 million gamers by the end of 2009.[16] Chinese experts contend that the Trojan horse attackers in China gain 95 percent of their revenue from victimizing online gaming accounts.[17]

Game Functionality Exploits

The more creative methods used by hackers is to exploit in-game features to carry out their attacks. Certain games will have embedded functionality that utilizes other applications. Exploits related to those third party applications can be leveraged and used to attack unsuspecting players. Zero-day vulnerabilities of third party applications make attacks of this nature difficult to foresee and defend against. A Zero-day vulnerability is an issue for which there is no security fix available. An example of this type of exploit can be seen with an Apple® QuickTime vulnerability and the game *Second Life*.

[11] Viruses, Malware Creeping into Online Games http://pcworld.about.com/od/gaming/Viruses-Malware-Creeping-into.htm

[12] Video gamers face malware deluge http://news.bbc.co.uk/2/hi/technology/8338227.stm

[13] Win32/Rimecud: MSRT's success story in January 2010
http://blogs.technet.com/mmpc/archive/2010/01/19/win32-rimecud-msrt-s-success-story-in-january-2010.aspx

[14] That game cheat may be cheating you http://antivirus.about.com/od/emailscams/a/mmorpg_hacks.htm

[15] Trojan-PSW:W32/OnlineGames http://www.f-secure.com/v-descs/trojan-psw_w32_onlinegames.shtml

[16] Study: 65 Million Online Gamers In China By Year-End
http://www.gamasutra.com/view/news/25053/Study_65_Million_Online_Gamers_In_China_By_YearEnd.php

[17] Chinese hackers feast on lucrative market
http://www.earthtimes.org/articles/show/308604,chinese-hackers-feast-on-lucrative-market--feature.html

Second Life is a virtual world that is played over the Internet. Users can interact with each other using avatars they create with a free utility called *Second Life* Viewer. The interesting aspect of the game is the virtual economy that is involved. The virtual world of *Second Life* has a currency called Linden dollars which have real monetary value. Linden dollars can be converted to real world money somewhere in the neighborhood of $1 to 275 Linden dollars.

A QuickTime 7.3 vulnerability in 2007 allowed for some security researchers to craft an exploit within *Second Life*. *Second Life* allows users to embed video files on the property they own and uses QuickTime to render the video. An exploit was surmised that allowed the attacker control of a victim's avatar once they walked past the property. The sample exploit would steal Linden dollars from victims that interacted with the object.[18]

Thou Shall Not Pass

It is evident there are risks associated with today's video games. Although game developers know their customers are being targeted, there are not many solutions that have been offered to protect the consumer. The standard action has been to inform and educate users of the hacker activity associated with gaming accounts.

Blizzard Entertainment is one of the rare companies that have taken steps in addressing the increased cases of compromised accounts. They currently sell an optional Two-Factor authentication token that adds another layer of security for user accounts. The token generates a one-time use digital code that would be required along with the account credentials.[19] The technology is currently an optional feature but there is speculation that the company may opt to make it mandatory for all accounts. It is important to realize that this extra layer of security is not ironclad. Banks that utilize this Two-Factor security have encountered incidents of theft as hackers are adapting and using real-time Trojans to counter this security measure.[20] One of the advantages in utilizing this security technology is that it slows the attacker down and makes it more costly for them to try to thwart this security model.

Blizzard also incorporates a system monitoring tool called Warden. This is a polymorphic program that checks for hacks, cheats, and key loggers on the user's machine. If it detects these programs it will shut the game client down and send the data back to the game company.[21]

The burden of ensuring account security ultimately lies with the end user. They need to be aware of the risks involved with their gaming accounts and exercise sound judgment in regards to safeguarding their account information. Maintaining computer system currency and keeping security products like anti-virus updated should be a given in any instance that deals with Internet security. It is important to realize that security products should serve as an additional layer of security, but the first line of defense should be the gamers' common sense.

Conclusion

The continued growth of the video game industry and the rate that new games are introduced each year provides a comfortable niche for hackers. The malicious activity is expected to continue and while it will shy some gamers away, a constant influx of new gamers provides a constant stream of fresh victims. To borrow a quote from a G.I. Joe public service announcement, "Now you know, and knowing is half the battle." Awareness to the issues that exist is key in dealing with the security risks that are prevalent in today's video gaming scene. Understanding the associated risks allows the end user to play the game and prevent themselves from getting played in the process.

[18] QuickTime hack allows Second Life currency theft http://blogs.zdnet.com/security/?p=713

[19] Battle.net Authenticator http://us.blizzard.com/store/details.xml?id=1100000822

[20] Real-Time Hackers Foil Two-Factor Security http://www.technologyreview.com/computing/23488/?a=f

[21] Computerworld on Blizzard's Warden at work http://www.wow.com/2009/03/09/computerworld-on-blizzards-warden-at-work

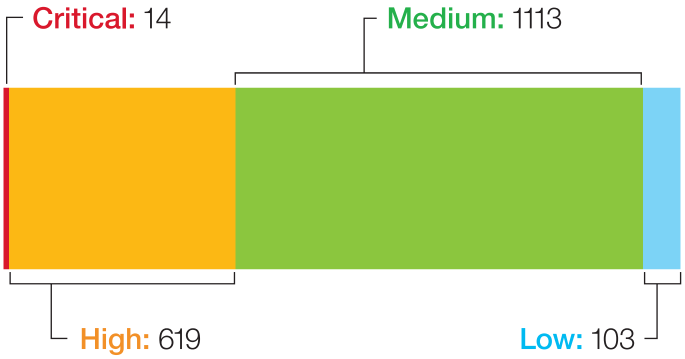
Prolific and Impacting Issues of Q1 2010

Significant disclosures

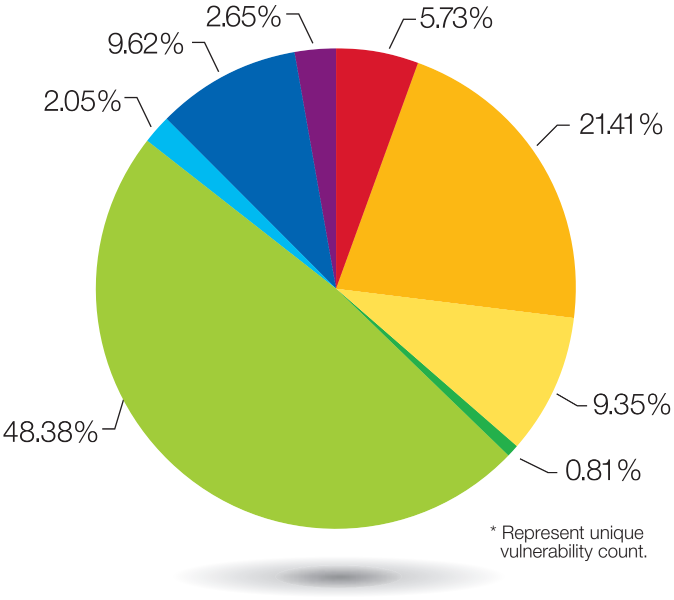
In Q1 2010, the X-Force team researched and assessed 1849 security related threats. A significant percentage of the vulnerabilities featured within the X-Force database became the focal point of malicious code writers whose productions include malware and targeted exploits.

The chart on the right 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. *

Total Vulnerabilities in Q1 2010: 1849



Source: IBM X-Force



* Represent unique vulnerability count.

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.

Only two weeks into the new year and the IBM threat level was elevated to AlertCon 2. This action took place in order to draw increased awareness to the active exploitation of a 0-day Microsoft Internet Explorer vulnerability. This vulnerability was utilized in high profile attacks on Google and at least 20 other large companies (see Operation Aurora below).

Microsoft Internet Explorer could allow a remote attacker to execute code on the system caused by an invalid pointer reference error. By persuading a victim to visit a specially-crafted Web page, a remote attacker could exploit this vulnerability to access an invalid pointer to a deleted object to execute arbitrary code with the privileges of the victim.

- A protection alert provided by IBM: Microsoft Internet Explorer Freed Object Code Execution[22]
  - IBM Protection Signatures: JavaScript_Shellcode_Detected, HTTP_IE_Script_Error_Code_Execution, JavaScript_Large_Unescape, JavaScript_Unescape_Obfuscation, HTML_Script_Extension_Evasion, JavaScript_Byte_Splitting
- CVE-2010-0249
- Microsoft Security Bulletin MS10-002: Cumulative Security Update for Internet Explorer (978207)[23]

The Pushdo botnet, primarily used for spamming, had been observed launching Distributed Denial of Service (DDoS) attacks against certain SSL-enabled Web sites earlier in the quarter. The DDoS attack involved sending thousands of malformed SSL requests to the target hosts in an attempt to use up resources. Infection means complete compromise of the target system which may lead to exposure of confidential information, loss of productivity, and further network compromise.

The Pushdo malware is also known as Pandex and some components are known as Cutwail. Command and Control (C&C) traffic generated by a Pushdo malware infection is detected as Trojan_Pushdo by Proventia. The recent SSL DDoS attacks are detected with the following IBM signature, SSL_Hello_Msg_DoS.

- A protection alert provided by IBM: Pushdo SSL DDoS Attacks[24]
  - IBM Protection Signatures: Trojan_Pushdo, SSL_Hello_Msg_DoS

[22] A protection alert provided by IBM: Microsoft Internet Explorer Freed Object Code Execution http://www.iss.net/threats/359.html

[23] Microsoft Security Bulletin MS10-002: Cumulative Security Update for Internet Explorer (978207) http://www.microsoft.com/technet/security/bulletin/ms10-002.mspx

[24] A protection alert provided by IBM: Pushdo SSL DDoS Attacks http://www.iss.net/threats/pushdoSSLDDoS.html

Microsoft's February 2010 Security Release contained two issues which the IBM X-Force Research & Development team considered most important. The first affects the Microsoft Windows SMB Client and could allow a remote attacker to execute arbitrary code on the system. This vulnerability is in a core component of most modern Microsoft Windows operating systems, including Windows 7. The easiest attack vector requires an attacker to set up an SMB server and entice a user to click a link to the server. Successful exploitation provides the attacker with complete control of the end user's system.

- A protection alert provided by IBM: Microsoft Windows SMB Client Remote Code Execution[25]
  - IBM Protection Signature: SMB_Negotiate_MaxSize_Overflow
- CVE-2010-0016
- Microsoft Security Bulletin MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)[26]

The second serious issue affects Microsoft Windows SMB Server. This vulnerability is in a core component of most modern Microsoft Windows operating systems, including server editions. If crafted properly, the attack would provide full remote code execution without any end user interaction, although a denial-of-service is more likely to occur. However, the attacker must first have authentication rights to the system and the guest account would not work in this scenario.

- A protection alert provided by IBM: Microsoft Windows SMB Server Remote Code Execution[27]
  - IBM Protection Signature: SMB_Copy_Source_Overflow
- CVE-2010-0020
- Microsoft Security Bulletin MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)[28]

[25] A protection alert provided by IBM: Microsoft Windows SMB Client Remote Code Execution Microsoft Windows SMB Client Remote Code Execution http://www.iss.net/threats/360.html

[26] Microsoft Security Bulletin MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251) http://www.microsoft.com/technet/security/bulletin/ms10-006.mspx

[27] A protection alert provided by IBM: Microsoft Windows SMB Server Remote Code Execution http://www.iss.net/threats/361.html

[28] Microsoft Security Bulletin MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx

IBM X-Force also highlighted two issues disclosed in the Microsoft March 2010 Security Release. The first vulnerability affects most modern Microsoft Windows operating systems, including Microsoft Vista. Microsoft Movie Maker is vulnerable to a buffer overflowcaused by improper bounds checking when processing malicious Movie Maker (.mswmm) files. Successful exploitation of this issue would provide an attacker with complete control over the endpoint target.

- A protection alert provided by IBM: Microsoft Movie Maker Buffer Overflow[29]
  – IBM Protection Signature: CompoundFile_Movie_Maker_Overflow
- CVE-2010-026
- Microsoft Security Bulletin MS10-016: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)[30]

The second vulnerability of interest affects Microsoft Excel. By persuading a victim to open a specially-crafted .XLSX file, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim. This vulnerability is in a core component of most modern Microsoft Office packages. The Microsoft Office Excel Viewer is a replacement for all previous Excel Viewer versions including Excel Viewer 97 and Excel Viewer 2003.

- A protection alert provided by IBM: Microsoft Excel XLSX code execution[31]
  – IBM Protection Signature: MS_Excel_XLSX_Parsing_Exec
- CVE-2010-0263
- Microsoft Security Bulletin MS10-017: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)[32]

[29] A protection alert provided by IBM: Microsoft Movie Maker Buffer Overflow http://www.iss.net/threats/362.html

[30] Microsoft Security Bulletin MS10-016: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561) http://www.microsoft.com/technet/security/bulletin/ms10-016.mspx

[31] A protection alert provided by IBM: Microsoft Excel XLSX code execution http://www.iss.net/threats/363.html

[32] Microsoft Security Bulletin MS10-017: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150) http://www.microsoft.com/technet/security/Bulletin/MS10-017.mspx

On March 9, 2010 Microsoft announced the investigation of new public reports of a remote code execution vulnerability affecting Internet Explorer versions 6 and 7. Internet Explorer 8 is not affected. There are targeted attacks attempting to exploit this vulnerability. Compromise of machines may lead to exposure of confidential information, loss of productivity, and further compromise such as malware. An attacker may embed a browser frame link on an otherwise non-malicious Web site to an exploit for this vulnerability or try to entice a user to click on a link included in an e-mail.

- A protection alert provided by IBM: Microsoft Internet Explorer use-after-free code execution[33]
  - IBM Protection Signatures: JavaScript_NOOP_Sled, JavaScript_Shellcode_Detected, JavaScript_Unescape_ Obfuscation
- CVE-2010-0806
- Microsoft Security Bulletin MS10-018: Cumulative Security Update for Internet Explorer (980182)[34]

[33] A protection alert provided by IBM: Microsoft Internet Explorer use-after-free code execution http://www.iss.net/threats/364.html

[34] Microsoft Security Bulletin MS10-018: Cumulative Security Update for Internet Explorer (980182) http://www.microsoft.com/technet/security/bulletin/ms10-018.mspx

Additional Q1 2010 Quarter highlights

This section of the report briefly covers some of the additional threats facing security professionals during Q1 2010.

Operation Aurora

On January 12, 2010 Google announced in their blog that in mid-December of 2009 they detected a highly sophisticated targeted attack on their corporate infrastructure.[35] Their investigation also led to the discovery of a much larger attack affecting another 20 or more large companies from various business sectors.

McAfee Labs dubbed the attacks 'Operation Aurora'.[36] The word "Aurora" was referenced in the binaries and believed to be a folder on the attacker's computer. The point of entry for the majority of the attacks was spear phishing as well as MSN Messenger.

The victim was tricked into clicking on malicious links that contained a zero-day exploit affecting Internet Explorer 6. This exploit caused the victim's computer to download and execute two pieces of malware from the attacker. Once the malware was executed, it opened up a backdoor to the victim's system giving the attackers unauthorized access to the network. IBM's blocking IPS signatures blocks the IE exploit if observed in the clear on a network. The IBM protection alert "Microsoft Internet Explorer Freed Object Code Execution" provides detailed product coverage.[37]

Educating end users plays an important role in protecting against this type of threat. Why would an attacker spend months creating a sophisticated exploit if they can just persuade someone on the inside to open a malicious PDF? Promoting safe computing practices can drastically reduce the amount of incidents in an organization's network. We encourage readers to listen to the Q4 2009 Threat Insight Quarterly podcast which discusses Operation Aurora and provides additional information: http://www-935.ibm.com/services/us/iss/xforce/trendreports/

SEO Poisoning

Search Engine Optimization (SEO) scams seemed to be a popular trend during the first quarter of 2010. Attackers have been using SEO techniques for several years now to spread their malware. To carry out this type of attack an attacker modifies the optimized search results of search engines to direct users to malicious sites.

Thus far there have been a number of high-profile incidents or tragedies for attackers to capitalize on in 2010. The earthquakes in Haiti and Chile were both subjects of major public interest and unfortunately a perfect vehicle for criminal entities to launch SEO and e-mail campaigns. To put this public interest into perspective CNN reported that as of mid-day January 13th (one day after the Haiti earthquake) four of the top ten Twitter topics were on Haiti or earthquake relief and eleven of the top twenty topics on Google Trends were Haiti or earthquake related.[38]

[35] A new approach to China http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[36] Operation "Aurora" Hit Google, Others http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/

[37] A protection alert provided by IBM: Microsoft Internet Explorer Freed Object Code Execution http://www.iss.net/threats/359.html

[38] Web users flock to Twitter, blogs for Haiti news http://www.cnn.com/2010/TECH/01/13/haiti.internet/index.html

The Vancouver 2010 Olympics also provided attackers with many opportunities to cause harm. Search results for Olympic-themed queries including wallpapers and screensavers led to malicious sites.[39] The tragic death of Olympian Nodar Kumaritashvilii resulted in multiple malware sites.[40]

Another topic that caught attackers' interests include the announcement of the Google Nexus One phone. One report indicated that searching for "buy Nexus One" provided around 4,000 malicious links.[41] And when scammers grow tired of exploiting real news events they can create their own news to gain profits through affiliate programs. An X-Force blog post published this quarter which discusses a hoax targeting college students that spammers exploited illustrates this phenomena.

Users should be cautious when clicking on links from search results. Unfortunately not all hosts that search engines point to are trustworthy. What appears to be a benign .edu or .com hostname could be a compromised site redirecting your browser to malware. We recommend visiting official Web sites when possible and encourage maintaining up-to-date anti-virus software. Enabling blacklisting on browsers that support it, such as the 'Block reported attack sites' setting in Firefox, can also help mitigate against this threat.

[39] On Olympics, St. Patrick's Day, Screensavers, and Wallpaper
http://www.avertlabs.com/research/blog/index.php/2010/02/23/on-olympics-st-patricks-day-screensavers-and-wallpaper/

[40] Olympic SEO Poisoning http://www.sophos.com/blogs/sophoslabs/v/post/8704

[41] BlackHat SEO attack targeting Google Nexus One (Updated)
http://pandalabs.pandasecurity.com/blackhat-seo-attack-targeting-google-nexus-one/

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), obtaining information from employees or stealing corporate records. Below are some of the major security breaches that became public during the fourth quarter:

AvMed Health Plans – Two laptops were stolen containing personal information including Social Security numbers of 208,000 past and present customers.

BlueCross BlueShield – The theft of 57 unencrypted hard drives from a BlueCross BlueShield of Tennessee training facility has put at risk the personal information of an estimated 220,000 to 500,000 members.

Citigroup – About 600,000 tax statements containing the recipient's Social Security numbers printed on the outside of the envelope were sent to their clients.

Educational Credit Management Corporation – The sensitive information of approximately 3.3 million individuals may have been compromised when portable media devices were stolen.

Iowa Racing and Gaming Commission – An improperly patched firewall allowed hackers to gain access to a computer server containing information on 80,000 current and former employees.

Lincoln National Corp. – About 1.2 million customers' personal information may have been compromised when it was discovered that shared passwords and usernames were being used to access the company's portfolio management system.

National Archives and Record Administration – The personal data of 250,000 Clinton administration staff and White House visitors sent to the National Archives may have been compromised when a hard drive containing this information went missing.

PricewaterhouseCoopers – Active and inactive employees who participated with the Public Employees' Retirement System (PERS) and the Teachers' Retirement System (TRS), including retireesI from 2003 and 2004, may have been compromised due to a security breach in which information was lost.

Valdosta State University – Unauthorized access to a computer server may have compromised the personal information of up to 170,000 students and faculty.

List of Contributors for this paper include:

Lyndon J. Sutherland – Cyber Threat Intelligence Analyst
IBM MSS Intelligence Center

Peter Q. Trinh – Security Intelligence Analyst
IBM MSS Intelligence Center

Michelle Alvarez – Team Lead & Cyber Threat Intelligence Analyst
IBM MSS Intelligence Center

IBM X-Force Database Team

References

AvMed laptop theft exposes Fort Lauderdale employees to risk
http://weblogs.sun-sentinel.com/news/politics/broward/blog/2010/03/avmed_laptop_theft_exposes_for.html

Thief steals 57 hard drives from BlueCross BlueShield of Tennessee
http://www.scmagazineus.com/thief-steals-57-hard-drives-from-bluecross-blueshield-of-tennessee/article/162178/

Citi exposes 600,000 social security numbers
http://www.finextra.com/news/fullstory.aspx?newsitemid=21170

Data theft targets 3.3 million with student loans
http://www.msnbc.msn.com/id/36060713

Hackers accesses Iowa Racing and Gaming Commission database
http://www.scmagazineus.com/hackers-accesses-iowa-racing-and-gaming-commission-database/article/163050/

Lincoln National Warns Customers of Potential Data Security Breach (January 14 & 15, 2010)
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=5#sID307

U.S. National Archives offers reward for missing hard drive
http://news.cnet.com/8301-1009_3-10246004-83.html

Price Waterhouse Coopers – Security Breach Fact Sheet
http://doa.alaska.gov/drb/pdf/price-waterhouse-security-breach-factsheet.pdf

US university hit by fresh data breach that exposes 170,000 social security numbers
http://www.scmagazineuk.com/us-university-hit-by-fresh-data-breach-that-exposes-170000-social-security-numbers/article/164207/

*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
April 2010

The use of third-party data, studies and/or quoted material does not represent an endorsement by IBM of the publishing organization, nor does it necessarily represent the viewpoint of IBM.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. All information contained in this document is current as of the initial date of publication only and is subject to change without notice. IBM shall have no responsibility to update such information. The information contained in this document does not affect or change IBM product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of IBM or third parties.

All information contained in this document was obtained in specific environments, and is presented as an illustration. The results obtained in other operating environments may vary. THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED ON AN “AS IS” BASIS WITHOUT ANY WARRANTY, EITHER EXPRESSED OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. In no event will IBM be liable for damages arising directly or indirectly from any use of the information contained in this document.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. Use of those Web sites is at your own risk.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

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