IBM Global Technology Services
July 2009

IBM Internet Security Systems X-Force Threat Insight Quarterly

Table of Contents

About the Report 3

Conficker, the Never Ending Story 4

Fraud Schemes; I love you. I will make you rich. Oh, and I need some money moved 16

Prolific and impacting issues of Q2 2009 30

References 46

About the report

The IBM Internet Security Systems™ 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 IBM Internet Security Systems (ISS) 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 ISS 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 ISS 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.

Conficker, the Never Ending Story

Introduction

On October 23, 2008, Microsoft issued an "out of cycle" advisory to repair a vulnerability in their remote procedure call (RPC) logic, which was already being actively exploited in the wild with limited attacks beginning in September of 2008. The following November, the first version of the Conficker family of malware appeared and began to scan and attack unpatched systems to exploit this vulnerability and infect millions of PCs worldwide.

Due to the sophistication and complexity of the malware itself and the threat posed by the large number of infected systems, industry leaders banded together to combat this particular menace. Initially referred to as the "Conficker Cabal," the group has grown and become known as the "Conficker Working Group," or CWG.

Conficker got a great deal of dire coverage in the news prior to April 1, 2009, due to the expected activation of yet another communications subsystem. While the motives of the authors remain murky at best, the doom and gloom scenarios fortunately proved unfounded and April 1 passed relatively quietly.

While Conficker has not done anything particularly destructive, to date, as some had predicted, it remains a serious threat and a very large botnet with active update capacity. The level of detected peer-to-peer communications activity continues to decrease slowly. But many machines are still infected and need to be cleaned of this malware. The machines that remain infected are fully capable of being updated with newer more malicious versions and payloads and remain a threat to other machines, particularly as new vulnerabilities are disclosed. These may be quickly exploited by malware and/or by updates propagated out through the Conficker P2P communications cloud.

This family of malware has grown increasingly resistant and defensive against security tools. Users will need up-to-date antivirus (AV) tools specifically equipped to deal with this threat. Without these tools, they may need to engage in technically difficult, manpower intensive, manual cleanups. Although some AV products can remove the malware, many infected systems in many situations will need to be wiped and reinstalled or reimaged to reliably remove any trace of this threat.

Over the last several months, the Conficker worm family evolved into a massive sophisticated malicious botnet arsenal and infrastructure of millions of compromised hosts. It is becoming increasingly difficult to contain this contagion, after the fact, and the threat of new versions with new tricks and unknown motives is looming. Patching against vulnerabilities which this worm is exploiting remains the most effective control.

While the news coverage over Conficker may have faded and the level of network traffic associated with this particular family of malware may be decreasing, this remains a serious threat driven by indeterminate motives that still need addressing.

Background

Early accounts of the exploit used by Conficker arose in September of 2008. Microsoft issued an out of cycle advisory on October 23, 2008, to repair the vulnerability and attempt to address the potential threat from the ongoing active exploitation in the wild. The AlertCon was raised to Level 2 in response to this threat on October 23 and restored to AlertCon 1 on October 30. Nonetheless, in November 2009, the first version of Conficker arose and began to scan and attack unpatched systems to exploit this vulnerability and infect millions of PCs worldwide. The exploit employed a specially crafted remote procedure call (RPC) over port 445/TCP to cause vulnerable systems to execute arbitrary code.

The first version of Conficker--Conficker A--merely propagated by exploiting the MS08-067 RPC vulnerability. MS08-067 is a vulnerability similar to MS06-040, which was first seen a couple of years ago. Conficker A attempted to download and install fake antivirus software.

The specific attack symptoms for the first generation (A) of the worm are as follows:

- *Attacks port 445 RPC*
- *Runs an HTTP server used to serve DLL to compromised machines*
- *Uses rundll32.exe to load DLL into running processes*
- *Uses multiple different paths to SYSTEM32.*

The second generation--Conficker B--did not attempt to install and promote fake AV. It did add to the worm propagation vectors the ability to propagate over Netbios shares and to propagate through USB key autorun on removable media. These are more mundane worm propagation techniques. Attempts by Confiker B to propagate over Netbios shares by brute forcing network accounts have resulted in some account lockouts and network disruptions.

At that point, Conficker incorporated a command and control (C&C) rendezvous system whereby infected systems would mathematically generate a list of 250 domain names, which it would attempt to contact for updates and further commands. Network infrastructure organizations collaborated on the analysis of the Conficker behavior and banded together into what they initially called the Conficker Cabal to attempt to counter this C&C infrastructure.

The specific attack symptoms for the second generation (B) of the worm are as follows:

- *Attacks port 445 RPC*
- *Runs an HTTP server used to serve DLL to compromised machines*
- *Uses scheduled tasks to re-infect across network*
- *Uses rundll32.exe used to load DLL into running processes; network aware*
- *Attempts to brute force and use network shares to re-infect other systems*
- *Uses Autorun.inf files to re-infect/reload/propagate the worm through removable media*

Early on March 5, 2009, a new version of Conficker--conventionally referred to as Conficker C--was detected. Conficker C introduced an expanded C&C capability generating a list of 50,000 potential domain names, of which 500 would be contacted each day, when operational. It also implemented a P2P infrastructure by which infected hosts could act as P2P servers, aid in the propagation of updates and remain in communications outside of the C&C communications structure.

Conficker C also sports a widely expanded defensive mechanism to protect itself. It additionally disables a wide variety of antivirus and security software and it blocks download sites and update sources.

It's worth noting that Microsoft has referred to this version of Conficker as "Conficker D" while using the term "Conficker C" to refer to an earlier variation of the B variant. This has caused some ongoing confusion in reports and literature.

On April 1, 2009, the updated C&C communication system in Conficker C was poised to swing into action. While the intent of the authors of the Conficker worm remains unknown, Conficker C did not cause any of the disruptions that were being circulated as possibilities prior to that date. In fact, Conficker C did very little on the activation date outside of a few reported attempts at communication.

A little more than a week after the April 1 start-up date, reports circulated about an update propagating. Some of the Conficker C sites downloaded a new component, Conficker E. Conficker E reintroduced some propagation capabilities using the previous methods and vulnerabilities. It also reintroduced efforts to promote fake antivirus software while expanding on the blocking list for antivirus and security tool sites. In response, several security tool sites added additional domains and advertised them for users to contact. This "cat and mouse" game of block, and new tool domains, makes it increasingly difficult for users to find tool sites and to be able to discriminate between legitimate sites and new fake sites. Some reports also indicated that the new component was also downloading the waladec malware to some infected systems.

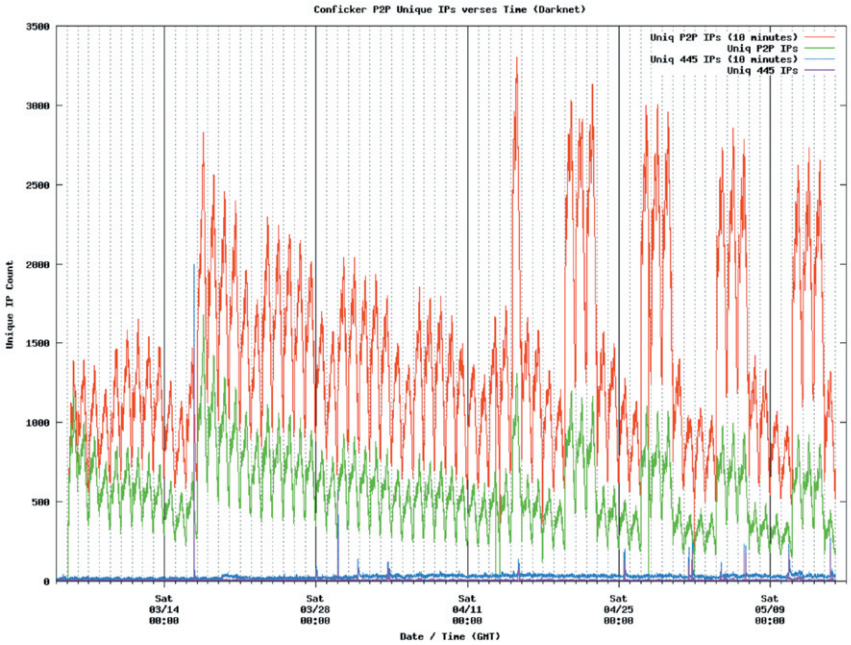
Conficker E also had a date, May 3, coded in. Unlike Conficker C, which activated a new command and control communications mode, on or about this date, Conficker E was programmed to stop working and erase itself. After erasure, Conficker E left behind previous generations and any payloads it had downloaded running on the infected systems. This has come to pass and Conficker E is no longer in operation but previous versions still are operating as before.

Due to the sophistication of the code and the development of this worm, it's generally felt that it is unlikely to be used for destructive purposes, which would be counter-productive. It's as equally likely to do nothing, as it is to run rampant and be disruptive. Updating itself to a newer version in a continuing effort of measure and counter-measure, and engaging in active money making schemes and other criminal activity seem more likely than either extremes in the ongoing changing landscape of this malware.

P2P Traffic

An illustration of the P2P communications cloud introduced by Conficker C can be seen in the following graph. Conficker C uses both TCP and UDP to attempt communications with other P2P systems and varies the destination ports it utilizes based on an algorithm that incorporates the IP address of the destination and, in some cases, the date. The ports that incorporate the date into the algorithm change every seven days. The complexity of this algorithm, varying on IP target and date, make this extremely difficult to filter at firewall egress points due to the sheer number and complexity of the filtering rules that would be required, and which would require a weekly change.

The graph below is from a "darknet" net telescope where the data is captured and then filtered for only those packets matching the port generation algorithms.



As can be seen from this graph, Conficker has not gone away and is not going away anytime soon.

Some notable characteristics of Conficker include a daily cycle of traffic that corresponds to machines being turned off and on during a normal business schedule, with a minimum on Saturday and Sunday. The onset on March 6 is the first appearance of Conficker C (Microsoft Conficker D). The jump in traffic on March 17 has been associated with a spread of Conficker C to a large number of .org domains. There has been a progressive decrease in the bulk source addresses over time to the point that the traffic later in the week is less than the original inception of Conficker C. The exception to this is traffic that first appeared as the isolated peak after midnight on the morning of Wednesday, April 15. Since then, traffic on Monday, Tuesday and Wednesday has been significantly elevated in UDP traffic relative to the other days of the week. Week to week after that increase, these daily peeks are showing a steady decline as well. The significance of this new behavior is unknown at this time.

Similar patterns are being reported by other members of the Conficker Working Group from the Conficker "sink holes," which are black holes configured to intercept the queries for the generated DNS patterns for C&C servers.

Preventive Actions

Several things need to be done to mitigate this threat. Foremost, is maintaining systems patched to the best software fix level available. This is even more important now with the P2P update capacity of Conficker coupled with the difficulty of filtering and blocking infected systems at security perimeters.

If you have infected systems, you may use Group Policies to stop the Conficker. worm from spreading across shares and removable media. Create a new policy that applies to all computers in a specific organizational unit (OU), site, or domain, as required in your environment. It is important to emphasize that these procedures will not remove the W32/Conficker.worm from the system or network. These procedures will only stop the spread of the malware.

Autorun or autoplay are also known vectors for propagating a variety of malware, including variants of Conficker. Autorun may be disabled, preventing malicious software from running when removable media, such as a USB key or camera memory card, are attached to a PC. This also means that certain functionality that users have come to expect will no longer behave as before. There has been a general level of dissatisfaction in the security community regarding the issue of autorun and autoplay on MS Windows. This has finally resulted in Microsoft beginning to disable this feature for rewritable removable media such as USB memory cards and removable drives. The new defaults, which have not as yet been widely disseminated, would still permit autorun on media such as CD-Roms and DVD's. Considering that these may also be rewritten under some conditions, and some USB keys have a "U3" partition that appears to be a CD-Rom device, it remains to be seen if even this level of restriction will be sufficient. Published articles have referred to autorun as the largest known unpatched Microsoft vulnerability in their products. Microsoft has published knowledge base articles describing how to properly disable autorun on its various products, including patches to earlier versions of Windows 2000 and Windows XP, in order to disable this feature.

Some organizations, part of the Conficker Working Group, are proceeding with attempts to neutralize parts of the C&C communications structure by setting up sinkholes. The sinkholes work by routing the requests for the precalculated and registered domain names that are part of the C&C infrastructure of this malware. While this is effective to some degree, it is more effective as an intelligence gathering tool for the security community. This is likely to be insufficient in the long run to block the behavior of the malware in and of itself, as the authors of the malware continue to adapt to the countermeasures. However, more participation in such groups aids in their effectiveness and benefits the entire community.

Corrective Actions

Each generation/variant thus far requires different cleaning techniques to remove the threat. Infected systems must be identified and cleaned up. Fortunately, there are ways to manually remove the latest version, and there are also removal tools available from several vendors such as Symantec, McAfee, and others to help users clean their systems. Vulnerable systems must be patched to prevent (re)infection. The P2P network must be neutralized, as well as the domain-based C&C communication network. Lastly, restricting access to the SVCHOST registry key will be needed. This will restrict permissions on the SVCHOST registry key so that it cannot be written to again.

Infected machines can be readily identified by network detection of the high P2P UDP traffic on high numbered ports. Infected internal systems may be identified using this technique behind firewalls. The level of P2P traffic already present outside of security perimeters reduces the effectiveness of identifying machines through network detection outside of those security perimeters.

The Conficker Working Group has also provided a "Conficker Eye Chart" linked from their home page, which includes several images linked deliberately from some of the blocked sites. The eye chart references several images from security vendors and several reference images from innocuous sites such as OpenBSD, Linux, and FreeBSD . By browsing to this site and comparing which images can be seen with the legend below the "eye chart" one can get a quick feel as to whether or not they might be infected and, if so, then possibly by which variant. This is using the behavior of the malware against itself to conveniently reveal itself to a casual user.

Organizations with up-to-date antivirus tools may find that their AV products can effectively clean this infection and that may be the most effective course for them. You should use an antivirus product to remove W32/Conficker.worm from the infected systems and network. Each antivirus vendor will have its own procedures and recommendations associated to removing this exploit. However, the Conficker family of worms has incorporated extensive defensive mechanisms and a complete rebuild may be the only prudent course of action for a compromised system. Therefore, companies may opt for manual removal if they have staff with the necessary technical expertise.

Many sites will likely opt for rebuilding to ensure no lingering traces of the infection remain. Procedures for rebuilding systems, often through an "imaging" mechanism, must ensure that newly installed systems are not vulnerable to this threat. Infected systems must be identified, isolated and cleaned. If you don't want to re-image all infected systems, there are several "hacks" and specific cleaning procedures that can be used to fight the exploit, thereby avoiding a complete rebuild.

Code has been developed that remotely fingerprint the presence of Conficker on compromised systems. Many OpenSource projects, such as nmap and nessus, as well as many AV vendors, are now incorporating this new information into their products and tools. There are now OpenSource python scripts available to perform Conficker scanning on networks.

In the face of ongoing infections, network administrators need to determine whether they have contaminated systems and then isolate and disinfect these systems. Most AV companies have now incorporated methods to disinfect systems. Some are now providing "run live" CD's that allow for booting a compromised system from a CD and scanning for infection. While manpower intensive, this method is one of the best for reliably dealing with increasingly defensive and evasive malware, especially those incorporating rootkit technologies.

Trend Microsystems has a knowledge base article on restoring access to update sites from infected machines titled, "How to restore access to Trend Micro and other security sites that have been blocked by malicious software infections." They suggest that you run the "net stop dnscache" command to restore access to security and updates sites that are being blocked by Conficker-C.

Conclusion

It is likely that new Conficker variants will appear with new tricks. The first line of defense against the ongoing threat is prompt patching and preventative action, such as disabling features such as autorun. Information sharing is essential to staying on top of the evolution of this threat and to continue to contain it. As always, it is best to contact your specific antivirus vendor for specific capabilities and products.

IBM Internet Security Systems has posted a flash video of "Conficker 'round the World" using Google Earth to create a picture of the infections that have been seen. IBM Internet Security Systems continues to provide updated coverage for various aspects of the Conficker family of malware as detailed in the "Conficker Worm / Downadup" threats reference page.

Fraud Schemes; I love you. I will make you rich. Oh, and I need some money moved

Introduction

The Internet is rife with fraud schemes and why not? In an Internet-less world, con artists used traditional means to locate and contact their potential victims. These traditional means lacked the speed and global reach of the Internet and often the con artists would be in physical touch with their victims. The widespread adoption of the Internet changed the world and brought scammers and their potential victims closer together.

During the writing of this article we received much assistance from the Fraud and Corporate Crime Group of the Queensland State Police in Australia in providing background and comments for this article. We gratefully acknowledge this support and thank the Queensland State Police, and in particular, Detective Superintendent Brian Hay and Detective Senior Constable Graeme Edwards, for their assistance.

> *"The Queensland Police Service Fraud and Corporate Crime Group has conducted a three year investigation named Operation Echo Track into the Advance Fee scam industry and identifying its effects on the Queensland community. This work will continue, as it is recognised that the criminal plague that is Advance Fee Fraud, is not slowing down, but rather gaining momentum, fuelled by technology, large criminal profits, and perhaps even the Global Financial Crisis."* [1]

1 *Detective Superintendent Brian Hay, Queensland State Police, Fraud and Corporate Crime Group.*

Fraud schemes can take many shapes and forms; however, for this article we are focusing on two specific forms of fraud, Advance Fee schemes and Romance scams. Both are relatively common forms of Internet fraud schemes and both are also synonymous with Nigeria. No doubt many of you have probably heard or read of the terms "Nigerian" or "419 scam" or other variations on the name. What might surprise you though, is how successful these two scams can be.

And there are reasons Nigeria came to be associated with the advance fee scams. A United States, State Department document from 1997 shows how some Nigerian advance fee fraud schemes were conducted prior to the widespread adoption of the Internet. An interesting note in the document is the estimation that approximately 3,000 letters involving advance fee frauds were mailed or faxed, per week, with the United States and Great Britain being the recipients of approximately 50 percent of that number[2].

Today, the United States Federal Bureau of Investigation (FBI) describes Nigerian criminal enterprises as the most significant among African criminal enterprises and operates in more than 80 countries. It is also noted that the Nigerian groups are globally famous for the financial frauds they have perpetrated, aside from the advance fee schemes, which include frauds based on insurance, healthcare billing, life insurance, bank, check, credit card, document fraud and also developing false identities[3].

---

2 *United States, Department of State, Bureau of International Narcotics and Law Enforcement Affairs, Nigerian Advance Fee Fraud*
http://www.state.gov/www/regions/africa/naffpub.pdf

3 *F.B.I. Web site: Organized Crime, African Criminal Enterprises*
http://www.fbi.gov/hq/cid/orgcrime/africancrim.htm

Ultimately, to be successful, these fraud schemes typically rely on something we hear much about—social engineering.

> *"The social engineering to which the victim is subjected can be quite simply unbelievable."*[4]

How do scammers find their victims?

To start, it is useful to understand how scammers select or make initial contact with their potential victims. And more often than not, it starts with spam. And perhaps ironically, when using spam to generate victims, it is more often the victim who finds the scammer; because, when the victim clicks the "reply" button, the scammer probably has no idea at all who the victim might be.

No doubt many have seen such spam arrive in their inbox. As to how many people actually respond, we have no way of knowing; but, like typical spam campaigns selling products, the spammers or sellers rely on a vey low ratio of responses to the number of emails sent. When looking back at the 1997 publication and the figure of 3,000 letters per week, it is easy to see why these fraud schemes transposed so well to the internet where 3,000 emails to a global audience can be sent in minutes, with less cost and possibly even lower risk to the scammer. Emails from scammers can also be more targeted, often using information obtained from Internet resources such as social networking sites.

Social networking sites have been a boon to online scammers who have quickly educated themselves on how to best exploit the Internet and who recognized the richness of the resources presented in such places. The high concentration of users and personal information allows for more specific targeting of potential victims. Dating sites, for example, provide scammers with fertile hunting grounds.

---

4 *Detective Superintendent Brian Hay, Queensland State Police, Fraud and Corporate Crime Group.*

> *"We have identified that the fraudsters have very aggressively targeted their victims through online dating sites. Once the fraudster has identified their victim, they are ruthless in their attempts to emotionally exploit the victims' desire for a partner".*[5]

Even forums that discuss religious studies, or the Bible, are hunting grounds for con artists who may present themselves as religiously oriented, eventually seeking donations from their victims for some worthy cause.

Scammers also keep lists of successfully conned victims, and once a victim has been identified and successfully conned, their identity and contact details may well be traded, sold or passed to another scammer running a different con.

And of course, traditional methods of victim selection still remain: phone books, newspapers, television and many other sources of information. Even obituaries in newspapers have been used as a source for information by criminals seeking to profit.

The mechanics of a scam

Advance fee scams always work along a simple principal: A victim pays money to the scammer in return for a promise that they will be provided something of far greater value in return. The "something" in advance fee frauds can be almost anything that has value: oil contracts, money transferred to the victim's bank account, gold. You name it; if it has value to the victim, the scammers will be happy to use it. And not all scammers cut and run after the victim pays the first supposed fee. Often they try to lure the victim along in hopes of extracting even more money from them.

---

5 *Detective Superintendent Brian Hay, Queensland State Police, Fraud and Corporate Crime Group.*

Con artists are experts in getting money from their victims, often doing it in such a way that the victim doesn't initially realize they've been scammed. In such a case, the scammer is often able to convince the victim to send even more money.

An illustration:
The Scammer convinces his victim to make a payment to either the scammer himself or perhaps his "Agent," in return for whatever it was the scammer promised his victim. But alas, after the initial payment was made, more money than was anticipated is needed to pay for lawyers, or perhaps to bribe an official, and so on. The scammer will play the victim until he thinks the revenue stream has dried up.

It's really that simple.

Romance schemes tend to run along the same lines, but are a little different in their construct. The advance fee scams tend to rely on the greed of their potential victim, who think they will get a large return on their investment (e.g., "You've won the Nigerian lottery, please send $175 U.S. dollars for your claim ticket…").

Romance schemes, on the other hand, play far more on the emotions of the victim and use that as leverage to obtain funds from them. Such a ploy is obvious to many, but when it comes to matters of the heart, there are numerous reasons why it might seem to make perfect sense to send someone you care about some money:

- *To purchase an airline ticket so he or she could come visit*
- *To help them with some medical bills*
- *or just "because"*

Regardless of the reason, payments are generally made through money transfer services, making it nearly impossible to track once the transaction has been completed.

How to find a scammer

It isn't difficult at all to find your very own scammer. As noted, just read your email. If you respond to an email, then the game, from the scammer's perspective, has begun.

While conducting research for this article, we conducted an experiment to see just how difficult it would be to find a scammer through an online dating service.

The Scenario:

The Setup: We registered an account at two different online dating services based in Australia and sat back and waited.

The Bait: We designed a profile that was of a middle aged man—single of course, and self-described as "lonely."

The Result: Within a week, we received a message sent through one of the dating services asking for a reply to an email address on one of the well known free email services. How could we not respond? We did, and as soon as we received our next email, we were rather certain we had found a scammer.

What we discovered: The IP address used by our scammer didn't appear to be located in Nigeria, but rather in Senegal, a country in western Africa. Surprisingly, this was, in fact, the country the scammer said she claimed to be living in, as a refugee in a refugee camp. Some research on the name used by the scammer and by looking up the content of the emails, led to the not-so-surprising discovery that the scammer was actively seeking victims in many countries, and in almost all cases, was using the same name and story.

The emails used in our test case appear to be templated, as we found similar versions archived on other Web sites where people had noted this particular scam. The emails even provided us a phone number that we could call to talk to our scammer, and though we didn't call the number, we are confident that it would lead to someone who would at least take a message for our scammer. One notable aspect of this scammer though, is that he or she is organized. Response time to our emails was generally no longer than 24 hours - service with a smile no doubt.

By the fourth email from our scammer, we were urged to contact the scammer's alleged bank and to act on her behalf to facilitate the transfer of almost $5 million to one of our accounts. Another seemingly obvious clue that this was a scam, was that the alleged bank's email address was hosted by a popular free email service. As the scam unfolded, we were told by the so-called bank, that there was a requirement that we would need to provide certain documentation in order to facilitate the transfer. It just so happened, that our scammer was also contacted by "the bank" and was able to point us to a source for the required documentation; a law firm in Senegal.

Another clue that we discovered, which the average victim probably would not typically notice, is that while the address and phone numbers provided for the bank appeared to be in London, the IP Address used in sending the bank's return email was physically located in Senegal. Additionally, we were able to locate the same telephone numbers given by the bank, in another scam, but using a different name for the bank than the one given to us.

Having worked through the initial roadblocks to reaching our ultimate goal of becoming $5 million richer, the next step, according to our scammer, was to contact the alleged law firm, which, for an approximate $1,500 USD, would provide us the required documentation needed to affect the funds transfer.

At this point, we ceased all communications with the scammer. There is little doubt that we would have encountered more issues and never seen any of the alleged monies, and that we would have been asked to keep on fronting money for one thing or another until either we had no money left, or we cut our losses.

While this does appear to be a very crude scam with templated emails and canned replies, it has been running in at least a similar manner for several years, even using the same name of the alleged woman sending the emails. While this scam might be best classified as a Romance scam, since the woman claimed to want to "…spend the rest of [her] life…" with our created persona, it is also effectively a form of advance fee scam. While it may seem unlikely that such a scam works often, if ever, given the number of years it has been going on, one has to wonder how frequently it does work. Perhaps, in our case, the romance aspect was but a hook, designed to whet our appetite enough to actually pursue the matter further where the scammer could provide us more personalized service and attempt to social engineer us into sending money. Regardless, about the only thing that is certain, is that we would never see the money we were promised.

On a sidenote, we also had another bite on our lonely bachelor advertisement; this one from a dear lady in Russia who was also interested in marrying us. We replied to the emails, but alas, our reply was unrequited.

Typically with Romance fraud schemes, we would expect it to start as an online romance and we wouldn't expect the fraudster to request any money until such a time as they believed they had endeared themselves to the victim. At such a time, a victim's emotions can be more easily preyed upon and therefore more likely that the victim would send money. Scammers may also set up their own profiles on social networking sites to attract potential victims and wait for approaches rather than be the initiator of contact. This lends the air of legitimacy to the victim, since it was they, not the scammer, who initiated the contact.

But just as in the case of advance fraud fee schemes, the first request for money will almost certainly not be the last. Rather, it will be the beginning of a long line of requests until, as the scammer sees it, the revenue stream had dried up or proves fruitless. These scammers are generally very accomplished social engineers and are very aware of how to manipulate their victims.

So why do these schemes actually work?

As we have already mentioned, many of these fraudsters are gifted with social engineering skills. But on the part of the victim, typically in advance fee scams, the reason these scams work is simple greed. The victims believe that they will make a large amount of money for doing something—something that is sometimes even illegal. They believe, at least initially, that the money they are sending to the scammer is actually an investment and will return a very large profit.

In romance schemes however, this is generally not the case. Instead, the victim's emotions are preyed upon and the victim could be said to be searching more for happiness than for financial profit. We also mentioned that religious forums are used by scammers to make contact with potential victims. These types of attempts prey on a person's "goodness" by asking them to do things to help others, such as support an orphanage or to generally help those less fortunate than themselves. Rather than exploiting a person's greed, they rely instead on the "kindness of strangers" who believe that they are helping someone.

In short, these schemes exploit human emotions and use social engineering to lead people to make decisions based on their feelings rather than on the facts or logic of the situation.

It's old and it's a cliché but it remains something of a truism in the vast majority of cases; if it seems too good to be true, it probably is.

How successful are these scams?

This is a somewhat difficult question to answer with any precision since not all victims of fraud will report the incident. Harking back to the F.B.I. information on Nigerian criminal enterprise however, they estimate the cost to the United States from Nigerian financial frauds approximates $1 billion to $2 billion each year. This appears to be a gross estimation, but even taken at the low end, $1 billion is a significant amount of money.

One notable case involving an American as the victim of a Nigerian advance fee fraud was brought to trial in Nigeria this year (2009). This scam is typical of Nigerian scams that claim to be representatives of a Nigerian-based petroleum company. The victim in this case was duped out of approximately $1 million USD made in several payments, the largest single payment being $425,000 USD. The scheme was typical in that it required the victim to make continued payments due to issues cropping up with completing the transaction, and that forged documentation was provided to the victim[6].

We can also look to Australia, where in a 2008 news article[7] it was reported that Australia (population approximately 21 million at the time) was losing at least $36 million AUD per year to so-called Nigerian scammers. According to the Queensland State Police, Australians were sending about $3 million AUD per month to Nigeria and at least 80% of the amount was considered fraud related. The article notes that some of the romance scam victims lost $35,000 AUD but that businesses had lost up to $5 million AUD. Perhaps most tellingly, as to how successful the scammers can be in the social engineering of their victims, is that the article mentions how, despite being advised by police that they were the victim in a fraud scheme, some victims kept on handing money to their scammer.

---

6 *EFCC, HOW NIGERIAN FRAUDSTER DUPED ME OF $1M- AMERICAN BUSINESSMAN*
http://www.efccnigeria.org/index.php?option=com_content&task=view&id=622&Itemid=34

7 *SMH, Scammers defraud Aussies of $36m a year: police*
http://www.smh.com.au/news/technology/nigerian-scam-shock/2008/08/20/1218911772460.html

Also from Australia, we find a 2009 news article outlining the case of a Nigerian national living in Australia being involved in a multi-million dollar financial scam. This scam was described as using "elaborate scenarios involving Saddam Hussein, a US Army general, Interpol and a string of fake lawyers and government diplomats," however, it is also noted in the article that the scammer was involved in another common Internet fraud: lottery scams. Known to have operated between 2005 and 2008, victims were enticed into the fraud schemes through emails or Web sites. This particular scammer, and he was only a part of the overall operation, was sentenced on 51 fraud and passport violation charges.[8]

But the U.S. and Australia aren't the only countries targeted. We can also look to the UK and research performed by Michael Peel and published by Chatham House in 2006, which notes that it had been estimated that "Nigerian-style advance fee frauds cost the economy £150 million annually, with the average losses per victim a not insignificant £31,000." This particular paper also provides interesting background on various schemes and some political and historical background on Nigeria[9].

These examples touch on only three countries, but should serve to illustrate just how prolific these schemes are and how profitable they can be for the scammers.

---

8 *Nigerian fraud scam mastermind sent to jail*
http://www.thewest.com.au/default.aspx?MenuID=77&ContentID=136307

9 *NIGERIA-RELATED FINANCIAL CRIME AND ITS LINKS WITH BRITAIN*
http://www.chathamhouse.org.uk/files/3377_nigeria1106.pdf

Is there a human cost to these schemes?

There is a human cost. In the typical advance fee schemes, people lose money and typically they will find themselves– at least–emotionally distressed. The more money they have lost, or the greater their loss impacts their lives, the more distressed they become. In romance frauds however, where not only is money lost but the victim's emotions and trust may have been seriously hurt, the damage can be very high.

Fraud victims have been known to attempt suicide, lose their marriages and have their businesses go bankrupt. Some victims may turn to crime themselves in order to replace at least some of the money they have lost. Such events take a heavy toll on individuals and families making it difficult to measure the full human cost. And in addition to the toll these frauds take on the victims, there is also very little chance of ever recuperating any of the money paid to the scammers, even if the scammer is caught and prosecuted.

Perhaps surprisingly, is the demographic of people who tend to suffer the greatest financial losses, and who appear to be the most vulnerable to social engineering deceptions:

> *"The largest losses tend to be inflicted upon mature, tertiary educated professional people who have generally been successful in life. Yet it is very often this group of individuals who refute law enforcement advice and continue to send money to the fraudsters after they have been advised they are a victim of a fraud."*[10]

10 *Detective Superintendent Brian Hay, Queensland State Police, Fraud and Corporate Crime Group*

How can the scams be prevented and what can be done?

In terms of prevention for the individual, the most important action—or inaction—one can take is to simply, not reply to emails promising something for literally nothing. No matter how enticing the email may seem, it is very unlikely to be true. While this may seem simple common sense advice, statistics suggest that people do reply. Many ISP's and email clients provide spam or junk filtering and we strongly advise that both individuals and organizations take advantage of such features, even if only to provide a clue that an email may well be just what it should appear to be, junk mail.

In corporate terms, spam filtering systems aid in keeping such emails away from employees and also aid in productivity by preventing end-users from having to spend time deleting unwanted spam. Such spam filtering gateways will often also provide the capability of filtering malware contained in emails.

> *"Education, cooperation and partnerships between law enforcement, government, industry and community groups is key to any chance of reducing the impact of this criminal scourge."*[11]

In terms of what can be done about these schemes and those who run them, the only real answer is reporting any such schemes or approaches to the relevant authorities. Your local authorities may be able to offer assistance with this. For example, the Queensland State Police in Australia provide excellent information and guidance on where and how to report such fraud. You can view this information on the Queensland Police Service's Web site at: http://www.police.qld.gov.au/programs/crimePrevention/eCrime/scams/default.htm

---

11 *Detective Superintendent Brian Hay, Queensland State Police, Fraud and Corporate Crime Group*

We should also note that Nigeria is not idle in working to combat these fraud schemes through measures such as the Economic and Financial Crimes Commission. The following is quoted from the introduction on their Web site "About" page:

> *The preponderance of economic and financial crimes like Advance Fee Fraud (419), Money Laundering, etc has had severe negative consequences on Nigeria, including decreased Foreign Direct Investments in the country and tainting of Nigeria's national image. The menace of these crimes and the recognition of the magnitude and gravity of the situation led to the establishment of the Economic and Financial Crimes Commission (EFCC). The legal instrument backing the Commission is the attached EFCC (Establishment) Act 2002 and the Commission has high-Ievel support from the Presidency, the Legislature and key security and law enforcement agencies in Nigeria.*[12]

The EFCC is charged with the responsibility of investigation and enforcement of all laws against economic and financial crimes and is also the designated financial intelligence unit in Nigeria. Additionally, it coordinates the various institutions involved in the fight against money laundering and enforcement of all laws dealing with economic and financial crimes in Nigeria.

Obviously, stopping crimes such as the advance fee frauds and romance scams is not an easy task. But those who do seek to prosecute and stop such crimes do need the help of the public through the reporting of such schemes and by providing as much information as possible to them. If you are a victim or know someone who is, please report the crime or urge the victim to do so.

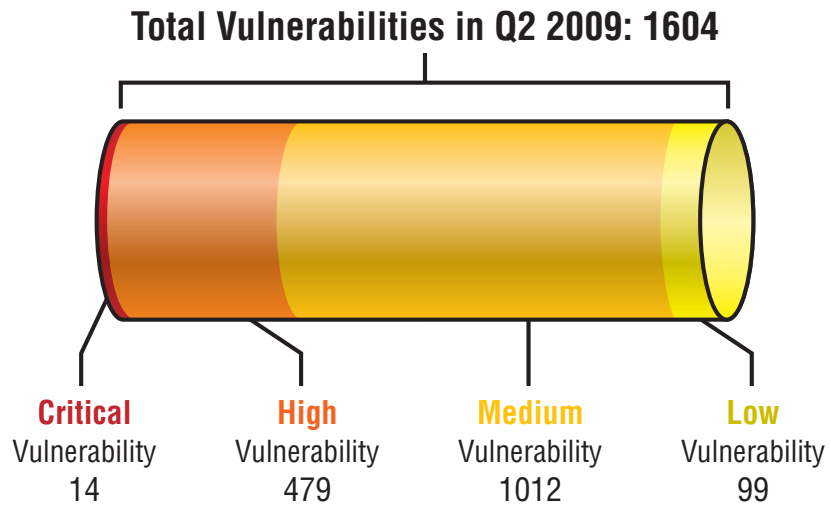
---

12 *Nigerian Economic and Financial Crimes Commission*
http://www.efccnigeria.org/index.php?option=com_content&task=category&sectionid=4&id=13&Itemid=29

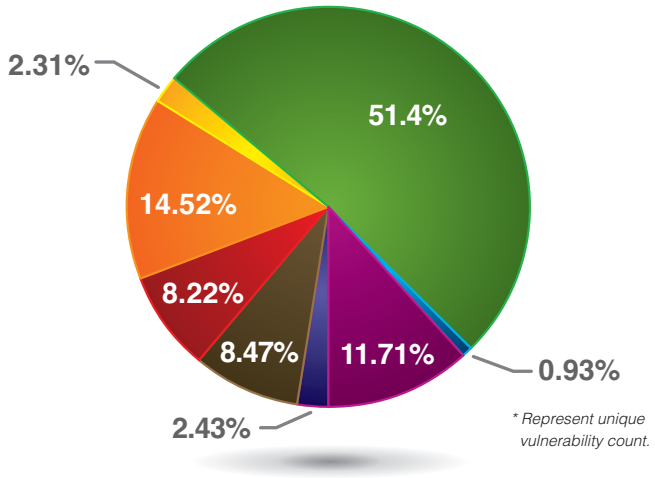
Prolific and impacting issues of Q2 2009

Significant disclosures

In Q2 2009, the X-Force team analysts researched and assessed 1604 security related threats. A significant percentage of the vulnerabilities featured within the X-Force team database became the focal point of malicious code writers whose productions include malware and targeted exploits.



The chart below categorizes the vulnerabilities researched by X-Force team 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. *



Bypass Security – 11.71%

Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner.

Data Manipulation – 14.52%

Manipulate data used or stored by the host associated with the service or application.

Denial of Service – 8.22%

Crash or disrupt a service or system to take down a network.

File Manipulation – 0.93%

Create, delete, read, modify, or overwrite files.

Gain Access – 51.4%

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 – 2.31%

Privileges can be gained on the local system only.

Obtain Information – 8.47%

Obtain information such as file and path names, source code, passwords, or server configuration details.

Other – 2.43%

Anything not covered by the other categories.

At the start of the second quarter, Microsoft® released a Security Advisory to announce that a vulnerability in their PowerPoint® presentation graphics program has been exploited in the wild. The X-Force team subsequently released a Protection Alert to address this critical issue. Microsoft Office PowerPoint could allow a remote attacker to execute arbitrary code on the system, caused by an error when handling .ppt files. To exploit the issue an attacker would have a user open a specially crafted PowerPoint file that could lead to the execution of arbitrary code with the rights of user. Microsoft later issued Security Bulletin MS09-017 to address this issue.

- *A protection alert provided by IBM ISS: Microsoft PowerPoint Remote Code Execution Vulnerability* [13]
  - *IBM ISS Protection Signatures: CompoundFile_Shellcode_Detected and Shellcode_Detected*
- *CVE-2009-0556*
- *Microsoft Security Bulletin MS09-017 – Critical: Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)* [14]

13 *A protection alert provided by IBM ISS: Microsoft PowerPoint Remote Code Execution Vulnerability*
http://www.iss.net/threats/322.html

14 *Microsoft Security Bulletin MS09-017 – Critical: Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)*
http://www.microsoft.com/technet/security/bulletin/ms09-017.mspx

In mid April 2009, the X-Force team published a Protection Alert to address a serious vulnerability disclosed in Microsoft's April 2009 Security Release. Microsoft DirectShow® application programming interface (API), which is part of Microsoft DirectX® API, could allow a remote attacker to execute arbitrary code on the system by persuading a victim to open a specially-crafted MJPEG (video) file. Microsoft DirectShow is a core component of Microsoft Windows® 2000, XP, and Server 2003 and is enabled by default. The use of malicious media files like images and movies has been prevalent in the past years and the use of malicious movies, in particular, substantially increased near the end of 2008.

- *A protection alert provided by IBM ISS: Microsoft DirectShow MJPEG Remote Code Execution* [15]
  - *IBM ISS Protection Signature: AVI_DirectShow_MJPEG_Decompression*
- *CVE-2009-0084*
- *Microsoft Security Bulletin MS09-011 - Critical: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)* [16]

15 *A protection alert provided by IBM ISS: Microsoft DirectShow MJPEG Remote Code Execution* http://www.iss.net/threats/324.html

16 *Microsoft Security Bulletin MS09-011 - Critical: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)* http://www.microsoft.com/technet/security/bulletin/ms09-011.mspx

The same day the aforementioned Protection Alert for the Microsoft DirectX issue was released, the X-Force team also produced a Protection Alert for a vulnerability in Adobe Acrobat® Reader® and Adobe Acrobat. This issue could allow an attacker to execute arbitrary code on a remote system by enticing a user to open a specially-crafted PDF file. Public exploit code and reports of targeted exploitation of this issue have surfaced.

- *A protection alert provided by IBM ISS: Adobe Reader and Adobe Acrobat GetIcon() Remote Code Execution* [17]
  - *IBM ISS Protection Signatures: PDF_Obfuscated_Stream and PDF_Encoded_JavaScript_Tag*
- *CVE-2009-0927*
- *Adobe Security Bulletin APSB09-04* [18]

While the Conficker botnet continued to cause problems for businesses, a new botnet made its debut in Q2 2009. Gumblar is a growing botnet that compromises traditionally non-malicious Web servers in order to exploit systems that visit those Web sites. Malware that redirects Google™ searches is planted on the target system, which provides the attackers with "pay-per-click" or possibly other types of income. The malware also looks for FTP credentials on the system and may use them to compromise additional Web sites.

17 *A protection alert provided by IBM ISS: Adobe Reader and Adobe Acrobat GetIcon() Remote Code Execution*
http://www.iss.net/threats/323.html

18 *Adobe Security Bulletin APSB09-04*
http://www.adobe.com/support/security/bulletins/apsb09-04.html

Compromised Web sites do not appear to host malware or exploits, but instead host links and redirects to malicious servers elsewhere. One of the original servers used the domain gumblar.cn, which changed to martuz.cn and will likely change again.

- *A protection alert provided by IBM ISS: Adobe Reader and Adobe Acrobat GetIcon() Remote Code Execution* [19]
  - *IBM ISS Protection Signatures: PDF_JavaScript_Exploit, PDF_Obfuscated_Stream, PDF_Encoded_JavaScript_Tag, PDF_JavaScript_Hex, PDF_JavaScript_Detected, PDF_Shellcode_Detected, Multimedia_File_Overflow, JavaScript_Obfuscation_Rue (PDF obfuscation), Swf_Suspicious_ActionScript (Flash obfuscation)*

19 *A protection alert provided by IBM ISS: Gumblar*
http://www.iss.net/threats/gumblar.html

In June 2009, four Protection Advisories were published for vulnerabilities found by X-Force team researchers. Two of these advisories were to address vulnerabilities in Xvid video codec. These issues could be exploited to compromise an application or system using the library. By persuading a victim to open a specially-crafted movie file, a remote attacker could overflow a buffer to corrupt memory and execute arbitrary code on the affected system with privileges of the victim. The DivX® codec is not vulnerable to this issue, which can make a vulnerable system appear safe due to its filter interpositioning. However, a knowledgeable attacker can bypass DivX and directly invoke the Xvid codec by using specific media types.

- *A protection advisory provided by IBM ISS: Xvid Codec MBlock Indexing Buffer Overflow* [20]
  - *IBM ISS Protection Signature: Codec_Range_Error*
- *CVE-2009-0893*
- *A protection advisory provided by IBM ISS: Xvid Codec Initialization Logic Buffer Overflow* [21]
- *CVE-2009-0894*
  - *IBM ISS Protection Signature: AVI_Very_Large*
- *Xvid.org: Xvid 1.2.2 released* [22]

---

20 *A protection advisory provided by IBM ISS: Xvid Codec MBlock Indexing Buffer Overflow* http://www.iss.net/threats/325.html

21 *A protection advisory provided by IBM ISS: Xvid Codec Initialization Logic Buffer Overflow* http://www.iss.net/threats/326.html

22 *Xvid.org: Xvid 1.2.2 released* http://www.xvid.org/News.64.0.html?&cHash=0170b4e439&tx_ttnews[backPid]=64&tx_ttnews[tt_news]=7

The third Protection Advisory released in June addresses multiple vulnerabilities affecting Adobe Acrobat and Adobe Reader. Adobe Acrobat and Adobe Reader are vulnerable to six vulnerabilities leading to remote code execution by improperly parsing JBIG2-encoded data streams in PDF files. If a user is enticed to open a malformed PDF file through email, a Web browser, or another vector, the vulnerabilities could be used to execute code with the privileges of that user. Malformed document files are frequently used by computer criminals to install spyware or other malware on victim PCs. Adobe has released patches for these issues.

- *A protection advisory provided by IBM ISS: Multiple JBIG2 Vulnerabilities in Adobe Acrobat and Adobe Reader* [23]
- *CVE-2009-0509, CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, CVE-2009-0888, CVE-2009-0889*
  - *IBM ISS Protection Signature: JBIG2_Adobe_Integer_Overflow, Image_Pattern_Overflow, Image_Pattern_Corruption, Image_Grid_Overflow, Image_Halftone_Corruption*
- *Adobe Security Bulletin APSB09-07* [24]

The last Protection Advisory of the second quarter addresses a Microsoft Visual Basic® ActiveX® remote code execution vulnerability. Plug-ins, like 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.

---

23 *A protection advisory provided by IBM ISS: Multiple JBIG2 Vulnerabilities in Adobe Acrobat and Adobe Reader*
http://iss.net/threats/327.html

24 *Adobe Security Bulletin APSB09-07*
http://www.adobe.com/support/security/bulletins/apsb09-07.html

Although this ActiveX control is not installed by default, most PCs have it. Nearly all Visual Basic applications include this DLL during the installation process, and, since it is considered a shared component of these applications, it is typically left on the system even after an uninstall. Hence, if a Visual Basic program has ever been installed on a computer, it probably has this ActiveX control installed. This makes the component highly prevalent and a lucrative target for attackers.

- *A protection advisory provided by IBM ISS: Microsoft Visual Basic ActiveX Remote Code Execution Vulnerability* [25]
- *CVE-2008-0024*
  - *IBM ISS Protection Signature: HTML_ATL_ActiveX_BO*
- *Microsoft Security Advisory (969898): Update Rollup for ActiveX Kill Bits* [26]

The X-Force team ended the quarter with a Protection Alert for a remote code execution issue affecting Microsoft DirectX. This vulnerability was being actively exploited, which led to its public disclosure by Microsoft. A core component of Microsoft Windows 2000, XP, and Server 2003, Microsoft DirectX is enabled by default. Successful exploitation of this issue would provide an attacker with complete control over the endpoint target.

---

25 *A protection advisory provided by IBM ISS: Microsoft Visual Basic ActiveX Remote Code Execution Vulnerability*
http://iss.net/threats/328.html

26 *Microsoft Security Advisory (969898): Update Rollup for ActiveX Kill Bits*
http://www.microsoft.com/technet/security/advisory/969898.mspx

Our analysts continue to observe exploitation of this issue. Currently, specially-crafted QuickTime® videos are being hosted on malicious Web sites, but these malicious files may also arrive through other vectors such as spam. The use of malicious media files, such as images and movies, has been prevalent in the past years and the use of malicious movies, in particular, substantially increased near the end of 2008.

- *A protection alert provided by IBM ISS: Microsoft DirectX Quartz.dll Remote Code Execution* [27]
- *CVE-2009-1537*
  - *IBM ISS Protection Signatures: MOV_Container_Overflow, QuickTime_DirectShow_Code_Execution, JavaScript_Obfuscation_Fre*
- *Microsoft Security Advisory (971778): Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution* [28]

---

27 *A protection alert provided by IBM ISS: Microsoft DirectX Quartz.dll Remote Code Execution*
http://iss.net/threats/330.html

28 *Microsoft Security Advisory (971778): Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution*
http://www.microsoft.com/technet/security/advisory/971778.mspx

Additional Q2 2009 highlights

This section of the report briefly covers some of the additional threats facing security professionals during Q2 2009.

Swine Flu – Cyber Threats and Continuity Planning

In April 2009, stories regarding the swine flu outbreak began circulating. The use of widely reported and alarming issues to induce victims into reading spam email has become a staple of the threat landscape. Spam messages purporting to offer books and materials for sale soon surfaced following news of the outbreak. At least one example of malware distribution based on swine flu spam has also been noted.

The spam generated appears to be largely pushing fake products for curing swine flu or items such as swine flu survival guides. The known malware, reported by Symantec, appears in the form of a malicious PDF file that exploits the vulnerability patched by Adobe in their security bulletin APSB09-04. The malicious file is purported to be a document that provides answers to questions about the H1N1 virus. Additionally, numerous swine flu related domain names have been registered. While many of these domain names may be legitimate, some may be used for nefarious purposes such as hosting malware.

In the information age, it is important to cultivate trustworthy and authoritative information sources. While sites like Twitter can provide instant reporting of first hand accounts during major news incidents, they can also be breeding grounds for uninformed speculation. One of the most essential information age skills is being able to gather input from diverse sources and filter it through expertise and experience in order to facilitate a comprehensive decision making process. In times of crises, such processes can then feed back into your business continuity and disaster recovery activities.

It is important for businesses to identify any risks they may face caused by the influenza pandemic. For example, clients should identify key personnel such as those who travel internationally frequently who may be at risk and review relevant emergency policies, plans and procedures. Additionally, we urge caution in handling email, particularly from untrusted sources with headlines relating to the influenza pandemic. We recommend seeking information on the pandemic from trusted and reputable sources such as government and the WHO Web sites.

Hactivism in Iran

On June 12, 2009, Iran held its tenth presidential election. Many voiced concern that electoral fraud had taken place and reports of politically motivated hacking, also known as hactivism, soon surfaced. Proponents encouraged others to support their case via Twitter where they posted instructions on how to launch distributed denial of service (DDoS) attacks against certain Iranian sites.

It is becoming increasingly more common for geopolitical events and military conflicts to include one or more cyber events. Cyber attacks are a widely used method of protest though DoS attacks and Web site defacements. In 2007, for instance, DDoS attacks against Estonia's Web sites successfully generated devastating effects on the country's information infrastructure. And during the Russia and Georgia conflict in 2008, the Web site of the President of Georgia came under DoS attack. Other Georgian sites hosted on the same IP address as this Web site also became unavailable. The cyber attacks against Georgia continued for several days with varying reports of scope and effect.

Major security breaches

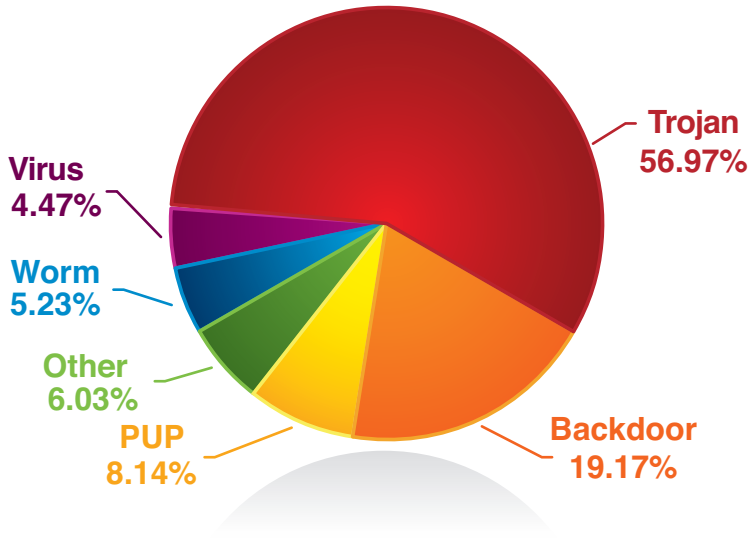
A number of high-profile security breaches are reported every year drawing attention to the need to protect consumer and employee information from the risk of exposure to malicious individuals/identity (ID) theft rings. In addition to the loss or misplacement of information, corporations and individuals 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 2nd Quarter:

- ***Aetna –*** *Hackers compromised an employment Web site and obtained e-mail addresses. It is unknown if other sensitive information, including Social Security numbers, were obtained. In response, 65,000 current and former employees were notified and offered credit monitoring.*
- ***Cornell University –*** *A stolen laptop has compromised the personal information of 45,000 members of the University's community to include current and former students as well as current and former faculty and staff members.*
- ***Federal Reserve Bank of New York –*** *A former employee at the Federal Reserve Bank was arrested on suspicion of obtaining loans using stolen identities. The former employee had worked as an IT analyst at the bank and had access to sensitive employee information.*
- ***Multiple financial institutions –*** *Malicious individuals rigged ATMs using skimmers and tiny cameras to steal account and password information from unsuspecting victims. The skimmer read and stored the personal information kept in the bank card's magnetic strip. The camera filmed victims typing in their PIN codes. The thieves then created their own fake ATM cards.*
- ***University of California –*** *A database breach was discovered during routine maintenance; messages were left behind by the hackers. The personal information of 160,000 current and former students and alumni may have been stolen. The databases had been illegally accessed by hackers beginning in October 2008, and continued until April 2009.*
- ***Virginia Department of Health Professions –*** *A hacker demanded $10 million in ransom for medical records obtained from the state's Prescription Monitoring Program (PMP) database. Notifications are being sent to 530,000 people whose prescription records may have contained Social Security numbers.*

Malcode corner

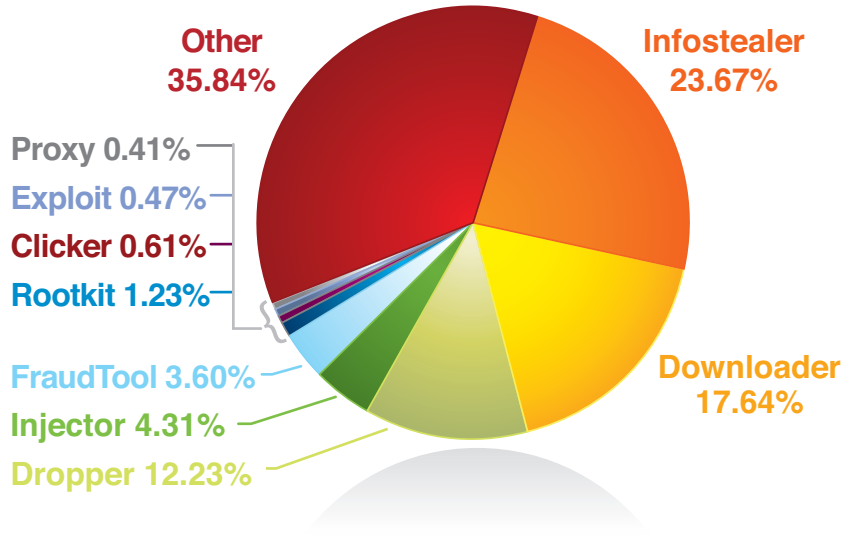
The IBM ISS X-Force Virus Prevention System (VPS) team's categorization of malcode is based on the most dominant features of the threat. The primary malcode categories are:

- ***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 Web site 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 embedded malware components into an affected system.*
- ***Exploit –*** *Documents or media files containing exploit code.*
- ***FraudTool –*** *Malware used to commit fraud. An example is malware that displays fake error or infection messages, and then entices the user to purchase fake tools or security software.*
- ***Generic –*** *Trojans that do not fall within the other subcategories.*
- ***Infostealer –*** *Spies and/or steals information; this includes password stealers, keystroke loggers and spyware.*
- ***Injector –*** *Injects an embedded malware component into another process. One purpose is for the embedded (and usually obfuscated) malware to evade antivirus detection. Another purpose is for the embedded malware to evade host-based firewalls by injecting it into a trusted process such as a browser or a system process.*
- ***Other –*** *Trojans that do not fall within the other subcategories.*
- ***Proxy –*** *Allows a remote attacker to relay connection through 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.*



List of Contributors for this paper include:

Michael Warfield – *Senior Researcher and Analyst, IBM MSS Intelligence Center*
Lyndon Southerland – *Threat Analyst Security Specialist, IBM MSS Intelligence Center*
Michelle Alvarez – *Team Lead, IBM MSS Intelligence Center*
IBM ISS X-Force Database team
IBM ISS X-Force Virus Prevention System (VPS) team

References

Conficker, the Never Ending Story

McAfee Inc.& Avert Labs, "Finding W32/Conficker.worm Whitepaper", Updated March 19, 2009.
http://download.nai.com/products/mcafee-avert/documents/combating_w32_conficker_worm.pdf

VIL description, updated for "W32/Conficker.worm.gen.c".
http://vil.nai.com/vil/content/v_154253.htm

IBM Internet Security Systems, "Conficker Worm / Downadup"
http://www.iss.net/threats/conficker.html

IBM Internet Security Systems, "Conficker 'round the World"
http://blogs.iss.net/archive/confickerroundthewor.html

Phillip Porras, Hassen Saidi, and Vinod Yegneswaran, "An Analysis of Conficker's Logic and Rendezvous Points".
http://mtc.sri.com/Conficker/

Jose Nazario, "The Conficker Cabal Announced," Arbor Networks, 12 February 2009.
http://asert.arbornetworks.com/2009/02/the-conficker-cabal-announced/

The Conficker Working Group
http://www.confickerworkinggroup.org

The Conficker Eye Chart
http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

"Group launches strategy to block Conficker worm from .ca domain".
http://www.cbc.ca/technology/story/2009/03/24/tech-090314-conficker.html

Microsoft Corporation, "Microsoft Security Bulletin MS08-067 - Criticial," 23 October 2008.
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

Microsoft Corporation, "Conficker Worm: Help Protect Windows from Conficker.A and Conficker.B".
http://technet.microsoft.com/en-us/security/dd452420.aspx
http://microsoft.com/conficker
http://www.microsoft.com/technet/security/advisory/967940.mspx
http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx
http://support.microsoft.com/kb/318803
http://support.microsoft.com/kb/962007

Trend Microsystems, "How to restore access to sites block by malware infections"
http://esupport.trendmicro.com/pages/How-to-restore-access-to-Trend-Micro-and-other-security-sites-that-have-been-blocked-by-malware-infections.aspx

Prolific and impacting issues of Q2 2009

Aetna says Web site hacked
http://www.upi.com/Business_News/2009/05/28/Aetna-says-Web-site-hacked/UPI-16751243566585/

Cornell Laptop Theft Could Be Identity Fraud Bonanza
http://www.usnews.com/blogs/paper-trail/2009/06/26/cornell-laptop-theft-could-b-identity-fraud-bonanza.html

Former Federal Reserve Bank employee arrested
http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1354835,00.html?track=sy160

Beware: ATM skimmers stealing money on the Eastside
http://www.examiner.com/x-1146-Seattle-Eastside-Family-Examiners~y2009m6d26-Beware--ATM-skimmers-stealing-money-on-the-Eastside

Hackers breach University of California database
http://ghanabusinessnews.com/2009/05/09/hackers-breach-university-of-california-database/

Reports: Thief holds Virginia medical data ransom
http://www.securityfocus.com/brief/957

Health Professions Announces Direct Notifications
http://www.dhp.state.va.us/misc_docs/DHPNewsRelease20090603.pdf

Swine Flu Subjects and e-Pharmacy Sites
http://www.avertlabs.com/research/blog/index.php/2009/05/01/swine-flu-subjects-and-e-pharmacy-sites/

Adobe Security Bulletin APSB09-04
http://www.adobe.com/support/security/bulletins/apsb09-04.html

Updated List of Domains - Swineflu related
http://isc.sans.org/diary.html?storyid=6280

IBM - Infrastructure recovery services
http://www-935.ibm.com/services/us/index.wss/offerfamily/bcrs/a1026935

Iranian hacktivism
http://isc.sans.org/diary.html?storyid=6583

Digital Fears Emerge After Data Siege in Estonia
http://www.nytimes.com/2007/05/29/technology/29estonia.html

Georgia accuses Russia of coordinated cyberattack
http://news.cnet.com/8301-1009_3-10014150-83.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.
07-09

SEL03003-USEN-00