



# **IBM Internet Security Systems X-Force Threat Insight Quarterly**

## **Table of Contents**

<b>About the Report</b>	<b>3</b>
<b>Cyberterrorism – A Tale of Two Incidents</b>	<b>4</b>
<b>Domain Name System Revisited – DNS Cache Poisoning</b>	<b>21</b>
<b>Prolific and Impacting Issues of 4th Quarter 2008</b>	<b>29</b>
<b>References</b>	<b>43</b>

**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](mailto:XFTAS@us.ibm.com).

### **Cyberterrorism – A Tale of Two Incidents**

As was reported widely in major news outlets around the world in late 2008, Russia and Georgia were involved in a military conflict over the region known as South Ossetia, a region that seeks complete autonomy from the Democratic Republic of Georgia. During the conflict, Georgia was widely reported to have come under heavy cyber attacks that some have alleged were carried out or orchestrated by Russian government forces or agents. Many reports have likened the attacks to those that targeted Estonia in 2007, which succeeded in separating Estonia from the greater Internet for several days.

More recently, terrorist attacks in India have resulted in several issues carrying the potential to escalate into a tense standoff between India and Pakistan. The attacks introduced a tactic not previously seen in terrorist attacks in India – the deliberate targeting of foreign nationals. India is a large center for outsourced IT work and also has a significant population of resident and transient foreign workers involved in various roles and business capacities. The attacks may present many potential problems for the IT sector in India, and potentially for global operations that rely on India for its outsourced IT expertise.

*(Note: For the purposes of this article, the X-Force team defines “cyberterrorism” as attacks carried out against IT assets, by individuals and/or groups not officially recognized as terrorist organizations.)*

Tale One: Georgia – Russia, Cyber War

There seems to be little information pointing to a Georgian cyber warfare capability or that Georgia has adopted policies around engaging in information or cyber warfare. In comparison with Russia, Georgia has a much smaller population and land area, and therefore, a more limited military and lower economic demographics. In Internet terms, there are far fewer Internet users and hosts than in Russia. From outside a country's borders, it is difficult to gauge or understand the level of reliance a country like Georgia has on the Internet and related services; however, services such as SMTP and HTTP will probably be heavily relied on for communications just as they are in most nations that have embraced the Internet.

Based on several public statements made regarding Russia's understanding of information warfare, it appears that Russia has understood the importance of Information and cyber warfare for many years. An excerpt from Professor V. I. Tsymbal's speech "Concept of Information Warfare," delivered at the Russian-United States conference on "Evolving Post Cold War national Security Issues" in Moscow in September 1995, underscores this point.

***"From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not . . . considering the possible catastrophic consequences of the use of strategic information warfare – means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces, . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself. <sup>1</sup>"***

---

<sup>1</sup> Detering Information Warfare: A New Strategic Challenge  
<http://www.carlisle.army.mil/USAWC/Parameters/96winter/thomas.htm>

More recently, the paper “Cyber Warfare: An Analysis of the means and motivations of selected states,” published in 2004, provides an interesting statement on Russia. While the statement pertains to a potential threat to the United States from Russia, it illustrates that Russia is estimated to have a comprehensive cyber warfare doctrine.

***“Russia’s armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia’s cyber warfare doctrine have disclosed discussions and debates concerning Moscow’s official policy. “Information weaponry,” i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine. Moscow also has a track record of offensive hacking into Chechen websites. Although we assess it likely that Moscow will continue to scout U.S. military and private sector networks and websites, available evidence is inadequate to predict whether Russia’s intelligence services or armed forces would attack U.S. networks, especially after taking into account present-day political and economic ties between the two nations. <sup>2</sup>”***

Russia is well connected to the rest of the world in Internet terms and while the percentage of Internet users versus overall population is not as high as that of many other nations, it remains that there is no shortage of technical sophistication. Georgia, in contrast, has far more limited connectivity, and a significantly lower number of users and Internet hosts. Georgia appears to draw its Internet bandwidth through Turkey and Azerbaijan, though traffic from Azerbaijan is reported as transiting through Russia. <sup>3</sup>

---

<sup>2</sup> *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*  
<http://www.ists.dartmouth.edu/projects/archives/cyber-warfare.html>

<sup>3</sup> *Georgia Clings to the 'Net*  
<http://www.renesys.com/blog/2008/08/georgia-clings-to-the-net.shtml>

#### Cyber Warfare in 2008 – A Case Study

The Russia and Georgia conflict in 2008 presents a unique opportunity to see how modern-day cyber warfare might be carried out. The first widely publicized shots in the cyber war ultimately waged against Georgia appear to have been fired in July 2008, when the Web site of the President of Georgia came under a denial of service (DoS) attack. Another government site, in addition to sites unrelated to the Georgian government, are also hosted on the same IP address and these also became unavailable because of the DoS attack.

According to the Shadowserver Foundation, a self-described, all-volunteer Internet watchdog group, the attack was a MachBot DDoS (Distributed Denial of Service) attack comprising HTTP, ICMP and TCP traffic. The Shadowserver Foundation further reported that they had observed at least one Web based C&C (Command and Control) server being used to direct the attacks. Curiously, the C&C host used in the attack came online in the weeks prior to the attack but was not observed as having been used in any other attacks. Physically, the C&C host was located in the United States, but the Shadowserver Foundation does not provide any conclusions on who might have been responsible for the attacks, though they do note that the MachBot is frequently used by Russian BotHerders. Additionally, the domain registration details for the domain the C&C host was operating from contained false information that appeared to tie back to Russia.<sup>4</sup>

---

<sup>4</sup> Shadowserver Foundation – Calendar – 2008-07-20  
<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080720>

Reportedly, South Ossetia's two online news services, osinform.ru and osradio.ru, were hacked on or around August 5, 2008. These sites operate from Russian domains and are reportedly Russian backed, but run by South Ossetia's state television and radio services. The osinform.ru site had its content replaced with content from Alania TV. Alania is reportedly supported by the Georgian government and domain registration information for the Alania TV domain points to a Georgian email address.<sup>5</sup>

Then, concurrent with the Russian military intervention, what amounts to a cyber war was launched against various Georgian Web sites and Internet services in general. In an apparent reference to a VoIP system, the following comment was made by Georgian president Mikhail Saakashvili in a phone interview with Wolf Blitzer from CNN. Blitzer had announced that Saakashvili was "on the line" some time earlier, but when he attempted to ask a question the line appeared to have been disconnected. Some time (apparently about 10 minutes) later the interview took place. The following excerpt was taken from that interview:

**BLITZER:** *All right. I think we've connected with the president of the republic of Georgia, Mikheil Saakashvili right now in Tbilisi. Mr. President, what is the latest as far as the actual battle, the fighting that is going on between your troops and the Russian troops?*

**SAAKASHVILI:** *Well, sorry, first of all, for this weird position, in a way. We sometimes – our lines get under cyber attack, that's a new technology these days of war. But I can hear you well.*<sup>6</sup>

---

<sup>5</sup> *Cyber War: Russia VS Georgia*  
[http://finchannel.com/index.php?option=com\\_content&task=view&id=17911&Itemid=55](http://finchannel.com/index.php?option=com_content&task=view&id=17911&Itemid=55)

<sup>6</sup> *CNN LATE EDITION WITH WOLF BLITZER*  
<http://transcripts.cnn.com/TRANSCRIPTS/0808/10/le.01.html>

There were also reports of attacks against Russian Web sites, though these were not widely reported by the media and it is difficult to gather the scope of these attacks. However, RIA Novosti reported <sup>7</sup> that its DNS servers and Web site had come under a “severe” DoS attack that lasted several hours. While it is not clear whether other Russian sites were targeted by attacks, at least some attacks carried out against hosts on Russian (.ru) domains appear to have been carried out by the same hosts or BotNets used to attack Georgian sites.

The cyber attacks against Georgia continued for several days with varying reports of scope and effect. Many of the western media reports regarding the cyber war appear to have been based on postings to the RBNexploit blog run by security researcher Jart Armin <sup>8</sup>.

#### Allegations, Speculation and Attacks

The cyber attacks against Georgian (and some Russian) sites appear to have comprised DDoS attacks and systems breaches or defacements. For example, the Web sites of the Georgian Parliament, and that of the President, were defaced and some content replaced. The attackers claimed to be a group from South Ossetia. Attacks, however, were not limited to government sites. <sup>9</sup>

BCP routing statistics provided on August 10, 2008, by the Renesys Corporation, a global Internet monitoring company, identified 309 prefixes that were geo-located to Georgia, originating from 26 autonomous systems. Additionally, the Renesys Corporation showed that over the preceding three-day period, up to 35 percent of the prefixes disappeared from the Internet and up to 60 percent of them were unstable. None of the outages were seen as permanent. <sup>10</sup>

---

<sup>7</sup> *Coordinated Russia vs Georgia cyber attack in progress*  
<http://blogs.zdnet.com/security/?p=1670>

<sup>8</sup> *Russian Business Network (RBN)*  
<http://rbnexploit.com/>

<sup>9</sup> *Shadowserver Foundation – Calendar – 2008-08-11*  
<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080811>

<sup>10</sup> *Georgia Clings to the 'Net*  
<http://www.renesys.com/blog/2008/08/georgia-clings-to-the-net.shtml>

Statistics published by Arbor Networks on August 12, 2008, show that the attacks averaged approximately 211Mbps but reached peaks of 814Mbps. The attacks were short-lived, with the average lasting around two hours and fifteen minutes, and the longest noted as having lasted six hours. They also noted that the attacks were more intense, but lasted for shorter time periods, than those against Estonia.

While speculation as to who was behind the attacks ran rampant, on August 12, 2008, the Shadowserver Foundation published more details. For instance, they observed that six C&C hosts were involved in the attacks against Georgia; however, in contrast to the C&C hosts used in the earlier DDoS attacks, these had been active for some time and were responsible for several attacks against a range of sites that included:

- *Adult and/or racially themed sites*
- *Russian news sites*
- *Sites with possible ties to criminal organizations such as carding and virtual currency sites*
- *Some seemingly random sites unconnected to the current crisis*

In short, the targets included a very broad range of previous targets, as well as some seemingly unrelated to Georgia. This would suggest that the botnets were part of criminal organizations' resources and were either hired out to the attackers or used by the owners themselves.

One very interesting report on August 13, 2008, provided some evidence of a "grass roots" movement apparently based in Russia. This group was disseminating via blogs, forums and Web sites, an attack script that users could download and run that would send ICMP packets using the 'ping' command to various Georgian sites. The published list contained approximately 20 Georgian targets. It appears though, that such a script would require numerous users in order to make a significant impact; though, this would be dependant on the parameters used with the ping command.<sup>11</sup>

Throughout the conflict, many media reports were based on information published by the rbnexploit blog<sup>12</sup>, an Internet blog devoted to providing information about the Russian Business Network (RBN), which, according to Wikipedia, is a "...multi-faceted cybercrime organization, specializing in and in some cases monopolizing personal identity theft for resale."

While the reports from the rbnexploit blog provided a wealth of information, at times it is difficult to substantiate some of their speculation with regard to the RBN and the Russian government. Regardless, it is likely that the view from inside Georgia, and the understanding of the local environment on the inside at the time of the attacks, is likely to have been quite different from that of an outsider.

One of the main claims made by the rbnexploit blog asserts RBN's involvement in the attacks on Georgia. The blog makes reference to the RBN being "nationalized" and goes as far as providing the names of two alleged RBN operatives who they claim were involved in the attacks. The blog also stated, "Further investigation of Mr. XXXXX and Mr. XXXX are likely to implicate the Russian authorities in the cyber first strike." It should be noted that, despite the inability to personally verify most of the information published by the rbnexploit blog, the blog has existed for some time and has done a considerable amount of reporting on the RBN. For those reasons, the rbnexploit blog is considered by many, as one of the most knowledgeable entities on the subject.

---

<sup>11</sup> *Shadowserver Foundation – Calendar – 2008-08-13*  
<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813>

<sup>12</sup> *Russian Business Network (RBN)*  
<http://rbnexploit.blogspot.com/>

In its blog postings, rbnexploit also reports a major spam campaign that it alleges is emanating from RBN IP ranges, which are based around a fictitious BBC story regarding the Georgian President, Mikheil Saakashvili. The spam campaign was verified by the University of Alabama (UAB);<sup>13</sup> however, it is questionable that the spam campaign is an escalation of the cyber war against Georgia as reported by the rbnexploit blog or headlined in the UAB article since much of the current virus-ridden spam piggybacks on current news headlines. For example, the Storm Worm gang made its name by trading on issues in the minds of the public. An article on UAB's Web site with an interview by Gary Warner, UAB Director of Computer Forensics Research says:

***“Several of the computers being used to send the new spam campaign are in Russia, including at least one computer owned by the Federal Agency of Education.” Warner said. Does this indicate a “Cyberwar?” Warner said far more likely is what was seen in Estonia: Russian youth activists organizing cyber attacks and cyber propaganda out of misplaced expressions of patriotism.***

***“These spam messages serve a dual purpose, a propaganda attack against Georgia, while adding compromised hosts to botnets controlled by pro-Russian individuals,” Warner said.***

A further spam campaign<sup>14</sup> that takes advantage of the situation has also been noted. It uses the subject of journalists being shot in Georgia to lure victims.

---

<sup>13</sup> UAB Spam Data Mine Uncovers Russian-Georgian Escalation  
<http://main.uab.edu/Sites/MediaRelations/articles/50618/>

<sup>14</sup> Malicious Russian-Georgian Spam Uses .ZIP Password  
<http://blog.trendmicro.com/malicious-russian-georgian-spam-uses-zip-password/>

Further to the grassroots concept, the rbnexploit blog provide a screenshot from the Web site “stopgeorgia.ru” showing targets selected for attack. In a box in the screenshot labeled “Info” is the following statement:

***“We – the representatives of the Russian hako-underground, will not tolerate provocations by the Georgian in all its manifestations. We want to live in a free world, but exist in a free-aggression and lies Setevom space.”***

It is noted that the image is a screen capture taken on August 10, 2008, and the translation of the site (which is in Russian) was performed by Google’s translation service.

A further translation, provided by a Russian speaking employee, reads slightly differently:

***“We are representatives of the Russian hacking-underworld, we shall not put up with provocation from Georgia in the way it is acting. We wish to live in a free world, and to exist free from aggression and lies in Cyberspace.”***

The stopgeorgia.ru site remained online for some time, and in what might be considered a situation of irony, the site appeared to be hosted in the United States with the address space having been rented to a Russia-based hosting service.

Whodunit ?

The question asked most often in relation to these attacks on Georgia is, “Which party, or parties, is responsible?” A popular theory is that the attacks against Georgia were carried out by the Russian government or military, or persons acting on the orders of the Russian government. Another popular theory is that the attacks were conducted by persons acting independent of the Russian government, but who probably share a similar sentiment towards Georgia and South Ossetia. These are similar to the speculation as to who was behind the attacks that were waged against Estonia.

Simply put, there is currently no public evidence available that allows one to conclude with any level of confidence that the attacks were executed by, or on the order of, the Russian government or military. Certainly, the Russian military action against Georgian forces and the cyber attacks against Georgia occurred concurrently, and while that may allow for theories of circumstance, it is not in itself a clear indication as to who the attackers are or that they acted on orders from the Russian government.

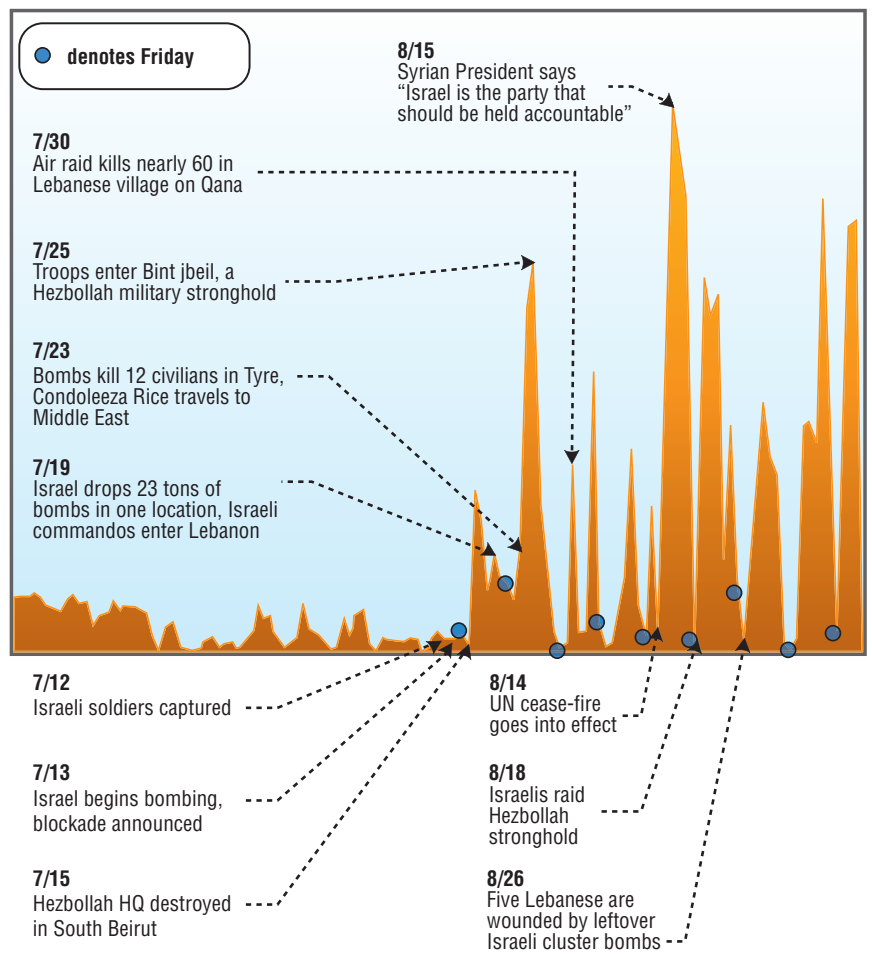
The IBM ISS analysts certainly do not discount that Russia appears to have an offensive cyber warfare capability that is professionally organized and prepared for action. The issue is that there is no evidence (speculation and convenience aside) to suggest this is what occurred in this recent situation.

Based on the most verifiable evidence, it appears most likely that the attacks were carried out by a loosely formed collection or coalition of people who were opposed to the Georgian activities, or who were perhaps simply supportive of South Ossetia or Russia. Similar to the “Revenge of the Flame” incident detailed in the last edition of the XFTIQ, this would appear to be yet another example of nationalism or patriotism being exploited, or exercised, by Internet users to express their opinions in a somewhat destructive or forceful manner.

The attacks appear very similar to the attacks against Estonia in 2007 in both an organizational and in a technical sense; however, those attacks were not waged in parallel with a full-scale military campaign. It can also be argued that the attacks against Estonia were more successful as they were able to completely sever Estonia from the Internet for several days. Those attacks were also speculated as having been carried out on the order of, or by, the Russian government and similarly the recent attacks on Lithuania.

With an increasing amount of government and private information and infrastructure control residing, even in parallel with offline fail-safes, it is becoming increasingly more common than uncommon for geopolitical events and military conflicts to include one or more cyber events. The infamous hacker war, which resulted from an incident between an American spy plane and a Chinese fighter jet in 2001, is perhaps a classic example of such.

Another excellent example is the conflict between Israel and Lebanon in 2006. During that conflict the IBM Threat Team conducted research in mapping cyber attacks against Israel to the various geopolitical and military events of the time.<sup>15</sup> The graph below shows the events that were believed to be the causes of the peaks in attacks.



<sup>15</sup> IBM Security Threats and Attack Trends Report, September 2006

India vs. Terrorism – The potential problems for IT

The recent terrorist attacks in India this past November, which included the targeting of foreigners, present a clear cause for concern for the security of foreign workers in India. It should be noted, that while the attacks did not target IT centers or workers, the fact that the attacks targeted places where large groups of foreigners gathered, is of concern, and could potentially lead to companies facing increased costs for the security and safety of foreign workers in India. This could lead to a withdrawal of outsourced IT favor for the country, which could mean that companies reduce the number of non-native staff that they maintain in-country. A possible worst-case scenario could result in an exodus of such workers if the situation deteriorates further and India is no longer considered a safe environment. Any of these situations could lead to issues with Indian based services.

Because these attacks included the targeting of foreign nationals, it is plausible that future attacks may target Indian companies that work with foreign companies, or nationals, particularly those that deal with US, British, or Israeli companies, as these were the nationalities apparently targeted in the most recent attacks. While Indian security forces will be on high alert in the near-future, further attacks remain possible.

Understanding the motivation behind such attacks could provide insight into the desired outcome of them. If the attacks were in any way designed to affect India's economy (the current attacks could be seen as affecting tourism for example), IT operations could become targets due to the income they provide to the Indian economy. Again, companies that outsource to India face the problems of increased security costs and potential interruptions to services due to attacks, if such attacks continue and/or escalate.

If the tensions between Pakistan and India escalate further and result in military strikes or full scale war, the situation should be viewed as seriously deteriorated for IT companies.

Also in line with current trends, any escalation of tensions or physical attacks are likely to lead to an increased level of cyber attacks similar to the previously mentioned cases with Estonia in 2007, and Georgia in 2008. Even the current events notwithstanding, a recent news report quotes a “feud” between Pakistani and Indian hackers vying to deface and control Indian and Pakistani Web sites. Looking at the cyber attacks against Estonia and Georgia, one of the most concerning aspects is the large scale DDoS attacks that crippled the Internet services to both countries for extended periods. Outsourcing interests in India depend heavily on effective Internet communications and major extended disruptions to those lines of communication could have a severe impact on the ability of companies based there to deliver services.

Threats to IT companies in India from terrorist groups are not new. In July 2005, Network World reported that documents seized from three members of the Lashkar-e-Toiba, (the group allegedly responsible for the current attacks) who were killed in an encounter with Indian police, revealed that they planned to carry out suicide attacks on software companies in Bangalore <sup>16</sup>. On January 9, 2009, the Indian publication “Business Line,” reported that in the previous week “six major IT firms in Bangalore such as Infosys, Wipro, Accenture and Cranes Software received a terror mail threatening to blow up their campuses in the city” <sup>17</sup>.

---

<sup>16</sup> Terrorists targeted India's outsourcing industry  
<http://www.networkworld.com/news/2005/0307terrotarge.html>

<sup>17</sup> Security fears may deter new outsourcing customers  
<http://www.thehindubusinessline.com/2009/01/07/stories/2009010751140400.htm>

While unrelated to the current events, two accidental severing of undersea fiber cables off the coast of Egypt <sup>18</sup> and Sicily <sup>19</sup> in January 2008 and December 2008, respectively, resulted in a reported 50 to 80 percent reduction in India's International Internet bandwidth and had a significant impact on the ability of India's IT companies to deliver. Due to the detrimental affect on India's economy and its ability to communicate to the wider world, undersea fiber cables may be considered potential targets in terrorist or state attacks.

Overall, it is prudent for companies that outsource to India to at least review their disaster recovery and service continuity plans. Also, for companies with workers located in India, relevant government travel warnings are worth noting. For example, the British and American governments issued advice for their nationals travelling to, or in, India. Currently, the alerts do not warn against travel to India, but do suggest maintaining a high level of vigilance and caution.

Outright war between India and Pakistan could lead to significant problems, while more terrorist attacks, or attacks specifically targeting IT companies, could also lead to greater problems. Not planning for such an eventuality could be courting disaster; therefore, it would be prudent to plan now for the worst and hope that the plans never require activation.

---

<sup>18</sup> *Severed cables disrupt internet*  
<http://news.bbc.co.uk/2/hi/technology/7218008.stm>

<sup>19</sup> *Third subsea cable repairs begin*  
<http://news.bbc.co.uk/2/hi/technology/7797162.stm>

#### Conclusion

Many already speculate that future wars will involve a cyber component and that attacks on Internet services will occur concurrent with military action, and in fact, such a scenario does appear to have already occurred. For example during the Israel Lebanon conflict in 2006, both Israel and Hezbollah forces appear to have waged war against each others' information systems.<sup>20</sup> But the difference here, is that these attacks did not just include Internet or cyber assets; they also targeted and included command and control, and communications systems. Perhaps the greater question will be whether or not governments or militaries will wage cyber war in parallel with traditional military campaigns in the future. So far, indications are that the answer to this question would be "Yes." Many nations have cyber warfare programs, though not all include an offensive capability. Arguably, the majority are of a defensive nature since most developed nations have an Internet infrastructure they have come to rely on.

While cyber attacks can be an effective way to deny service or plant false information, the reality remains that a more conventional weapons attack against sites housing infrastructure equipment would probably be the most effective means of interrupting infrastructure services. Communications, and command and control systems are always a target in a conflict and, perhaps in a sense, there has never been any question as to whether Internet systems will be targeted – especially as governments come to rely upon them more.

Based on present evidence, it is a near certainty that cyber attacks will accompany geopolitical events in the future. In fact, if cyber attack events were to suddenly cease now, it would seem very unusual since cyber attacks are a widely used method of protest though DoS attacks and Web site defacements.

Even as some cyberterrorism will always be the purvey of individuals making a statement, criminal enterprise will continue to interject itself through such occurrences as it seeks to take advantage of any situation for profit, even if only to use an event's sensationalism as a spam delivery vehicle. Criminal enterprise will also likely continue to provide a "for hire" role to others. We have already seen examples of this in the breaking of CAPTCHA implementations to create fake e-mail accounts in order to provide botnets for hire, and possibly even to provide consulting expertise on subjects such as how to successfully conduct a cyber warfare campaign.

---

<sup>20</sup> *Middle East conflict provokes surge of cyber attacks*  
[http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/article697253.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/article697253.ece)

## **Domain Name System Revisited – DNS Cache Poisoning**

### **Introduction**

In the January 2008 edition of the XFTIM, we featured an article titled, “Toward a Robust Domain Name System.” The article explored the general area of hardening DNS servers against a variety of attacks and misfortunes. More recently, at the BlackHat USA 2008 conference, one of the presenters, Dan Kaminsky, detailed new ways in which caching name servers can be attacked and poisoned with false information.

Details of the DNS vulnerability highlighted in Kaminsky’s presentation became known in the security community shortly after various vendors had posted updates for their DNS implementations for those vulnerabilities. The updates were coordinated with Kaminsky in advance of his presentation and were jointly published months before his talk. Within two weeks of the patches being published, others determined much of the nature of the vulnerability and were able to reproduce much of the work and post the details, well before the presentation. This was followed soon after by several public releases of exploit code and at least one unconfirmed attack on a DNS name server.

In spite of multiple public releases of exploit code, there were no major attacks or disruptions in the weeks leading up to the BlackHat conference. During this time, updates to name servers had a chance to propagate out, lessening the chance of widespread exploitation.

It has also come to light that other network components, such as Network Address Translation (NAT) devices and firewalls, may also have an impact on the DNS vulnerability and that some NAT devices may actually nullify the hardening of the name servers provided by the updates. Some of these devices require updates to firmware or site-specific configurations to correct their deficiencies.

### **DNS Cache Poisoning**

Cache poisoning is a popular attack against the DNS. In a cache poisoning attack, an attacker feeds falsified information to a caching name server to redirect queries to servers under the attacker's control. This facilitates phishing and malware distribution. These attacks are almost always localized and tend to clear up as caches expire; but, it can be an extremely vexing problem when and where it occurs.

Modern name servers incorporate various defensive mechanisms to prevent cache poisoning. An important note though, is that if a name server is forwarding to another caching name server, that first name server depends on the second one to prevent cache poisoning. This is a "weakest link" situation that can occur if a smaller organization runs its own name server that forwards to their Internet Service Provider (ISP).

The recent cache poisoning exploits focus on the caching name servers, which recursively forward resolver requests to other name servers and then cache the responses. They do not generally impact end-client resolvers, since those rarely do any caching and an attack would only impact individual systems for very limited periods of time. Nor do cache poisoning attacks impact authoritative name servers, since those are driven by configuration files and by master / slave relationships. To poison a cache, the attacker must spoof a response to a legitimate query and include the false information in the spoofed packet. That packet must then beat the legitimate response back to the requester.

To foil such attacks, as well as differentiate between multiple requests and responses, the DNS queries include a query ID (QID), a 16-bit number. Older name servers would simply increment this number making it extremely easy for an attacker to guess. The attacker would merely need to trick the name server into querying one of his own name servers and then guess the QID for subsequent queries. Patches to name server software randomized the QID making it thousands of times more difficult to guess.

In the past, name servers would communicate with each other exclusively using port 53 for both the source and destination ports on UDP. This made things relatively trivial to guess when sending back forged packets. Later versions of the software defaulted to allowing the operating system to choose the “source port,” which was generally much better. In order to forge a return packet, the attacker would have to guess both the source port of the query and the QID while knowing the address of the downstream name server from which the response was expected. This was generally fairly difficult.

Further strengthening the resilience of the name servers to cache poisoning are heuristics that prevent arbitrary “glue records” and “additional information” from being injected into the cache. Information in a response that is not relevant to the query is simply discarded. That change, made some time ago, closed off entire avenues of cache poisoning attacks.

Despite these preventative measures, the BlackHat presentation showed that it is still possible, using multiple queries and only a moderate flood of responses, to accomplish this and quickly corrupt the cache on a name server with false data that appear relevant to the query. The latest round of patches to the caching name servers provide for strongly randomized source ports making it more than 65,000 times harder to forge the reply than in the fixed port case, and somewhat more difficult than in cases where the operating system determines the port.

In general, the attacker must determine certain information about the name server to be attack, such as the address of the name server, the addresses of name servers from which query responses are expected, and its behavior in regards to query source ports and QID's. In the case of caching name servers with fixed forwardings, the attacker would never see a query directly from the forwarding name server since it forwards all requests to a predetermined set of name servers. In the case of full recursion name servers, the attacker can determine the address of a name server to attack by tricking it into querying a name server under the attacker's control. For this reason, certain forwarding-only name servers, such as DNSmasq, may appear as vulnerable, while actually being extremely difficult to exploit in reality. This also creates a mitigation avenue through the use of static forwardings and avoiding full recursive queries in the caching name servers.

The author of a recently announced exploit claimed to be able to corrupt the cache in a fully patched, up-to-date, BIND name server. However, the author points out that it took two attackers more than 10 hours connected using Gigabit ethernet. These numbers are actually reasonably in-line with the results already known.

How do I tell if I'm vulnerable?

A tool featured on Dan Kaminsky's blog does a decent job of testing a DNS resolver to indicate if it is vulnerable to these attacks. There are also very informative tools hosted by DNS-OARC, including a browser-based tool and a tool that can be used through "dig," a popular and common DNS diagnostic tool, on the command line. The perspective that these tools have is not absolutely definitive. Attackers on the local network may have vectors available to them that these tools cannot test. It does appear though, that these tools faithfully simulate the approach that most remote attacks are likely to take, and so they provide a very valuable reference.

## DNSSEC

DNSSEC, or Secure DNS, is an enhancement to the basic DNS to improve its security. DNSSEC provides security signatures on responses, transactions, and zones make it more difficult to spoof and poison the DNS information. DNSSEC has been around for some time but its deployment has been lackluster. Deploying DNSSEC is not a trivial undertaking and does not have an immediately apparent return on investment. The features of DNSSEC are desirable in the long run; but, when everything is working, there is no incentive to deploy DNSSEC. And when things are broken, everyone is too busy just getting things running again. The intrinsic resilience of the basic DNS service actually contributes to the lack of DNSSEC deployment; because, basic DNS works well enough on its own the majority of the time. Widespread deployment of DNSSEC would have prevented these latest threats in the first place.

Times may be changing for DNSSEC though. Announcements from the Department of Homeland Security as well as the National Institute of Standards and Technology (NIST) and other government agencies, indicate that all zones under the entire .gov zone will soon be signed using DNSSEC. The Public Interest Registry (PIR), responsible for the .org zone, has a DNSSEC working group. Several ccTLD's (Country Code Top Level Domains) are either already signed or in the process of deploying DNSSEC. All modern flavors of name servers support DNSSEC and trial deployments of DNSSEC-enabled caching name servers are underway. The Department of Commerce and ICANN, the Internet Corporation for Assigned Names and Numbers, have both invited public comments on responsibility for signing the "root zone," which is vital for DNSSEC operations.

#### Recommendations

There are many ways to enhance the resiliency and robustness of a DNS deployment and protect against DNS cache poisoning:

- ***Split the DNS functionality between specialized name servers.*** *Even though a given DNS server can serve as an authoritative name server, a caching server and a recursive resolver, split up this functionality. The authoritative name servers servicing your zones should have recursion completely disabled. This helps prevent abuse of your name servers for DDoS attacks against other sites.*
- ***Restrict access to caching name servers to internal clients only.*** *Although the caching name servers acting as resolvers for your clients would have recursion enabled, these do not need to be exposed to clients outside of your organization. You can then marshal DNS activity into and out of your networks through these well defined paths, thus also limiting the threat from DNS based “covert tunnels,” another nefarious threat not covered in this article.*
- ***Distribute the caching name servers.*** *While small organizations may rely on a few caching name servers, larger organizations can benefit from a larger number of distributed caching name servers. Distributing the caching name servers cuts down on query latency at the cost of some increased DNS traffic. Having only a few caching servers creates a bottleneck for DNS queries and creates potential single points of failure. More name servers spread the load, reduce the query latency and eliminate single points of failure.*
- ***Keep name server software updated.*** *Bugs in name server software have been discovered and will continue to be discovered. By having deep redundancy in the distribution of name servers, updating of name server software is actually facilitated. Selected slaves can be updated and tested while others maintain a stable baseline. Once updated servers are verified, the remaining slaves can be updated. Similarly, with multiple distributed caching servers, the caching servers can be individually updated and tested with no threat to the authoritative zone servers and no risk to the clients they serve.*

- **Place caching name servers behind stateful firewalls.** Stateful firewalls can prevent caching name servers from being flooded by spoofed DNS responses. Since this attack requires thousands of spoofed packets, many of which will have incorrect port numbers, some creative firewall rules can reduce the threat by triggering on wrong port guesses and blocking other spoofed packets. This should be considered only in the case of active aggressive attacks as a mitigation strategy, since it raises the possibility of other DoS attack avenues.
- **Test NAT devices and upgrade as necessary.** If you have a server behind a NAT device, some NAT devices will undo the UDP port randomness introduced by the patch. Fortunately, Linux iptables and OpenBSD's pf are not vulnerable, but many popular NAT devices are. If you have such a device, you can either move your DNS server to a DMZ segment where it need not be NATed, or you can forward requests from that DNS server to a patched server that is not behind the NAT.
- **Fix misconfigured firewalls rules.** Firewalls that allow outside traffic with inside addresses, or that interfere with DNS port randomization, must be fixed. Firewalls may be managed by IT groups separate from the DNS management who are not properly aware of the problems.
- **Utilize a secure forwarding service.** If you are unable to patch a server, you can mitigate some attack vectors by forwarding requests from that server to a patched server or forwarding service. OpenDNS is one example of a secure DNS service that will accept forwards. The Internet Software Consortium (ISC), authors of the BIND name server package, also offer a secure forwarding service for their customers.
- **Test any servers that you rely on or forward to.** If you are relying on your ISP's DNS infrastructure, either directly, or through a forward, and the testing tools above are indicating that you are vulnerable, you may need to escalate the issue with your ISP.
- **Implement DNSSEC.** Consider configuring and supporting DNSSEC for authoritative zones and verifying DNSSEC signatures. DNS domain owners that want their data protected against spoofing to the end-user, must sign their zones. ISP and Enterprise DNS administrators who provide caching recursive name servers to their users should enable DNSSEC validation. Maybe one day we'll get there.
- **CERT Bulletin, Vulnerability Note VU#800113, offers very good advice for mitigation.** The CERT Security advisory goes into greater depth and detail on the vulnerability specifics and various mitigation strategies.

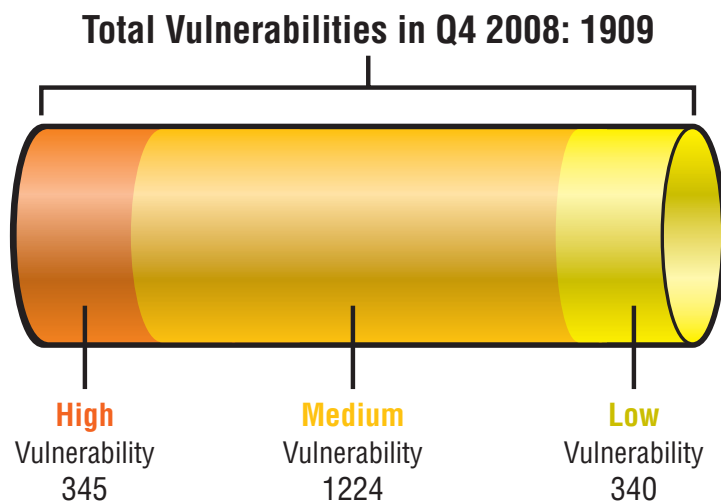
### **Conclusion**

The entire Internet, as we know it, depends on the Domain Name System, a fundamental core protocol infrastructure. The DNS is an old service and protocol. Despite this, and in spite of not having a security-driven design from the start, the DNS is exceptionally resilient. Unfortunately, misconfiguration, DoS/DDoS attacks, and cache poisoning threaten the DNS and an unacceptably high number of DNS servers remain vulnerable to known threats. There are, however, many ways to enhance the resiliency and robustness of the DNS. Simply following DNS best practices will help organizations mitigate many of these threats. While some planning is needed to enhance resiliency and produce a robust DNS deployment, the result is a stable and highly maintainable DNS that is resistant to attack. DNSSEC is becoming a more viable and useful option to both deploy and validate, and should be seriously considered by both consumers and producers of DNS information.

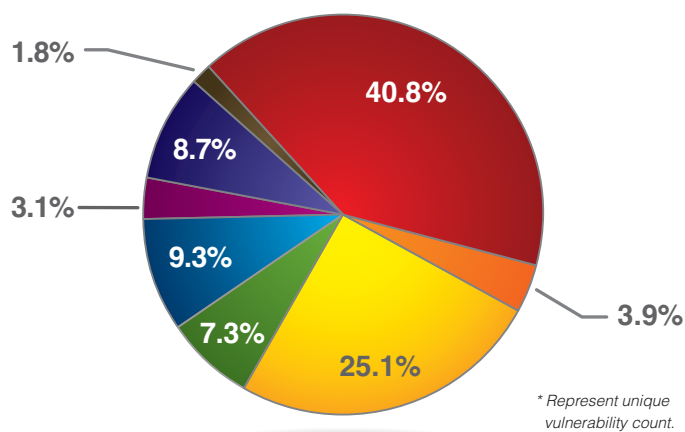
### Prolific and Impacting Issues for 4th Quarter, 2008

#### Significant disclosures

In the fourth quarter of 2008, the X-Force team analysts researched and assessed 1909 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 – 8.7%**

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

**Data Manipulation – 25.1%**

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

**Denial of Service – 7.3%**

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

**File Manipulation – 1.8%**

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

**Gain Access – 40.8%**

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 – 3.9%**

Privileges can be gained on the local system only.

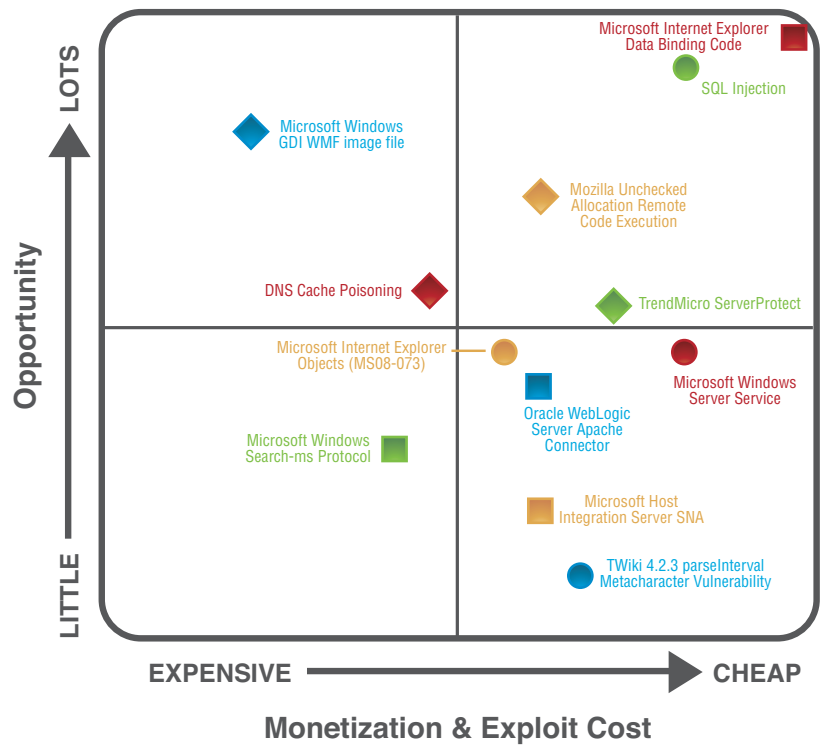
**Obtain Information – 9.3%**

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

**Other – 3.1%**

Anything not covered by the other categories.

The graph below plots the following vulnerabilities and categorizes them into one of four quadrants based on the opportunity they present to a criminal and the cost of realizing that opportunity. Only issues that make it to the top right quadrant resulted in widespread exploitation. The others did not present enough of a financial opportunity, or they were too expensive to monetize.



An issue affecting the Oracle WebLogic Server Apache Connector, discovered by the X-Force Team, was disclosed just two weeks into the start of the fourth quarter 2008. By sending a specially crafted http request, an attacker could overflow the stack and potentially execute arbitrary code. In addition to the aforementioned vulnerability, Oracle's October 2008 Critical Patch Update (CPU) fixed 35 other vulnerabilities across hundreds of Oracle products.

- *IBM Internet Security Systems Protection Advisory: Oracle WebLogic Server Apache Connector Remote Code Execution*<sup>21</sup>
  - *IBM ISS Protection Signature: HTTP\_Application\_Server\_Stack\_Bo*
- *Oracle October 2008 Critical Patch Update (CPU)*<sup>22</sup>

A Protection Alert was also published on the same day to address a serious issue disclosed in Microsoft's October security release. The Microsoft Host Integration Server is vulnerable to unauthenticated remote code execution, caused by a design flaw in the SNA Remote Procedure Call (RPC) service. Successful exploitation would grant an attacker the privileges of the SNA RPC service.

- *IBM Internet Security Systems Protection Alert: Microsoft Host Integration Server RPC Service Remote Code Execution*<sup>23</sup>
  - *IBM ISS Protection Signature: MSRPC\_HostIntegration\_NullSession\_Exec*
- *Microsoft Security Bulletin MS08-059 – Critical: Vulnerability in Host Integration Server RPC Service Could Allow Remote Code Execution (956695)*<sup>24</sup>

---

<sup>21</sup> *IBM Internet Security Systems Protection Alert: Oracle WebLogic Server Apache Connector Remote Code Execution*  
<http://iss.net/threats/304.html>

<sup>22</sup> *Oracle October 2008 Critical Patch Update (CPU)*  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>

<sup>23</sup> *IBM Internet Security Systems Protection Alert: Microsoft Host Integration Server RPC Service Remote Code Execution*  
<http://iss.net/threats/305.html>

<sup>24</sup> *Microsoft Security Bulletin MS08-059 – Critical: Vulnerability in Host Integration Server RPC Service Could Allow Remote Code Execution (956695)*  
<http://www.microsoft.com/technet/security/Bulletin/MS08-059.mspx>

The IBM ISS Threat Level was raised to AlertCon 2 on October 23, 2008, in response to a critical issue affecting Microsoft Windows Server Service. A remote attacker could execute arbitrary code on the system, caused by a vulnerability in the RPC service. Public exploit code targeting this issue quickly became available. In the initial days after vulnerability disclosure, public exploitation was fairly low. However, in late November, 2008, the number of sources and attacks surpassed the 1,000 mark and within three days the number of attacks started growing exponentially, passing the 1,000 mark.

- *IBM Internet Security Systems Protection Alert: Microsoft Windows Server Service RPC Code Execution*<sup>25</sup>
  - *IBM ISS Protection Signatures:*
    - *Microsoft S MSRPC\_Srvsvc\_Bo*
    - *MSRPC\_Srvsvc\_Path\_Bo*
- *Microsoft Security Bulletin MS08-067 – Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644)*<sup>26</sup>

---

<sup>25</sup> *IBM Internet Security Systems Protection Alert: Microsoft Windows Server Service RPC Code Execution*  
<http://iss.net/threats/306.html>

<sup>26</sup> *Microsoft Security Bulletin MS08-067 – Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644)*  
<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

On November 11, 2008, the X-Force team released four Protection Advisories covering a total of eight vulnerabilities discovered in Trend Micro ServerProtect. The first two of these vulnerabilities (Advisories 307 and 308) were reported to Trend in late 2006. Since then, the X-Force team discovered and reported additional vulnerabilities, with the last being disclosed in January of 2008. Further details on the chain of events that led up to these advisories can be found in the X-Force blog posting titled, “The Scoop on the X-Force TrendMicro Advisories.”

- *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect Unauthenticated Remote Administration*<sup>27</sup>
  - *IBM ISS Protection Signature: MSRPC\_Unauth\_Admin\_Access*
- *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect [PROCEDURE NAME REDACTED] Heap Overflow*<sup>28</sup>
  - *IBM ISS Protection Signature: MSRPC\_AV\_Heap\_Overflow*
- *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect [PROCEDURE NAME REDACTED] Heap Overflows (3)*<sup>29</sup>
  - *IBM ISS Protection Signature: MSRPC\_TrendMicro\_Suspicious\_Call*
- *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect [PROCEDURE NAME REDACTED] Heap Overflows (3)*<sup>30</sup>
  - *IBM ISS Protection Signature: MSRPC\_AV\_ScanConfig\_BO*
- *TrendMicro: ServerProtect for Microsoft Windows/Novell NetWare*<sup>31</sup>

---

<sup>27</sup> *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect Unauthenticated Remote Administration*  
<http://iss.net/threats/307.html>

<sup>28</sup> *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect [PROCEDURE NAME REDACTED] Heap Overflow*  
<http://iss.net/threats/308.html>

<sup>29</sup> *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect [PROCEDURE NAME REDACTED] Heap Overflows (3)*  
<http://iss.net/threats/310.html>

<sup>30</sup> *IBM Internet Security Systems Protection Advisory: Trend Micro ServerProtect [PROCEDURE NAME REDACTED] Heap Overflows (3)*  
<http://iss.net/threats/310.html>

<sup>31</sup> *TrendMicro: ServerProtect for Microsoft Windows/Novell NetWare*  
<http://www.trendmicro.com/download/product.asp?productid=17>

The X-Force team also discovered a vulnerability in Mozilla Firefox. The vulnerability is caused by the way that Firefox handles malicious http-index-format MIME types. If successfully exploited, a remote attacker could execute arbitrary code as the browser user.

- *IBM Internet Security Systems Protection Advisory: Mozilla Unchecked Allocation Remote Code Execution*<sup>32</sup>
  - *IBM ISS Protection Signature: HTTP\_Client\_Converter\_Null\_Ptr\_BO*
- *Mozilla Foundation Security Advisory 2008-54*<sup>33</sup>

In December, a Protection Advisory was released to address a vulnerability in TWiki discovered by IBM X-Force. A meta-character vulnerability allows for command injection through the search facility. This can be exploited to inject and execute commands via specially crafted HTTP GET requests.

- *IBM Internet Security Systems Protection Advisory: TWiki 4.2.3 parseInterval Metacharacter Vulnerability*<sup>34</sup>
  - *IBM ISS Protection Signature: HTTP\_Web\_App\_Cmd\_Exec*
- *TWiki Security Alert: TWiki SEARCH variable allows arbitrary shell command execution*<sup>35</sup>

---

<sup>32</sup> *IBM Internet Security Systems Protection Advisory: Mozilla Unchecked Allocation Remote Code Execution*  
<http://www.iss.net/threats/311.html>

<sup>33</sup> *Mozilla Foundation Security Advisory 2008-54*  
<http://www.mozilla.org/security/announce/2008/mfsa2008-54.html>

<sup>34</sup> *IBM Internet Security Systems Protection Advisory: TWiki 4.2.3 parseInterval Metacharacter Vulnerability*  
<http://www.iss.net/threats/312.html>

<sup>35</sup> *Security Alert: TWiki SEARCH variable allows arbitrary shell command execution*  
<http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305>

Later in the month, Microsoft released its Security Bulletins for December. The X-Force team released four Protection Alerts associated with vulnerabilities patched by Microsoft in these bulletins. The first Protection Alert addresses an issue in Internet Explorer that could allow a remote attacker to execute arbitrary code on a system through improper handling of certain HTML objects. The second Protection Alert highlights a remote code execution vulnerability affecting Microsoft Windows GDI, caused by improper handling of integer calculations within a WMF image file. Another remote code execution vulnerability affecting Microsoft Internet Explorer is addressed in the third Protection Alert. The final Protection Alert describes a vulnerability in the Windows search-ms protocol. Improper validation of parameters could lead to a remote compromise. This protocol is accessible through Web browsers, so an attacker could exploit this vulnerability by convincing a user to visit a malicious Web page.

- *IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer HTML objects uninitialized memory code execution*<sup>36</sup>
  - *IBM ISS Protection Signature: HTML\_IE\_Objects\_Code\_Execution*
- *Microsoft Security Bulletin MS08-073 - Critical: Cumulative Security Update for Internet Explorer (958215)*<sup>37</sup>
- *IBM Internet Security Systems Protection Alert: Microsoft Windows GDI WMF image file integer overflow*<sup>38</sup>
  - *IBM ISS Protection Signature: Image\_WMF\_GDI\_Image\_Overflow*
- *Microsoft Security Bulletin MS08-071 – Critical: Vulnerabilities in GDI Could Allow Remote Code Execution (956802)*<sup>39</sup>

---

<sup>36</sup> *IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer HTML objects uninitialized memory code execution*  
<http://iss.net/threats/313.html>

<sup>37</sup> *Microsoft Security Bulletin MS08-073 - Critical: Cumulative Security Update for Internet Explorer (958215)*  
<http://www.microsoft.com/technet/security/bulletin/ms08-073.mspx>

<sup>38</sup> *IBM Internet Security Systems Protection Alert: Microsoft Windows GDI WMF image file integer overflow*  
<http://iss.net/threats/314.html>

<sup>39</sup> *Microsoft Security Bulletin MS08-071 – Critical: Vulnerabilities in GDI Could Allow Remote Code Execution (956802)*  
<http://www.microsoft.com/technet/security/bulletin/ms08-071.mspx>

- *IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer embedded object code execution*<sup>40</sup>
  - *IBM ISS Protection Signature: HTML\_IE\_Embedded\_Object\_Code\_Execution*
- *Microsoft Security Bulletin MS08-073 – Critical: Cumulative Security Update for Internet Explorer (958215)*<sup>41</sup>
- *IBM Internet Security Systems Protection Alert: Microsoft Windows search-ms protocol code execution*<sup>42</sup>
  - *IBM ISS Protection Signature: HTML\_Win\_SearchProtocol\_Code\_Exec*
- *Microsoft Security Bulletin MS08-075 – Critical: Vulnerabilities in Windows Search Could Allow Remote Code Execution (959349)*<sup>43</sup>

---

<sup>40</sup> *IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer embedded object code execution*  
<http://iss.net/threats/315.html>

<sup>41</sup> *Microsoft Security Bulletin MS08-073 – Critical: Cumulative Security Update for Internet Explorer (958215)*  
<http://www.microsoft.com/technet/security/bulletin/ms08-073.mspx>

<sup>42</sup> *IBM Internet Security Systems Protection Alert: Microsoft Windows search-ms protocol code execution*  
<http://iss.net/threats/316.html>

<sup>43</sup> *Microsoft Security Bulletin MS08-075 – Critical: Vulnerabilities in Windows Search Could Allow Remote Code Execution (959349)*  
<http://www.microsoft.com/technet/security/bulletin/ms08-075.mspx>

On the same day that Microsoft released its December Security Bulletins, reports surfaced of an unpatched remote code execution vulnerability in Internet Explorer. The IBM ISS Threat Level was subsequently raised to AlertCon 2, and an X-Force Protection Alert was released to address this issue. Exploits for this issue have been observed in the wild. Additionally, this exploit appears to have been integrated into the Asprox botnet, which has been using SQL injection to add this exploit along with others to Web sites vulnerable to SQL injection.

- *IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer Data Binding Code Execution*<sup>44</sup>
  - *IBM ISS Protection Signatures:*
    - *HTML\_IE\_SPAN\_Objects\_Code\_Exec*
    - *Javascript\_Suspicious\_Hex\_String*
    - *JavaScript\_NOOP\_Sled*
    - *JavaScript\_Shellcode\_Detected*
    - *SQL\_Injection*
- *Microsoft Security Bulletin MS08-078 - Critical: Security Update for Internet Explorer (960714)*<sup>45</sup>

---

<sup>44</sup> *IBM Internet Security Systems Protection Alert: Microsoft Internet Explorer Data Binding Code Execution*  
<http://iss.net/threats/317.html>

<sup>45</sup> *Microsoft Security Bulletin MS08-078 – Critical: Security Update for Internet Explorer (960714)*  
<http://www.microsoft.com/technet/security/bulletin/ms08-078.mspx>

### **Additional 4th Quarter highlights**

This section of the report briefly covers some of the additional threats facing security professionals during the fourth quarter of 2008.

#### Major security breaches

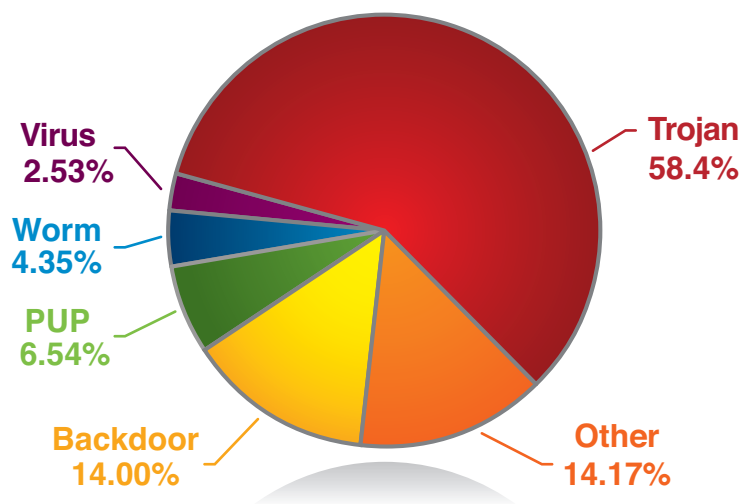
A number of high-profile security breaches are reported each year, drawing attention to the need to protect consumer and employee information from the risk of exposure to malicious individuals/identity (ID) theft rings. In addition to the loss or misplacement of information, corporations and individuals 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 in Q4 of this year:

- **CheckFree** – Account information of 160,000 was compromised due to a domain hijacking.
- **Express Scripts** – Hackers attempted to extort money by claiming they had obtained access to millions of the company's customers.
- **Pamela Systems** – Databases containing names and email addresses of individuals using the Pamela component from within Skype were compromised resulting in a Pay-Pal phishing campaign.
- **The Planet** – The Planet, a hosting provider, was compromised exposing the accounts of 25,000 clients.
- **T-Mobile** – T-Mobile acknowledged a breach that occurred in 2006 exposing records of 17 million German customers.
- **University of Indianapolis** – Computer systems at the University of Indianapolis were compromised exposing the personal information of 11,000 students.
- **Arizona Department of Economic Security** – Five hard drives containing the personal information of up to 40,000 children were stolen.
- **Starbucks** – A laptop containing private information on 97,000 employees was stolen
- **University of Florida** – A data breach at the University of Florida exposed personal records of 330,000 patients of it College of Dentistry.
- **Luxottica** – A system compromise exposed payroll records for 59,000 employees.
- **RBS WorldPay** – Private records of 1.5 million clients were exposed due to a system compromise.

### Malcode corner

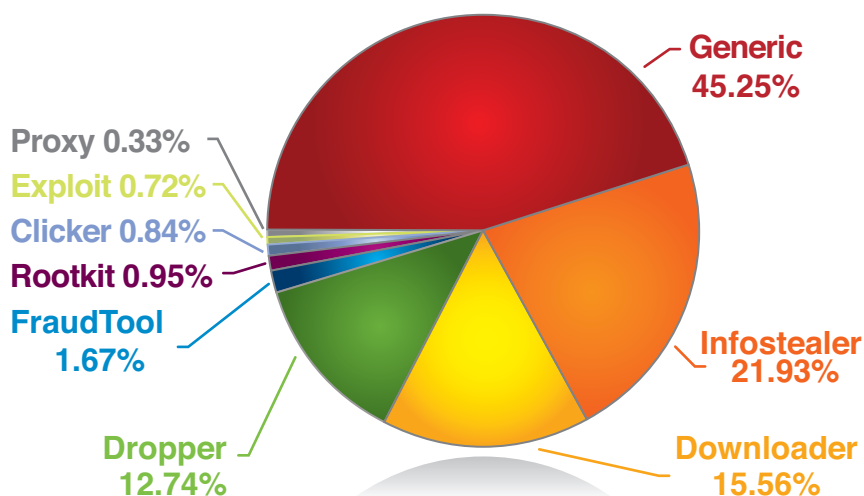
The IBM ISS X-Force Virus Prevention System (VPS) team's categorization of malcode is based on the most dominant features of the threat. The primary malcode categories are:

- **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 malware components into an affected system.
- **Exploit** – Documents or media files containing exploit code.
- **FraudTool** – Malware used to commit fraud. An example of this could include malware that displays fake errors or infection messages, which then incites 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. Common tools include password stealers, keystroke loggers and spywares.
- **Proxy** – Allows a remote attacker to relay connection via the affected system in order to hide its real origin.
- **Rootkit** – Components used by other malware to give itself the capability to hide themselves from the user and security software.



List of Contributors for this paper include:

**Michelle Alvarez** – *Team Lead, IBM MSS Intelligence Center*

**Michael Warfield** – *Senior Researcher and Analyst,  
IBM MSS Intelligence Center*

**Lyndon Southerland** – *Threat Analyst Security Specialist,  
IBM MSS Intelligence Center*

**Michael Vucelich** – *Threat Analyst, IBM MSS Intelligence Center*

**Brad Sherrill** – *Team Lead, IBM ISS X-Force Database*

**IBM ISS X-Force Virus Prevention System (VPS) team**

## References

### Domain Name System Revisited – DNS Cache Poisoning

DNS Best Practice Resources

[http://www.infoblox.com/library/dns\\_resources.cfm](http://www.infoblox.com/library/dns_resources.cfm)

DNS Attack Factsheet, March 8, 2007

<http://www.icann.org/announcements/announcement-08mar07.htm>

Dan Kaminsky's Blog

<http://www.doxpara.com/>

Frequently Asked Questions about Query Port Randomization issue  
and Setting up BIND to forward to patched name server

<http://www.isc.org/index.pl>

Responding to the DNS vulnerability and attacks

<http://blogs.iss.net/archive/dnsrespond.html>

DNS Operations, Analysis, and Research Center (DNS-OARC) Tools  
testing for DNS servers

<https://www.dns-oarc.net/>

DNS querying and testing tools

<http://dnsstuff.com>

CERT - Multiple DNS implementations vulnerable to cache poisoning

<http://www.kb.cert.org/vuls/id/800113>

DNSSEC Deployment Initiative

<http://www.dnssec-deployment.org/>

**Prolific and impacting issues of 4th quarter 2008**

The Scoop on the X-Force TrendMicro Advisories

<http://blogs.iss.net/archive/trend.html>

University of Florida discloses patient-record data breach

<http://www.networkworld.com/news/2008/111208-ufla.html?hpg1=bn>

Missing laptop puts Starbucks workers' data at risk

[http://seattlepi.nwsource.com/business/389259\\_starbucks25.html](http://seattlepi.nwsource.com/business/389259_starbucks25.html)

T-Mobile Loses the Personal Information of 17 Million Subscribers

<http://news.softpedia.com/news/T-Mobile-Loses-the-Personal-Information-of-17-Million-Subscribers-95014.shtml>

The Personal Details of Millions of American Patients Stolen by Hackers

<http://news.softpedia.com/news/The-Personal-Details-of-Millions-of-American-Patients-Stolen-by-Hackers-97437.shtml>

Finextra: CheckFree Web site hijacked by Eastern European criminals

<http://www.finextra.com/fullstory.asp?id=19396>

The Planet Warns of Security Breach  
web-hosting-news/101708\_The\_Planet\_Warns\_of\_Security\_Breach  
Hackers threaten University of Indianapolis security

[http://www.purduexponent.com/?module=article&story\\_id=12978](http://www.purduexponent.com/?module=article&story_id=12978)

Extortion used in Express Scripts database breach

[http://news.cnet.com/8301-10789\\_3-10084187-57.html](http://news.cnet.com/8301-10789_3-10084187-57.html)

Info of 40,000 kids on stolen hard drives

[http://www.upi.com/Top\\_News/2008/11/04/Info\\_of\\_40000\\_kids\\_on\\_stolen\\_hard\\_drives/UPI-98011225842906/](http://www.upi.com/Top_News/2008/11/04/Info_of_40000_kids_on_stolen_hard_drives/UPI-98011225842906/)

Hacker accesses Luxottica Retail employee information

<http://breach.scmagazineblogs.com/2008/11/25/hacker-accesses-luxottica-retail-employee-information/>

*\* 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.*



© Copyright IBM Corporation 2009

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

Produced in the United States of America.

February 2009

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. ADDME, Ahead of the threat, BlackICE, Internet Scanner, Proventia, RealSecure, SecurePartner, SecurityFusion, SiteProtector, System Scanner, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

Mozilla and Firefox is a registered trademark of the Mozilla Foundation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Trend Micro Incorporated and ServerProtect are trademarks of Trend Micro, registered in the U.S. and are trademarks in other countries.

Microsoft, Windows, DirectX, ActiveX, Excel, Media player, Vista, and SQL Server are trademarks or registered trademarks of the Microsoft Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

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.

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