

# IBM X-Force Threat Insight Quarterly



## Contents

- 2** About the Report
- 3** Evolution: From Nuisance to Weapon
- 8** Prolific and Impacting Issues of Q1 2011
- 16** References

## About the report

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

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

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

We welcome your feedback. Questions or comments regarding the content of this report should be addressed to [XFTAS@us.ibm.com](mailto:XFTAS@us.ibm.com).

## Evolution: From Nuisance to Weapon

Creeper, Wabbit, Animal, Elk Cloner, Brain, Vienna, Lehigh, Stoned, Jerusalem. These are the names of early examples of what today we generally simply refer to as malware which appeared between 1971 and 1987.

This was the beginning. These examples infected various platforms and delivered various payloads, some just a simple message echoed to a screen. While Sci-Fi writers such as John Brunner in “Shockwave Rider” wrote conceptually about viruses and worms, it was not until 1984 that Fred Cohen<sup>1</sup> gave such programs a true mathematical definition. The age of the “Computer Virus” was upon us.

Creeper<sup>2</sup> is arguably the first virus, or more accurately, worm, and infected only DEC PDP-10 computers. While it was written as a demonstration, it spread through ARPANET in 1971 with a simple payload, a text message which read, “I’m the creeper, catch me if you can!”. The characteristics of self replication and spreading via a network are important concepts in malware which remain with us today. In response to Creeper, came the Reaper, a virus in itself which spread across the same network however its goal, was to delete instances of Creeper. It can be argued that Reaper was the first example of anti-virus software. Its task was to detect and remove malware. However code that executes on a system or spreads across a network without permission is not welcome at all. More recently, the same technique has been used by modern malware used to create botnets attempting to remove instances of other botnet malware so as to take control on the affected system.

One of the more notable examples here is Brain<sup>3</sup>, a boot sector infector which originated in Pakistan and released in 1986, was one of the first examples of malware that infected PC’s running MS-DOS. It infected the boot sector of FAT formatted removable media (read Floppies) and was actually written as a means to control software piracy. It was not as such malicious however that did not stop it from infecting victims other than the intended targets. The authors had even placed their contact information in the code which resulted in them having to get their telephone line disconnected due to the number of calls they received from irate victims of Brain.

In December 1987 Christmas Tree Exec<sup>4</sup> appeared on IBM mainframes causing significant disruption on EARN, BITNET with IBM’s VNET. A user would receive an email which invited them to execute “CHRISTMAS”, which would draw a Christmas tree on their terminal. It did indeed do this, and also sent itself to other users located through the NAMES and NETLOG files. While this technique for replication might seem very familiar now, it wasn’t then. The author of the malware stated the intention of the code was simply to send a greeting to a few friends but it resulted in his being barred from access to their system.

Moving forward to 1988, we come to one of the most famous items of malware in history and we begin to see the signs of sophistication creeping in. The Robert Morris Worm<sup>5</sup> was unique at the time because it exploited vulnerabilities in sendmail, finger and weak passwords. It also was able to infect multiple architectures. Its transport was the fledgling Internet. When it was released into the wild, it began clogging systems and soon resulted in a denial of service condition which directly or indirectly affected most systems attached to the Internet.

<sup>1</sup> Fred Cohen & Associates  
<http://all.net/resume/bio.html>

<sup>2</sup> 25th anniversary of the computer virus? Not so fast  
[http://news.cnet.com/8301-13506\\_3-9745010-17.html](http://news.cnet.com/8301-13506_3-9745010-17.html)

<sup>3</sup> Searching for the first PC virus in Pakistan  
<http://campaigns.f-secure.com/brain/index.html>

<sup>4</sup> Security Digest Archives  
<http://securitydigest.org/rutgers/mirror/pyrite.rutgers.edu/christmas.exec>

<sup>5</sup> Morris Worm  
[http://en.wikipedia.org/wiki/Morris\\_worm](http://en.wikipedia.org/wiki/Morris_worm)

The effect of Robert Morris' worm was significant enough to lead to the establishment of the CERT Coordination Center<sup>6</sup> at Carnegie Mellon University. According to Robert Morris, the creator of the worm, it was not written with malicious intent rather it was written as a tool to gauge the size of the Internet. The devastation it caused was an unintended consequence. Morris was however convicted of violating the 1986 United States Computer Fraud and Abuse Act<sup>7</sup> (amended since 1986) and was sentenced to three years probation, four hundred hours of community work and a fine of \$10,000.

In early 1989 we see Polymorphic encryption in the wild, a very notable stage of virus evolution. Predicted by Fred Cohen, brought into existence by Mark Washburn<sup>8</sup> and the 1260 virus but, arguably most famously seen in the Mutation Engine written by the legendary Dark Avenger<sup>9</sup>. Polymorphism, simply put is the code's ability to periodically modify itself which is done to evade detection. The Dark Avenger has never been positively identified but a paper written by Sara Gordon<sup>10</sup> who interviewed the Dark Avenger (online) and published in 1993 provides a glimpse into the mind of the author. The viruses created by the Dark Avenger were very infectious and damaging.

Deserving of a mention from 1991 is the virus known as Michelangelo<sup>11</sup>. The mention however is not simply for the virus, rather the hype that with it. There were wild and dire predictions that Michelangelo would wreck havoc. How widely spread the virus was is not easy to determine. It seemed to spread globally, but the estimates of the number of computers that would be affected on March 6 1992, with some reports quoting up to five million, turned out to be off target. Various experts and pundits made many claims<sup>12</sup> regarding the number of infected computers, how the virus spread, and ways in which users could avoid damage by the virus when the trigger date was reached. The virus itself was a DOS boot sector infector and remained dormant, until the trigger date.

It is in 1999 that we really begin to see evolution in how we understand viruses today, with Happy99<sup>13</sup> and Melissa<sup>14</sup> as poignant examples. Happy99 can be considered the first virus to be propagated by email as we commonly know it today. Melissa on the other hand was a worm delivered inside a Word document. Once active, one of the tasks of the worm was to replicate by sending itself to the first fifty users in the victims address book. This not only spread the virus quickly, but email traffic generated started clogging email servers. At the time, Melissa may have been the fastest spreading virus in history.

<sup>6</sup> Meet CERT  
[http://www.cert.org/meet\\_cert/](http://www.cert.org/meet_cert/)

<sup>7</sup> Unites States Code: TITLE 18, 1030. Fraud and related activity in connection with computers  
<http://www.law.cornell.edu/uscode/18/1030.html>

<sup>8</sup> 1260 (computer virus)  
[http://en.wikipedia.org/wiki/1260\\_\(computer\\_virus\)](http://en.wikipedia.org/wiki/1260_(computer_virus))

<sup>9</sup> Dark Avenger  
[http://en.wikipedia.org/wiki/Dark\\_Avenger](http://en.wikipedia.org/wiki/Dark_Avenger)

<sup>10</sup> Inside the Mind of Dark Avenger  
<http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html>

<sup>11</sup> Michelangelo (computer virus)  
[http://en.wikipedia.org/wiki/Michelangelo\\_%28virus%29](http://en.wikipedia.org/wiki/Michelangelo_%28virus%29)

<sup>12</sup> Michelangelo Fiasco: a Historical Timeline  
<http://vmyths.com/column/1/1992/6/1/>

<sup>13</sup> Email-Worm.Win32.Happy  
<http://www.securelist.com/en/descriptions/old22314>

<sup>14</sup> Virus:W32/Melissa  
<http://www.f-secure.com/v-descs/melissa.shtml>

In 1988 when the Morris worm went wild, the Internet had around 100,000 systems attached to it. By December 1998, four months prior to Melissa, the Internet had some 148 million users. It is self evident that the impact of Melissa was more widely felt than the impact of the Morris worm. The author of Melissa was apprehended and sentenced<sup>15</sup> to 20 months in a US federal prison, three years of supervised release after completion of the prison sentence and fined \$5,000.

Also worth keeping in mind is by this time the majority of Internet users were running the Microsoft® Windows® operating system which by then had become the operating system most targeted by virus writers. By March 2000, the number of Internet users had grown to 304 million users and in May 2000, the world learned to say IloveYou<sup>16</sup>.

Starting on or around May 4, 2000, emails with the subject line of “IloveYou” began arriving into email inboxes. The email contained an attachment named “LOVE-LETTER-FOR-YOU.TXT.vbs” (or variation of) and the .vbs extension was hidden on Windows systems unless the default file viewing options had been changed by the user. This led victims to believe the attached file was a harmless text file which many opened. Once a victim had opened the .vbs file the code caused the email to be sent from the victim to every entry in the victim’s Windows Address Book. It also made changes to the victim’s system.

The original emails containing the worm were sent from the Philippines where the worm was written. By May 5, there were reported estimates<sup>17</sup> of 45 million computers infected with

IloveYou or the ten or so variants that had also surfaced within the first 24 hours. It was also reported that<sup>18</sup> this worm caused the Pentagon, CIA, and the British Parliament to shut down their email systems. Estimates of the financial cost of the damage caused by IloveYou and variants range up to \$5.5 billion. The concepts of hiding extensions, social engineering, and exploiting scripting engines remain valid even today.

We then saw a wave of highly infectious malware such as Code Red, Nimda, and Slammer seemed commonplace. Nowadays we generally don’t see malware with the same direct and visible impact of IloveYou, Code Red or Slammer. What we see now is huge numbers of new or variations of existing malware detected each day, probably topping 50,000 per day.

Some important things to keep in mind. The first is that the great majority of malware up until 2003-2004 was written by individuals. In some cases, there was no malicious intent. In most cases there was no direct financial motivation on the part of the writers. In fact, malware writers were looked down on by many, not simply because the code they created was causing damage, but because they were widely regarded as poor programmers. That however is probably an unfair judgment in at least some cases like the Dark Avenger and the Mutation Engine. Also, the Internet, the ubiquitous network we commonly use today reached two billion users<sup>19</sup> in early 2011. This is a huge playing field compared to the early days. Malware is truly entrenched and here to stay for the foreseeable future. Somewhere along the way things took a turn as cybercrime which had been growing up, began to utilize malware.

<sup>15</sup> Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison  
<http://www.justice.gov/criminal/cybercrime/melissaSent.htm>

<sup>16</sup> VBS.ILoveYou.A - CA Technologies  
<http://gsa.ca.com/virusinfo/virus.aspx?ID=9024>

<sup>17</sup> Experts estimate damages in the billions for bug  
<http://news.cnet.com/2100-1001-240112.html>

<sup>18</sup> Tech Scares of the Decade  
<http://www.cio.in/article/tech-scares-decade>

<sup>19</sup> Number of Internet users reaches 2 billion  
<http://news.ninensn.com.au/technology/8202354/number-of-internet-users-reaches-2-blm>

Malware has become a staple in today's cybercrime landscape. Primarily, it is the medium used to steal information and build botnets. Malware delivered in one way or another infects a PC and turns it into a botnet client or zombie. Think Storm botnet. The worm was dubbed Storm by F-Secure because the first iterations of it was spread in messages about the windstorm Kyrill. This worm also used many other subjects to encourage victims into viewing messages and webpages and downloading or opening malicious files. The Storm botnet is one of many that have come and gone but at the time it was very notable because of its millions of zombie clients. Social engineering in one form or another remains with us today, often used as a means of enticing victims to open a malicious file or webpage.

There's been ransomware, which is not entirely new but does surface from time to time. A typical ransomware scenario would cause a victim's files to become encrypted. To get the files decrypted, the victim would pay a sum of money to the attacker.

Another classic item of malware is Zeus. Zeus is used to steal financial information and obtain user credentials from its victims. Zeus will also merge infected PCs into its botnet which has millions of zombie clients. Zeus is a commercial package which can be bought on underground forums. It has a development cycle and even a hardware based licensing system, to prevent piracy and unlicensed use of the software.

Malware is now commonly used in targeted attacks which are often the source of previously unknown vulnerabilities discovered in the wild when malware utilizes them. Perhaps one

of the most infamous targeted attacks was against a number of major companies, widely known as Operation Aurora<sup>20</sup>. The operation ran from mid 2009 through to the end of the year, being publicly disclosed by Google on January 12, 2010.

Google's disclosure outlined that the attack targeted intellectual properties, but further, that the primary goal of the attack was to access the Gmail accounts of certain activists. Another well known example of malware used in a similar attack is Ghostnet<sup>21</sup>. In this case it was malware found in foreign ministries and embassies and the offices of the Dalai Lama. Malware has indeed come a long way from the humble beginning of text messages echoed to a terminal. So what could be left? Well, there's cyber war.

There are certain episodes in the history of cyber warfare that stand apart in the context of malware. The use of botnets in large scale Distributed Denial of Service (DDoS) attacks launched against nation states. The weapons were botnets, and behind every bad botnet is some malware. The widely reported attacks on Estonia<sup>22</sup>, Lithuania<sup>23</sup> and Georgia<sup>24</sup>, all demonstrate the crippling effects sustained DDoS attacks can have. Without the botnets to launch the attacks these attacks would be far more difficult to conduct.

Malware has evolved from somewhat humble beginnings to become a principal weapon in cyber crime, espionage and warfare. Malware is no longer the preserve of the lone virus writer but rather can be developed by professionals with specific goals in mind. But this simply brings us to the current pièce de résistance of malware, Stuxnet<sup>25</sup>.

<sup>20</sup> A new approach to China  
<http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>

<sup>21</sup> Major cyber spy network uncovered  
<http://news.bbc.co.uk/2/hi/7970471.stm>

<sup>22</sup> Hackers Take Down the Most Wired Country in Europe  
[http://www.wired.com/politics/security/magazine/15-09/ff\\_estonia?currentPage=all](http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all)

<sup>23</sup> Lithuania Weathers Cyber Attack, Braces for Round 2  
[http://voices.washingtonpost.com/securityfix/2008/07/lithuania\\_weathers\\_cyber\\_attac\\_1.html](http://voices.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html)

<sup>24</sup> Cyber Attacks Against Georgia: Legal Lessons Identified  
[www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf](http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf)

<sup>25</sup> W32.Stuxnet Dossier  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)

Stuxnet did not just move the goalposts for malware, it has changed the playing field and rules of the game as well. Stuxnet encompassed virtually every aspect of malware. It is a worm, a trojan, and a rootkit. It exploited no less than four previously unknown vulnerabilities, infected multiple platforms including attacking PLC (Programmable Logic Controller) devices. It attacks SCADA (Supervisory Control And Data Acquisition) systems and was designed to sabotage an operation while remaining undetected.

While there has been much speculation as to who is behind Stuxnet with no definitive answer, there are certain things we can observe from the malware itself and its workings. It was not developed by an individual but a team, over a period of time. The development team had a great deal of intelligence on the target systems, evident from the targets defined from the Stuxnet code. While it spread within its targeted enterprise, it did not appear to spread beyond its target. The limited number of infections found outside the target was incidental. Its goal appears to have been to sabotage certain functions of a manufacturing or processing system, while hiding and providing feedback that systems were operating normally. In short, there seems to be very significant resources and finances behind Stuxnet. There appears to be no suitable profit motive necessary for a criminal operation to commit resources to such a project.

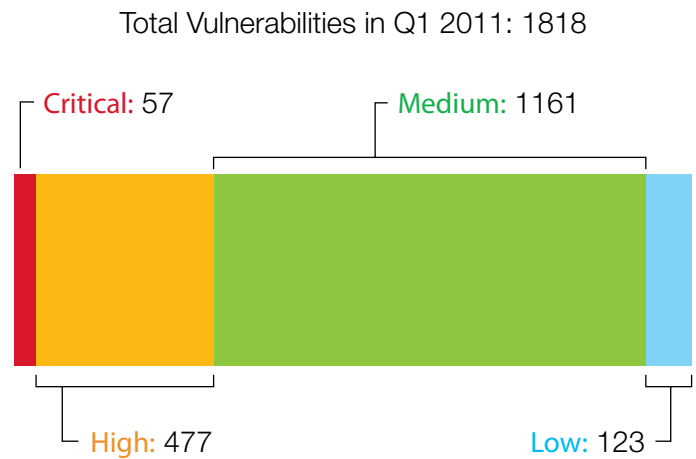
From 1971 to 2011, malware has effectively been weaponized in ways that the science fiction authors wrote about and early virus writers would only have dreamed about. Yet still many of the basic features remain. So where does that leave us today?

Anti-virus strategies are more important today than ever before. Whether domestic or corporate, reputable and up to date anti-virus solutions should be in use. IDS/IPS systems can aid in preventing attacks and in detecting malicious network traffic such as communications between zombie botnet clients and their command and control hosts. Sensible Ingress and Egress filtering are always recommended. Talking to a reputable managed security services provider can also be advantageous as they can provide not only management of critical protection systems but also trained analysts who can provide assistance which can be especially helpful when dealing with previously unknown threats. So whether you have a PDP-10 tucked away somewhere still running and somehow connected to the Internet or you are responsible for an entire modern enterprise you face the same basic threats. Arm yourself.

## Prolific and Impacting Issues of Q1 2011

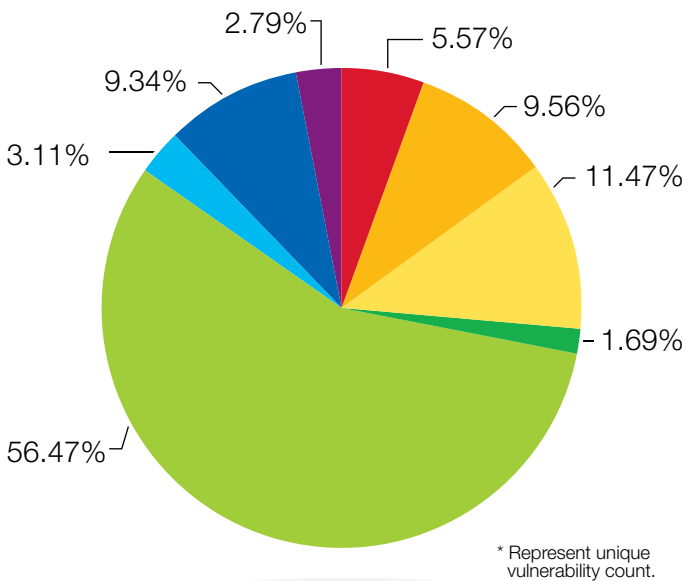
### Significant disclosures

In Q1 2011, the X-Force team researched and assessed 1818 security related threats. A significant percentage of the vulnerabilities featured within the X-Force database became the focal point of malicious code writers whose productions included malware and targeted exploits.



Source: IBM X-Force

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. \*



Source: IBM X-Force

<b>Bypass Security</b>	Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner.
<b>Data Manipulation</b>	Manipulate data used or stored by the host associated with the service or application.
<b>Denial of Service</b>	Crash or disrupt a service or system to take down a network.
<b>File Manipulation</b>	Create, delete, read, modify, or overwrite files.
<b>Gain Access</b>	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.
<b>Gain Privileges</b>	Privileges can be gained on the local system only.
<b>Obtain Information</b>	Obtain information such as file and path names, source code, passwords, or server configuration details.
<b>Other</b>	Anything not covered by the other categories.

During the first week of January, a vulnerability was publicly disclosed and exploit code was published affecting certain versions of the Windows Graphics Rendering Engine. Attacks looking to exploit this vulnerability require a user to open a malicious document file with embedded thumbnails or other Microsoft Office documents with malicious images which could contain code to gain privileges.

- A protection alert provided by IBM: Microsoft Windows Graphics Rendering Engine buffer overflow<sup>26</sup>
  - IBM Protection Signatures: CompoundFile\_Windows\_Thumbnail\_Overflow, CompoundFile\_Shellcode\_Detected
- CVE-2010-3970
- Microsoft Security Bulletin MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)<sup>27</sup>

There were two other 0-day vulnerabilities that surfaced in January for which IBM X-Force released Protection Alerts. The first, affects the Microsoft Windows Fax Cover Page Editor. A remote attacker could execute arbitrary code if a victim is tricked into opening a malicious Fax Cover Page document. The second issue is a buffer overflow vulnerability in Microsoft IIS7 and could also result in remote code execution.

- A protection alert provided by IBM: Microsoft Windows Fax Cover Page Editor could allow denial of service<sup>28</sup>
  - IBM Protection Signature: FAX\_Coversheet\_Shellcode\_Detected
- CVE-2010-4701
- A protection alert provided by IBM: Microsoft IIS FTP Interpret-As-Command (IAC) Overflow<sup>29</sup>
  - IBM Protection Signature: FTP\_IIS\_IAC\_Overflow
- CVE-2010-3972
- Microsoft Security Bulletin MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)<sup>30</sup>

<sup>26</sup> A protection alert provided by IBM: Microsoft Windows Graphics Rendering Engine buffer overflow  
<http://www.iss.net/threats/406.html>

<sup>27</sup> Microsoft Security Bulletin MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)  
<http://www.microsoft.com/technet/security/Bulletin/MS11-006.msp>

<sup>28</sup> A protection alert provided by IBM: Microsoft Windows Fax Cover Page Editor could allow denial of service  
<http://www.iss.net/threats/408.html>

<sup>29</sup> A protection alert provided by IBM: Microsoft IIS FTP Interpret-As-Command (IAC) Overflow  
<http://www.iss.net/threats/407.html>

<sup>30</sup> Microsoft Security Bulletin MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)  
<http://www.microsoft.com/technet/security/bulletin/ms11-004.msp>

An IBM Protection Alerts was also published in January for an issue affecting Windows Backup Manager and addressed in Microsoft's January Security Release. An attacker which persuades a user to open such a file on a remote SMB or WebDAV share could then supply arbitrary code which would be executed with the privileges of the current user.

- A protection alert provided by IBM: Microsoft Windows Backup Manager Could Allow Remote Code Execution<sup>31</sup>
  - IBM Protection Signatures: HTTP\_Windows\_Backup\_Mgr\_DLL\_Hijacking, SMB\_Windows\_Backup\_Mgr\_DLL\_Hijacking
- CVE-2010-3145
- Microsoft Security Bulletin MS11-001: Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935)<sup>32</sup>

February witnessed the publication of the most number of Protection Alerts and Advisories for the first quarter – a total of seven. One of the Protection Alerts was produced for a vulnerability addressed in Microsoft's February Security Release. A Microsoft Internet Explorer uninitialized memory corruption vulnerability can lead to remote code execution.

Another Protection Alert released the same day in February also highlighted a Microsoft issue, however, this vulnerability affecting Microsoft Windows was not addressed by Microsoft until March. Public exploit code had been made available for this issue and in March, Google indicated that they had observed highly targeted attacks against their users exploiting this issue<sup>33</sup>.

- A protection alert provided by IBM: Microsoft Internet Explorer Remote Code Execution<sup>34</sup>
  - IBM Protection Signature: Script\_IE\_Document\_Corruption
- CVE-2011-0036
- Microsoft Security Bulletin MS11-003: Cumulative Security Update for Internet Explorer (2482017)<sup>35</sup>
- A protection alert provided by IBM: Microsoft Windows MHTML Could Allow Information Disclosure<sup>36</sup>
  - IBM Protection Signatures: MHTML\_CRLF\_Injection, MHTML\_Handler\_Detected
- CVE-2011-0096
- Microsoft Security Bulletin MS11-026: Vulnerability in MHTML Could Allow Information Disclosure (2503658)<sup>37</sup>

<sup>31</sup> A protection alert provided by IBM: Microsoft Windows Backup Manager Could Allow Remote Code Execution <http://www.iss.net/threats/405.html>

<sup>32</sup> Microsoft Security Bulletin MS11-001: Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935) <http://www.microsoft.com/technet/security/bulletin/MS11-001.msp>

<sup>33</sup> MHTML vulnerability under active exploitation <http://googleonlinesecurity.blogspot.com/2011/03/mhtml-vulnerability-under-active.html>

<sup>34</sup> A protection alert provided by IBM: Microsoft Internet Explorer Remote Code Execution <http://www.iss.net/threats/409.html>

<sup>35</sup> Microsoft Security Bulletin MS11-003: Cumulative Security Update for Internet Explorer (2482017) <http://www.microsoft.com/technet/security/bulletin/MS11-003.msp>

<sup>36</sup> A protection alert provided by IBM: Microsoft Windows MHTML Could Allow Information Disclosure <http://www.iss.net/threats/410.html>

<sup>37</sup> Microsoft Security Bulletin MS11-026: Vulnerability in MHTML Could Allow Information Disclosure (2503658) <http://www.microsoft.com/technet/security/bulletin/MS11-026.msp>

IBM X-Force also published two Protection Advisories for vulnerabilities they found affecting Adobe Shockwave. Compromise of machines using affected versions of Adobe Shockwave Player may lead to exposure of confidential information, loss of productivity, and further network compromise. Remote code execution could be achieved by enticing a user to visit a web page that loads a specially crafted Director file that exploits this vulnerability.

- A protection advisory provided by IBM: Adobe Shockwave (invalid array index) Remote Code Execution<sup>38</sup>
  - IBM Protection Signature: RIFF\_Director\_Movie\_Detected
- CVE-2010-4306
- Adobe Security bulletin APSB11-01: Security update available for Shockwave Player<sup>39</sup>
- A protection advisory provided by IBM: Adobe Shockwave (constant table) Remote Code Execution<sup>40</sup>
  - IBM Protection Signature: RIFF\_Director\_Movie\_Detected
- CVE-2010-4307
- Adobe Security bulletin APSB11-01: Security update available for Shockwave Player<sup>41</sup>

Later in the month, IBM X-Force published three Protection Alerts to address several different threats. The first Protection

Alert indicates coverage for zwShell which is a Trojan dropper associated with the “Night Dragon” attack discussed in the “Additional Q1 2011 Quarter highlights” section below. This Trojan dropper is designed for creating a customizable backdoor remote administration tool to be installed on target machines. The backdoor can then be used to open a remote desktop or shell to the target system.

- A protection alert provided by IBM: zwShell Command And Control<sup>42</sup>
  - IBM Protection Signature: Trojan\_zwShell\_CnC
- McAfee Foundstone Professional Services and McAfee Labs: Global Energy Cyberattacks: “Night Dragon”<sup>43</sup>

In February, a 0-day memory corruption vulnerability affecting Microsoft Windows surfaced as did proof-of-concept code targeting this issue. Microsoft later addressed this issue as part of their March Security Release.

- A protection alert provided by IBM: Microsoft Windows Server Browser Election Request buffer overflow<sup>44</sup>
  - IBM Protection Signature: SMB\_Mailslot\_Election\_Overflow
- CVE-2011-0654
- Microsoft Security Bulletin MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)<sup>45</sup>

<sup>38</sup> A protection advisory provided by IBM: Adobe Shockwave (invalid array index) Remote Code Execution  
<http://www.iss.net/threats/412.html>

<sup>39</sup> Adobe Security bulletin APSB11-01: Security update available for Shockwave Player  
<http://www.adobe.com/support/security/bulletins/apsb11-01.html>

<sup>40</sup> A protection advisory provided by IBM: Adobe Shockwave (constant table) Remote Code Execution  
<http://www.iss.net/threats/411.html>

<sup>41</sup> Adobe Security bulletin APSB11-01: Security update available for Shockwave Player  
<http://www.adobe.com/support/security/bulletins/apsb11-01.html>

<sup>42</sup> A protection alert provided by IBM: zwShell Command And Control  
<http://www.iss.net/threats/413.html>

<sup>43</sup> McAfee Foundstone Professional Services and McAfee Labs: Global Energy Cyberattacks: “Night Dragon”  
<http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>

<sup>44</sup> A protection alert provided by IBM: Microsoft Windows Server Browser Election Request buffer overflow  
<http://www.iss.net/threats/415.html>

<sup>45</sup> Microsoft Security Bulletin MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)  
<http://www.microsoft.com/technet/security/bulletin/MS11-015.msp>

The third Protection Alert addresses a denial of service vulnerability affecting Oracle's JRE and JDK 6 Update 23 and earlier, 5 Update 27 and earlier and JRE 1.4.2\_29 and earlier for Windows, Solaris, and Linux. An unauthenticated user can exhaust resources on a system utilizing Apache Tomcat with a vulnerable version of the JRE. Exploitation is simple and there are many reports of how to carry out such an attack.

- A protection alert provided by IBM: Sun Java Double.parseDouble() denial of service<sup>46</sup>
  - IBM Protection Signature: HTTP\_Tomcat\_AcceptLanguage\_DoS
- CVE-2010-4476
- Oracle Java SE and Java for Business Critical Patch Update Advisory - February 2011<sup>47</sup>

A Protection Alert was released to highlight one of the vulnerabilities addressed in Microsoft's March Security Release.

- A protection alert provided by IBM: Microsoft Windows Media Could Allow Remote Code<sup>48</sup>
  - IBM Protection Signature: ASF\_DVR\_MS\_Code\_Exec
- CVE-2011-0042
- Microsoft Security Bulletin MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)<sup>49</sup>

In mid-March, reports surfaced of a vulnerability affecting Adobe Flash being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Excel (.xls) file delivered as an email attachment. Platforms affected include the latest Adobe Flash 10 versions for Windows, Macintosh, Linux and Solaris operating systems, Android OS and the Authplay component shipped with Adobe Reader 9.x and 10x versions. Exploitation of this vulnerability can result in remote code execution with privileges of the current user.

- A protection alert provided by IBM: Adobe Flash Player authplay.dll code execution<sup>50</sup>
  - IBM Protection Signature: CompoundFile\_Nested\_SWF
- CVE-2011-0609
- Security bulletin APSA11-01: Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat<sup>51</sup>

<sup>46</sup> A protection alert provided by IBM: Sun Java Double.parseDouble() denial of service  
<http://www.iss.net/threats/414.html>

<sup>47</sup> Oracle Java SE and Java for Business Critical Patch Update Advisory - February 2011  
<http://www.oracle.com/technetwork/topics/security/javacpufeb2011-304611.html>

<sup>48</sup> Microsoft Windows Media Could Allow Remote Code Execution  
<http://www.iss.net/threats/416.html>

<sup>49</sup> Microsoft Security Bulletin MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)  
<http://www.microsoft.com/technet/security/bulletin/MS11-015.msp>

<sup>50</sup> A protection alert provided by IBM: Adobe Flash Player authplay.dll code execution  
<http://www.iss.net/threats/417.html>

<sup>51</sup> Security bulletin APSA11-01: Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat  
<http://www.adobe.com/support/security/advisories/apsa11-01.html>

**Additional Q1 2011 Quarter highlights**

This section of the report briefly covers some of the additional threats facing security professionals during Q1 2011.

**“Night Dragon”**

In February, McAfee issued a report detailing a large scale attack directed against global companies in the energy industry. The operation, which has been dubbed “Night Dragon”, uses SQL injection, spear phishing, and other targeted exploits, to gain access to “proprietary operations and project-financing information on oil and gas field bids and operations.”

This attack is similar to other Advanced Persistent Threats (APT) that have been in the news over the past few years. The tactics and techniques used by these attackers are generally just sophisticated enough to get the job done, but they are highly successful and are able to remain hidden for significant lengths of time.

Customers can protect themselves by leveraging best practices in secure applications, as well as through leveraging SQL injection protection mechanisms, malicious document protection, rogue channel detection, and of course constant vigilance. We also recommend customers remain vigilant in protecting information assets that are essential to ongoing business operations.

**Hactivist Group - Anonymous**

The hactivist group Anonymous has existed in one form or another since 2003. However, operations staged by this group in Q1, including the attack on HBGary Federal and the release of Bank of America documents, has brought them more into the spot light.

Anonymous appears to have begun casting itself as a venue for publishing documents provided by whistle blowers or obtained through other means, such as documents obtained from the various HBGary servers that were reportedly accessed by Anonymous. Anonymous also posted a series of emails between employees of Balboa Insurance a part of the Countrywide acquisition by Bank of America. A member of Anonymous claimed via Twitter that the emails represented “fraud” because the bank hid foreclosure errors from “federal auditors,” among other charges.

Because of the large numbers of participants in various Anonymous operations, and the wide range of skills present, any particular operation may vary in sophistication and effectiveness. An attack may be quite sophisticated. It can be carried out over a protracted period, patiently gathering information even after the target has been compromised so that sensitive information and new opportunities can be identified and exploited. Alternatively, another operation can be organized by a small group and then posted in the IRC chats so that volunteers can participate by using the setup instructions available in the chat. The latter situation tends to be quite variable based upon the popularity of the proposed operation and what other operations may already be under way.

In general, most of Anonymous' tools and methods are well known and well understood having been refined over the years. Use of modified web load testing tools such as Low Orbit Ion Cannon is a relatively recent innovation, but is still in the range of classic distributed denial of service attacks, the major difference being volume and ease of use.

Anonymous rarely exhibits unusual techniques. Some attacks have shown a good deal of elegance and sophistication, probably indicating experienced attackers. That said, the tools and range of abilities are rarely new, and are mostly subject to the normal range of security countermeasures.

SQL injection was utilized in the HBGary attack to obtain passwords and account information which gave the attackers further access into the network. SQL injection is covered in various methods in all IDS vendors. It is key to have this protection tuned and in blocking mode to be effective against attacks.

Many successful operations by Anonymous were effective only following a successful social engineering effort. More often than not phishing and spear phishing efforts lead to key information that allowed an operation to go forward. Failure to achieve social engineering goals seems to have limited the group to Denial of Service attacks and opportunistic defacement, which still achieves their goals.

#### **List of Contributors for this paper include:**

##### **IBM MSS Intelligence Center**

Michelle Alvarez – Team Lead & Cyber Threat Intelligence Analyst

Lyndon Sutherland

##### **IBM X-Force Database Team**

## **References**

### **Prolific and Impacting Issues of Q1 2011**

Global Energy Cyberattacks: "Night Dragon"

<http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>

HBGary Federal hacked and exposed by Anonymous

<http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/>

Hackers Just Released What They Say Is A Damning Trove Of Emails About Bank Of America And Its Mortgage Practice

<http://www.businessinsider.com/anonymous-hackers-bank-of-america-wikileaks-emails-documents-2011-3>



---

© Copyright IBM Corporation 2011

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

Produced in the United States of America  
May 2011  
All Rights Reserved

IBM, the IBM logo, ibm.com and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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.

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.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

\* 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.



Please Recycle