IBM Internet Security Systems
X-Force® 2007 Trend Statistics
Table of Contents

Management Overview 3
  2007 Highlights 3

Vulnerability Analysis 5
  2007 Vulnerability Count 6
  2007 Vulnerability Disclosures per Year 6
  Vulnerabilities per Month 8
  Vulnerabilities per Week 9
  Vulnerabilities by Day of the Week 10
  Weekend vs. Weekday 11
  Classic High/Medium/Low Vulnerability Impact Breakdown 12
  Common Vulnerability Scoring System (CVSS) Breakdown 14
  Five Vendors with the Most Vulnerability Disclosures 16
  Remote vs. Local Exploitation 20
  Consequences of Exploitation 21

Web Browser Exploitation Trends 23
  Obfuscation and Encryption 24
  Windows-based Web Browser Vulnerabilities 25

Spam and Phishing Analysis 28
  Basics about the determination of geographical distributions 28
  From which countries does spam originate? 29
  Where are the Web pages contained in spam messages hosted? 30
  What is the average byte size of spam messages? 31
  What are the most popular subject lines of spam? 32
  What is the language distribution of spam? 32
  How many spams are image-based? 33
  How many spams are animated GIF-based? 34
  How many spams are PDF spam? 35
  How much spam is phishing? 37
  Where do phishing e-mails come from? 38
  Where are Web pages contained in phishing emails hosted? 39
  What are the most popular subject lines of phishing? 40

Web Content Trends 41
  Analysis 42
  Current Status of Unwanted Internet Content 43
  Current Distribution of Adult Content 44
  Current Distribution of Social Deviance Content 45
  Current Distribution of Criminal Content 46

Malcode Analysis 47
  Malcode Categorization 49
  Malcode Categorization Trends 50
  Malcode Additions 51
  Top 10 Most Common Malware 52
Management Overview


2007 Highlights

Vulnerabilities

- Fewer vulnerabilities were publicly disclosed in 2007 in comparison to 2006 – a 5.4 percent decrease overall.
- Although total vulnerability disclosures went down, the number of reported high severity vulnerabilities increased by 28 percent in comparison with 2006.
- The busiest day of the week for vulnerability disclosures continued to be Tuesday, with 1,361 new vulnerabilities disclosed on this day of the week in 2007.
- Again in 2007, the vendors with the most vulnerability exposures were some of the largest software distributors in the world: Microsoft, Apple, Oracle, IBM and Cisco. Still, all of these vulnerabilities combined only account for 13.6 percent of all disclosed vulnerabilities.
- Of all the vulnerabilities disclosed in 2007, only 50 percent can be corrected through vendor patches.
- Nearly 90 percent of 2007 vulnerabilities could be remotely exploited, up one percentage point from 2006.
Web Browser Exploitation

- Most in-the-wild browser exploits are generated by Web exploit toolkits.
- In 2006, using browser obfuscation for Web-based exploits started gaining traction. With the prevalence of Web exploit toolkits, nearly all in-the-wild browser exploits seen by the end of 2007 were obfuscated and/or encrypted.
- Critical vulnerabilities for Mozilla Firefox were dramatically lower in 2007 compared to 2006.

Spam and Phishing

- For the first time ever, spam message size decreased sharply to pre-2005 levels, corresponding with the decrease observed in image-based spam distribution.
- While image-based spam decreased in 2007, X-Force monitored short-lived attempts to use PDF and MP3 attachments in spam messages—new techniques for 2007.
- Of the top 20 companies targeted by phishing in 2007, 19 are in the banking industry and one conducts recruiting.

Web Content

- 9 percent of Internet content was classified as unwanted (criminal, pornography, etc) as compared to 12.5 percent in 2006.
- The U.S. far outpaces other countries as the primary hosting source of adult, socially deviant and criminal content on the Internet, accounting for roughly 40-48 percent in each content category.
- The U.S. and Germany were the only two countries consistently among the top three hosting sources for each type of “unwanted” Internet content monitored throughout 2007.
Malcode

- X-Force collected and analyzed nearly 410,000 new malware samples in 2007, almost a third more than it researched in 2006.
- Trojans represent the largest category of malware in 2007 — 109,246 varieties account for 26 percent of all malware.
- The most frequently occurring malware on the Internet was Trojan.Win32.Agent — 26,573 varieties in 2007 account for 24 percent of all Trojans.
- The most common worm in 2007 was Net-Worm.Win32.Allaple with 21,254 varieties. It is a family of polymorphic worm that propagates by exploiting Windows® vulnerabilities instead of using e-mail.

Vulnerability Analysis

X-Force remained extremely busy analyzing and documenting vulnerabilities in 2007. The 6,437 new vulnerabilities represent 20.7 percent of all vulnerabilities chronicled during the ten year existence of the X-Force Database. To avoid any ambiguity regarding the characterization of vulnerabilities, the IBM Internet Security Systems (ISS) definition below is applied to this report.

Vulnerability is any computer-related vulnerability, exposure, or configuration setting that may result in a weakening or breakdown of the confidentiality, integrity, or accessibility of the computing system.
2007 Vulnerability Count

For the first time, X-Force witnessed a reduction (-5.4 percent) in new vulnerability disclosures from the previous year. The drop could represent an anomaly, a statistical correction or a new trend in the amount of disclosures.

2005 and 2006 saw large spikes in vulnerability growth (approximately 41 percent each year) that were well above the X-Force Database historical average (27 percent a year). The 5.4 percent decline in 2007 could simply be a statistical correction to the growth in vulnerabilities in 2005 and 2006. Although the number of disclosures dipped in 2007, the drop (5.4 percent) is less dramatic than the decrease in vulnerability growth witnessed between 2002 and 2003 – as shown in Figure 1 and Table 1.

Although there was a decrease in overall vulnerabilities, high-priority vulnerabilities increased by 28 percent. Researchers could simply be focusing on the sometimes more difficult, high-priority finds.

![Vulnerability Disclosures per Year](image)

Figure 1: Total Vulnerability Disclosures from 2000 – 2007

1 The X-Force database chronicles not only vulnerabilities, but also security-related patches, audits, and methods of vulnerability detection and protection. In the past, X-Force has reported the sum of these issues along with vulnerabilities. The vulnerability statistics in this report show vulnerabilities only.
Table 1: Detailed Vulnerability Disclosure Statistics from 2000-2007

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Vulnerabilities</th>
<th>Monthly Average</th>
<th>Weekly Average</th>
<th>Annual Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>1,343</td>
<td>112</td>
<td>26</td>
<td>---</td>
</tr>
<tr>
<td>2001</td>
<td>1,553</td>
<td>129</td>
<td>30</td>
<td>15.6%</td>
</tr>
<tr>
<td>2002</td>
<td>2,637</td>
<td>220</td>
<td>51</td>
<td>69.8%</td>
</tr>
<tr>
<td>2003</td>
<td>2,785</td>
<td>232</td>
<td>54</td>
<td>5.6%</td>
</tr>
<tr>
<td>2004</td>
<td>3,417</td>
<td>285</td>
<td>66</td>
<td>22.7%</td>
</tr>
<tr>
<td>2005</td>
<td>4,824</td>
<td>402</td>
<td>93</td>
<td>41.2%</td>
</tr>
<tr>
<td>2006</td>
<td>6,803</td>
<td>567</td>
<td>131</td>
<td>41.0%</td>
</tr>
<tr>
<td>2007</td>
<td>6,437</td>
<td>536</td>
<td>124</td>
<td>-5.4%</td>
</tr>
</tbody>
</table>
Vulnerabilities per Month

The average number of new vulnerabilities disclosed per month increased steadily from 2000 through 2006. In 2007, in correlation with the observed annual decline, X-Force also noticed a slight decrease in monthly growth.

Figure 2 displays the number of new vulnerabilities researched monthly by X-Force during 2007. The horizontal plots on the chart show the monthly averages of 2003, 2004, 2005, and 2006. When comparing the vulnerability disclosure rate of 2007 to 2006 on a monthly basis, the disclosure rate was higher during six months (January, March, April, May, July, and October), and was lower during the other six months. May, with January not far behind, had the largest number of vulnerabilities reported in 2007, while September had the lowest.

![Vulnerabilities per Month 2007](image)
Vulnerabilities per Week
The busiest week for vulnerability disclosure during 2007 was week 28 (July 9 - 15) with 159 new vulnerabilities disclosed. In 2006, the busiest week was just before Thanksgiving and in 2005 it was the week before Christmas, which had been the standard for many years. Both 2006 and 2007 have bucked this historical trend.

Figure 3 breaks down 2007 vulnerability disclosure on a week-by-week basis.

Weekly Percentage of Vulnerability Disclosures 2007

Figure 3: Vulnerability Disclosures from Week to Week in 2007
Vulnerabilities by Day of the Week

X-Force chronicled 959 vulnerabilities on Mondays during 2007, followed by 1,361 on Tuesdays, the most of any day of the week. Wednesday, Thursday and Friday saw a gradual decline in new vulnerability disclosures, while Saturday and Sunday continued to be well below the weekday average. Figure 5 shows 2007 vulnerability disclosure by day of the week.

The jump in Tuesday vulnerabilities can be explained by the large number of vendor-released vulnerabilities and patches on the second Tuesday of each month. Microsoft started the trend by regularly disclosing its vulnerabilities on the second Tuesday of each month, and other vendors seem to be following suit for a variety of competitive and strategic reasons. As such, Patch Tuesday, as it’s known in security circles, should keep Tuesday one of the busiest days of the week in the foreseeable future.

Figure 4: Vulnerability Disclosures by Day of the Week in 2007
Weekend vs. Weekday

In 2006, X-Force observed that more vulnerabilities were being disclosed on weekends than in prior years. In 2000 - 2005, 11.6 percent of vulnerabilities were disclosed on Saturday and Sunday, while 2006 saw a significant jump in weekend vulnerability disclosure with 17.6 percent. As Figure 5 shows, that trend continues with 16 percent of vulnerabilities disclosed on a weekend in 2007, down only slightly from 2006.

Table 2 puts weekend vs. weekday vulnerability disclosure in historical perspective.

<table>
<thead>
<tr>
<th>Year</th>
<th>Weekend</th>
<th>Weekday</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>10.1%</td>
<td>89.9%</td>
</tr>
<tr>
<td>2001</td>
<td>10.7%</td>
<td>89.3%</td>
</tr>
<tr>
<td>2002</td>
<td>14.3%</td>
<td>85.7%</td>
</tr>
<tr>
<td>2003</td>
<td>15.9%</td>
<td>84.1%</td>
</tr>
<tr>
<td>2004</td>
<td>10.4%</td>
<td>89.6%</td>
</tr>
<tr>
<td>2005</td>
<td>8.1%</td>
<td>91.9%</td>
</tr>
<tr>
<td>2006</td>
<td>17.6%</td>
<td>82.4%</td>
</tr>
<tr>
<td>2007</td>
<td>16.0%</td>
<td>84.0%</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>13.7%</strong></td>
<td><strong>86.3%</strong></td>
</tr>
</tbody>
</table>

Table 2: Weekday vs. Weekend Ratio Vulnerability Disclosure from 2000 - 2007
Classic High/Medium/Low Vulnerability Impact Breakdown

X-Force thoroughly analyzes and assesses exploitation impact for each vulnerability it records. By examining the breakdown of vulnerability disclosures since 2000, X-Force noticed that the percentage of high impact vulnerabilities had been decreasing over time. However, 2007 experienced a slight upswing in the number of high impact vulnerabilities — from 16.2 percent in 2006 to 22 percent in 2007, representing 28 percent growth in the total number of high impact vulnerabilities. As Figure 6 reveals, this is the first such increase since 2004.

Figure 6: Ratio of High, Medium, and Low Impact Vulnerabilities since 2000 based on X-Force Metrics
X-Force continues to define high, medium, and low impact vulnerabilities by the following guidelines:

- **High**: Security issues that allow immediate remote or local access, or immediate execution of code or commands with unauthorized privileges. Examples are most buffer overflows, backdoors, default or no password, and bypassing security on firewalls or other network components.

- **Medium**: Security issues that have the potential to grant access or allow code execution via complex or lengthy exploit procedures, or low risk issues applied to major Internet components. Examples are cross-site scripting, man-in-the-middle attacks, SQL injection, denial of service of major applications, and denial of service resulting in system information disclosure (such as core files).

- **Low**: Security issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not to directly gain unauthorized access. Examples are brute force attacks, non-system information disclosure (configurations, paths, etc.), and denial of service attacks.
Common Vulnerability Scoring System (CVSS) Breakdown

The Common Vulnerability Scoring System (CVSS) is the industry standard for rating vulnerability severity and risk based on metrics (base and temporal) and formulas. The base metrics are comprised of characteristics that generally do not change over time. Base metrics include access vector, complexity, authentication and the impact bias. Temporal metrics are made up of characteristics of a particular vulnerability that can and often do change over time, and include the exploitability, remediation level and report confidence. A complete explanation of CVSS and its metrics can be found on the CVSS Web site at http://www.first.org/cvss/.

Table 3 represents the risk level associated with both the base and temporal CVSS scores, while Figure 7 divides 2007 vulnerabilities according to CVSS risk levels.

<table>
<thead>
<tr>
<th>CVSS Base/Temporal Score</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Critical</td>
</tr>
<tr>
<td>7.0 - 9.9</td>
<td>High</td>
</tr>
<tr>
<td>4.0 - 6.9</td>
<td>Medium</td>
</tr>
<tr>
<td>0.0 - 3.9</td>
<td>Low</td>
</tr>
</tbody>
</table>

*Table 3: CVSS Base/Temporal Score and Corresponding Risk Level*
Vulnerabilities identified as critical by CVSS are vulnerabilities that are installed by default, network-routable, do not require authentication to access and will allow an attacker to gain system or root level access.

In 2007, about 2 percent of all vulnerabilities were deemed critical. IBM ISS began scoring all vulnerabilities according to the CVSS standard in July 2006. During 2006, 3 percent of all vulnerabilities were considered critical.

The temporal score considers more up-to-date and pertinent specifics about a particular vulnerability, such as patch, exploit, and confidence information. The temporal score starts with the base score and adjusts depending on whether a patch exists, if an exploit has been discovered, and if the vendor has confirmed the vulnerability.
Figure 8 applies CVSS temporal metrics to vulnerabilities disclosed by CVSS in 2007 and displays the percentage of each criticality rating.

![CVSS Temporal Score Risk Level 2007](image)

**Figure 8: Percentage of 2007 Vulnerabilities Based on CVSS Temporal Metrics**

**Five Vendors with the Most Vulnerability Disclosures**

In 2007, the top five vendors with the most vulnerabilities disclosed in their product lines accounted for 13.6 percent of all disclosed vulnerabilities. This equates to 878 of the 6,437 vulnerabilities recorded in the X-Force Database in 2007 (see Figure 9). Table 4 reveals who the top five vendors are and the total number and percentages of vulnerabilities found in 2007.

Please note that the statistics do not account for each vendor’s market share or the number of products each manufactures. In other words, mass-produced and distributed software is likely to have more vulnerability disclosures.
Figure 9: Percentage of 2007 Vulnerabilities from Top Five Vendors

Table 4: Number and Percentage of Vulnerabilities Reported Among Top Five Vendors
When considering the rate at which the industry is fixing vulnerabilities, it’s beneficial to look at how or if the top vendors are making improvements to their products. Figure 10 shows that 20 percent of the top five vendors’ vulnerabilities remain unpatched — a 6 percent increase compared to 2006.

At first glance, leaving 20 percent of vulnerabilities unpatched may seem high. However, half of the vulnerabilities reported in 2007 have no vendor patch available to fix them. The top five vendors have a much better fix rate in comparison so one could argue that the top five vendors are leading the way in fixing vulnerabilities. A comparison of Figures 10 and 11 illustrates these points.

![Figure 10: Patched vs. Unpatched Vulnerabilities for Top Five Vendors in 2007](image)
Figure 11: Patched vs. Unpatched Vulnerabilities for Other Vendors in 2007
Remote vs. Local Exploitation

The most significant vulnerabilities are those that can be exploited remotely. Remote vulnerabilities can be exploited over the network, while local vulnerabilities can only be exploited by logging in to the local host or from the desktop. Vulnerabilities falling into both remote and local categories can be exploited by both vectors.

The trend observed in 2006 continued in 2007, with an overwhelming 89.4 percent of all vulnerabilities allowing remote exploitation, up from 88.4 percent in 2006. As Table 5 shows, the percentage of remote vulnerabilities has been growing since 2000.

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage of Remote Vulnerabilities</th>
<th>Percentage of Local Vulnerabilities</th>
<th>Percentage of Both Local and Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>43.6%</td>
<td>56.4%</td>
<td>0.0%</td>
</tr>
<tr>
<td>2001</td>
<td>57.4%</td>
<td>42.6%</td>
<td>12.0%</td>
</tr>
<tr>
<td>2002</td>
<td>75.7%</td>
<td>24.3%</td>
<td>7.1%</td>
</tr>
<tr>
<td>2003</td>
<td>76.6%</td>
<td>23.4%</td>
<td>5.0%</td>
</tr>
<tr>
<td>2004</td>
<td>73.3%</td>
<td>26.7%</td>
<td>5.0%</td>
</tr>
<tr>
<td>2005</td>
<td>84.8%</td>
<td>15.2%</td>
<td>2.1%</td>
</tr>
<tr>
<td>2006</td>
<td>88.4%</td>
<td>11.6%</td>
<td>1.4%</td>
</tr>
<tr>
<td>2007</td>
<td>89.4%</td>
<td>10.6%</td>
<td>1.0%</td>
</tr>
</tbody>
</table>

*Table 5: Percentage of Vector Exploitation Types in Vulnerabilities Since 2000*
Consequences of Exploitation

As a component of expert analysis, X-Force records the primary consequence of each vulnerability’s exploitation. The consequences are defined as the most common effect of exploitation and are divided into nine categories:

- **Bypass Security**: Circumvent security restrictions such as a firewall or proxy, IDS system, or a virus scanner.
- **Data Manipulation**: Manipulate data used or stored by the host associated with the service or application.
- **Denial of Service**: Severely limit or crash a program, computer system or network.
- **File Manipulation**: Create, delete, read, modify or overwrite files.
- **Gain Access**: Obtain local and remote access. This also includes vulnerabilities through which an attacker can execute code or commands, typically allowing him access to the system.
- **Gain Privileges**: Privileges can be gained on the local system only.
- **Obtain Information**: Obtain information such as file and path names, source code, passwords, or server configuration details.
- **Informational**: Service name disclosure.
- **Other**
Figure 12 reveals the percentage of 2007 vulnerabilities that fall into each category.

![Vulnerabilities' Consequences 2007](image)

**Figure 12: Vulnerabilities’ Consequences in 2007**

The primary consequence of vulnerability exploitation in 2007 was Gain Access, a continuation from 2006. If a “gain access” vulnerability is exploited, an attacker can then perform other attacks that could lead to exploitation of other vulnerabilities on the system.
Web Browser Exploitation Trends

X-Force has observed continued growth in Web browser exploitation through its Project Whiro crawlers and analysis of network activity monitored by IBM ISS Managed Security Services (MSS). During the second half of 2007, X-Force deployed a new crawler version which enables better inspection of obfuscated Web browser attacks in the wild. One significant benefit of the X-Force exploit-seeking crawler is that it can run intraday over a relatively small percentage of the Web rather than crawling the entire Web over an extended period of time.

A trend that became prevalent in 2007 was the use of IFrames and other methods of hosting links to malicious content. IFrames make third-party content appear as if it is a part of the URL displayed by the browser, when, in fact, the content within the IFrame is hosted by another server. X-Force research has focused on the methods used by the malicious Web servers to exploit browsers and not on the number of IFrames, spam, or other methods in which the purveyors of these sites entice users to click a link.

Underground exploit sales through ICQ-based brokers also continued to flourish in 2007, and the newer trend of exploit toolkit leasing became more prevalent. Leasing allows attackers to get a piece of the action with a smaller initial investment. However, the exact number of toolkit installations purchased is unknown. Reports confirm that attack toolkits have been found at online file storage sites leading X-Force to suspect widespread piracy. In addition, attackers will occasionally modify an exploit toolkit if a new exploit becomes public.

Due to the ubiquity of Web exploit toolkits in the wild and the rapid rate at which they are updated or customized with new exploits, it is not incredibly meaningful to analyze the most popular exploits. If a public proof-of-concept for a browser exploit is available, it will likely be used in one of these exploit toolkits.
Obfuscation and Encryption

Encrypted exploits are contained in streams of encrypted data present in a script such as JavaScript that is decoded on the client’s machine and then executed. Obfuscation may be used by an encrypted exploit, but in general it is not. Obfuscated exploits simply are rearranged in a way that makes it difficult for intrusion detection and prevention systems (IDS and IPS) to match a signature.

Prior to 2006, obfuscated web-browser exploits were not prevalent enough to cause concern in security communities. Such exploits were almost exclusively used in targeted attacks designed to breach known failings in an organization’s perimeter security defenses. Today, the presence of obfuscated attacks has changed markedly.

Throughout 2007, the growth of Web exploit obfuscation and encryption increased substantially. X-Force estimated that nearly 80 percent of Web exploits used obfuscation and/or self-decryption — not to be confused with HTTPS/SSL — in the first half of 2007. By the end of 2007, X-Force believed this rate had reached nearly 100 percent, mostly caused by toolkits such as mPack influencing the underground market. While non-obfuscated exploits still exist, they are rapidly becoming extinct.
Windows-based Web Browser Vulnerabilities

This section analyzes critical vulnerabilities affecting the two most popular Windows-based Web browsers, Microsoft® Internet Explorer and Mozilla Firefox. The analysis does not include vulnerabilities affecting third-party plug-ins, such as ActiveX controls, XPIs, or other add-ons. Although this section discusses browser vulnerabilities in terms of what was patched, both vendors appear to have released patches for all critical vulnerabilities that were disclosed in 2007.
Microsoft released Internet Explorer (IE) patches for 28 critical vulnerabilities in 2007. Compared with the X-Force assessment for 2006, the overall number and type of vulnerabilities are very similar—even down to their respective category allocations.

Memory corruption vulnerabilities have overwhelmingly plagued IE throughout 2007, and X-Force expects this to continue during 2008. While there have not been any security zone bypass issues of a critical nature, the number of critical miscellaneous issues has increased by four since the first half of 2007. These issues include logic bugs that may result in remote code execution or a serious URL spoofing scenario.
Mozilla released Firefox patches for 36 critical vulnerabilities during 2007. Compared with the X-Force assessment for 2006 (64 patched critical vulnerabilities), the number of reported critical vulnerabilities for Firefox on Windows has dramatically decreased by nearly 44 percent. Almost every vulnerability category saw its number halve with the exception of the miscellaneous “other” category which increased by one. X-Force will be watching closely in 2008 to see how these numbers continue to compare against Internet Explorer.

Firefox had a surprisingly low number of reported memory corruption issues in 2007 vs. Internet Explorer. Compared with 2006, the 2007 charts for both Internet Explorer and Firefox bear a striking resemblance.
Spam and Phishing Analysis

IBM ISS premier content filtering services provide a world-encompassing view of spam and phishing attacks. With millions of e-mail addresses actively monitored, X-Force has identified numerous advances in the spam and phishing technologies attackers use.

On an average day, IBM ISS analyzes more than 150,000 unique spam messages. Using a fuzzy-fingerprint technology, IBM ISS defines a “unique” spam message as one that is at least 10 percent different from any other spam message ever received.

This section answers the following questions:

• From which countries does spam originate?
• Where are the Web pages contained in spam messages hosted?
• What is the average byte size of spam?
• What are the most popular subject lines of spam?
• What is the language distribution of spam?
• How many spams are image-based?
• How many spams are animated GIF-based?
• How many spams are PDF spam?
• How much spam is phishing?
• Where do phishing emails come from?
• Where are the Web pages contained in phishing emails hosted?
• What are the most popular subject lines of phishing?
• Which companies are the most targeted by phishings?
Determining Geographical Distributions


The geographical distribution was determined by requesting the IP addresses of the hosts (in the case of the content distribution) or of the sending mail server (in the case of spam and phishing) responding to the IP-to-Country Database.

Spam – Country of Origin

The following map shows the origination point for spam globally. The country of origin indicates the location of the server that sent the spam e-mail. X-Force believes that most spam e-mail is sent by bot networks. Since bots can be controlled from anywhere, the nationality of the actual attackers behind a spam e-mail may not be the same as the country from which the spam originated.

The map in Figure 15 shows that more than one-eighth of worldwide spam comes from servers in the U.S.

Figure 15: Geographical Distribution of Spam Senders

- U.S.A. 15%
- Russia 9.9%
- Germany 5.3%
- South Korea 5.3%
- Poland 4.6%
- Brazil 4.6%
- Italy 3.9%
- Turkey 3.9%
- China 3.8%
- Spain 3.5%
Spam – Country of Origin for Embedded Web Links
The map shows where the spam URLs contained in spam messages are hosted.

Figure 16: Geographical Distribution of Spam URLs
Spam – Average Byte Size

Spam messages have grown in size in 2005 and 2006, increasing from an average of 6 kilobytes to more than 10 kilobytes. However, in the last three quarters, the size declined even below early 2005 levels.

This decrease correlates closely with the downward trend of image-based spam (see below). In the last months of 2007, there was a strong tendency towards short, plain text spams with few words and only one URL.
Spam – Most Popular Subject Lines

The most popular subject lines of spam in the second term of 2007 appear below:

<table>
<thead>
<tr>
<th>Subject Line</th>
<th>Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re:</td>
<td>7.18%</td>
</tr>
<tr>
<td>&lt;empty subject line&gt;</td>
<td>2.78%</td>
</tr>
<tr>
<td>The Pharmacy America Trusts</td>
<td>2.12%</td>
</tr>
<tr>
<td>The United States National Medical Association</td>
<td>1.47%</td>
</tr>
<tr>
<td>Fw:</td>
<td>1.47%</td>
</tr>
<tr>
<td>Replica Watches</td>
<td>1.12%</td>
</tr>
<tr>
<td>Man Lebt nur einmal - probiers aus !</td>
<td>0.97%</td>
</tr>
<tr>
<td>Can you tell me what’s wrong, and how we can fix it?</td>
<td>0.96%</td>
</tr>
<tr>
<td>You’ve received an ecard from a Partner!</td>
<td>0.85%</td>
</tr>
<tr>
<td>You’ve received a greeting ecard from a Worshipper!</td>
<td>0.81%</td>
</tr>
</tbody>
</table>

Spam – Most Popular Languages

The top five languages used in spam messages in 2007 appear below:

<table>
<thead>
<tr>
<th>Language</th>
<th>Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>88.3%</td>
</tr>
<tr>
<td>German</td>
<td>5.1%</td>
</tr>
<tr>
<td>Japanese</td>
<td>1.7%</td>
</tr>
<tr>
<td>Russian</td>
<td>1.7%</td>
</tr>
<tr>
<td>Spanish</td>
<td>0.6%</td>
</tr>
</tbody>
</table>
Spam – Image-Based

Image-based spam has challenged anti-spam solutions since mid-2005. However, during the second quarter of 2007, the percentage of image-based spam declined significantly. By the end of the year, it represented only 5 percent of all spam. X-Force questions whether image-based spam will continue to exist or whether new types of image-based spam will emerge in 2008.

Figure 18: Percentage of Image-Based Spam Since 2005
Spam – Animated GIF-Based

The fate of animated GIF spam is similar to its big brother Image-based Spam. It essentially became an insignificant percentage of all spam by the end of 2007.

Figure 19: Percentage of Animated GIF-Based Spam Since July 2007
Spam – PDF Attachments

In summer 2007, X-Force observed a new method of spam delivery – e-mail containing PDF attachments with spam messages. At first, some security vendors were not able to parse the attachments to search for spam, but they soon adapted their techniques. As a result, the PDF spam trend lasted for a few weeks, and then dropped off.

Figure 20: Percentage of PDF-based Spam Since July 2007
For just a few hours over the summer, PDF spam comprised 10-20 percent of all spam. Figure 21 shows the peak in activity.

The highest amounts of PDF-based spam were measured on August 2nd, 8th, and 12th. Since August 22nd, no PDF spams were seen, except for a minor PDF spam episode in October 2007. Additional statistics on PDF spam can be found at http://blogs.iss.net/archive/PDFSpam.html and http://blogs.iss.net/archive/PDFSpamv20.html.

MP3 spams also made a short appearance in 2007. Spam e-mail using this technique was observed in October, but only for a few days. The volume was much lower than the PDF spam activity over the summer. Interestingly, the MP3 spam source code was very similar to the PDF spam. Details on MP3 spam can be found at http://blogs.iss.net/archive/mp3-spam.html.
2008 will prove whether PDF and MP3 spam win further recognition or remain a short episode in spam history. The latter scenario is most likely because users are required to do much more (open a PDF or other document, in some cases even start an MP3 file or unpack a ZIP file) to make PDF and MP3 spam work compared with spam methods using text and/or images.

**Phishing – Overall Percentage of Spam**

The percentage of spam that is considered phishing rose to 1 percent by the end of 2007.

![Figure 22: Percentage of Spam that is Phishing](image-url)
Phishing – Country of Origin

The following map highlights countries of origin for phishing e-mails. The country of origin indicates the location of the server that sent the phishing e-mail. X-Force believes that most phishing e-mail is sent by bot networks. Since bots can be controlled from anywhere, the real attackers behind a phishing scam could reside in a different country than the location of the server sending the e-mail. The statistics presented more likely indicate the location of hosts infected with spam/phishing bots than the nationality of the person controlling the phishing scam.

Figure 23: Geographical Distribution of Phishing Senders
Phishing – Country of Origin for Embedded Web Links

The map shows where the Phishing URLs contained in phishing messages are hosted.

Distribution of Phishing URLs

- U.S.A. 29.3%
- South Korea 13.3%
- China 10.4%
- Thailand 8.0%
- Kazakhstan 6.0%
- Germany 3.2%
- Romania 2.8%
- United Kingdom 2.4%
- Turkey 2.2%
- Austria 2.2%

Figure 24: Geographical Distribution of Phishing URLs
Phishing – Most Popular Subject Lines

The most popular subject lines of phishing in the second term of 2007 appear below:

<table>
<thead>
<tr>
<th>Subject Line</th>
<th>Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;empty subject line&gt;</td>
<td>22.21%</td>
</tr>
<tr>
<td>Account Security Measures!</td>
<td>3.86%</td>
</tr>
<tr>
<td>Important Notice - E*TRADE FINANCIAL Corp</td>
<td>3.21%</td>
</tr>
<tr>
<td>Important notice!</td>
<td>2.01%</td>
</tr>
<tr>
<td>Volksbanken Raiffeisenbanken AG: 02/11/2007</td>
<td>1.94%</td>
</tr>
<tr>
<td>Security Measures!</td>
<td>1.82%</td>
</tr>
<tr>
<td>Citibank Account Security!</td>
<td>1.77%</td>
</tr>
<tr>
<td>Citibank Bank Notice!</td>
<td>1.75%</td>
</tr>
<tr>
<td>Citibank Account Security Measures!</td>
<td>1.74%</td>
</tr>
</tbody>
</table>
Web Content Trends

This section of the report summarizes the amount and distribution of “bad” Web content that is typically unwanted by businesses based on social principles and corporate policy. Unwanted or “bad” Internet content is associated with three types of Web sites: adult, social deviance and criminal. Table 6 lists the IBM ISS Web filter categories that correspond with these types of sites.

The Web filter categories are defined in detail at: http://www.iss.net/products/Proventia_Web_Filter/Database_Categories.html

<table>
<thead>
<tr>
<th>Web Site Type</th>
<th>Web Filter Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>Pornography</td>
</tr>
<tr>
<td></td>
<td>Erotic/Sex</td>
</tr>
<tr>
<td>Social Deviance</td>
<td>Political Extreme/Hate/Discrimination</td>
</tr>
<tr>
<td></td>
<td>Sects</td>
</tr>
<tr>
<td>Criminal</td>
<td>Anonymous Proxies</td>
</tr>
<tr>
<td></td>
<td>Computer Crime</td>
</tr>
<tr>
<td></td>
<td>Illegal Activities</td>
</tr>
<tr>
<td></td>
<td>Illegal Drugs</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
</tr>
<tr>
<td></td>
<td>Violence/Extreme</td>
</tr>
<tr>
<td></td>
<td>Warez/Hacking/Illegal Software</td>
</tr>
</tbody>
</table>

Table 6: Web Filter Categories Associated with Unwanted Web Content
Analysis

X-Force captured information about the content distribution of the Internet by counting the hosts classified into the various categories of the IBM ISS Web filter database.

Counting hosts is an accepted method for determining content distribution and provides the most realistic assessment. When using other methodologies — like counting Web pages/sub pages—results may differ.

The IBM ISS data center is constantly reviewing and analyzing new Web content data. Consider the following statistics related to the IBM ISS data center:

- It analyzes 150 million new Web pages and images each month.
- Since 1999, it has analyzed 7.8 billion Web pages and images.

The IBM ISS Web Filter Database has:

- 62 filter categories
- 95 million entries
- 100,000 new or updated entries added each day
Current Status of Unwanted Internet Content

Currently, nearly 9 percent of the Internet deals with unwanted content such as pornography, criminal content, etc.

Figure 25: Content Distribution of the Internet
Current Distribution of Adult Content

Figure 26: Geographical Distribution of Adult Content

- U.S.A. 48.2%
- Germany 18.1%
- Netherlands 6.3%
- South Korea 5.1%
- Canada 4.5%
- France 4.3%
- Russia 2.3%
- United Kingdom 1.7%
- China 1.1%
- Poland 0.9%
Current Distribution of Social Deviance Content

Distribution of Social Deviance Content

- U.S.A. 47.9%
- Germany 22.3%
- Netherlands 7.0%
- Canada 4.8%
- France 2.9%
- United Kingdom 2.5%
- China 2.4%
- Italy 2.1%
- Spain 0.8%
- Poland 0.8%

Figure 27: Geographical Distribution of Social Deviance Content
Current Distribution of Criminal Content

Distribution of Criminal Content

- U.S.A. 41.6%
- South Korea 11.6%
- Germany 11.2%
- Canada 6.6%
- Netherlands 5.3%
- Italy 4.6%
- France 3.5%
- China 3.0%
- United Kingdom 2.9%
- Russia 2.9%

Figure 28: Geographical Distribution of Criminal Content
Malcode Analysis

Malware volume continued to increase in 2007 and also became increasingly sophisticated. X-Force analyzed nearly 410,000 new malware samples throughout the year, a more than 30 percent increase over 2006.

Trojans comprise the largest category of malware, in contrast to 2006 when downloaders were the most common category (Trojans and worms followed closely behind). 2007 figures reveal that there are almost 60 percent more Trojans than worms (the closest category), and that downloaders have trailed off significantly from 2006 levels.

Continuing the trend in 2006, malcode is becoming less distinct in its categorization. Malcode continued to absorb or borrow new technologies being used by other successful malware. As X-Force continues to monitor malcode in 2008, the classic categories of virus, worm, spyware, backdoor, etc. are becoming largely irrelevant. Modern malware is now the digital equivalent of the Swiss Army knife, and 2007 data continues to support this.
Moving forward, X-Force's classification of malware should be based on the most dominant features of the threat. Malware analyzed in 2007 is divided into the following categories:

- **Worm** – Self-propagates over a network.
- **Backdoor** – Provides functionality for an attacker to connect back to the victim's system without supplying authorized login credentials.
- **Virus** – Infects a host and does some form of damage to the host, but cannot self-propagate.
- **Password Stealer (PWS)** – Designed to steal login credentials for specific online applications and is a key component in identity theft attacks.
- **Downloader** – Low-profile malware that exists to install itself so that it can then download and install a more sophisticated or updated malware agent.
- **Keylogger** – Captures all key strokes and stores the information away for later retrieval by the attacker.
- **Dialer** – Uses modem connections to either dial back to the attacker or causes the victim to use primary rate dialing numbers when making connections.
- **Trojan** – Appears to be a legitimate file before installing itself and often with rootkit functionality.
- **Miscellaneous** – All other malware not falling into one of the above primary categories.
Malcode Categorization

The malware samples collected by X-Force during 2007 fall into a number of categories. Trojans make up the largest class of malware in 2007 as opposed to downloaders, which were the largest category in 2006.

Figure 29: 2007 Malcode Characterization Breakdown
Malcode Categorization Trends

Other than a spike at the end of the year, mainly caused by Net-Worm.Win32. Allaple, worm activity remained relatively consistent throughout 2007. This reflects smaller outbreaks of specific malware families and, thus, shorter and more contained serial variant attacks from worms. For example, Nuwar, the original Storm worm and propagator of Peacomm, was easily detectable. Hence, the propagation technique shifted to mass spamming. In contrast, X-Force has observed a consistent increase in Trojans as the dominant malcode threat, which comes as no surprise given the focus on using Trojans for sustained targeted attacks.
Malcode Additions

The following chart depicts the absolute volume of new malware identified by X-Force for 2007. Of particular note is the shift away from mass-mailing worms to sophisticated, targeted Trojan attacks with rootkits and other blended threats.

Figure 31: 2007 Malcode Additions
### Top 10 Most Common Malware

#### Top 10 2007 Malcode
- Trojan.W32.Agent
- Net-Worm.Win32.Allaple
- Trojan-Downloader.Win32.Small
- Trojan-Downloader.Win32.Zlob
- Trojan-Downloader.Win32.Agent
- Email-Worm.Win32.Zhelatin
- Virus.Win32.Virut
- Email-Worm.Win32.Mixor
- Trojan-Spy.Win32.BZub
- Trojan-PSW.Win32.Delf

#### Top 10 2007 Rootkits
- Rootkit.Win32.Agent
- Rootkit.Win32.Vanti
- Rootkit.Evilotus
- Rootkit.Win32.Delf
- Trojan.NTRootkit
- Rootkit.Win32.Podnuha
- Rootkit.Win32.Fuzen
- Rootkit.Win32.Ntrtk
- Rootkit.Win32.Small
- Rootkit.Win32.HideProc

#### Top 10 2007 Backdoors
- Backdoor.Win32.Hupigon
- Backdoor.Win32.Agent
- Backdoor.Win32.Delf
- Backdoor.Win32.Rbot
- Backdoor.Win32.Bifrose
- Backdoor.IRC.Zapchast
- Backdoor.Win32.Small
- Backdoor.Win32.SdBot
- Backdoor.Win32.VB
- Backdoor.Win32.IRCBot

#### Top 10 2007 Trojans
- Trojan.Win32.Agent
- Trojan-Spy.Win32.BZub
- Trojan.Win32.Delf
- Trojan.Win32.Smal
- Trojan-Spy.Win32.Bancos
- Trojan-Spy.Win32.Perfloger
- Trojan-Downloader.Win32.IstBar
- Trojan-Clicker.Win32.Agent
## Top 2007 Worms

- Net-Worm.Win32.Allaple
- Email-Worm.Win32.Zhelatin
- Email-Worm.Win32.Mixor
- Worm.Win32.Viking
- Email-Worm.Win32.NetSky
- Worm.W32.Agent
- Email-Worm.Win32.Warezov
- Email-Worm.Win32.Bagle
- Email-Worm.Win32.Scano
- Worm.W32.Delf

## Top 2007 Viruses

- Virus.Win32.Virut
- Virus.Win32.Agent
- Virus.Win32.Parite
- Virus.Win32.Delf
- Virus.Win32.Kies
- Virus.Win32.AutoRun
- Virus.Win32.Small
- Virus.Win32.Sality
- Virus.Boot
- Virus.DOS.Trivial

## Top 2007 Password Stealers

- Trojan-PSW.Win32.OnlineGames
- Trojan-PSW.Win32.Delf
- Trojan-PSW.Win32.Agent
- Trojan-PSW.Win32.Nilage
- Trojan-PSW.Win32.Sinowal
- Trojan-PSW.Win32.QQShou
- Trojan-Spy.Win32.ProAgent
- Trojan-Spy.Win32.Bancos
- Trojan-Spy.Win32.BZub
- Trojan-PSW.Win32.QQPass

## Top 2007 Downloaders

- Trojan-Downloader.Win32.Small
- Trojan-Downloader.Win32.Zlob
- Trojan-Downloader.Win32.Agent
- Trojan-Downloader.Win32.Banload
- Trojan-Downloader.Win32.Delf
- Trojan-Downloader.Win32.Tibs
- Trojan-Downloader.Win32.Obfuscated
- Trojan-Downloader.Win32.Adload
- Trojan-Downloader.Win32.VB
- Trojan-Downloader.Win32.Tiny
### Top 10 2007 Mass Mailers

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email-Worm.Win32.Mydoom.m</td>
<td></td>
</tr>
<tr>
<td>Email-Worm.Win32.NetSky.q</td>
<td></td>
</tr>
<tr>
<td>Email-Worm.Win32.NetSky.t</td>
<td></td>
</tr>
<tr>
<td>Trojan-Dropper.Win32.Agent.bzp</td>
<td></td>
</tr>
<tr>
<td>Password-protected-EXE</td>
<td></td>
</tr>
<tr>
<td>Email-Worm.Win32.Nyxem.e</td>
<td></td>
</tr>
<tr>
<td>Email-Worm.Win32.NetSky.y</td>
<td></td>
</tr>
<tr>
<td>Trojan-Spy.Win32.KeyLogger rp</td>
<td></td>
</tr>
<tr>
<td>Email-Worm.Win32.Zafi.d</td>
<td></td>
</tr>
<tr>
<td>Email-Worm.Win32.Bagle.gt</td>
<td></td>
</tr>
</tbody>
</table>

### About IBM ISS

IBM ISS is the trusted security expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the X-Force team – a world authority in vulnerability and threat research. For more information about IBM ISS, please contact your IBM representative or IBM Business Partner. You may also call 1 800 776-2362 or visit [ibm.com/services/us/iss](http://ibm.com/services/us/iss).