

**IBM Internet Security Systems**  
Ahead of the threat.™



## **Cyber Attacks On The Rise: IBM 2007 Midyear Report**

**August 2007**

## Table of Contents

<b>Management Overview</b>	<b>1</b>
2007 First Half Highlights	1
<b>Vulnerability Analysis</b>	<b>3</b>
First Half 2007 Vulnerability Count	4
Vulnerabilities During 1H 1997-2007	5
Vulnerabilities per Month	5
Vulnerabilities per Week	6
Vulnerabilities by Day of the Week	7
Weekend vs. Weekday	8
Classic High/Medium/Low Vulnerability Impact Breakdown	9
Common Vulnerability Scoring System (CVSS) Breakdown	10
Top Vulnerable Vendors	12
Remote vs. Local Exploitation	14
Consequences of Exploitation	14
<b>Spam and Phishing Analysis</b>	<b>16</b>
Basics about the determination of geographical distributions	17
From which countries does spam originate?	17
Where are the Web pages contained in spam messages hosted?	17
What is the average byte size of spam messages?	18
What are the most popular subject lines of spam?	18
What amount of spam exhibited a Reply-To: different from the From: message data?	19
What amount of spam had a Return-Path: different from the From: message data?	19
What is the language distribution of spam?	20
How much spam is image-based?	20
How many e-mail servers did spam and phishing pass through before reaching its destination?	21
Where do phishing emails come from?	21
Where are Web pages contained in phishing e-mails hosted?	22
What are the most popular subject lines of phishing?	22
Which companies are the most targeted by phishing attacks?	23
<b>Web Content Trends</b>	<b>23</b>
Analysis	23
Current Status of Unwanted Internet Content	24
Current Distribution of Adult Content	25
Current Distribution of Social Deviance Content	25
Current Distribution of Criminal Content	25
<b>Malcode Analysis</b>	<b>26</b>
Malcode Categorization	27
Malcode Categorization Trends	28
Top 10 Most Common Malware	28
<b>Web Browser Exploitation Trends</b>	<b>31</b>
Most Popular Exploits	32
Obfuscation and Encryption	32
Windows-based Web Browser Wrap-up	33

## **Management Overview**

So far 2007 has been a very interesting and unexpected year on many security fronts. The IBM Internet Security Systems™ X-Force® research and development team discovered, analyzed and recorded new vulnerabilities and the status of varying threats throughout the first six months of this year. The data has been compiled in this report.

## **2007 First Half Highlights**

### **Vulnerabilities**

- There were a total of 3,273 vulnerabilities\* entered in the first half of 2007, a 3.3 percent decrease over the first half of 2006. This is the first time that vulnerability disclosure numbers have decreased in the first half of the year in the history of the X-Force database.
- January was the busiest month of the first half of the year with 600 vulnerabilities.
- Week three (January 15-21) was the busiest week of the first half of 2007 for new vulnerabilities, with 149 new vulnerabilities added.
- The most popular day for vulnerability disclosures was Tuesday, with disclosure of 25 percent of all vulnerabilities in the first half of 2007. This is up from 24.2 percent in 2006.
- Weekend disclosure of vulnerabilities for the first half of 2007 remained steady against 2006 figures – 17.4 percent in 2007 compared to 17.6 percent in 2006.
- Two percent of vulnerabilities under the Common Vulnerability Scoring System (CVSS) were evaluated as being critical impact vulnerabilities with a score of 10.
- The top three vulnerable vendors in the first half of 2007 are Microsoft, Apple and Oracle.
- The top five vulnerable vendors accounted for 12.6 percent of all vulnerabilities.
- 21 percent of the vulnerabilities identified within the top five vulnerable vendors' products were unpatched at the end of the first half of 2007.

- 90 percent of all vulnerabilities uncovered in the first half of 2007 can be exploited remotely.
- More than half (51.6 percent) of the vulnerabilities in the first half of 2007 would allow an attacker to gain access to the host after successful exploitation.

\*A vulnerability is defined as any computer-related exposure or configuration setting that may result in a weakening or breakdown of the confidentiality, integrity or accessibility of the computing system.

#### **Spam and Phishing**

- The U.S., Poland and Russia are the three largest originators of spam worldwide, with the U.S. accounting for one eighth of worldwide spam.
- The U.S. continues to lead the world as the final Web destination for products promoted through spam e-mail messages. The U.S. hosts more than one third of spam-related Web sites.
- For the first time, spam message size decreased in the first half of 2007 rather than continuing on a linear growth pattern. This decrease corresponds with the decrease in image-based spam.
- Europe now accounts for the largest source of phishing e-mail, with Spain counting for 17.9 percent of the world-wide volume alone.
- Almost half of all fraudulent phishing Web sites are hosted within the U.S.

#### **Web Content**

- "Unwanted" content decreased to 10 percent in the first half of 2007—down from 12.5 percent in 2006.
- Web sites that host pornographic or sex-related content account for 9.9 percent of the Internet.
- The U.S. continues to be the top hosting country for "unwanted" content such as violence and crime, pornography and sex, computer crime, and illegal drugs. This continues to mirror the observations from 2006.

#### Malcode

- The largest threat category of malware so far in 2007 is Trojans – 61,161 varieties accounting for 28 percent of all malware.
- The most frequently occurring malware on the Internet was Trojan.Win32.Agent – 26,573 varieties in the first half of 2007 accounting for 43 percent of all Trojans.
- The most common worm in the first half of 2007 was Email-Worm.Win32.Mixor – 12,120 varieties. The most successful family of network propagating worm was W32.Mydoom.M@mm.

#### Web Browser Exploitation

- The most popular exploit used on the Internet to infect Web browsers with malware was Visual Studio WMI Object Broker ActiveX.
- Approximately 80 percent of Web-based exploits are obfuscated in some way, with JavaScript being the most common obfuscation vector.

### **Vulnerability Analysis**

The IBM Internet Security Systems (ISS) X-Force has been cataloguing, analyzing and researching vulnerability disclosures since 1997. With more than 33,000 security vulnerabilities catalogued, it maintains the largest and most authoritative vulnerability database in the world. This unique database enables X-Force researchers to understand the dynamics that make up vulnerability discovery and disclosure.

In fact, X-Force researchers have analyzed many more 'disclosures' than the 33,000+ recorded in the X-Force Vulnerability Database. On average each year, a large percentage of public vulnerability disclosures are incorrect and are not recorded in the database. These disclosures are rejected because they are re-discoveries of existing and older vulnerabilities. Or, after careful research, the X-Force decides they are merely software bugs with no vulnerability context and closer to audit-level notifications.

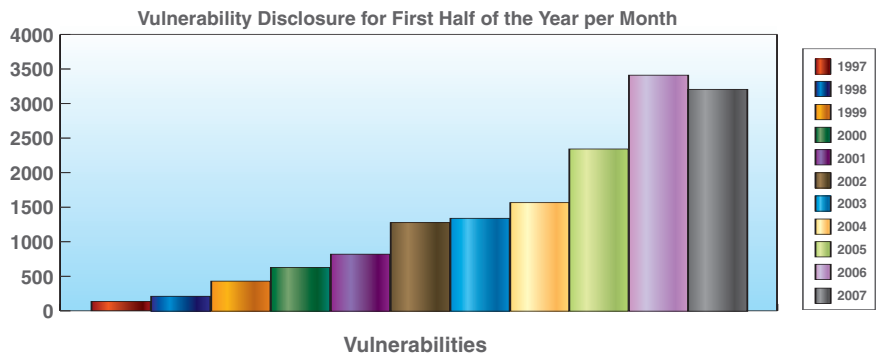
The next section covers the following areas of analysis:

- First half 2007 vulnerability count
- Vulnerabilities per month
- Vulnerabilities per week
- Vulnerabilities by day of week
- Weekday vs. weekend vulnerability disclosures
- Classic high/medium/low vulnerability impact breakdown
- Common Vulnerability Scoring System (CVSS) breakdown
- Top 10 vulnerable vendors
- Remote vs. local exploitation
- Consequences of exploitation

### **First Half 2007 Vulnerability Count**

During the first half of 2007, 3,273 vulnerabilities were disclosed, a 3.3 percent decrease over the first half of 2006. This is the first time the X-Force has observed a decrease in vulnerability disclosure in the ten-year history of its database.

A comparison of vulnerabilities discovered during the first half of the year over the past 10 years can be observed in the following graph:



**Vulnerabilities During 1H 1997-2007**

Year	Vulnerabilities	Avg per month	Avg per week	% increase year over year
1997	106	18	4	
1998	142	24	5	34.0%
1999	353	59	14	148.6%
2000	601	100	23	70.3%
2001	802	134	31	33.4%
2002	1292	215	50	61.1%
2003	1387	231	53	7.4%
2004	1513	252	58	9.1%
2005	2350	392	90	55.3%
2006	3384	564	130	44.0%
2007	3273	546	126	-3.3%

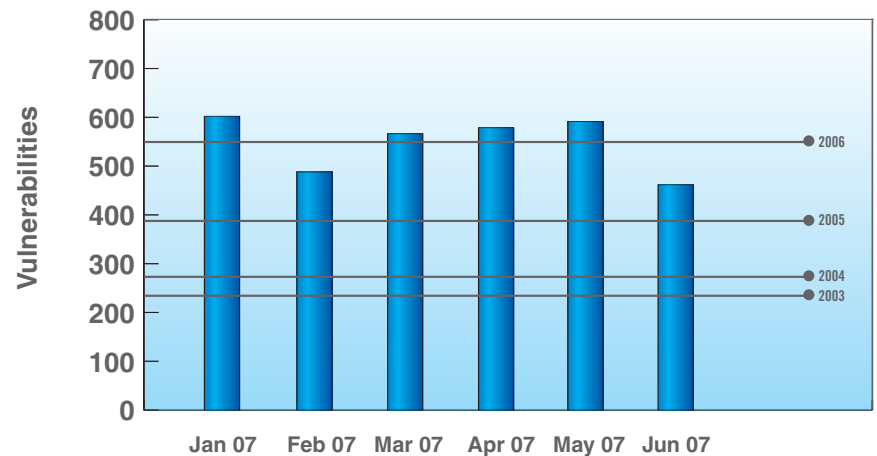
**Vulnerabilities per Month**

The average number of vulnerabilities per month increased steadily from 2000 through 2006, but in the beginning half of 2007, the X-Force started to observe a slight decrease.

The following chart shows the number of new vulnerabilities researched by the X-Force during the first six months of 2007. The black lines running across the chart represent the average number of vulnerabilities released during the first half of 2003, 2004, 2005 and 2006. In February and in June 2007, the vulnerability disclosure rate fell below the average vulnerability disclosure rate in 2006.

Month	Count
Jan-07	600
Feb-07	480
Mar-07	569
Apr-07	579
May-07	591
Jun-07	454

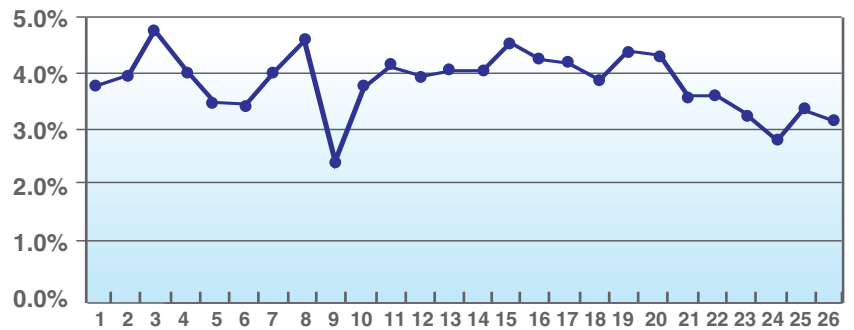
**Vulnerabilities per Month During 1H 2007**



### Vulnerabilities per Week

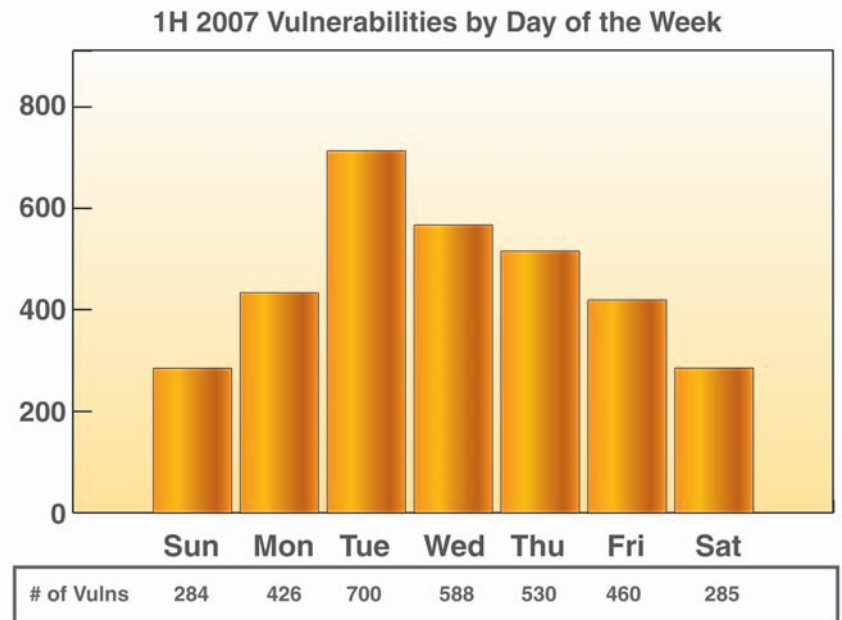
During the first half of 2007, the busiest week for vulnerability disclosure was January 15 through 21 – the third week of the calendar year. Historically, the week prior to Christmas has been the busiest week for vulnerability disclosure. In 2006, the highest number of vulnerability disclosures occurred the week before Thanksgiving. The graph below plots vulnerability disclosure during the first 26 weeks of 2007. Only time will tell if the coming weeks in 2007 will produce greater numbers of vulnerabilities.

Vulnerability Disclosure per week 1H 2007



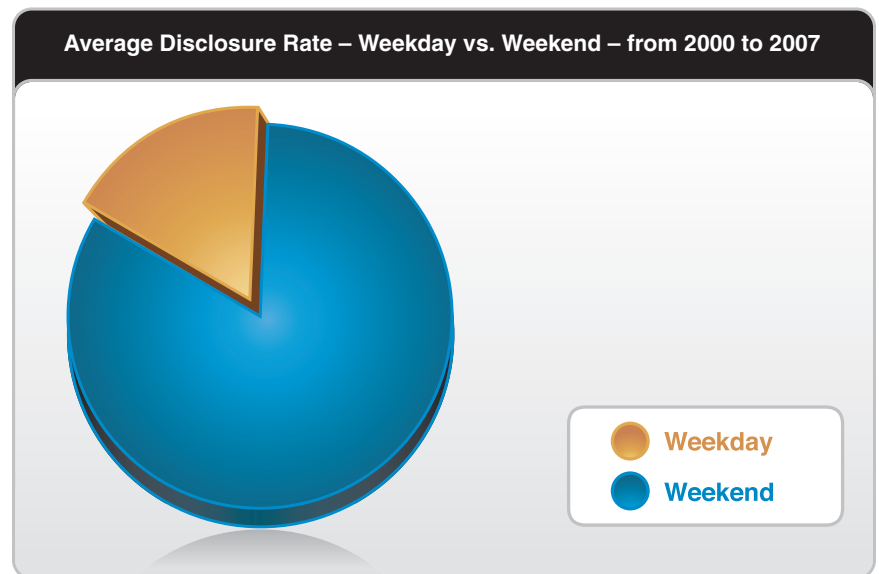
### **Vulnerabilities by Day of the Week**

In the first half of 2007, the popularity of Tuesday disclosure continued from the initial increase observed by the X-Force in 2006. Microsoft regularly discloses its vulnerabilities on the second Tuesday of each month, and more vendors seem to be adopting Microsoft's strategy for regular, planned disclosures. In 2006, the slowest day of the week for vulnerability disclosure was Friday. So far in 2007, the day of the week with the least amount of vulnerability disclosures is Sunday.



**Weekend vs. Weekday**

In 2006, the X-Force noticed that more vulnerabilities were being disclosed on the weekend than in prior years. In the first half of 2007, that trend continues with 17.4 percent of vulnerabilities being disclosed on a weekend, down only slightly from the 2006 average of 17.6 percent.

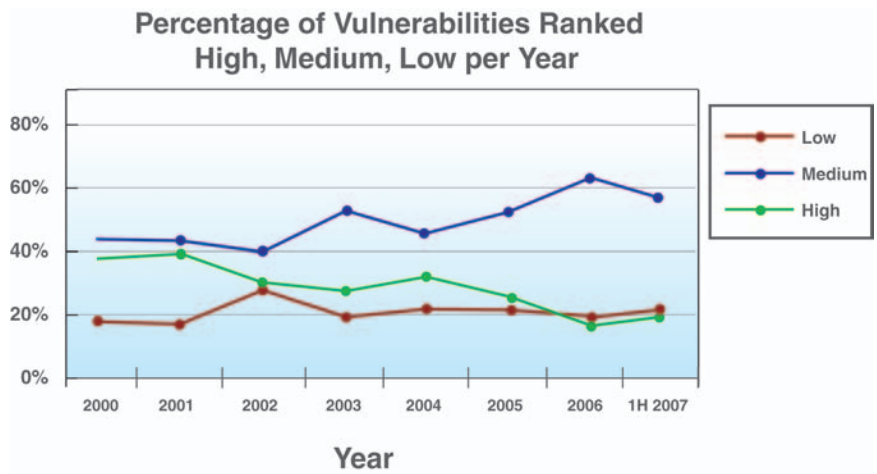


2000	2001	2002	2003	2004	2005	2006
10.1%	10.7%	14.3%	15.9%	10.4%	8.1%	17.6%
89.9%	89.3%	85.7%	84.1%	89.6%	91.9%	82.4%

1H 2007	Avg.
17.4%	13.6%
82.6%	86.4%

### Classic High/Medium/Low Vulnerability Impact Breakdown

Each vulnerability documented by the X-Force is analyzed and its exploitation impact is assessed. By examining the breakdown of vulnerability disclosures since 2000, the X-Force has noticed that high impact vulnerabilities have been decreasing over time. However, the first 26 weeks of 2007 has shown a slight up-tick in the number of high impact vulnerabilities – from 16 percent in 2006 to 21 percent in 2007.



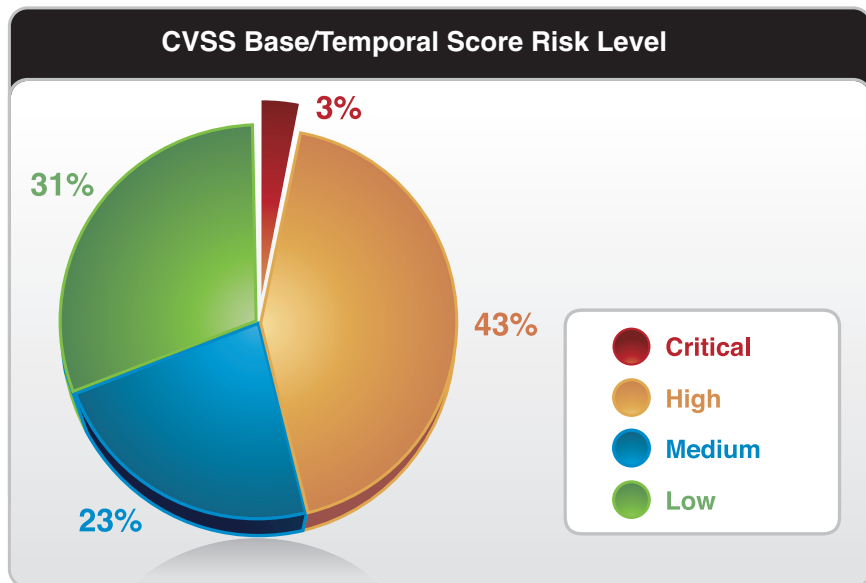
The X-Force defines high, medium and low impact vulnerabilities according to the following criteria:

- **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 potentially 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 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 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. The temporal metrics include vulnerability characteristics that can change over time, and include the exploitability, remediation level and report confidence.

The following graphs represent the risk level associated with the CVSS score, according to the following chart:



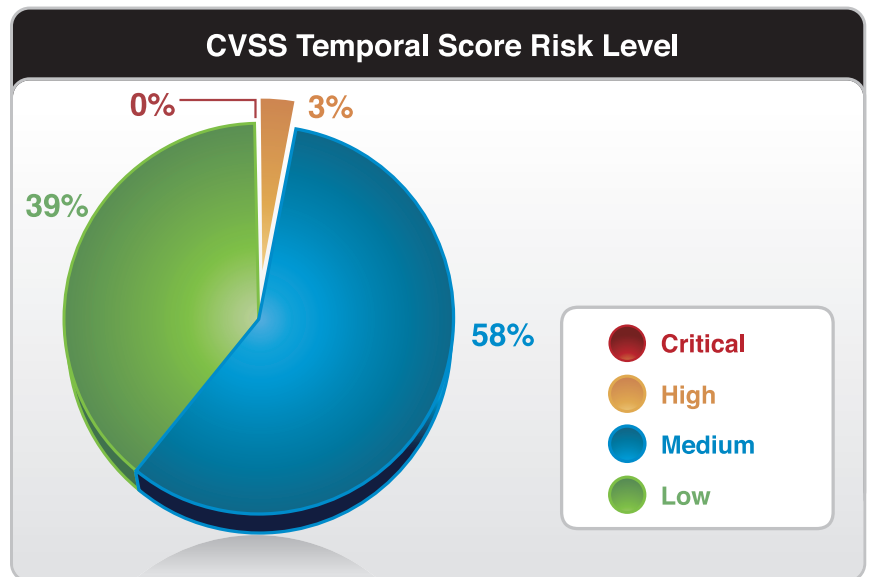
CVSS Base/Temporal Score	Risk Level
10.0	Critical
7.0 – 9.9	High
4.0 – 6.9	Medium
0.0 – 3.9	Low

Vulnerabilities identified as “critical” 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 the first half of 2007, two percent of all vulnerabilities received a “critical” rating. IBM ISS began scoring all vulnerabilities against the CVSS standard in July 2006. During the 2006 timeframe, three percent of all vulnerabilities entered were considered “critical.”

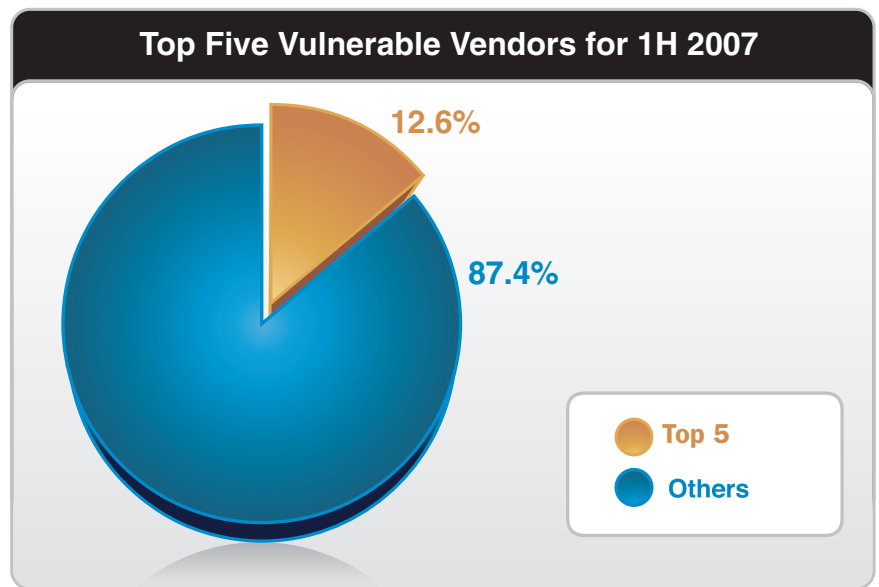
The temporal score provides more information about the vulnerability, such as patch, exploit and confidence information. The temporal score starts with the base score and adjusts it depending on whether a patch and/or exploit exists, and whether the vendor has confirmed the vulnerability.

The graph below shows the percentage of high, medium and low impact vulnerabilities in the first half of 2007 according to CVSS temporal scores.



### Top Vulnerable Vendors

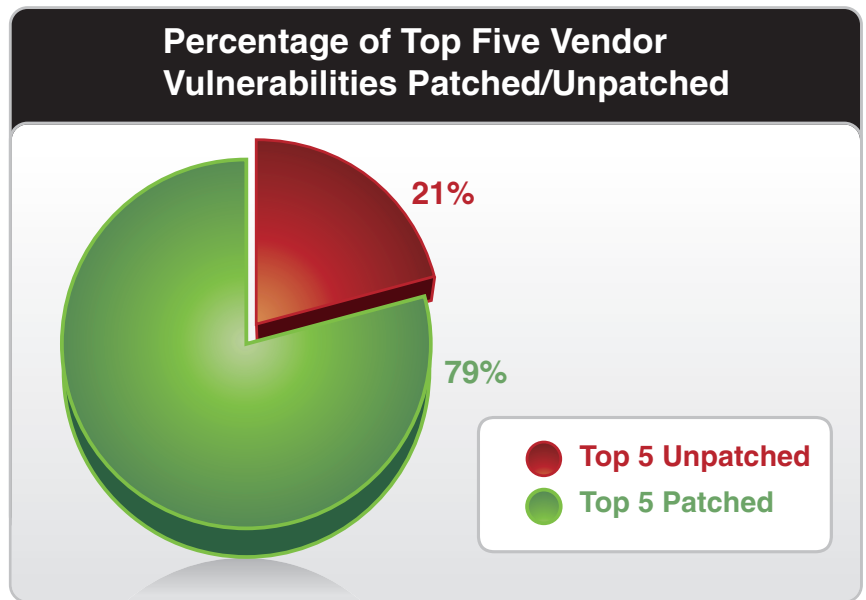
In the first half of 2007, the top five vulnerable vendors accounted for 12.6 percent of all disclosed vulnerabilities – or 411 of the 3,273 vulnerabilities disclosed.



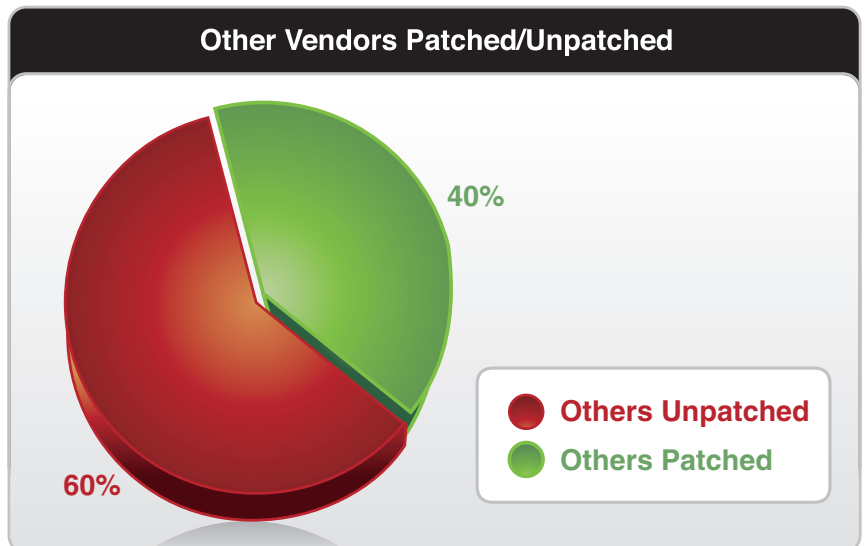
The following chart displays the top 10 vendors and their percentage of the total number of vulnerabilities publicly disclosed in the first half of 2007.

Vendor	Percentage of 1H 2007 Vulnerabilities
Microsoft	4.2%
Apple	3.0%
Oracle	2.0%
Cisco	1.9%
Sun	1.5%
IBM	1.3%
Mozilla	1.3%
XOOPS	1.2%
BEA	1.1%
Linux kernel	0.9%

According to the chart below, 21 percent of the vulnerabilities disclosed by the top five vulnerable vendors in the first half of 2007 remain unpatched. This represents an increase from the first half of 2006 during which only 14 percent of the top vendors' vulnerabilities remained unpatched.

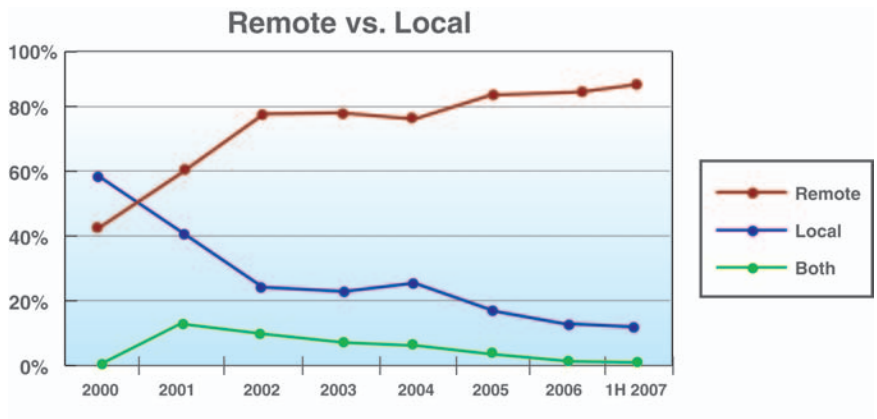


While it may seem concerning that the top five vulnerable vendors still have un-patched vulnerabilities, 60 percent of vulnerabilities from all other vendors remain un-patched in the first half of 2007.



### Remote vs. Local Exploitation

Vulnerabilities subject to remote exploitation are particularly important. The graph below depicts remotely-exploitable vulnerabilities – those capable of being exploited over the network – compared with local exploitation occurring only after logging in to the local host from the desktop.



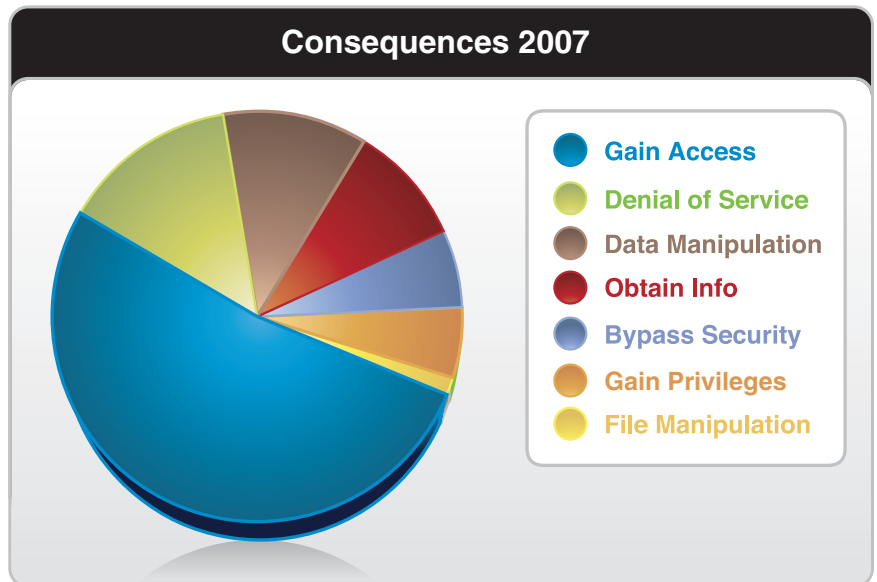
Vulnerabilities subject to remote exploitation far outweigh those vulnerable to local exploitation. So far in 2007, an astounding 90 percent of all vulnerabilities allow remote exploitation, up from 88 percent in 2006.

### Consequences of Exploitation

As part of its analysis of each vulnerability, the X-Force records the primary consequence of exploitation. The consequences are defined as the most common effect of exploitation and are divided into nine categories described below:

- **Bypass Security** – An attacker can bypass security restrictions such as a firewall, proxy, IDS system or a virus scanner.
- **Data Manipulation** – An attacker is able to manipulate data stored or used by the host associated with the service or application.
- **Denial of Service** – An attacker can crash or disrupt a service or system to take down a network.
- **File Manipulation** – An attacker can create, delete, read, modify or overwrite files.

- **Gain Access** – An attacker can obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system.
- **Gain Privileges** – Privileges can be gained on the local system only.
- **Obtain Information** – An attacker can obtain information such as file and path names, source code, passwords or server configuration details.
- **Informational** – Service name disclosure.
- **Other**



Gain Access	Denial of Service	Data Manip.	Obtain Info	Bypass Security	Gain Priv.	File Manip.
51.6%	13.4%	11.2%	9.3%	6.0%	5.7%	1.1%

The trend from 2006 continues, as the number one consequence of exploitation remains Gain Access, with a total of 51.6 percent of vulnerabilities.

## **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, the X-Force has identified numerous advances in the spam and phishing technologies used by attackers.

On an average day, IBM ISS analyzes more than 150,000 unique spam messages – a “unique” spam message being one that is at least 10 percent different than any other spam message ever received.

This section includes the following analysis:

- 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 amount of spam exhibited a Reply-To: different from the From: message data?
- What amount of spam had a Return-Path: different from the From: message data?
- What is the language distribution of spam?
- How much spam is image-based?
- How many e-mail servers did spam and phishing pass through before reaching its destination?
- Where do phishing e-mails come from?
- Where are the Web pages contained in phishing e-mails hosted?
- What are the most popular subject lines of phishing?
- Which companies are the most commonly targeted by phishing attacks?

### Basics about the determination of geographical distributions

The following statistics use the IP-to-Country Database provided by WebHosting.Info (<http://www.webhosting.info>), available from <http://ip-to-country.webhosting.info>.

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

### From which countries does spam originate?

The following map shows the origination point for spam globally and the U.S. accounting for more than one-eighth of worldwide spam.

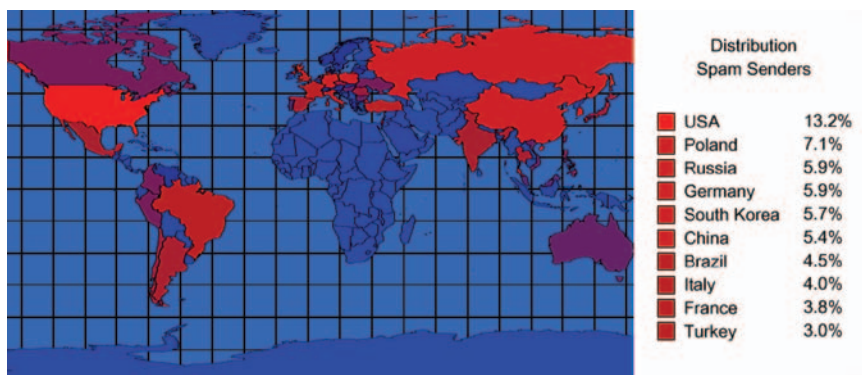


Figure 1 – Geographical distribution of spam senders

### Where are the Web pages contained in spam messages hosted?

The map shows where the spam URLs are hosted.

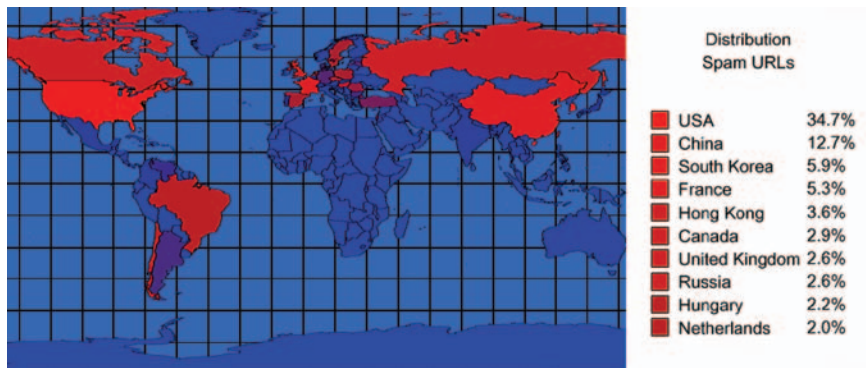


Figure 2 – Geographical distribution of spam URLs

**What is the average byte size of spam messages?**

Spam messages grew in size in 2005 and 2006, increasing from an average of 6 kilobytes to more than 10 kilobytes. But in the second quarter of 2007, the size declined to the level of mid-2006.

This trend correlates closely with the decrease in image-based spam (see below).

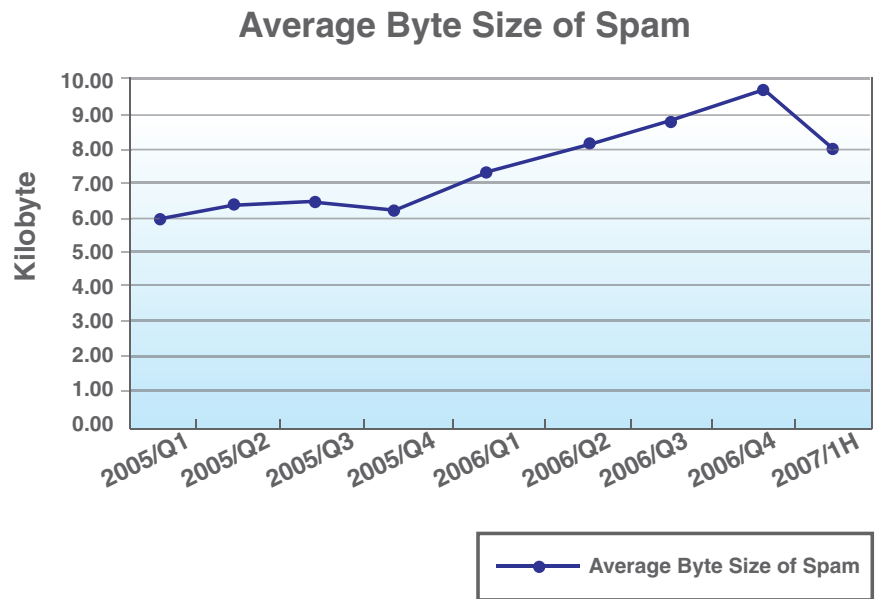


Figure 3 – Average byte size of spam since 2005

**What are the most popular subject lines of spam?**

The most popular subject lines of spam in the first half of 2007 appear below:

Subject Line	Quota
Re:	2.21%
<empty subject line>	0.83%
FDA approved on-line pharmacies	0.47%
300% Bonus für Ihre erste Einzahlung!	0.46%
Hi	0.43%
Play and make big money.	0.39%
Bis 1000 Euro Frei!	0.26%
How does Cialis work?	0.21%
RX from Canada	0.18%
Can you imagine that you are healthy?	0.17%

**What amount of spam exhibited a Reply-To: different from the From: message data?**

The usage of Reply-To: data differing from From: data remains low, but in the last month it rose significantly from below one percent to more than three percent.

**Amount of spam with REPLY-TO: different from FROM:**

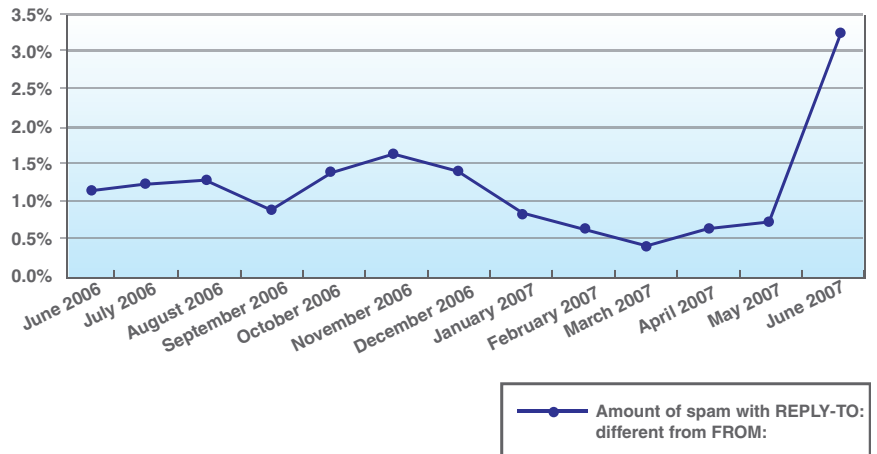


Figure 4 – Amount of spam with Reply-To: different from From:

**What amount of spam had a Return-Path: different from the From: message data?**

The usage of Return-Path: data differing from From: data was declining markedly in the second half of 2006, but slightly increased in the first half of 2007.

**Amount of spam with RETURN-PATH: different from FROM:**

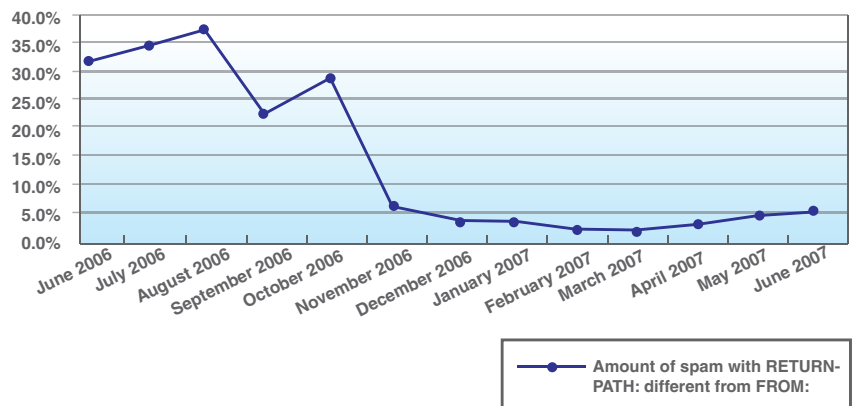


Figure 5 – Amount of spam with Return-Path: different from From:

### What is the language distribution of spam?

The top five languages used in spam messages in the first half of 2007 appear below:

Language	Quota
English	86.35%
German	6.74%
Russian	2.93%
Japanese	1.14%
Spanish	0.45%

### How much spam is image-based?

At least since mid-2005, image-based spam has been one of the biggest anti-spam challenges. However, in the second quarter of 2007, the percentage of image-based spam declined to the level of mid-2006.

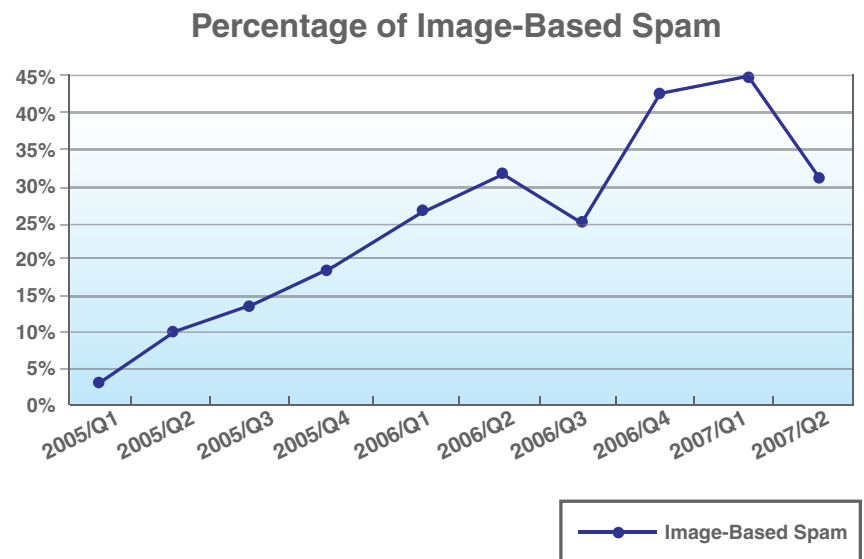


Figure 6 – Percentage of image-based spam since 2005

**How many e-mail servers did spam and phishing pass through before reaching its destination?**

The number of e-mail servers spam and phishing pass through is slightly increasing. Since most phishing messages are generated by phishing kits and sent via botnets, the botnet agents mostly send spam messages directly to the recipient – which results in a lower number of e-mail servers phishing e-mails are passed through in comparison with the number that spam e-mails pass through.

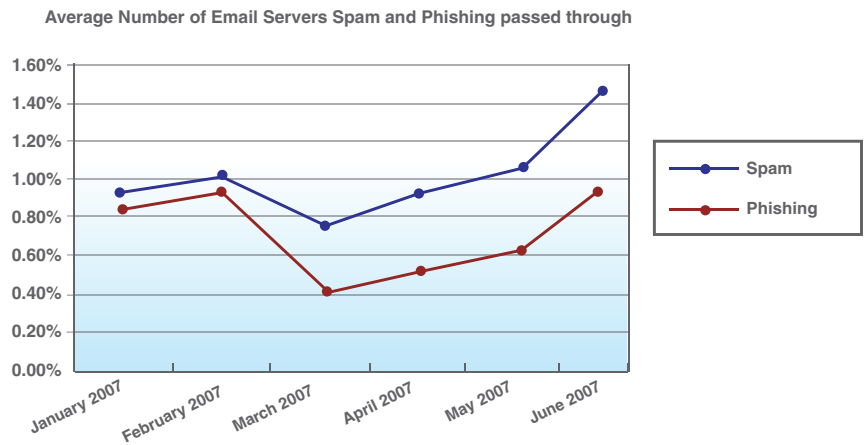


Figure 7 – Average number of e-mail servers spam and phishing are passed through

**Where do phishing emails come from?**

The following map highlights countries of origin for phishing e-mails.

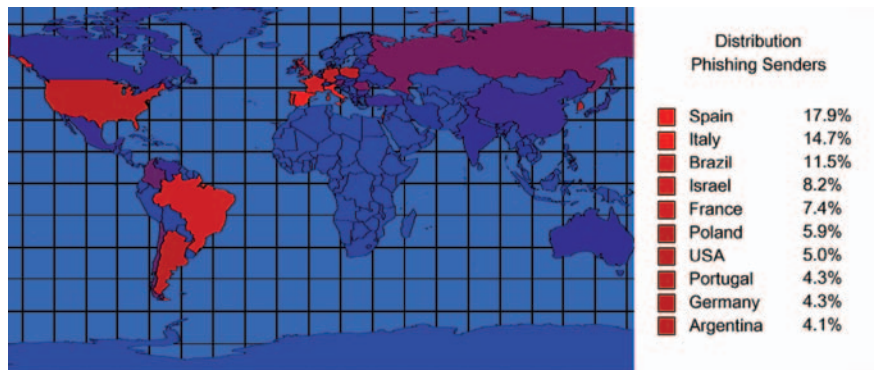


Figure 8: Geographical distribution of phishing senders

### Where are Web pages contained in phishing e-mails hosted?

The map shows where the phishing URLs are hosted.

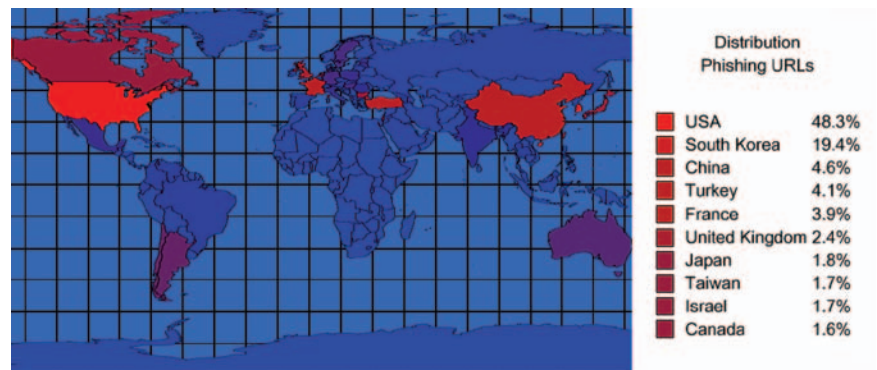


Figure 9 – Geographical distribution of phishing URLs

### What are the most popular subject lines of phishing?

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

Subject Line	Quota
<empty subject line>	1.56%
Notification.	1.14%
Notice.	0.34%
Account Security Measures!	0.23%
obligatorisch zu lesen	0.17%
amtlicher Bescheid	0.16%
Internet-Banking	0.16%
eiliger Bescheid	0.16%
Wichtige Information	0.16%
Achtung	0.16%

### **Which companies are the most targeted by phishing attacks?**

The following companies (in alphabetical order) were the top 20 phishing targets in the first half of 2007:

- Bank of The West
- Bank of America
- Branch Banking & Trust
- Chase
- Citibank
- Deutsche Bank
- E\*Trade Financial
- Ebay
- Fifth Third Bank
- National City
- North Fork Bank
- PNC Bank
- PayPal
- Postbank
- Regions Bank
- Sparkasse
- U.S. Bank
- Volksbanken Raiffeisenbanken
- Washington Mutual
- Western Union

### **Web Content Trends**

This section gives an overview of the percentage and distribution of “bad” Web filter categories around adult content, criminal content and other unwanted or questionable Web categories.

- Current status of unwanted Internet content
- Current distribution of adult content
- Current distribution of social deviance content
- Current distribution of criminal content

### **Analysis**

The content distribution of the Internet and its growth were determined by counting the hosts classified in the corresponding Web filter categories of the IBM ISS Web Filter Database.

Counting hosts is the most common method to determine content distribution of the Internet and provides the most realistic overview. When using another methodology (like counting Web pages/sub pages), other results may arise.

The IBM ISS Web Filter Database is constantly reviewing and analyzing new Web content. Consider the following IBM ISS Web Filter Database statistics:

- Analyzes 150 million new Web pages and images each month.
- Has analyzed 6.9 billion Web pages and images since 1999.

The IBM ISS Web Filter Database maintains the following characteristics:

- 62 filter categories
- 80 million entries
- 100,000 new or updated entries added each day

### **Current Status of Unwanted Internet Content**

Currently, more than 10 percent of the Internet deals with unwanted content such as pornography, crime, adult or socially deviant content (sex, drugs, piracy, etc.) or crime-oriented information or endeavours.

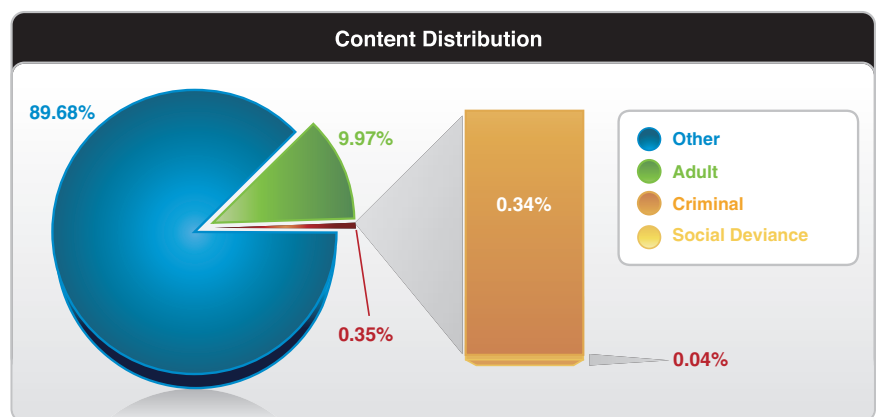


Figure 10 – Content distribution of the Internet

**Current Distribution of Adult Content**

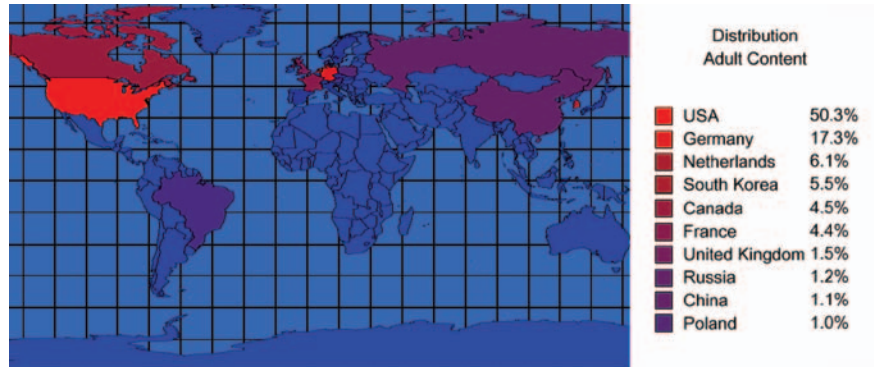


Figure 11 – Geographical distribution of adult content

**Current Distribution of Social Deviance Content**

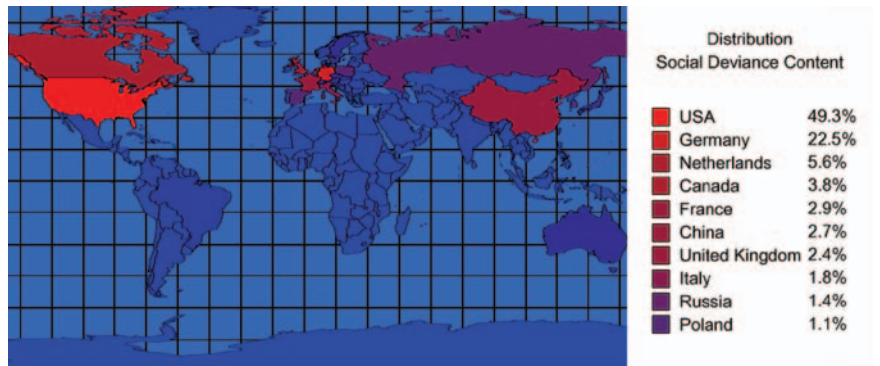


Figure 12 – Geographical distribution of social deviance content

**Current Distribution of Criminal Content**

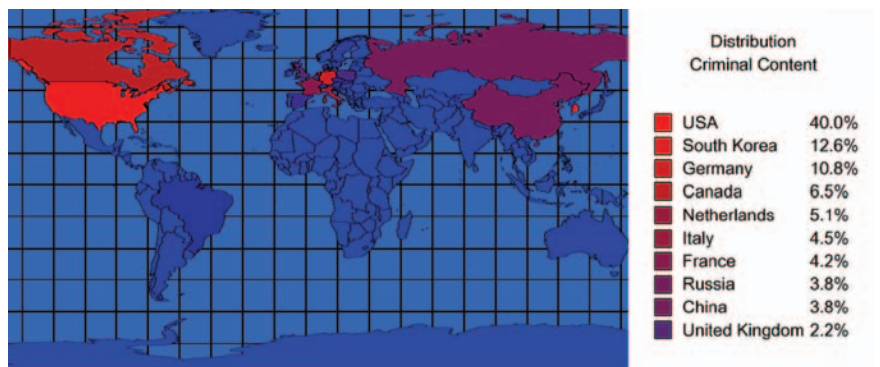


Figure 13 – Geographical distribution of criminal content

## **Malcode Analysis**

So far 2007 has been a record year for malware, with new records in volume and sophistication occurring on a monthly basis. The X-Force has identified, studied and analyzed more than 210,000 new malware samples throughout the year. The 1H 2007 figures have already increased in volume over the total number of malware samples observed in all twelve months of 2006.

Trojans comprise the most voluminous category of malware so far, in contrast to 2006 when downloaders were the most common category (Trojans and worms followed closely behind). 2007 figures reveal that the amount of Trojans is nearly double the next closest category, worms, 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 the X-Force continues to monitor malcode in 2007, the classic categories of virus, worm, spyware, backdoor, etc. are largely irrelevant. Modern malware is now the digital equivalent of the Swiss Army knife, and 2007 data continues to support this.

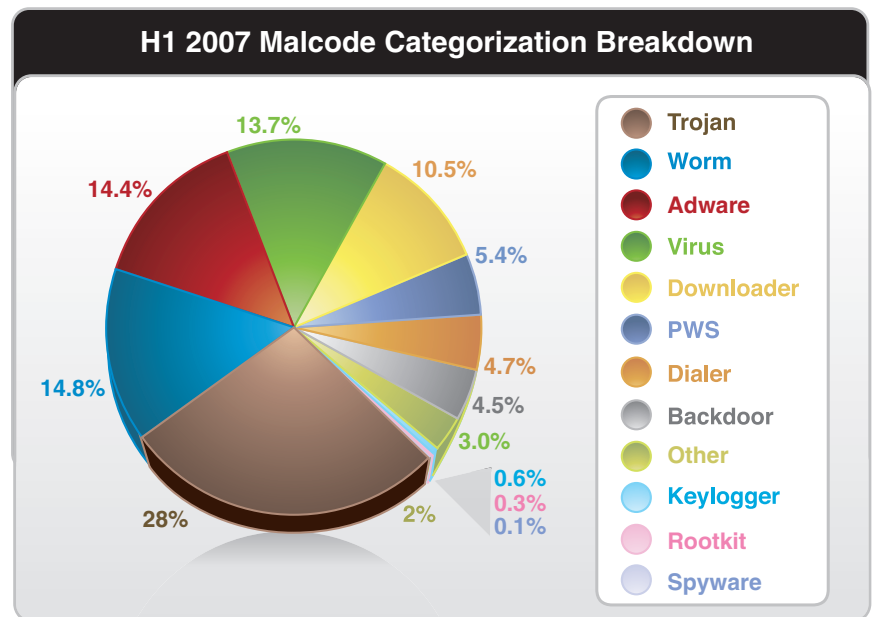
Moving forward the X-Force's classification of malware should be based on the most dominant features of the threat. Malware analyzed in the first half of 2007 is divided into the following buckets:

- **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 the 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 presses 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 billing numbers when making connections.
- **Trojan** – Appears to be a legitimate file before installing itself – often with rootkit functionality.
- **Miscellaneous** – All other malware not falling into one of the above primary categories.

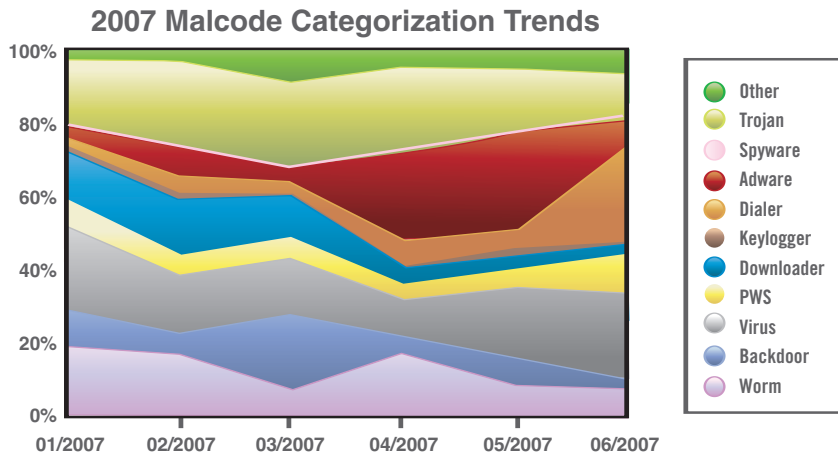
### Malcode Categorization

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



**Malcode Categorization Trends**

So far in 2007, the categorization distribution changed less on a monthly basis, which reflects smaller outbreaks of specific malware families and thus shorter and more contained serial variant attacks from worms for the first six months. However, the 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.



**Top 10 Most Common Malware**

The top 10 most popular exploits for each category researched are listed below.

Top 10 1H 2007 Malcode
Trojan.W32.Agent
Trojan-Downloader.Win32.Zlob
Trojan-Downloader.Win32.Small
Email-Worm.Win32.Mixor
Email-Worm.Win32.Zhelatin
Trojan-Downloader.Win32.Agent
Trojan-Spy.Win32.BZub
Trojan-PSW.Win32.Delf
Trojan.Win32.Small
AdWare.Win32.Virtumonde

### Top 10 Backdoors

Top 10 1H 2007 Backdoor
Backdoor.Win32.Hupigon
Backdoor.Win32.Agent
Backdoor.Win32.Delf
Backdoor.Win32.Bifrose
Backdoor.IRC.Zapchast
Backdoor.Win32.Small
Backdoor.Win32.Rbot
Backdoor.Win32.Optix
Backdoor.Win32.Beastdoor
Backdoor.Win32.Iroffer

### Top 10 Rootkits

Top 10 1H 2007 Rootkit
Rootkit.Win32.Agent
Rootkit.Win32.Vanti
Rootkit.Evilotus
Rootkit.Win32.Delf
Trojan.NTRootkit
Rootkit.Win32.Fuzen
Rootkit.Win32.Ntrtk
Rootkit.Win32.Jamilla
Trojan.NeverDet
Rootkit.Win32.PePatch

### Top 10 Trojans

Top 10 1H 2007 Trojan
Trojan.Win32.Agent
Trojan-Spy.Win32.BZub
Trojan.Win32.Delf
Trojan.Win32.Small
Trojan-Spy.Win32.Banker
Trojan-Spy.Win32.Bancos
Trojan-Spy.Win32.Perfloger
Trojan-Downloader.Win32.IstBar
Trojan-Downloader.Win32.Zlob
Trojan-Spy.Win32.Ardamax

### Top 10 Worms

Top 10 1H 2007 Worm
Email-Worm.Win32.Mixor
Email-Worm.Win32.Zhelatin
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
Worm.Win32.Feebs

### Top 10 Viruses

Top 10 1H 2007 Virus
Virus.Win32.Agent
Virus.Win32.Virut
Virus.Win32.Delf
Virus.Win32.Small
Virus.DOS.Trivial
Virus.Boot
Virua.DOS.Vienna
Virus.MSWord
Virus.Win32.Xorala
Virus.Win32.Parite

### Top 10 Password Stealers

Top 10 1H 2007 PSW
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.QQRob
Trojan-PSW.Win32.OnlineGames

### Top 10 Downloaders

Top 10 1H 2007 Downloader
Trojan-Downloader.Win32.Zlob
Trojan-Downloader.Win32.Small
Trojan-Downloader.Win32.Agent
Trojan-Downloader.Win32.Tibs
Trojan-Downloader.Win32.Delf
Trojan-Downloader.Win32.Banload
Trojan-Downloader.Win32.Obfuscated
Trojan-Downloader.Win32.Adload
Trojan-Downloader.Win32.IstBar
Trojan-Downloader.Win32.Swizzor

### Top 10 Mass Mailers

Top 10 1H 2007 Total
W32.Mydoom.M@mm
W32.Sality.U
W32.Netsky.P@mm
W32.Erkez.D@mm
W32.Blackmal.E@mm!enc
Trojan.Packed.13
Trojan.Toosogen
W32.Mydoom.L@mm
W32.Mixor.Q@mm
W32.Blackmal.E@mm

### Web Browser Exploitation Trends

The X-Force has observed continued growth in Web browser exploitation through its various Web exploit crawlers and analysis of IBM Managed Security Services operational alerting data.

Processing this data and extracting trend information is difficult due to the relationship model used by the delivery mechanism. For example, if there is one site with a particular exploit, but a thousand URLs link to that particular site, a straight count of one-to-one sites does not work very well.

### **Most Popular Exploits**

1. MS06-073, Visual Studio WMI Object Broker ActiveX [Bug: Functionality]
2. MS07-017, Animated Cursor [Bug: Overflow]
3. MS06-057, WebView ActiveX [Bug: Overflow]

The two most popular Web browser vulnerabilities that have been exploited during 2007 did not originate from 2007. The people behind the malicious Web sites discovered this year must have cause to believe that these patched vulnerabilities are still useful as both stand-alone exploits as well as toolkit components. The X-Force believes that unless attackers have a true zero-day exploit, only users that regularly patch will apply newly-available protection.

Underground exploit sales through ICQ-based brokers continue to flourish as well as some new trends including exploit/toolkit leasing. Leasing enables attackers to test exploitation techniques with a smaller initial investment. However, the number of purchased vs. pirated toolkit installations remains unknown. Some evidence proves that attackers will occasionally modify an exploit toolkit if a new exploit becomes public. As a result, a market for modified toolkit sales exists.

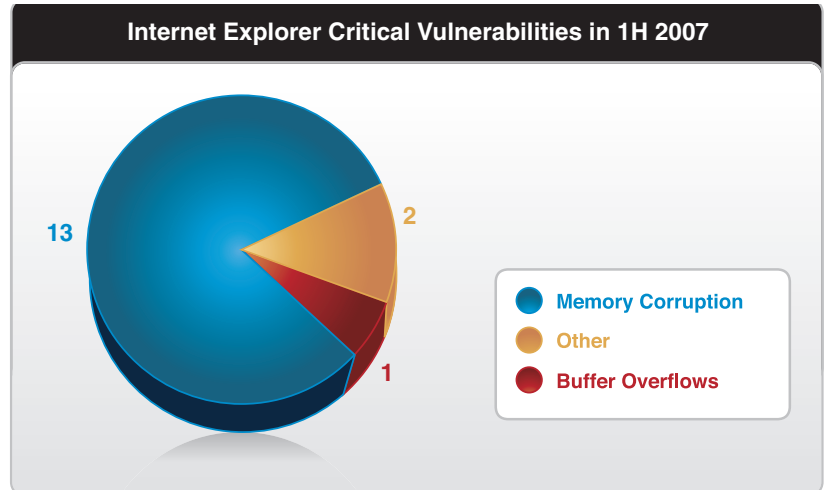
### **Obfuscation and Encryption**

The growth of Web exploit obfuscation and encryption has continued from the second half of 2006. 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 to match a signature.

Prior to last year, the use of obfuscated Web browser exploits were statistically insignificant, and were almost exclusively used in targeted attacks designed to breach known failings in organizations' perimeter security defenses.

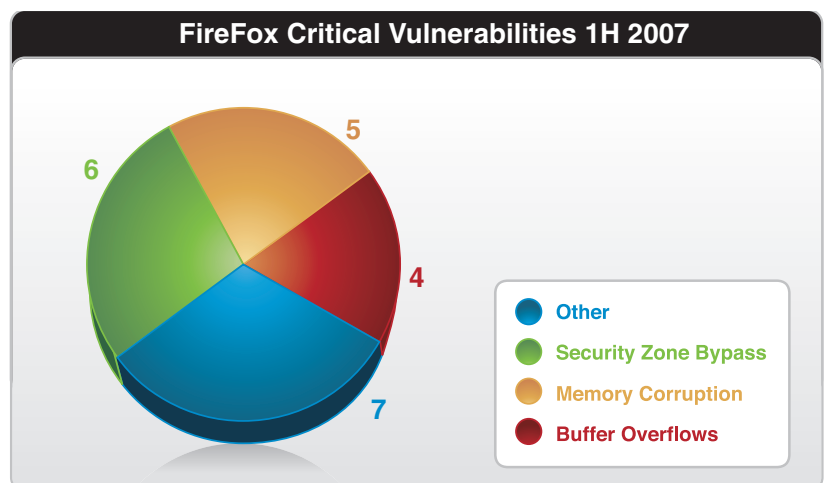
Today, nearly 80 percent of Web exploits are obfuscated – including most self-decrypting exploits. Encryption utilization has exploded through the prevalence of exploit toolkits such as mPack, well exceeding the estimated 70 percent mark for 2006. In terms of unique exploits/toolkits vs. installations seen in the wild during the first half of 2007, slightly less than 30 percent use encryption.

### Windows-based Web Browser Wrap-up



Microsoft® Internet Explorer has had 16 critical vulnerabilities patched during the first half of 2007. This does not take into account any of the third party plug-ins (ActiveX) for which vulnerabilities were reported.

As anticipated, memory corruption vulnerabilities have overwhelmingly dogged Internet Explorer during the first half of 2007 and are expected to continue through the second half. However, the X-Force's second prediction that the "other" category would increase has not come to pass. Interestingly, there have not been any critical security zone bypasses reported during this timeframe.



FireFox has had 22 critical vulnerabilities patched during the first half of 2007. This does not take into account any of the third party plug-ins (XPI) for which vulnerabilities were reported.

Just as reported in our 2006 wrap-up, both memory corruption issues and security zone bypass techniques have been reported in virtually the same amount for FireFox. Thus while memory corruption issues are still problematic for FireFox, Internet Explorer is far more prone to them while less prone to security zone bypasses. This trend is likely to continue during the second half of 2007. It is surprising that the overall distribution of FireFox critical vulnerabilities is fairly even – a significant departure from 2006.



© Copyright IBM Corporation 2007

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

Produced in the United States of America  
08-07  
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.

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

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.

IBM assumes no responsibility regarding the accuracy of the information provided herein and use of such information is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

---