2010 IBM X-Force® Trend & Risk Report
The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today’s security problems
- Develop new technology for tomorrow’s security challenges
- Educate the media and user communities

X-Force Research

14B analyzed Web pages & images
40M spam & phishing attacks
54K documented vulnerabilities
Billions of intrusion attempts daily
Millions of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

© 2011 IBM Corporation
- **Section I—Threats**
  - Topics that comprise “Threats” and describe the attacks aimed at the enterprise that security specialists face.
  - Latest attack trends as identified by IBM.

- **Section II—Operating Secure Infrastructure**
  - Topics surrounding the weaknesses in process software, and infrastructure targeted by today’s threats.
  - Security compliance best practices, operating cost reduction ideas, automation, lowered cost of ownership, and the consolidation of tasks, products, and roles.
  - Present data tracked across IBM during the process of managing or mitigating these problems.

- **Section III—Developing Secure Software**
  - Proven processes and techniques for developing secure software.
  - Discussion on how enterprises can find existing vulnerabilities and help prevent new ones from being introduced.
  - Static and dynamic security testing done by the Rational AppScan group in all stages of application development and share insights

- **Section IV—Emerging Trends in Security**
  - Developing technology that presses upon enterprises for future investments
  - Explaining where threats and exploits are being utilized in these early technology adoptions and how enterprises can stay focused.
Vendors Reporting the Largest Number of Vulnerability Disclosures in History

- Vulnerability disclosures up **27%**.
  - Web applications continue to be the largest category of disclosure.

- Significant increase across the board signifies efforts that are going on throughout the software industry to improve software quality and identify and patch vulnerabilities.
Patches Still Unavailable for Many Vulnerabilities

- **44%** of all vulnerabilities disclosed in 2010 had no vendor-supplied patches to remedy the vulnerability.
  - Most patches become available for most vulnerabilities at the same time that they are publicly disclosed.
  - However some vulnerabilities are publicly disclosed for many weeks before patches are released.

### Patch Release Timing – First 8 Weeks of 2010

<table>
<thead>
<tr>
<th>Patch Timeline</th>
<th>All</th>
<th>Top Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same Day</td>
<td>3400</td>
<td>1814</td>
</tr>
<tr>
<td>Week 1</td>
<td>192</td>
<td>34</td>
</tr>
<tr>
<td>Week 2</td>
<td>55</td>
<td>11</td>
</tr>
<tr>
<td>Week 3</td>
<td>57</td>
<td>12</td>
</tr>
<tr>
<td>Week 4</td>
<td>33</td>
<td>7</td>
</tr>
<tr>
<td>Week 5</td>
<td>27</td>
<td>7</td>
</tr>
<tr>
<td>Week 6</td>
<td>22</td>
<td>4</td>
</tr>
<tr>
<td>Week 7</td>
<td>17</td>
<td>3</td>
</tr>
<tr>
<td>Week 8</td>
<td>16</td>
<td>8</td>
</tr>
</tbody>
</table>
Public Exploit Exposures Up in 2010

- Public exploit disclosures up **21%** in 2010 versus 2009
  - Approximately **14.9%** of the vulnerabilities disclosed in 2010 had public exploits, which is down slightly from the 15.7% last year
  - However more vulnerabilities were disclosed this year, so the total number of exploits increased.
  - The vast majority of public exploits are released the same day or in conjunction with public disclosure of the vulnerability.

![Public Exploit Disclosure Timing by Weeks](image1)

![Public Exploit Disclosures 2006-2010](image2)

<table>
<thead>
<tr>
<th>Exploit Timing</th>
<th>0 Days</th>
<th>1 Week</th>
<th>2 Weeks</th>
<th>3 Weeks</th>
<th>4 Weeks</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Days</td>
<td>854</td>
<td>270</td>
<td>18</td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>
Exploit Effort vs. Potential Reward

- Economics continue to play heavily into the exploitation probability of a vulnerability.
- All but one of the 25 vulnerabilities in the top right are vulnerabilities in the browser, the browser environment, or in email clients.
- The only vulnerability in this category that is not a browser or email client side issue is the LNK file vulnerability that the Stuxnet worm used to exploit computers via malicious USB keys.
Top Attacks seen by X-Force in 2010

- Automated SQL Injection attacks
- Lateral scanning of the entire Internet for services with weak passwords
- The SQL Slammer worm was responsible for a huge amount of malicious traffic in 2010 but traffic levels dropped off significantly in March, 2011. (For more info see the Frequency-X Blog.)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Event Name</th>
<th>Trend Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SQL_SSRP_Slammer_Worm</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>SQL_injection</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>PsExec_Service_Accessed</td>
<td>Slightly Up</td>
</tr>
<tr>
<td>4</td>
<td>SSH_Brute_Force</td>
<td>Slightly Down</td>
</tr>
<tr>
<td>5</td>
<td>JScript_CollectGarbage</td>
<td>Up</td>
</tr>
<tr>
<td>6</td>
<td>HTTP_Unix_Passwords</td>
<td>Slightly Up</td>
</tr>
<tr>
<td>7</td>
<td>SMB_Mass_Login</td>
<td>Down</td>
</tr>
<tr>
<td>8</td>
<td>SMB_Empty_Password</td>
<td>No Change</td>
</tr>
<tr>
<td>9</td>
<td>SQL_Empty_Password</td>
<td>Up</td>
</tr>
</tbody>
</table>

Table 1: Top MSS high volume signatures and trend line
SQL Injection Attacks

- During each of the past three years, there has been a globally scaled SQL injection attack some time during the months of May through August.
- The anatomy of these attacks is generally the same: they target .ASP pages that are vulnerable to SQL injection.
The drive-by-download process

Desktop Users

Browse The Internet

Web server with embedded iframe

Malicious iframe host

Downloader installed

Exploit material Served

Malware installed and activated

Web browser targeted
SQL Injection Attack Tools

- Automatic page-rank verification
- Search engine integration for finding "vulnerable" sites
- Prioritization of results based on probability for successful injection
- Reverse domain name resolution
- etc.
Web App Vulnerabilities Continue to Dominate

- Nearly half (49%) of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.
Real World Conclusions from Web App Assessments

- In 2010, for the first time, we now find that Cross-Site Request Forgery (CRSF) vulnerabilities are more likely to be found in our testing than Cross-Site Scripting (XSS) vulnerabilities.

- XSS and SQL injection are both attributed directly to a lack of input control. The likelihood of finding it in 2010 is more than 60%.
Improvement Between Application Testing Cycles

- There is a significant decline in the likelihood of finding application vulnerabilities in a retest.
- In many cases this reduction is more than half that of the original.
- Demonstrates the importance of testing applications but also follow up and mitigation.

Note: Charts show which vulnerabilities were 50% or more likely to appear in a Web assessment for each industry.
The drive-by-download process

Desktop Users

Browse The Internet

Web server with embedded iframe

Malicious iframe host

Downloader installed

Exploit material Served

Malware installed and activated

Web browser targeted
New exploit packs show up all the time

BleedingLife Exploit Pack was looked down upon in the beginning of its start. As time went on and users began to take a chance with this pack, they've eventually understood BL is no normal pack. With less exploits and a higher rate than other packs, BL has really made a name for itself. Now, BL has turned into a series. BL v1, BL v2, BL Mini-Java, BL Java Edition, BL Adobe Edition. And... Here before us, BL v2 Reloaded.

If you want a low cost, high rate and great quality pack... Purchase BleedingLife v2 Reloaded!

EXPLOITS:
- CVE-2008-2992
- CVE-2010-0188
- CVE-2010-0842
- CVE-2010-1297
- CVE-2010-2884
- CVE-2010-3552
- JavaSignedApplet (Requires user interaction but can be disabled.)
- All exploits bypass ASLR and DEP where needed.

AVERAGE RATE:
- BL v2 has an average rate between 30% - 40%
- SS/Proof coming soon...

PAYMENT OPTIONS:
- BleedingLife v2 Reloaded - $400.00
- FUD Update - $50.00
- Domain Change - $50.00
- Liberty Reserve & WebMoney ONLY!
- Previous v2 Buyers - FREE Update!
Client-Side Vulnerabilities: Web Browser, Document Reader & Multimedia Player Vulnerabilities Continue to Impact End Users

- Web browsers and their plug-ins continue to be the largest category of client-side vulnerabilities.
- 2010 saw an increase in the volume of disclosures in document readers and editors as well as multimedia players.
Suspicious Web Pages and Files Show No Sign of Waning

- Obfuscation activity continued to increase during 2010.
- Attackers never cease to find new ways to disguise their malicious traffic via JavaScript and PDF obfuscation.
  - Obfuscation is a technique used by software developers and attackers alike to hide or mask the code used to develop their applications.
Proliferation of Mobile Devices Raises Security Concerns

- 2010 saw significant increases in the number of vulnerabilities disclosed for mobile devices as well as number of public exploits released for those vulnerabilities.
  - Motivations of these exploit writers is to “jailbreak” or “root” devices enabling various functionality not intended by manufacturers.
  - Malicious applications were distributed in the Android app market that used widely disseminated exploit code to obtain root access to devices and steal information.
Spear Phishing and Social Engineering on the Rise

- Social networks represent a vehicle for malware authors to distribute their programs in ways that are not easily blocked. Examples include:
  - Antivirus 2009, which lures users into downloading a fake AV product.
  - The Koobface Worm which infiltrated Facebook, Myspace, and other social networking sites.
  - The Jahlav Trojan which used Twitter to infect Mac users.

- “There is no patch for stupid.”
Advanced Persistent Threat

- Example of e-mail with malicious PDF

Washington — President Obama, in his 2010 Trade Policy Agenda sent to Congress March 1, pledged the United States will build on existing trade agreements to strengthen the global trading system and uphold American values and commitments around the world.

The agenda items highlighted by USTR include the following:

- Support and strengthen a rules-based trading system. The United States strongly supports an ambitious and balanced Doha agreement that liberalizes three core market-access areas: agriculture, goods, and services.

- Enforce rights in the rules-based trading system. USTR will strengthen further monitoring and enforcement, bringing cases at the World Trade Organization (WTO) as necessary, will increase focus on non-tariff barriers that hinder exports, and will fully enforce labor and environmental rights in trade agreements.

- Enhance U.S. growth, job creation and innovation. The United States will emphasize bilateral relations with emerging markets as well as with long-standing key partners, and will pursue regional engagement, particularly negotiation of a Trans-Pacific Partnership Agreement to access key markets in the Asia-Pacific for decades to come.

- Work to resolve outstanding issues with pending free trade agreements (FTAs) and build on existing agreements. Proper conclusion and implementation of the pending FTAs with Panama, Colombia and South Korea can bring significant economic benefits. In 2010, USTR will continue to consult with Congress and the public and to engage with these nations to address outstanding issues. It will also strengthen relationships with current partners such as Canada, Mexico, Japan and the European Union.

- Facilitate progress on national energy and environmental goals. Good trade policy can accelerate the success of sound energy and environmental initiatives and can complement sustainable growth. USTR will support fast-tracking action with willing partners in the WTO’s work on liberalizing trade in innovative, climate-friendly goods and services through tariff reductions and other initiatives.

- Foster stronger partnerships with developing and poor nations. The Obama administration supports expanding trade opportunities to stimulate market-led growth and help improve the lives of people in the least-developed nations. Opportunities created by open markets and preferences such as the Generalized System of Preferences require complementary measures such as technical assistance and market-based and rule-of-law reforms to maximize their benefits, USTR said.
Stuxnet and Advanced Persistent Threats (APT)

- APT previously thought to be exploitation of cyber-defense systems for the purpose of economic, political or military gain -- now associated with any targeted, sophisticated or complex attack regardless of attacker motive.

- Often a high-value target is an end-user system such as one that belongs to a person who has access to sensitive data.

- Stuxnet took advantage of Zero day exploits with no workaround or patch.
Bot Network Activity on the Rise in 2010

- Trojan Bot networks continued to evolve in 2010 by widespread usage and availability.
- Zeus (also known as Zbot and Kneber) continue to evolve through intrinsic and plugin advances.
- Various bot networks based on Zeus were responsible for millions of dollars in losses over the last few years.
- Microsoft led operation resulted in the takedown of a majority of Waldec botnet in late February.
  - Communication between Waledac’s command and control centers and its thousands of zombie computers was cut off in a matter of days.
- Much of the other activity seen is Zeus.
Zeus Crimeware Service

Hosting for costs $50 for 3 months.

This includes the following:

- Fully set up ZeuS Trojan with configured FUD binary.
- Log all information via internet explorer
- Log all FTP connections
- Steal banking data
- Steal credit cards
- Phish US, UK and RU banks
- Host file override
- All other ZeuS Trojan features
- Fully set up MalKit with stats viewer integrated.
- 10 IE 4/5/6/7 exploits
- 2 Firefox exploits
- 1 Opera exploit
- Add your own to view statistics

We also host normal ZeuS clients for $10/month.

This includes a fully set up zeus panel/configured binary.
Spammers made a continuous effort in 2010 to regularly change technical contents of spam messages rather than increasing volume.

- Moving from random text spam combined with random URLs, ZIP Attachments, HTML attachments, to significantly increasing the average byte size of spam.
- The amount of URL spam using well-known and trusted domain names declined slightly in the 2nd half of 2010, for the first time in more than two years.
Spam Continues to Change to Avoid Detection

- **90%** of spam is classified as URL spam.
- Spammers continue to use “trusted” domains and “legitimate links” in spam messages to avoid anti-spam technologies.
- US, India, Brazil, and Vietnam were the top four spam-sending countries, accounting for nearly one-third of worldwide spam.
- The US once again takes the top position for the first time since 2007.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>flick.com</td>
<td>radikal.ru</td>
<td>livelfistore.com</td>
<td>livelfistore.com</td>
<td>imagehack.us</td>
<td>imagehack.us</td>
</tr>
<tr>
<td>2.</td>
<td>imageshack.us</td>
<td>imageshack.us</td>
<td>imagebo.com</td>
<td>imageshack.us</td>
<td>imageshost.ru</td>
<td>imageshost.ru</td>
</tr>
<tr>
<td>3.</td>
<td>radikal.ru</td>
<td>livelfistore.com</td>
<td>radikal.ru</td>
<td>imageshost.ru</td>
<td>myimg.de</td>
<td>pikucha.ru</td>
</tr>
<tr>
<td>4.</td>
<td>livelfistore.com</td>
<td>flick.com</td>
<td>imagehack.us</td>
<td>imgr.com</td>
<td>xs.to</td>
<td>mgur.com</td>
</tr>
<tr>
<td>5.</td>
<td>webmd.com</td>
<td>live.com</td>
<td>googlegroups.com</td>
<td>myimg.de</td>
<td>imgr.com</td>
<td>myta4iri.com</td>
</tr>
<tr>
<td>6.</td>
<td>picosoho.ru</td>
<td>imagebo.com</td>
<td>live.com</td>
<td>xs.to</td>
<td>tinypic.com</td>
<td>mojainage.com</td>
</tr>
<tr>
<td>7.</td>
<td>live.com</td>
<td>copololo.biz</td>
<td>akomaitech.net</td>
<td>icontact.com</td>
<td>livelfistore.com</td>
<td>myimg.de</td>
</tr>
<tr>
<td>8.</td>
<td>superbashore.com</td>
<td>teetorder.ru</td>
<td>gonestory.com</td>
<td>tinyphoto.com</td>
<td>icontact.com</td>
<td>twimg.com</td>
</tr>
<tr>
<td>9.</td>
<td>tmbrr.com</td>
<td>laughexcite.ru</td>
<td>bestanswer.ru</td>
<td>live.com</td>
<td>googlegroups.com</td>
<td>icontact.com</td>
</tr>
<tr>
<td>10.</td>
<td>tagreat.com</td>
<td>hismouth.ru</td>
<td>wrotekde.ru</td>
<td>binkyou.net</td>
<td>images-amazon.com</td>
<td>twitter.com</td>
</tr>
</tbody>
</table>

### Top Ten Domains Used in Spam

#### Spam Domains vs. Trusted Domains

<table>
<thead>
<tr>
<th>Rank</th>
<th>July 2010</th>
<th>August 2010</th>
<th>September 2010</th>
<th>October 2010</th>
<th>November 2010</th>
<th>December 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>imageshack.us</td>
<td>yahoo.com</td>
<td>the.com</td>
<td>businessinsider.com</td>
<td>rolex.com</td>
<td>pfizer.com</td>
</tr>
<tr>
<td>2.</td>
<td>icontact.com</td>
<td>the.com</td>
<td>of.com</td>
<td>mrgo.me</td>
<td>msn.com</td>
<td>viagra.com</td>
</tr>
<tr>
<td>3.</td>
<td>the.com</td>
<td>icontact.com</td>
<td>man.com</td>
<td>4freeimagehost.com</td>
<td>bit.ly</td>
<td>msn.com</td>
</tr>
<tr>
<td>4.</td>
<td>myimg.de</td>
<td>feetspic.com</td>
<td>pfizerhelpfulanswers.com</td>
<td>bit.ly</td>
<td>pfizer.com</td>
<td>rolex.com</td>
</tr>
<tr>
<td>5.</td>
<td>of.com</td>
<td>of.com</td>
<td>and.com</td>
<td>postimage.org</td>
<td>cc.co</td>
<td>bit.ly</td>
</tr>
<tr>
<td>7.</td>
<td>byru.com</td>
<td>and.com</td>
<td>in.com</td>
<td>pfizer.com</td>
<td>royalbele.com</td>
<td>newpztizmed5k.com</td>
</tr>
<tr>
<td>8.</td>
<td>and.com</td>
<td>facebook.com</td>
<td>yahoo.com</td>
<td>pfizer.com</td>
<td>royalfreeasable.com</td>
<td>images.net</td>
</tr>
<tr>
<td>9.</td>
<td>in.com</td>
<td>in.com</td>
<td>a.com</td>
<td>uploadgeek.com</td>
<td>luxurystorewatch.com</td>
<td>corsfowk.com</td>
</tr>
<tr>
<td>10.</td>
<td>tastymighty.com</td>
<td>a.com</td>
<td>x-misc.com</td>
<td>vipplaye.com</td>
<td>basincokk.com</td>
<td>onlinepftzsrct2.com</td>
</tr>
</tbody>
</table>

### Table 3: Most common domains in URL spam, 2010

<table>
<thead>
<tr>
<th>Country</th>
<th>% of Spam</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>10.9%</td>
</tr>
<tr>
<td>India</td>
<td>8.2%</td>
</tr>
<tr>
<td>Brazil</td>
<td>8.1%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>5.4%</td>
</tr>
<tr>
<td>Russia</td>
<td>5.2%</td>
</tr>
</tbody>
</table>

### Table 4: Geographical Distribution of Spam Senders – 2010

<table>
<thead>
<tr>
<th>Country</th>
<th>% of Spam</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>4.4%</td>
</tr>
<tr>
<td>Germany</td>
<td>3.7%</td>
</tr>
<tr>
<td>South Korea</td>
<td>3.3%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>3.0%</td>
</tr>
<tr>
<td>Romania</td>
<td>2.9%</td>
</tr>
</tbody>
</table>
Phishing Attacks Continue to Decline

- In 2010, Phishing emails slowed and the volume did not reach the levels seen at the end of 2009.

- India is the top sender in terms of phishing volume, while Russia is in second place, and Brazil holds third place.
  - Newcomers in the top 10 are Ukraine, Taiwan, and Vietnam, while Argentina, Turkey, and Chile disappeared from this list.

- Over time popular subject lines continue to drop in importance.
  - By 2010, the top 10 most popular subject lines only represented about 26 percent of all phishing emails

<table>
<thead>
<tr>
<th>Country</th>
<th>% of Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>15.5%</td>
</tr>
<tr>
<td>Russia</td>
<td>10.4%</td>
</tr>
<tr>
<td>Brazil</td>
<td>7.6%</td>
</tr>
<tr>
<td>USA</td>
<td>7.5%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>6.3%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country</th>
<th>% of Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Korea</td>
<td>4.7%</td>
</tr>
<tr>
<td>Colombia</td>
<td>3.0%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>2.2%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>2.2%</td>
</tr>
<tr>
<td>Poland</td>
<td>1.8%</td>
</tr>
</tbody>
</table>

Table 7: Geographical Distribution of Phishing Senders – 2010
Phishing Targets Financial & Credit Card Industries

- **50.1%** of phishing is targeted at the financial industry vs. **60.9%** in 2009.
- **77%** of all financial phishing targets in the 2010 are located in North America vs. **95%** in 2009.
  - 22% of financial phishing targets are located in Europe
- **19%** of phishing emails were targeted at credit cards.
Commercial phishing kits make it easy for a novice to start in the business.
“Bad” Web Content Tries to Evade Filters

- Approximately 7% of the Internet contains unwanted content such as pornographic or criminal Web sites.

- Anonymous proxies, which hide a target URL from a Web filter, have steadily increased more than quintupling in number since 2007.
For More IBM X-Force Security Leadership

**X-Force Trend Reports**

**X-Force Security Alerts and Advisories**
Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring. Find out more at [http://xforce.iss.net/](http://xforce.iss.net/)

**X-Force Blogs and Feeds**
For a real-time update of Alerts, Advisories, and other security issues, subscribe to the X-Force RSS feeds. You can subscribe to the X-Force alerts and advisories feed at [http://iss.net/rss.php](http://iss.net/rss.php) or the Frequency X Blog at [http://blogs.iss.net/rss.php](http://blogs.iss.net/rss.php)