IBM SECURITY DAY 2011

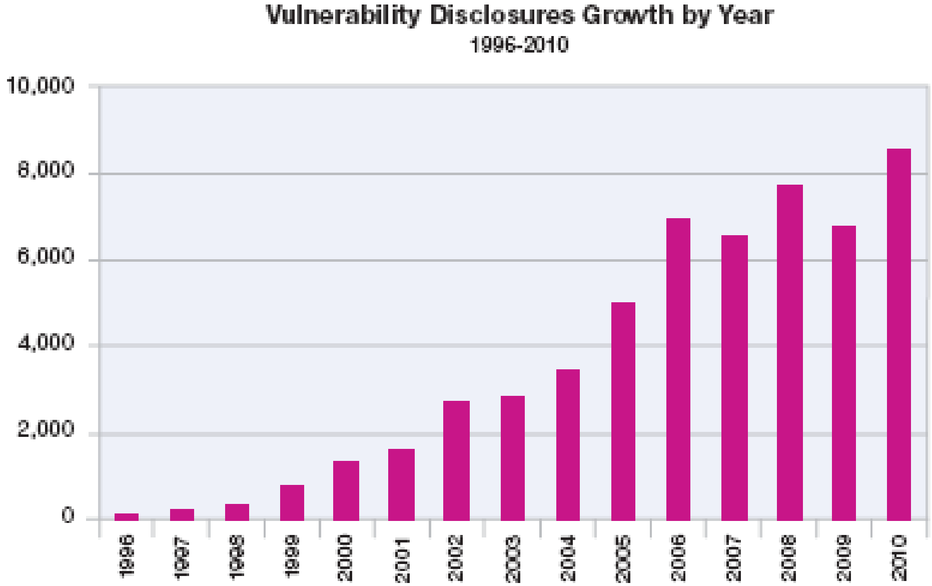
Innovare con sicurezza per aprire al futuro

Jean Paul Ballerini

X-Force: risultati ultimo report

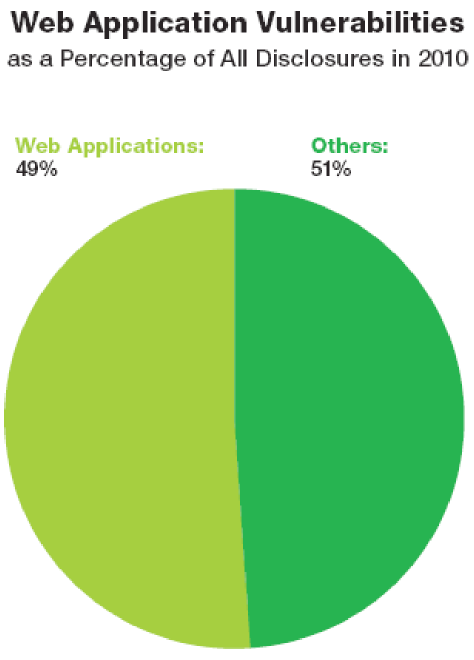
Largest Number of Vulnerability Disclosures in History

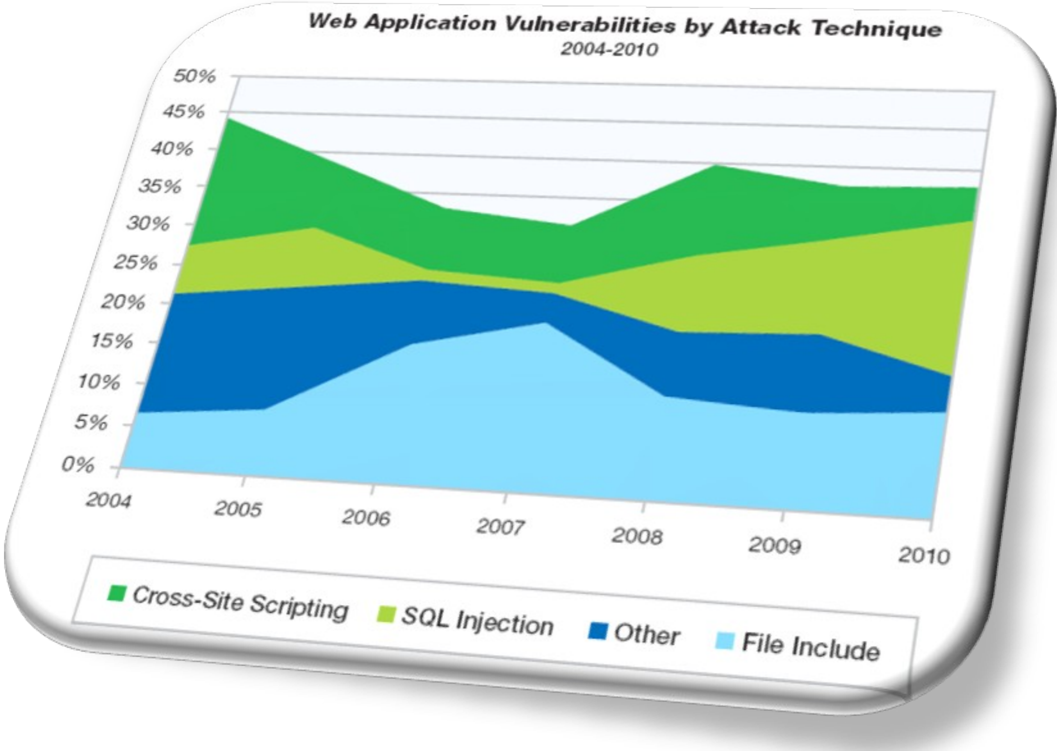
- Vulnerability disclosures up 27%.
  - Web applications continue to be the largest category of disclosure.
- Significant increase across the board signifies efforts that are going on throughout the software industry to improve software quality and identify and patch vulnerabilities.



Web App Vulnerabilities Continue to Dominate

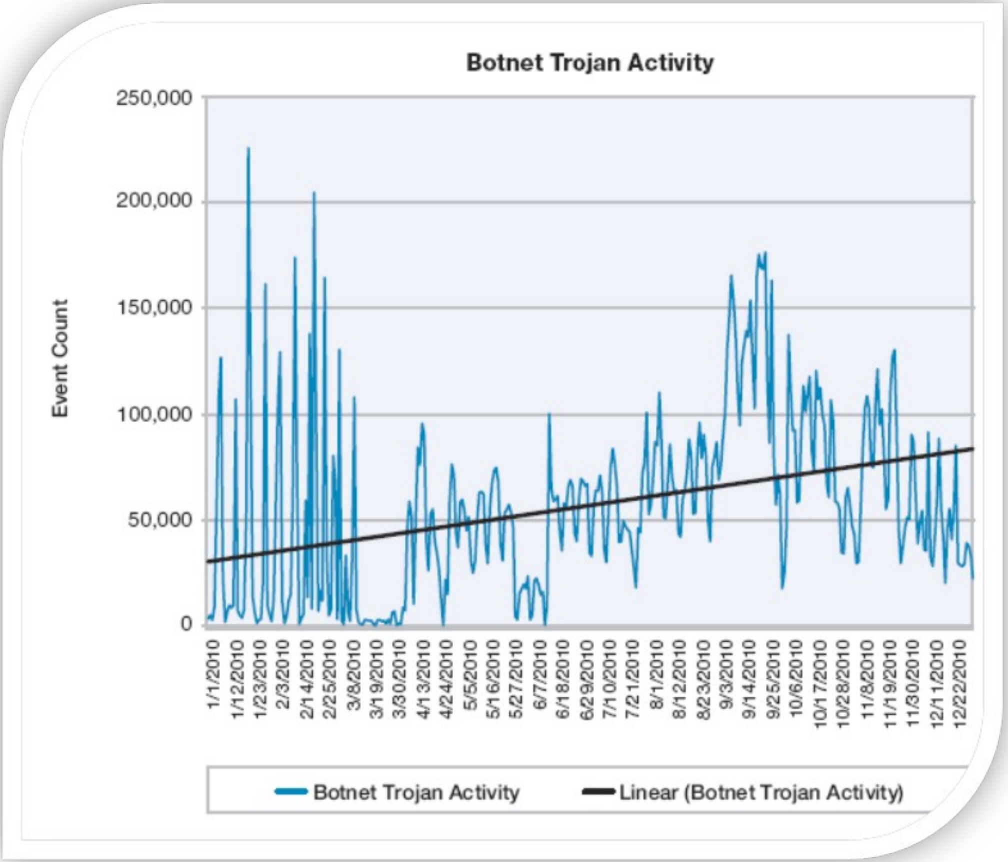
- Nearly half (**49%**) of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.


Web Application Vulnerabilities
as a Percentage of All Disclosures in 2010


Web Application Vulnerabilities by Attack Technique
2004-2010

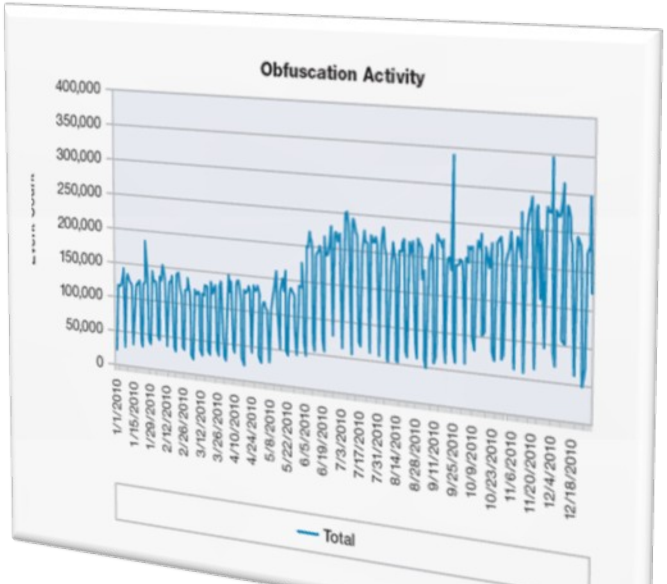
Bot Network Activity on the Rise

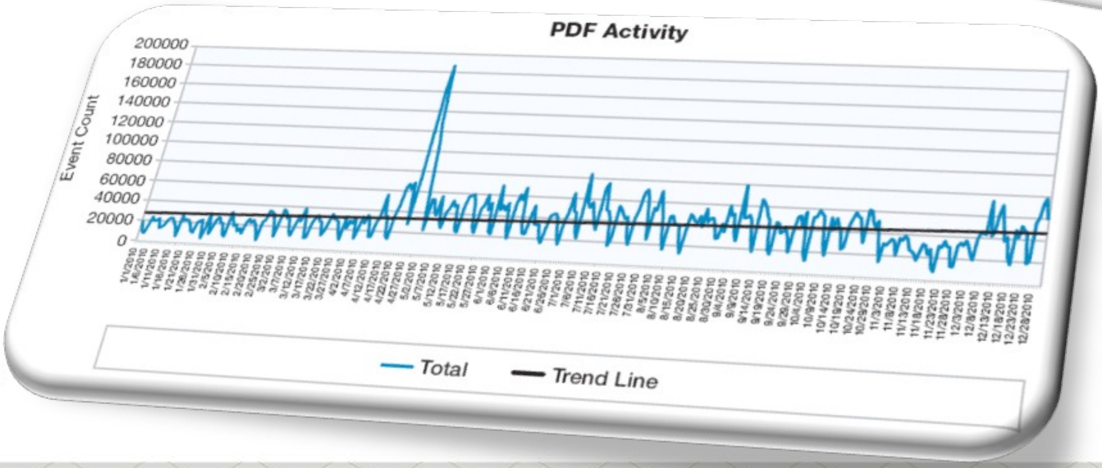
- Trojan Bot networks continued to evolve in 2010 by widespread usage and availability.
- Zeus (also known as Zbot and Kneber) continue to evolve through intrinsic and plugin advances.
- Various bot networks based on Zeus were responsible for millions of dollars in losses over the last few years.
- Microsoft 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.
- Other activity seen is Zeus



Suspicious Web Pages and Files

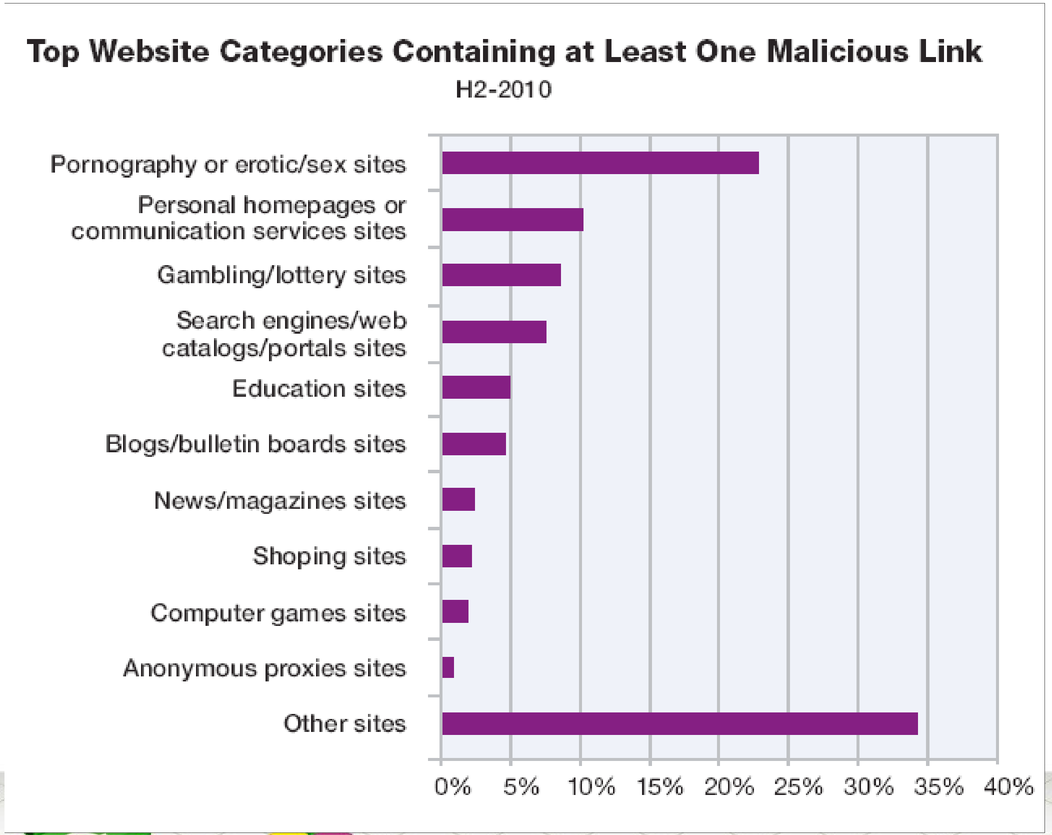
- Obfuscation activity continued to increase during 2010.
- Attackers never cease to find new ways to disguise their malicious traffic via JavaScript and PDF obfuscation.
  - Obfuscation is a technique used by software developers and attackers alike to hide or mask the code used to develop their applications.

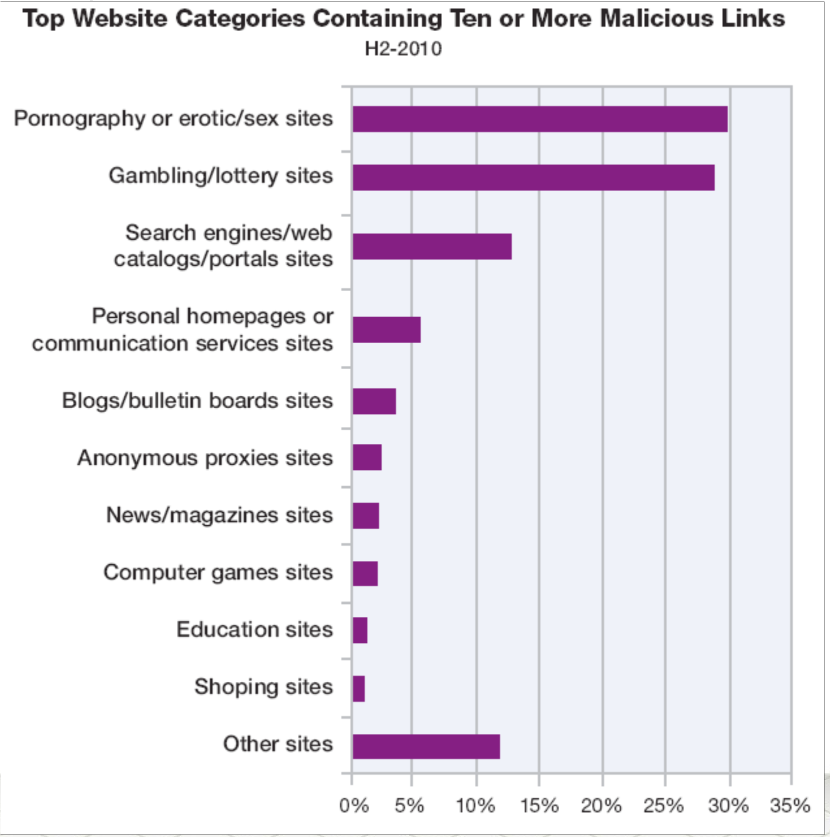




Websites Hosting Bad Links

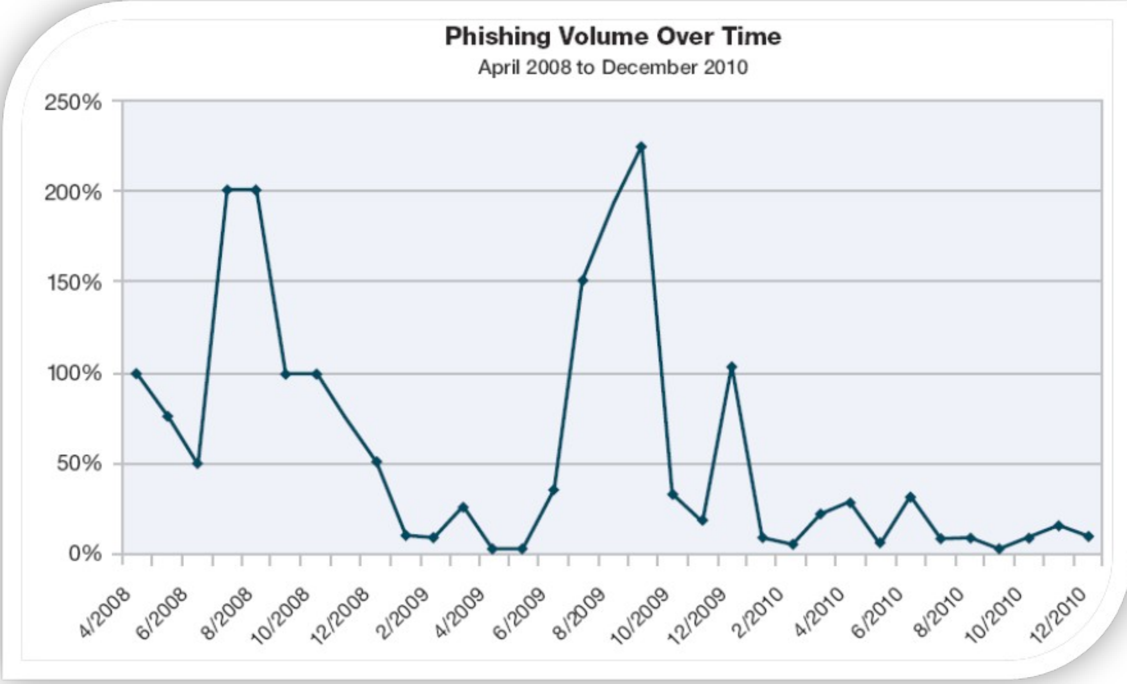
- Professional “bad” Web sites like pornography, gambling, or illegal drugs Web sites have seen increases in links to malware links in 2010.
- Out of the categories of Websites that host 10 or more of these links, pornography accounts for nearly 30 percent and gambling accounts for nearly 29 percent.
  - It’s possible these kinds of Web sites knowingly use these links for profit.

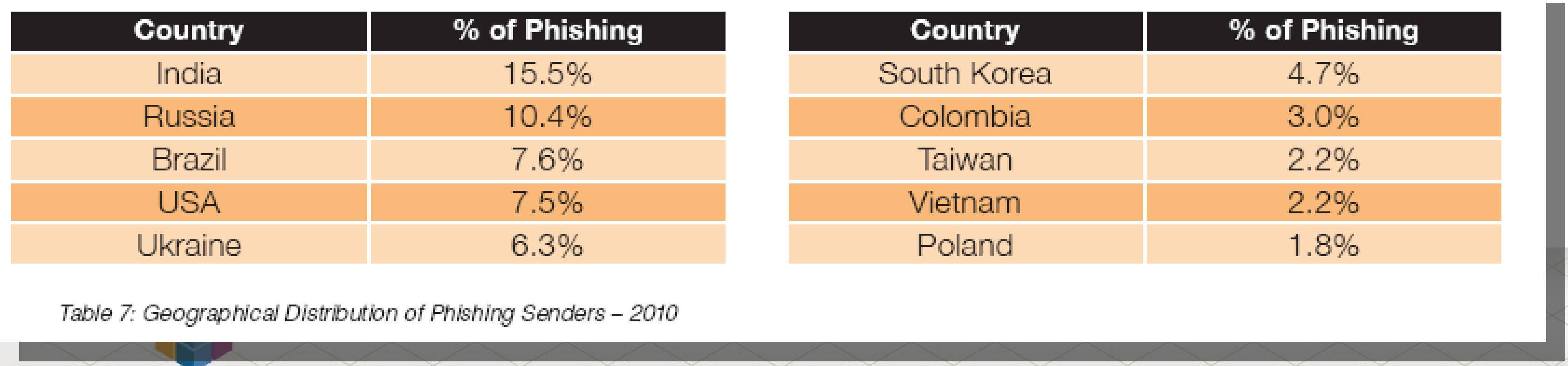




Phishing Attacks still Declining

- 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





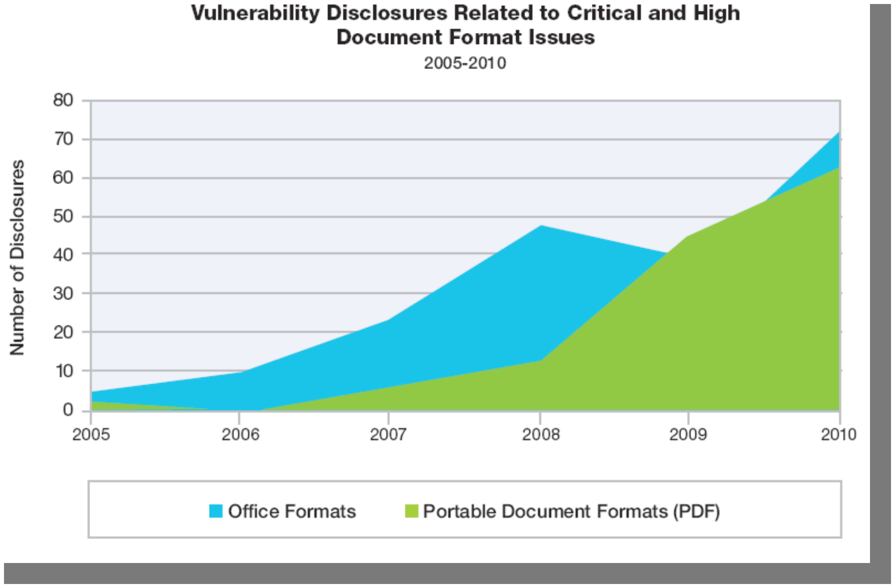
Country	% of Phishing
India	15.5%
Russia	10.4%
Brazil	7.6%
USA	7.5%
Ukraine	6.3%

Country	% of Phishing
South Korea	4.7%
Colombia	3.0%
Taiwan	2.2%
Vietnam	2.2%
Poland	1.8%

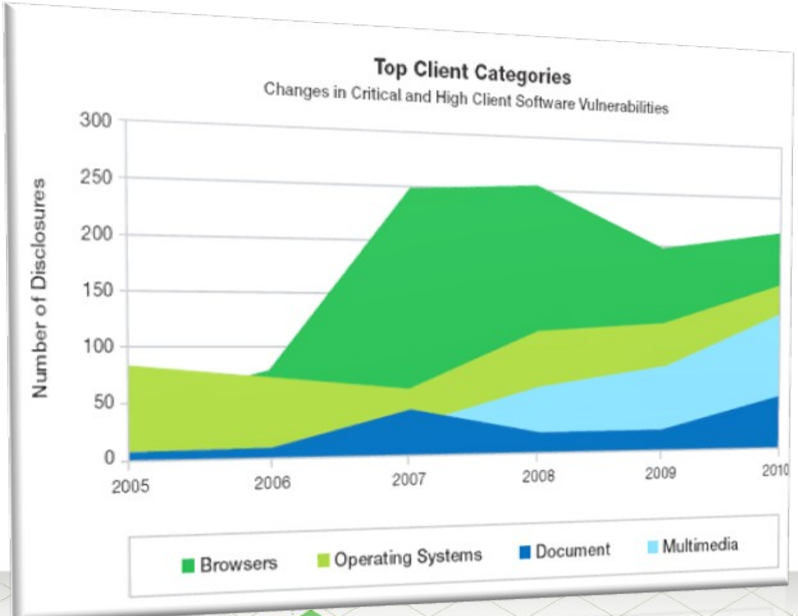
Table 7: Geographical Distribution of Phishing Senders – 2010

Client-Side Vulnerabilities

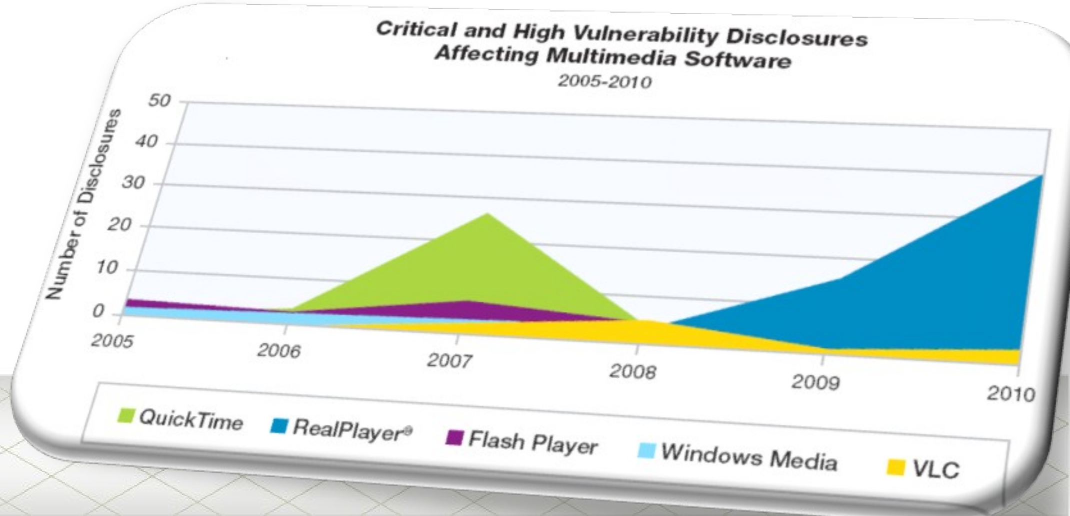
- Web browsers and their plug-ins continue to be the largest category of client-side vulnerabilities.
- 2010 saw an increase in the volume of disclosures in document readers and editors as well as multimedia players.



Vulnerability Disclosures Related to Critical and High Document Format Issues
2005-2010



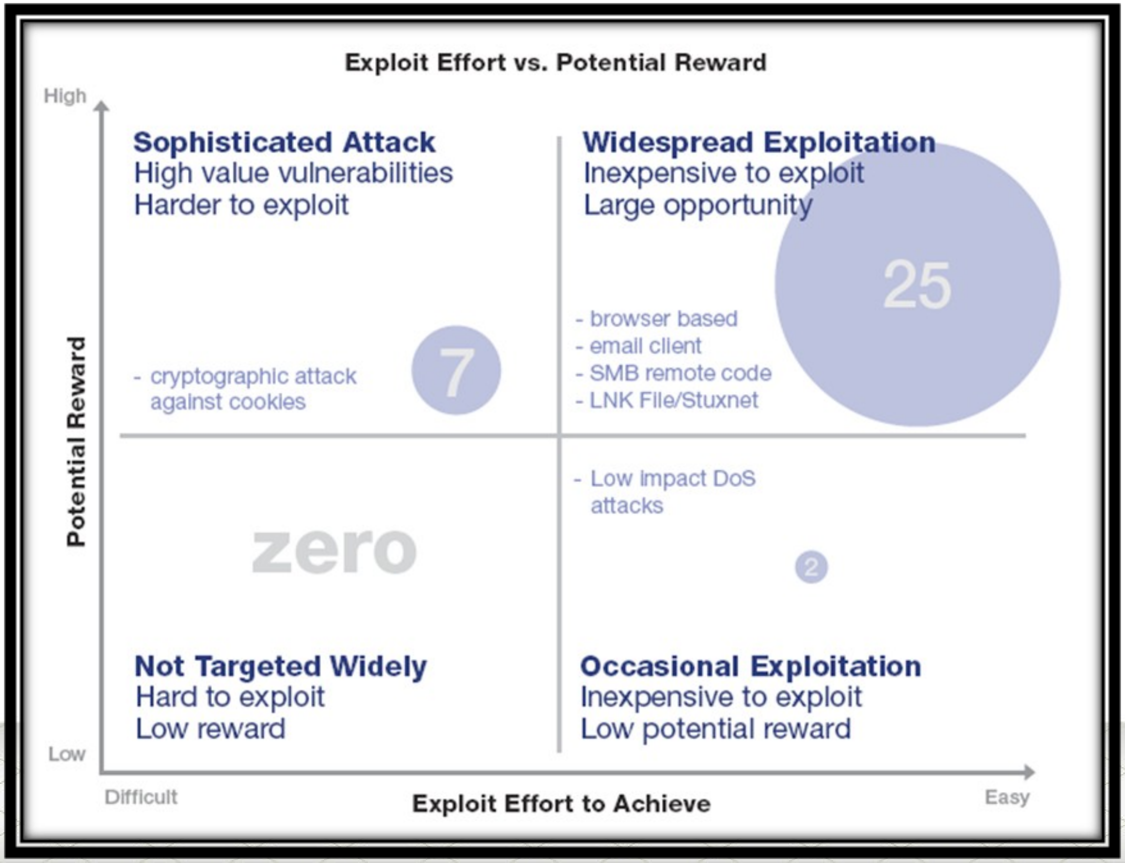
Top Client Categories
Changes in Critical and High Client Software Vulnerabilities



Critical and High Vulnerability Disclosures Affecting Multimedia Software
2005-2010

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.



Exploit Effort vs. Potential Reward

Sophisticated Attack
High value vulnerabilities
Harder to exploit

- cryptographic attack against cookies

Widespread Exploitation
Inexpensive to exploit
Large opportunity

- browser based
- email client
- SMB remote code
- LNK File/Stuxnet

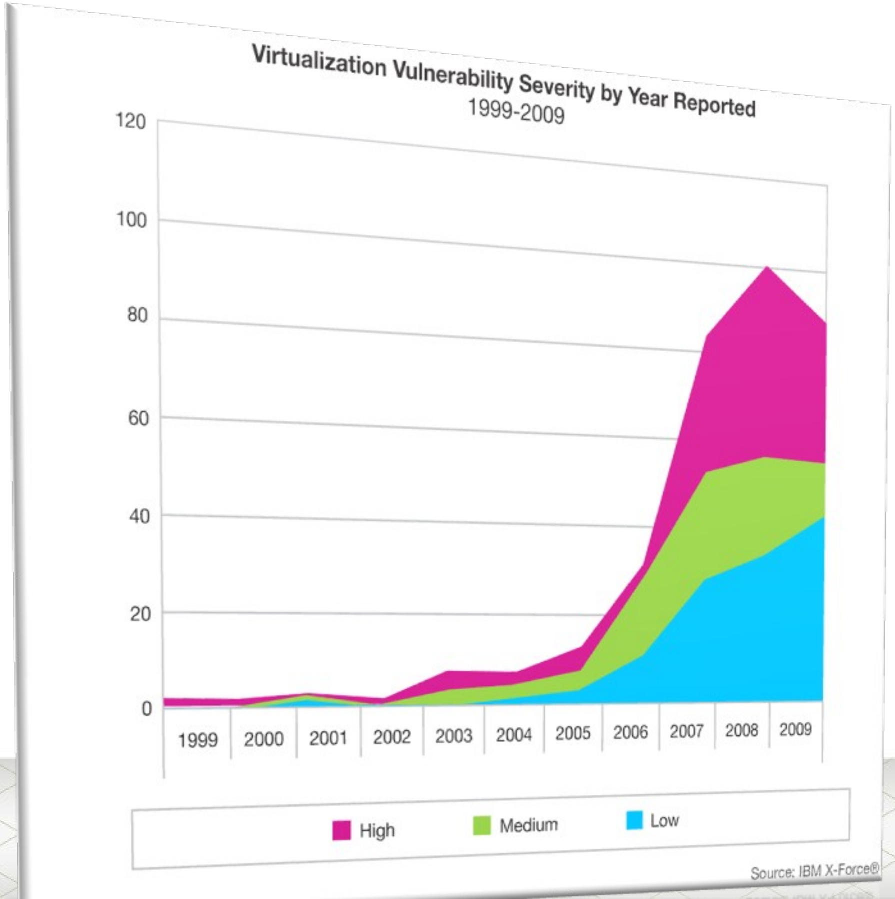
Not Targeted Widely
Hard to exploit
Low reward

Occasional Exploitation
Inexpensive to exploit
Low potential reward

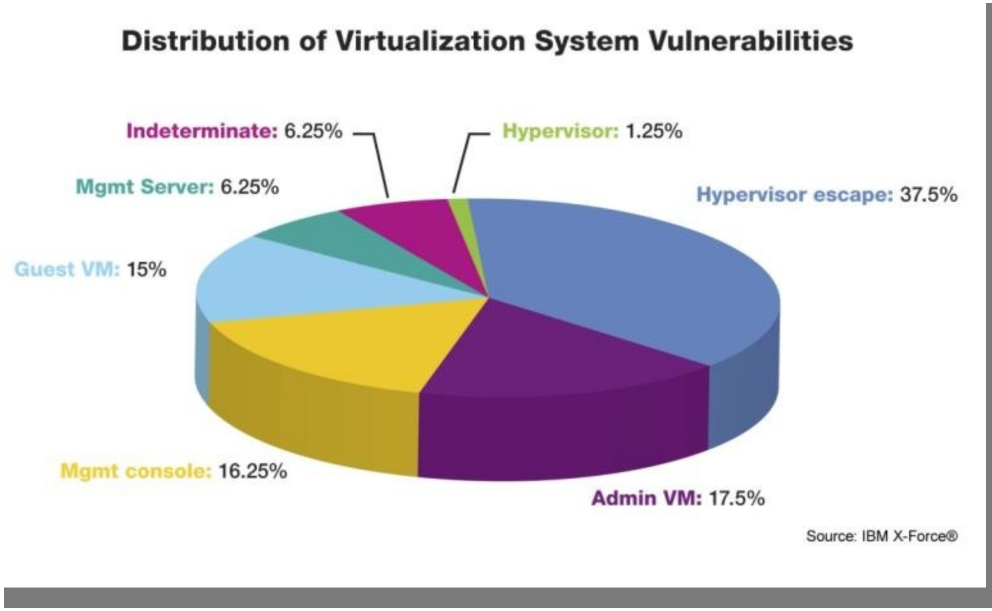
- Low impact DoS attacks

Virtualization Security Increasingly a Focus

- **37.5%** of server class vulnerabilities affect the hypervisor



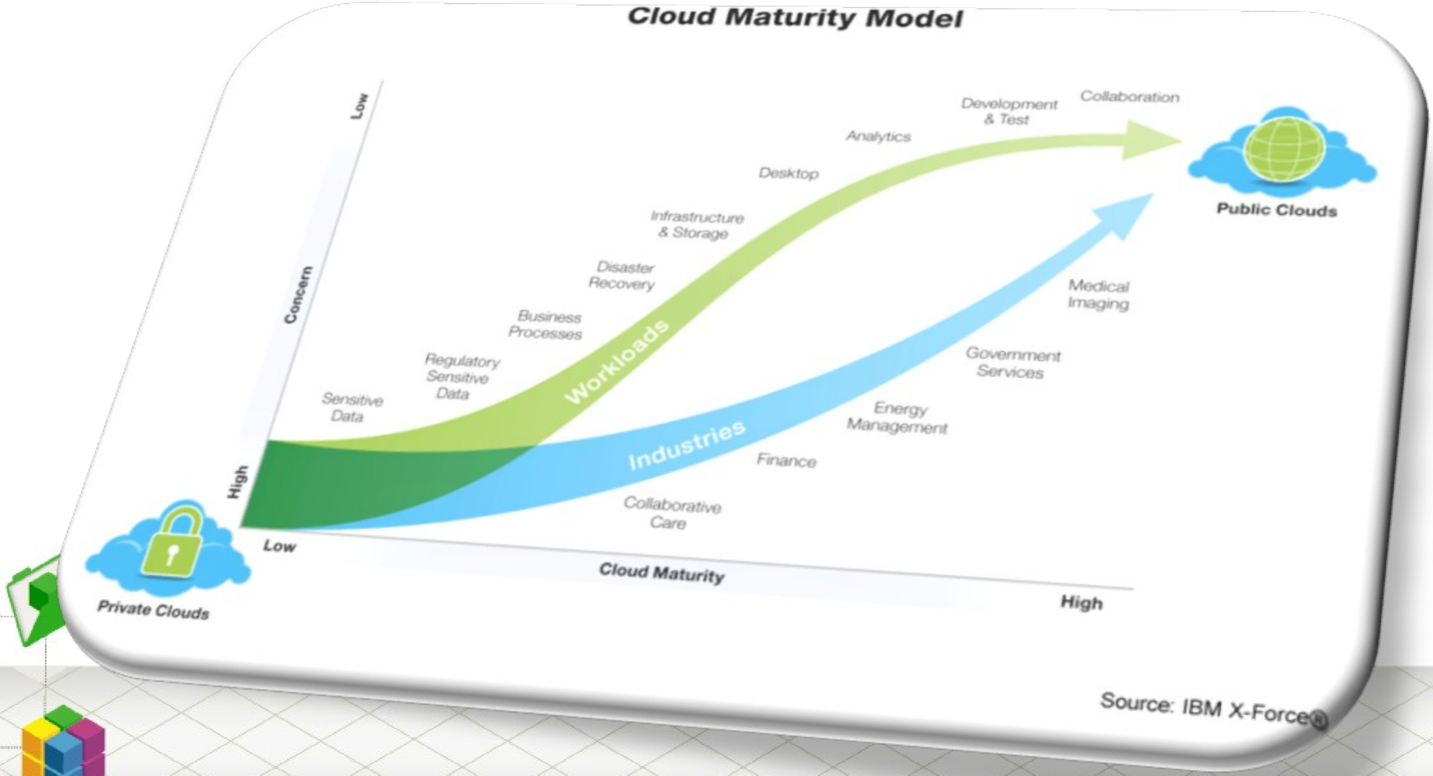
Source: IBM X-Force®



Source: IBM X-Force®

Cloud Security

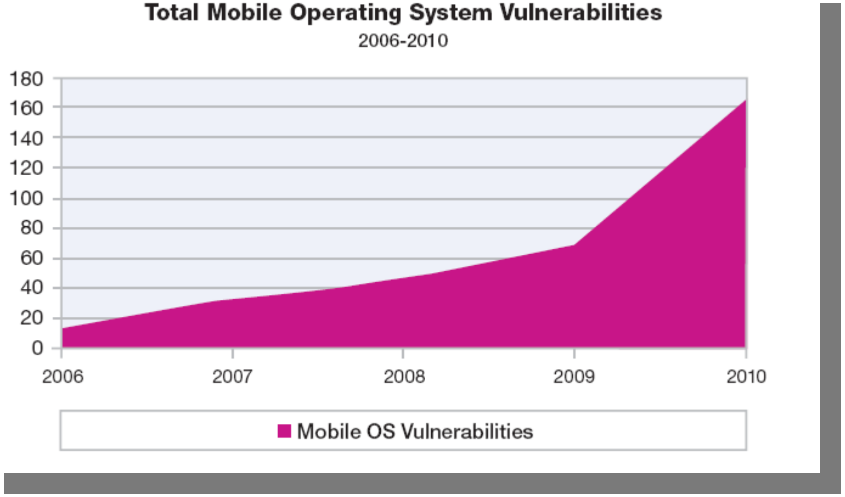
- Adoption of cloud security continues to evolve and knowledge around this emerging technology increased.
  - Providing an infrastructure that is secure by design with purpose-built security capabilities that meet the needs of the specific applications moving into the cloud.
  - As more sensitive workloads move into the cloud, the security capabilities will become more sophisticated.

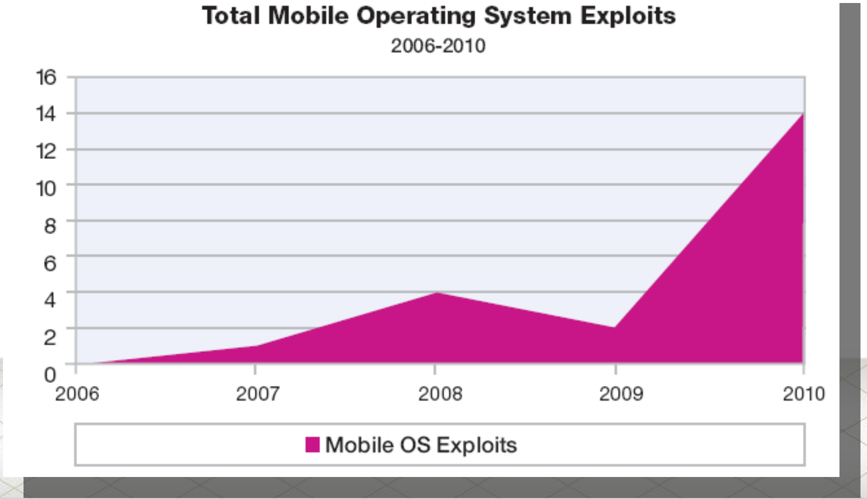


Source: IBM X-Force®

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.
  - Malicious applications were distributed in the Android app market.





For More IBM X-Force Security Leadership

X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security,. Find out more at http://www-935.ibm.com/services/us/iss/xforce/trendreports/

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/

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 or the Frequency X Blog at http://blogs.iss.net/rss.php

Dr. Jean Paul Ballerini
jpballerini@it.ibm.com
IBM Security Solutions