PCTY2011

Pulse Comes to You

Optimising the World's Infrastructure

Corporate & Cyber Security Trends – 2010 and beyond

From the 2010 IBM X-Force® Trend & Risk Report

Dr. Jean Paul Ballerini
WW IBM Security Solutions Sales Enablement, X-Force Spokesperson

Agenda

- IBM's Threat Management R&D: X-Force
- 2010 Trend Report
- Q&A

Mission - Provide the most respected security brand to our Customers and Business Partners.

IBM X-Force Research and Development

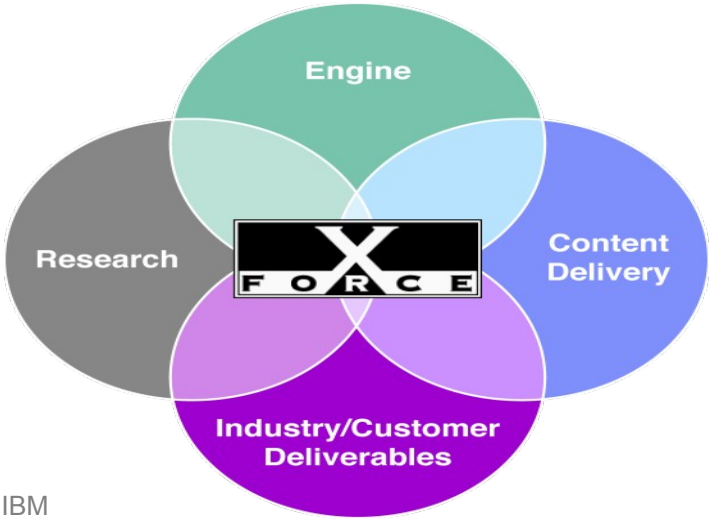
The world's leading enterprise security R&D organization

Engine

- Support content stream needs and capabilities
- Support requirements for engine enhancement
- Maintenance and tool development

Research

- Support content streams
- Expand current capabilities in research to provide industry knowledge to the greater IBM



Global security operations center (infrastructure monitoring)

Content Delivery

- Continue third party testing Dominance
- Execute to deliver new content streams for new engines

Industry/Customer Deliverables

- Blog, Marketing and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

IBM Security – One of the Largest Players in the World

9 Security Operations Centers + 9 Security Research Centers + 11 Security Solution Development Centers + 133 Monitored Countries + 900+ Professional Services Security Consultants + 600+ field security specialists + 4,500 Security Delivery Experts + 400+ security operations analysts

- 20,000+ Devices under Contract
- 3,700+ MSS Clients Worldwide
- 9 Billion+ Events Managed Per Day

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

World’s largest URL filter list

Topicality

- Crawlers collect image and text data from the Internet 24 hours a day on 365 days, which adds up to **200 million pages** each month
- Every day, customers receive updates, equaling some **150,000 changes**

Quality

- Largest URL database meets practically every filtering requirement by means of indexed URLs in **68 categories**

Quantity

- World's largest URL filter list contains **170 million sites**
- World's largest database with **10 billion** evaluated web pages and images

Spam Database

Topicality

- World wide distributed Spam Collectors collect spam 24 hours a day on 365 days -> up to **1.6 m. unique spams** per day
- Update cycle for costumer: 12 times daily

Quality

- Approx. **45 mio.** hot and relevant spam signatures in the database
- > 99.7+ % spam recognition
- < 0.01 % over blocking

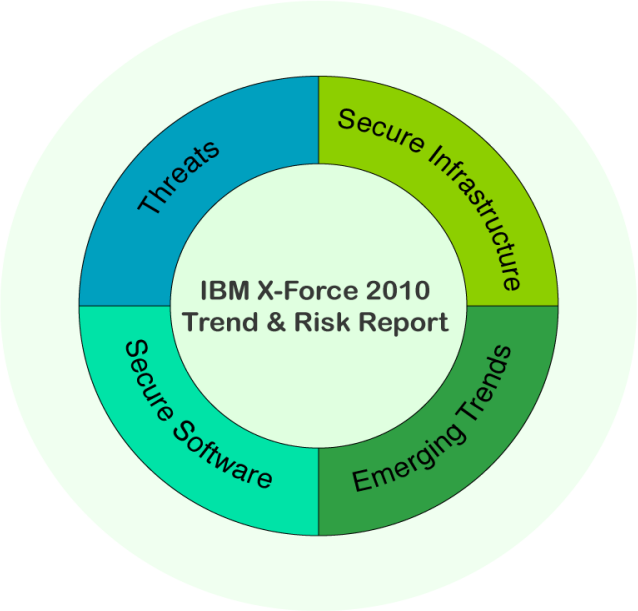
Quantity

- Additional methods for an efficient spam recognition (Bayes Filter, URL Checker, Meta Heuristics, Flow Control, Structure Analysis, Phishing detection, …)

Agenda

- IBM's Threat Management R&D: X-Force
- 2010 Trend Report
- Q&A

New layout and design



Section I–Threats

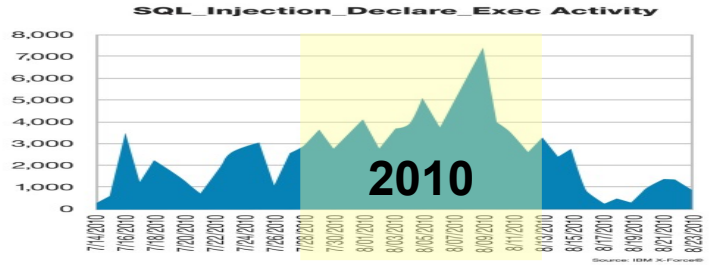
Section II—Operating Secure Infrastructure

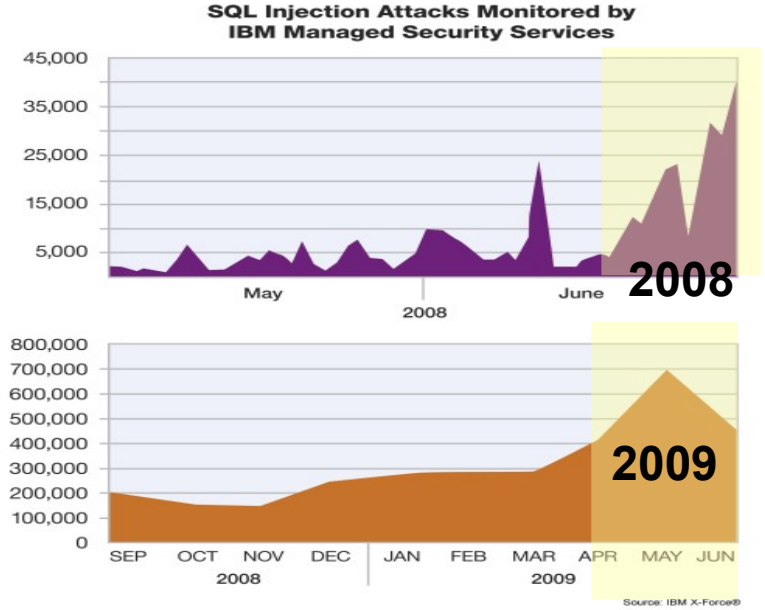
Section III— Developing Secure Software

Section IV—Emerging Trends in Security

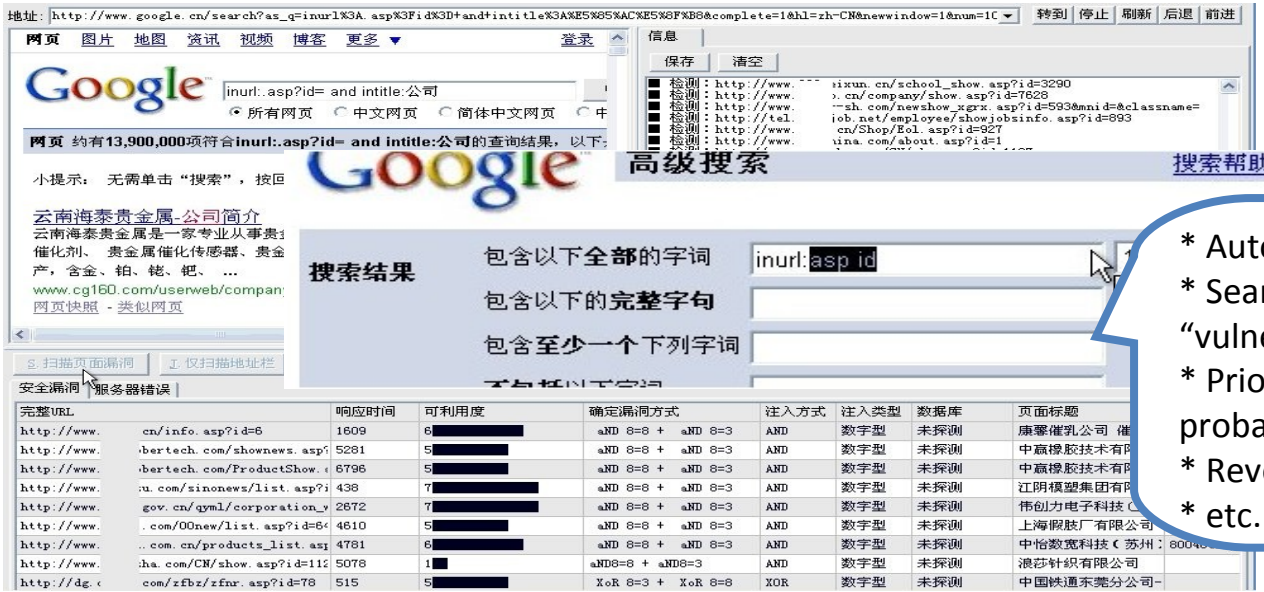
SQL Injection Attacks

- 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.



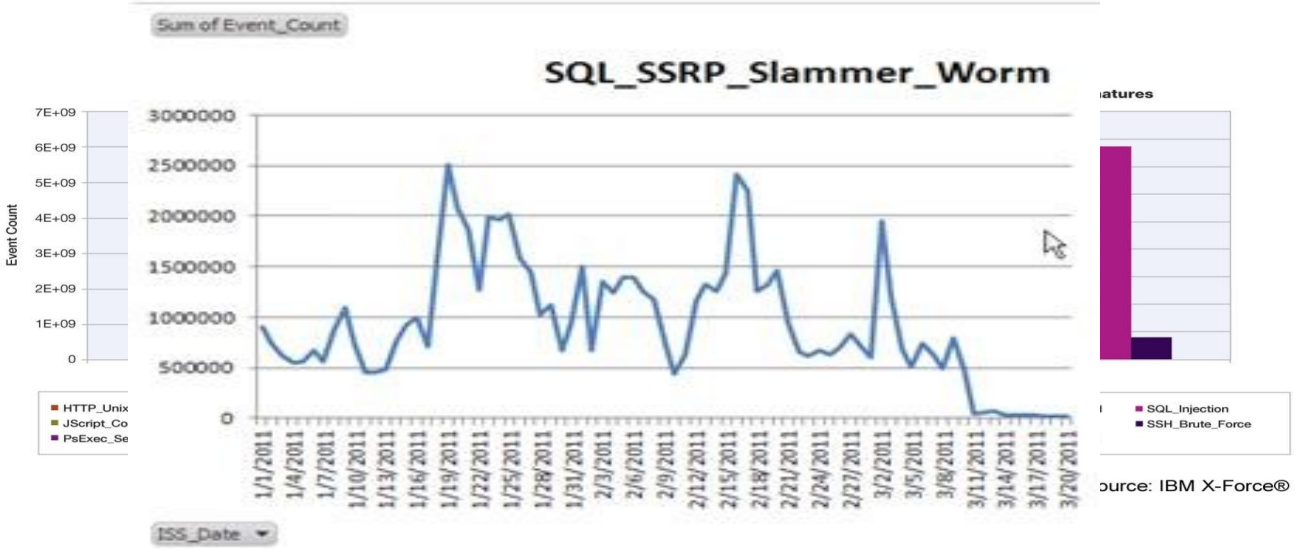


SQL Injection Attacks



* 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.

SQL Slammer Worm still dominating in 2010

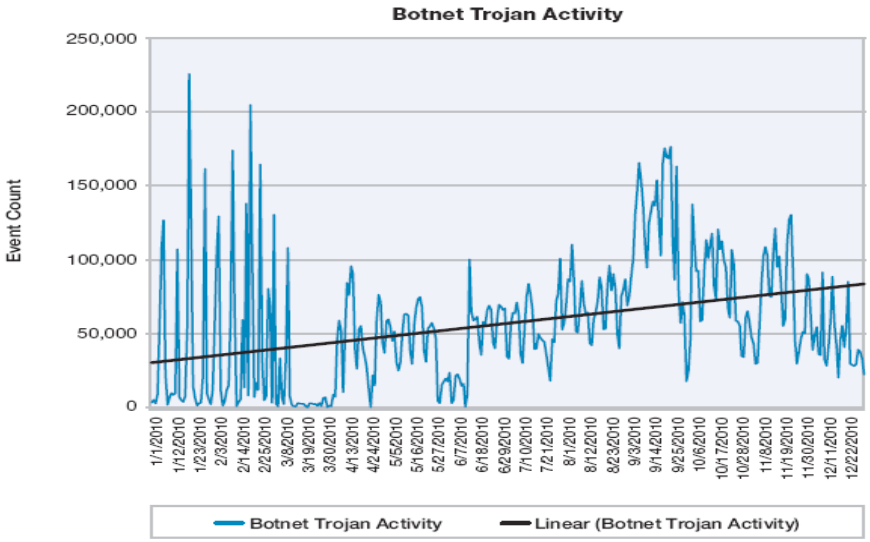


ource: IBM X-Force®

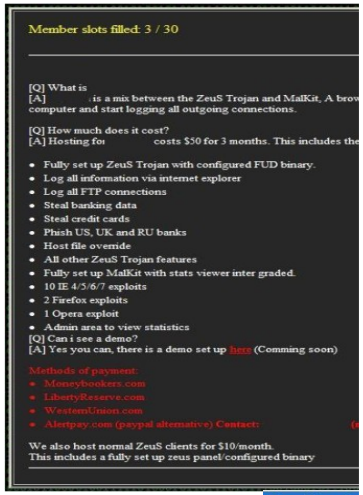
Breaking news: At publish time of this report X-Force witnessed a near complete drop across sensors for SQL Slammer.
Read more about this on the X-Frequency Blog

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.
- Other activity seen is Zeus



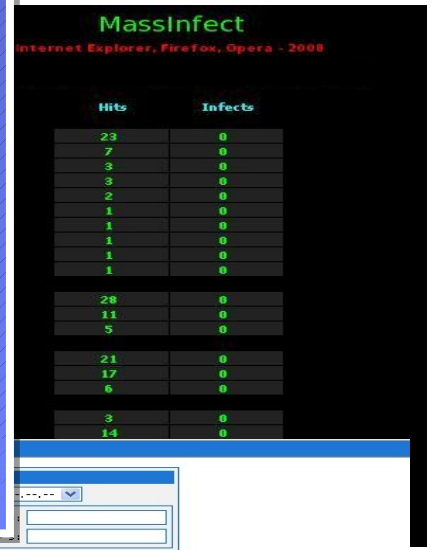
Zeus Crimeware Service

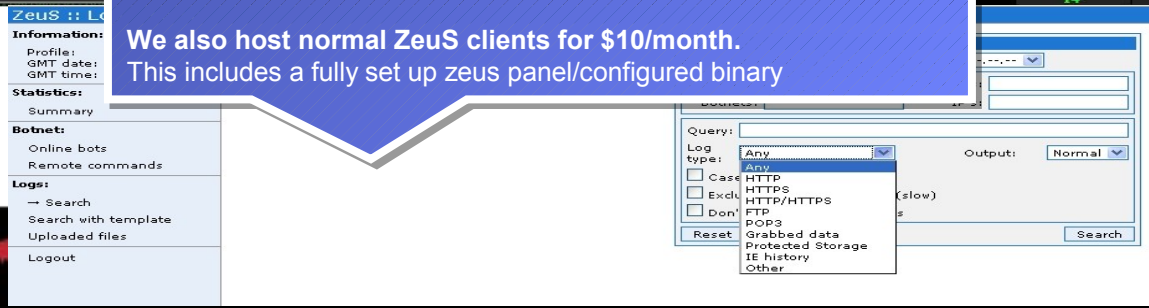


Hosting for costs **$50 for 3 months.**
This includes the following:

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 inter graded.
10 IE 4/5/6/7 exploits
2 Firefox exploits
1 Opera exploit“

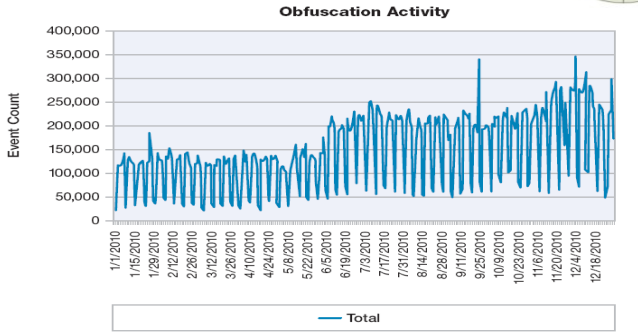
We also host normal ZeuS clients for $10/month.
This includes a fully set up zeus panel/configured binary

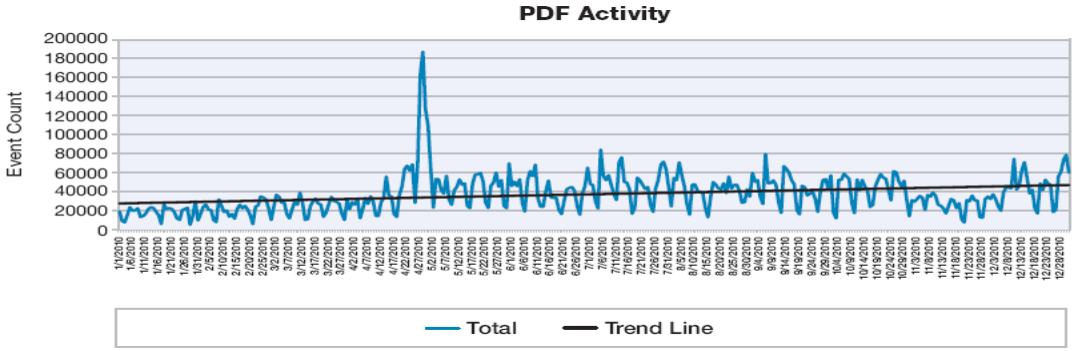




Suspicious Web Pages and Files Show No Sign of Waning

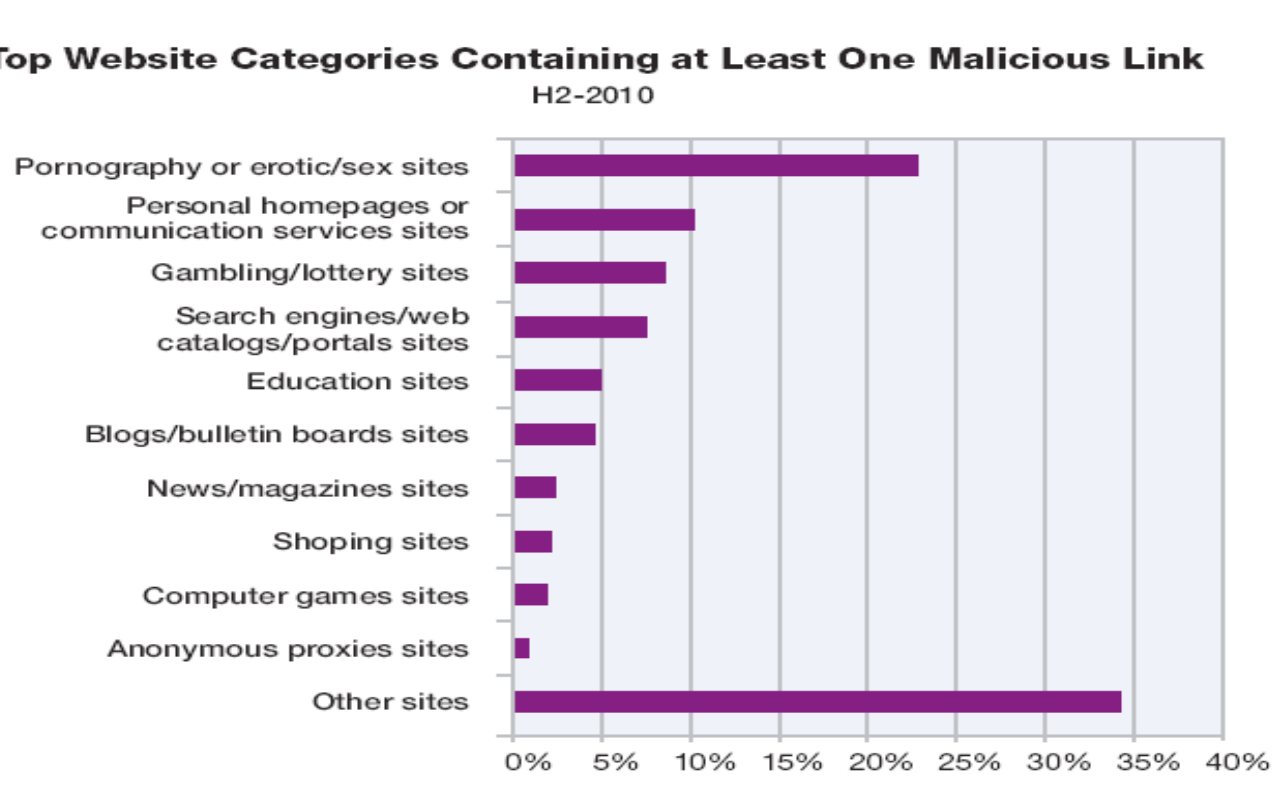
- Obfuscation activity continued to increase during 2010.
- Attackers never cease to find new ways to disguise their malicious traffic via JavaScript and PDF obfuscation.
    - Obfuscation is a technique used by software developers and attackers alike to hide or mask the code used to develop their applications.





Websit

- Profession
  gambling,
  increases
- Out of the
  more of th
  nearly 30 p
  nearly 29 p
  - It's pc
    know



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.

Rank	January 2010	February 2010	March 2010	April 2010	May 2010	June 2010
1.	flickr.com	radikal.ru	livefilestore.com	livefilestore.com	imageshack.us	imageshack.us
2.	imageshack.us	imageshack.us	imageboo.com	imageshack.us	imageshost.ru	imageshost.ru
3.	radikal.ru	livefilestore.com	radikal.ru	imageshost.ru	myimg.de	pikucha.ru
4.	livefilestore.com	flickr.com	imageshack.us	imgur.com	xs.to	imgur.com
5.	webmd.com	live.com	googlegroups.com	myimg.de	imgur.com	mytasvir.com
6.	picsochka.ru	imageboo.com	live.com	xs.to	tinypic.com	mojoimage.com
7.	live.com	capalola.biz	akamaitech.net	icontact.com	livefilestore.com	myimg.de
8.	superbshore.com	feetorder.ru	gonestory.com	tinypic.com	icontact.com	twimg.com
9.	tumblr.com	laughexcite.ru	bestanswer.ru	live.com	googlegroups.com	icontact.com
10.	fairgreat.com	hismouth.ru	wrotelike.ru	binkyou.net	images-amazon.com	twitter.com

Rank	July 2010	August 2010	September 2010	October 2010	November 2010	December 2010
1.	imageshack.us	yahoo.com	the.com	businessinsider.com	rolex.com	pfizer.com
2.	icontact.com	the.com	of.com	migre.me	msn.com	viagra.com
3.	the.com	icontact.com	msn.com	4freeimagehost.com	bit.ly	msn.com
4.	myimg.de	feetspicy.com	pfizerhelpfulanswers.com	bit.ly	pfizer.com	rolex.com
5.	of.com	of.com	and.com	postimage.org	co.cc	bit.ly
6.	imgur.com	ratherwent.com	bit.ly	imgur.com	royalfoote.com	product45h.com
7.	by.ru	and.com	in.com	pfizer.com	royalbelie.com	newpfizermed5k.com
8.	and.com	facebook.com	yahoo.com	viagra.com	royalreleasable.com	xmages.net
9.	in.com	in.com	a.com	uploadgeek.com	luxurystorewatch.com	cordfork.com
10.	tastymighty.com	a.com	x-misc.com	vipplayerq.com	basincook.com	onlinepfizersoft2.com

Table 3: Most common domains in URL spam, 2010

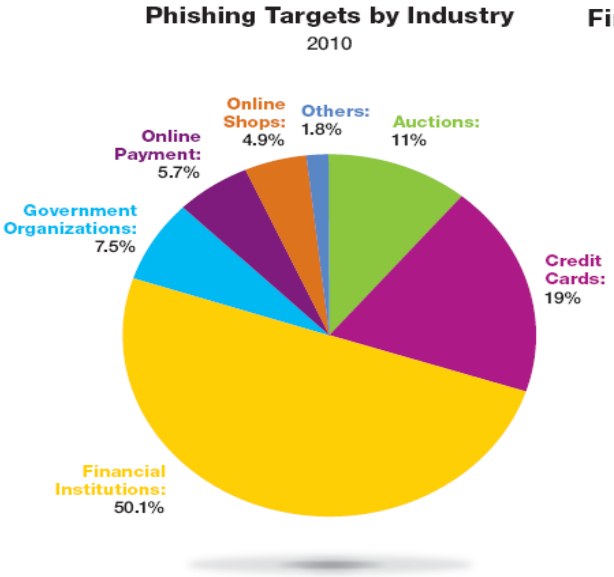
Country	% of Spam
USA	10.9%
India	8.2%
Brazil	8.1%
Vietnam	5.4%
Russia	5.2%

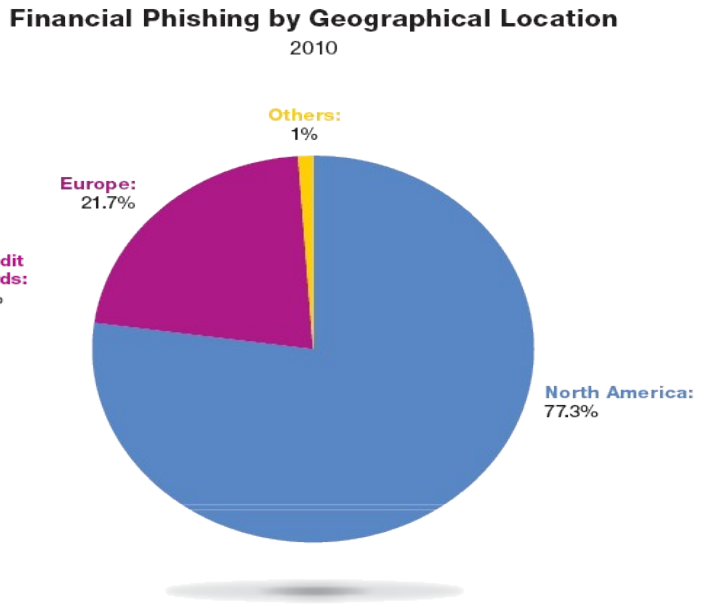
Country	% of Spam
United Kingdom	4.4%
Germany	3.7%
South Korea	3.3%
Ukraine	3.0%
Romania	2.9%

Table 5: Geographical Distribution of Spam Senders – 2010

Phishing Targets Financial & Credit Card Industries

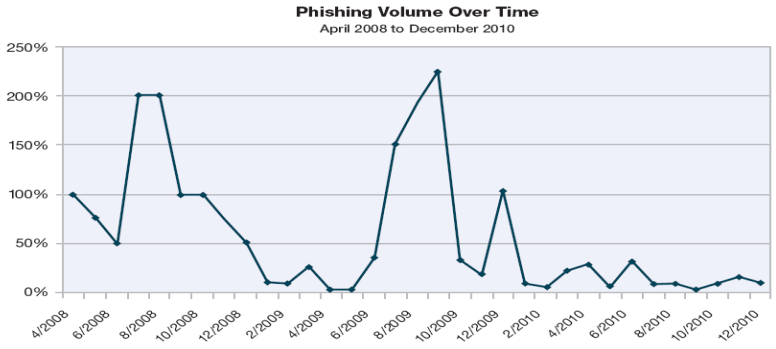
- **50.1%** of phishing is targeted at the financial industry vs. **60.9%** in 2009.
- **77%** of all financial phishing targets in the 2010 are located in North America vs. **95%** in 2009.
  - **22%** of financial phishing targets are located in Europe
- **19%** of phishing emails were targeted at credit cards.





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

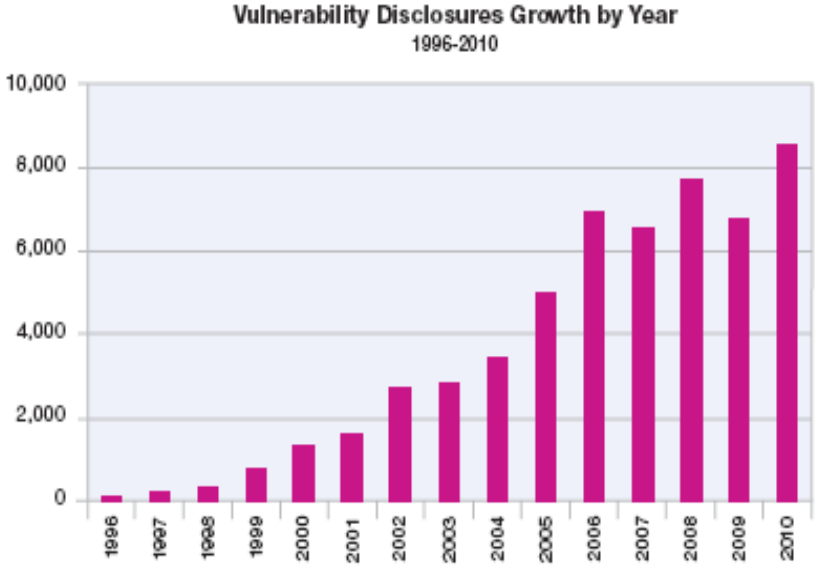


Country	% of Phishing
India	15.5%
Russia	10.4%
Brazil	7.6%
USA	7.5%
Ukraine	6.3%

Table 7: Geographical Distribution of Phishing Senders – 2010

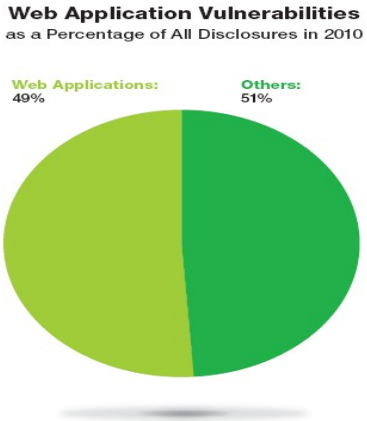
Vendors Reporting the Largest Number of Vulnerability Disclosures in History

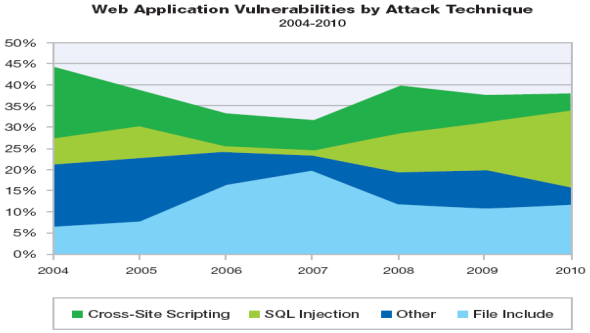
- Vulnerability disclosures up 27%.
  - Web applications continue to be the largest category of disclosure.
- Significant increase across the board signifies efforts that are going on throughout the software industry to improve software quality and identify and patch vulnerabilities.

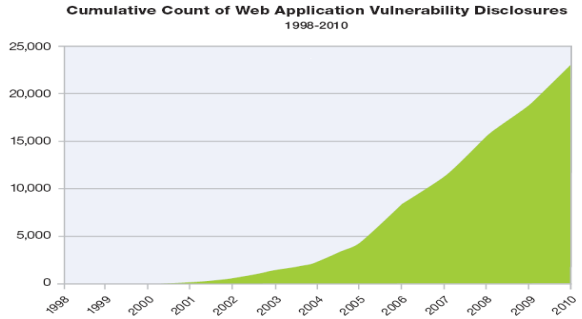


Web App Vulnerabilities Continue to Dominate

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

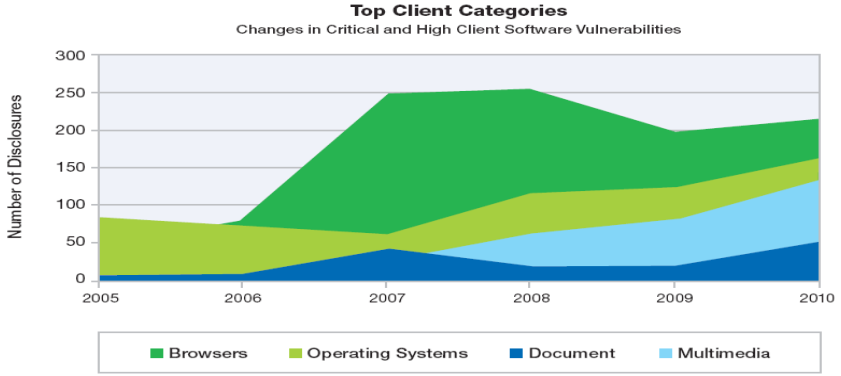


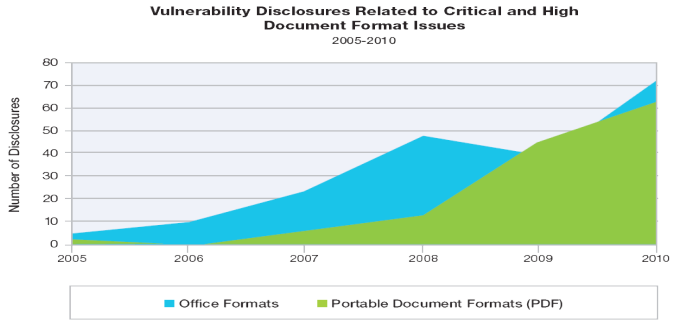


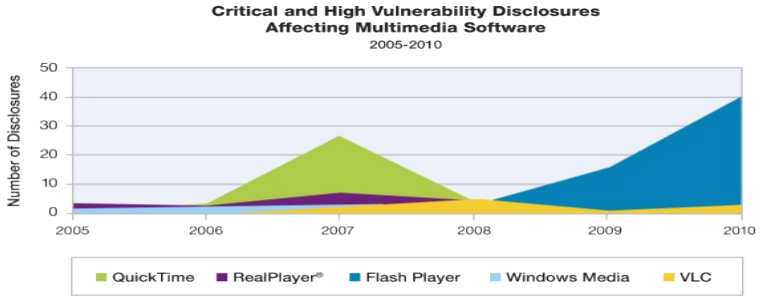


Client-Side Vulnerabilities

- 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.







Source: IBM X-Force®

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.

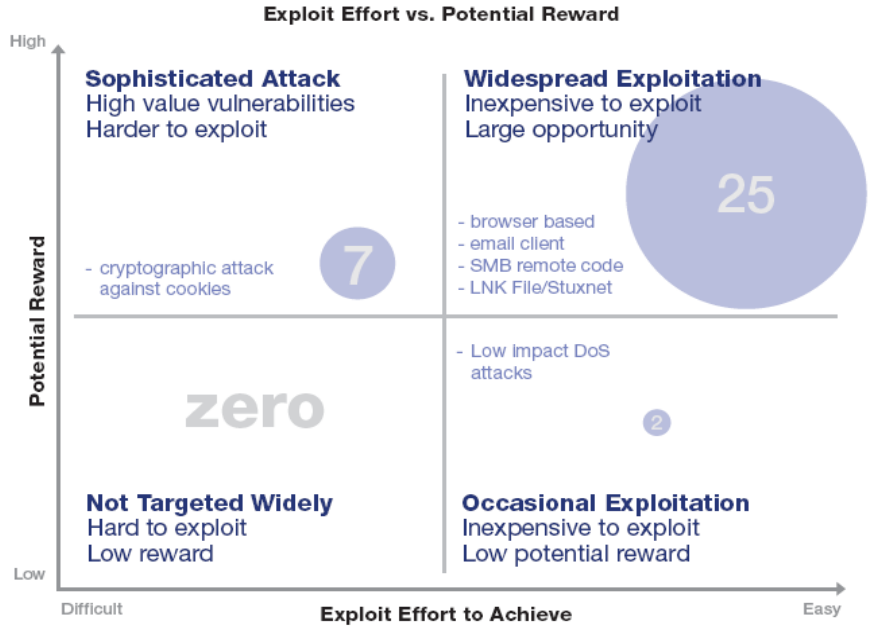
Patch Timeline	All	Top Vendors
Same Day	3400	1814
Week 1	192	34
Week 2	55	11
Week 3	57	12
Week 4	33	7
Week 5	27	7
Week 6	22	4
Week 7	17	3
Week 8	16	8

Table 12: Patch release timing 2010

Patch Release Timing – First 8 Weeks of 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.



Advanced Persistent Threats (APT)

Advanced

- Using exploits for unreported vulnerabilities (zero day)
- Advanced, custom malware that isn't detected by antivirus products
- Coordinated attacks using a variety of vectors

Persistent

- Attacks lasting for months or years
- Resistant to remediation attempts
- Attackers are dedicated to the target – they WILL get in

Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they're actually "out to get you"

Sophisticated Targeted Attacks

Reconnaissance

- Identification of a target and method of compromise
- Initial target is not always the true target

Social Engineering

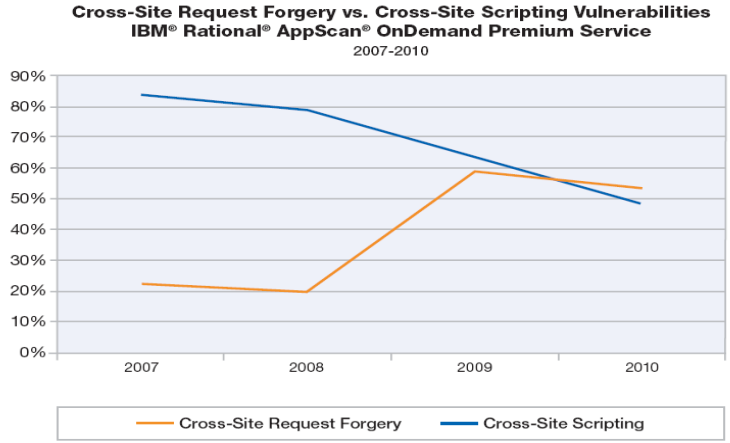
- Most commonly spear-phishing (email or IM that appears to come from a known trusted source)
- Message contains a malicious payload or a link to a web page that has malicious code

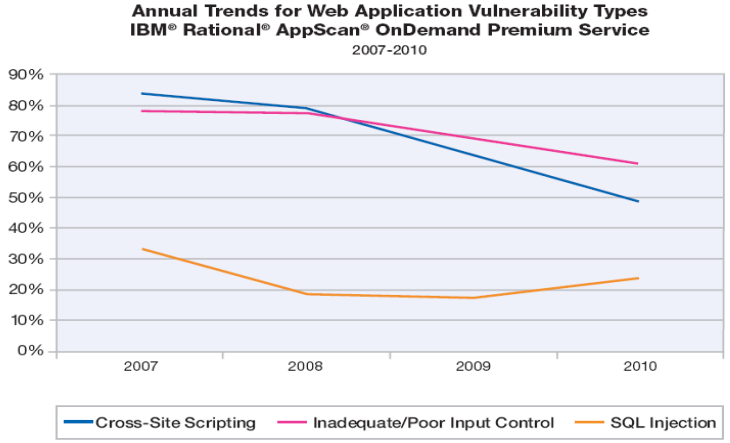
0-Day Tools

- Attacks involve exploitation of never-before-seen vulnerabilities discovered by the attackers
- Not all malware in APT cases is undetectable but the majority of malware used during the initial compromise is custom

Real World Conclusions from Web App Assessments

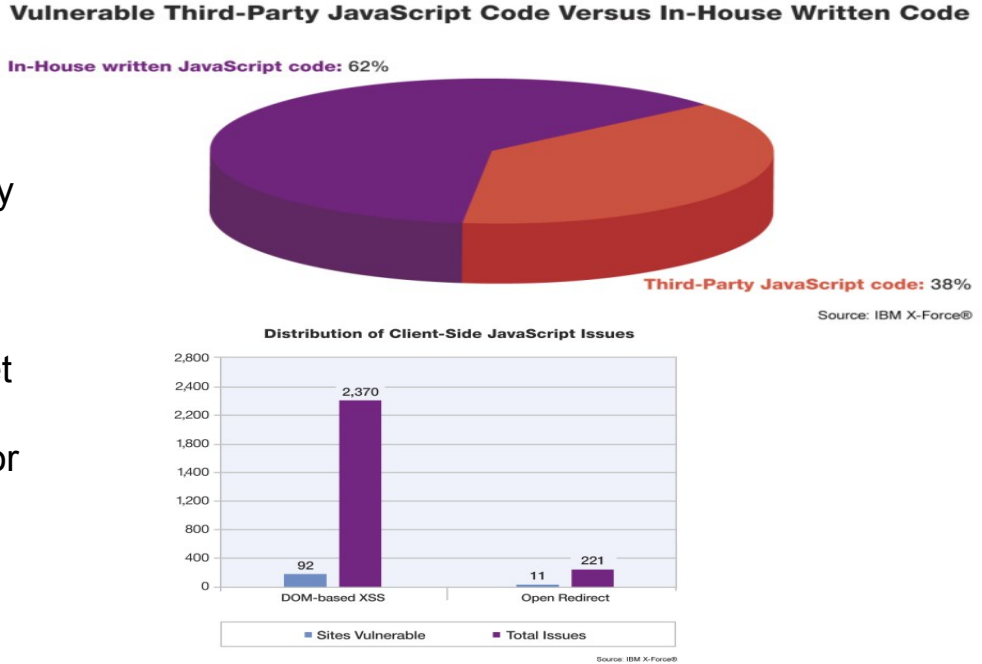
- In 2010, for the first time, we now find that Cross-Site Request Forgery (CRSF) vulnerabilities are more likely to be found in our testing than Cross-Site Scripting (XSS) vulnerabilities.
- XSS and SQL injection are both attributed directly to a lack of input control. The likelihood of finding it in 2010 is more than **60%**.





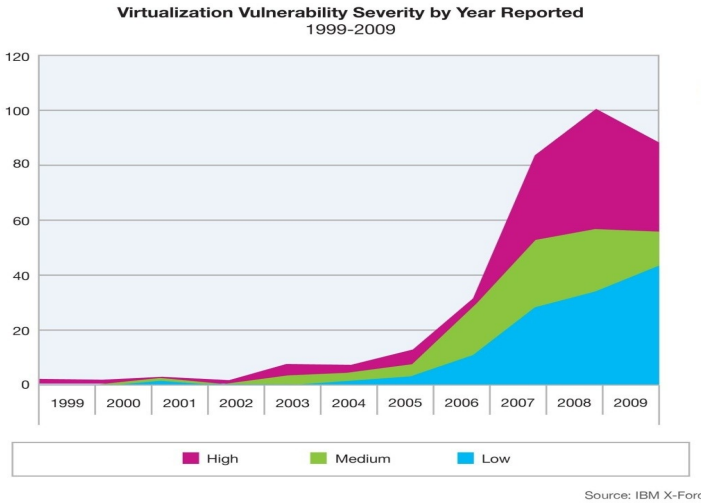
Distribution of Client-Side JavaScript Issues

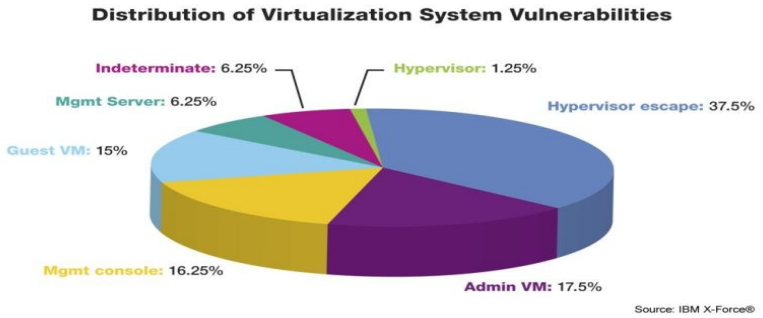
- Client-side vulnerabilities are quite common in modern web applications, especially those that rely on JavaScript for performing client-side logic—i.e. Web 2.0, AJAX and rich Internet applications.
- In addition, a substantial number of the existing JavaScript client-side vulnerabilities on the Internet are introduced from 3rd party code that is not developed in-house, and usually is not reviewed for security issues.



Virtualization Security Increasingly a Focus

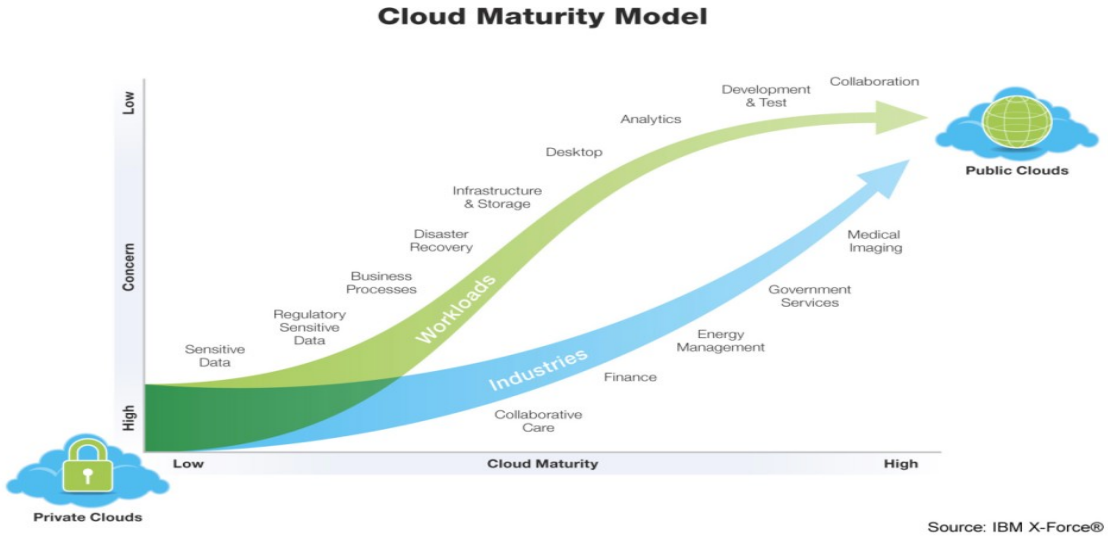
- **37.5%** of server class vulnerabilities affect the hypervisor





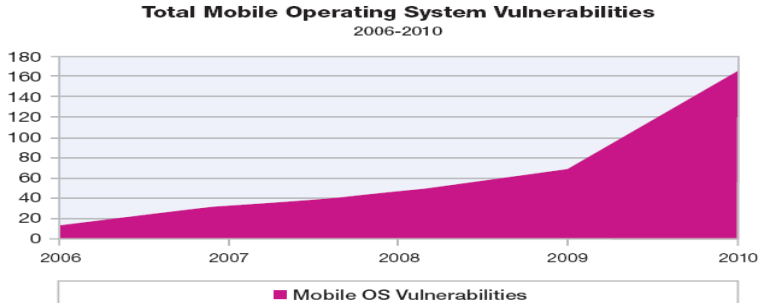
Cloud Security

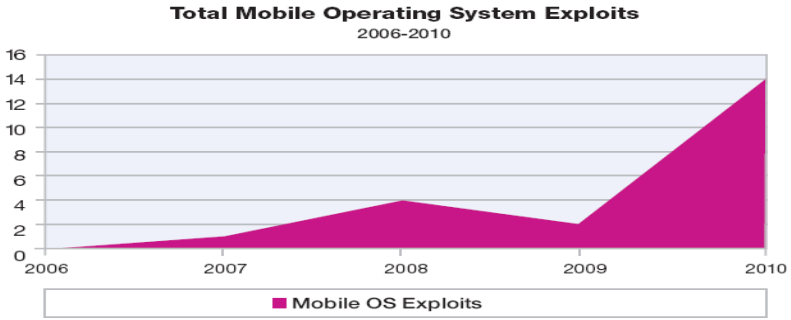
- Adoption of cloud security continues to evolve and knowledge around this emerging technology increased.
  - Providing an infrastructure that is secure by design with purpose-built security capabilities that meet the needs of the specific applications moving into the cloud.
  - As more sensitive workloads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



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.





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

Agenda

- IBM's Threat Management R&D: X-Force
- 2010 Trend Report
- Q&A

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