2009 IBM X-Force®

Trend & Risk Report Briefing

James Barrett, IBM Security Solutions

IBM Software

PCTY2010

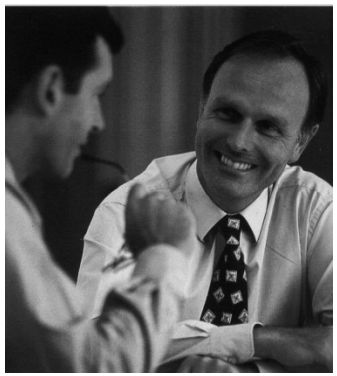
Pulse Comes to You

THE TRUTH

A 

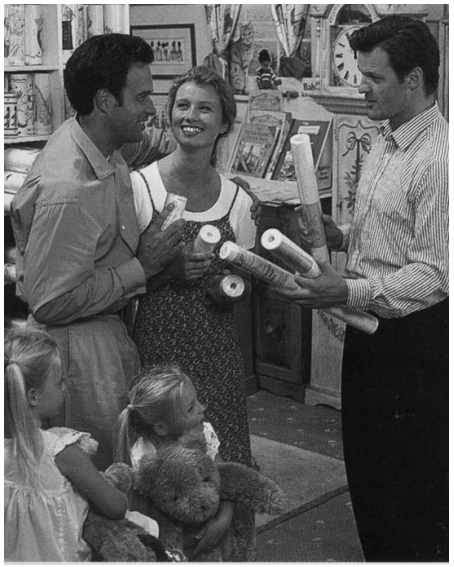
comes in all shapes

At least 70% of them are trusted people



Partners

Employees



Customers

Vendors

People just don't think --Before they act

The Importance of Research to Security: IBM Internet Security Systems X-Force Research Team

Research → Technology → Solutions

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

XForce Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

The X-Force team delivers reduced operational complexity –
helping to build integrated technologies that feature "baked-in" simplification-
"Protecting people from themselves"

Report Summary -- Attacks Continue Across all Security Domains

Application and Process

- 6,601 new vulnerabilities were discovered in 2009, an 11% decrease over 2008, largely due to declines in SQL injection and Active X vulnerability disclosures.
- 49% of all vulnerabilities are Web application vulnerabilities.
- 52% of all vulnerabilities disclosed had no vendor-supplied patches available at the end of 2009.

Data and Information

- PDF-related vulnerabilities have far surpassed those affecting Office documents.
- Vast majority of Web-based exploitation centered around Web exploit toolkits in contrast to purpose-built lone sources.
- US continues as the top hoster of malicious Web links.

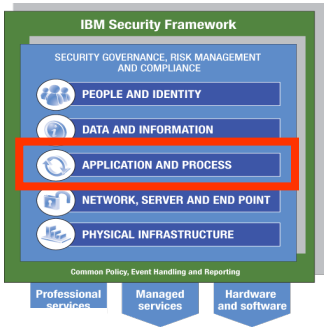
Network, Server, and End Point

- 7.5 percent of the Internet is considered “socially” unacceptable, unwanted, or flat out malicious.
- New malicious Web links increased by 345% compared to 2008.

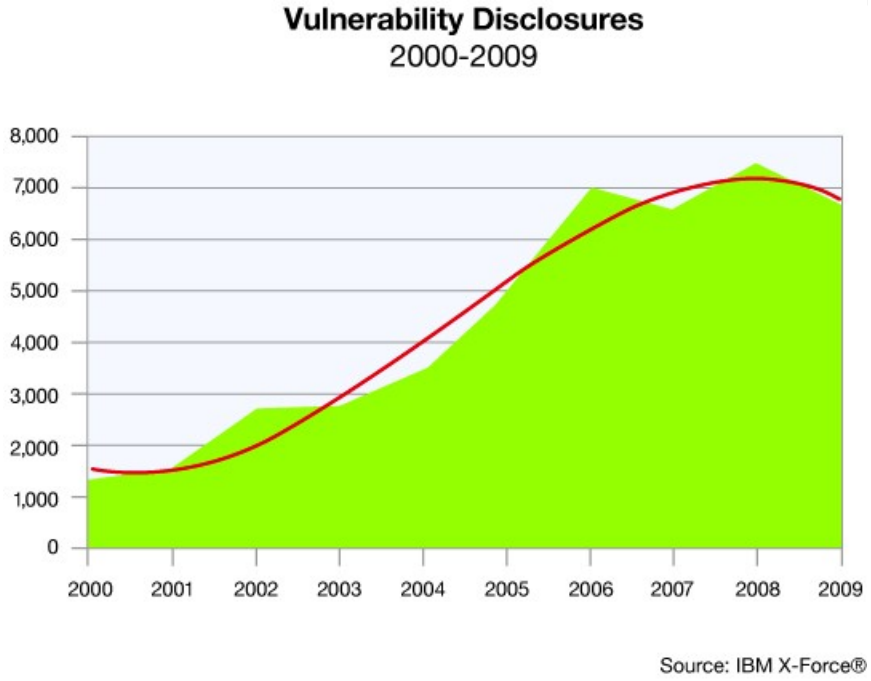
People and Identity

- Majority of spam (80%) is still classified as URL spam—spam messages that include URLs that a person clicks to view the spam contents.
- Amount of URL spam using well-known and trusted domain names continue to increase.
- 60.9% of phishing is targeted at the finance industry, 20.4% targeted at government organizations

Disappearance of Low Hanging Fruit: Vulnerability Disclosures & Exploitation Declines



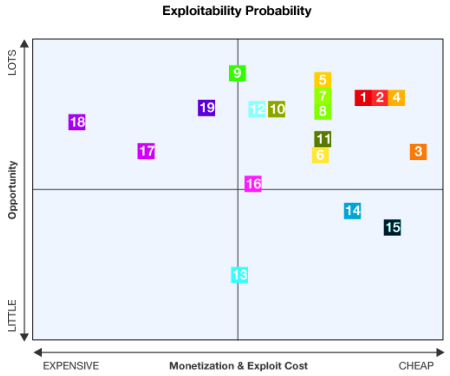
- Declines in some of the largest categories of vulnerabilities.
  - Web applications continue to be the largest category of disclosure.
  - SQL Injection and File Include, have declined.
  - ActiveX controls which mostly impact client applications has also declined.
- Tuesdays continue to be the busiest day of the week for vulnerability disclosures.
- 2009 vulnerability disclosures by severity had no significant changes from 2008 percentages.



Source: IBM X-Force®

The Economics of Attacker Exploitation

- Economics continue to play heavily into the exploitation probability of a vulnerability.
- Web Browser and Document Reader vulnerabilities are very profitable and easily executable.



1	December 15, 2009	Adobe Acrobat and Acrobat Reader Remote Code Execution
	October 9, 2009	Adobe Acrobat and Acrobat Reader Remote Code Execution
	July 22, 2009	Adobe Acrobat and Adobe Flash Remote Code Execution
2	November 23, 2009	Microsoft Internet Explorer mshtml.dll RCE
	July 6, 2009	Multiple Microsoft Video Control ActiveX Remote Code Execution Vulnerabilities
	July 20, 2009	Microsoft Office Web Components Spreadsheet ActiveX Control RCE
3	September 10, 2009	Microsoft Windows SRV2.SYS Remote Code Execution Vulnerability
4	July 16, 2009	Mozilla Firefox Font HTML Tags Remote Code Execution
5	July 14, 2009	Multiple Microsoft DirectShow Remote Code Execution Vulnerabili-
6	November 10, 2009	Microsoft Windows WSDAPI Remote Code Execution Vulnerability
7	October 13, 2009	Microsoft Windows Indexing Service ActiveX Control Remote Code Execution Vulnerability
	September 8, 2009	Microsoft Windows JScript Remote Code Execution Vulnerability
8	August 11, 2009	Network Security Services (NSS) Parser Remote Code Execution Vulnerability
9	August 11, 2009	Network Security Services (NSS) Certificate Security Bypass Vulnerability
10	October 13, 2009	Multiple Microsoft Windows GDI+ Image Remote Code Execution Vulnerabilities
	August 11, 2009	Microsoft Windows AVI Remote Code Execution Vulnerability
	November 10, 2009	Microsoft Windows Kernel Font Code Execution Vulnerability
	July 14, 2009	Multiple Microsoft Windows Embedded OpenType Font Engine Remote Code Execution Vulnerabilities
11	August 11, 2009	Microsoft WINS Replication Remote Code Execution Vulnerability
12	August 11, 2009	Microsoft Windows RDP Services Client ActiveX Control Remote Code Execution Vulnerability
	July 28, 2009	Microsoft Internet Explorer ATL Killbit Evasion Vulnerability
	July 28, 2009	Multiple Microsoft Visual Studio Active Template Remote Code Execution Vulnerabilities
13	November 9, 2009	Transport Layer Security (TLS) Handshake Renegotiation
14	August 11, 2009	ISC BIND dns_db_findrdataset() DoS Vulnerability
15	September 2, 2009	Microsoft Internet Information Services FTP Remote Code Execution Vulnerability
16	December 9, 2009	HP OpenView Network Node Manager Remote Code Execution Vulnerability
17	December 1, 2009	Novell eDirectory Remote Code Execution Vulnerability
18	July 14, 2009	ISC DHCP Client Buffer Overflow Vulnerability
19	October 13, 2009	Microsoft Internet Explorer Arguments Remote Code Execution Vulnerability

Source: IBM X-Force®

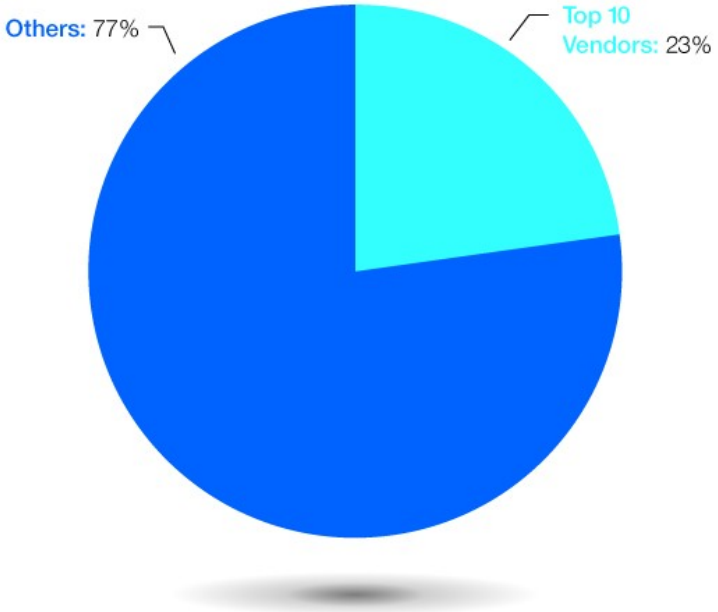
Apple, Sun and Microsoft Top Vendor List for Disclosures

- Top ten vendors account for nearly a quarter (**23%**) of all disclosed vulnerabilities, up from **19%** in 2008.
- Significant changes to the Top Ten List including:
  - Microsoft dropped from #1 to #3 after holding top spot since 2006.
  - Adobe makes it's debut on the top ten list at number nine.

Ranking	Vendor	Disclosures
1.	Apple	3.8%
2.	Sun	3.3%
3.	Microsoft	3.2%
4.	IBM	2.7%
5.	Oracle	2.2%
6.	Mozilla	2.0%
7.	Linux	1.7%
8.	Cisco	1.5%
9.	Adobe	1.4%
10.	HP	1.2%

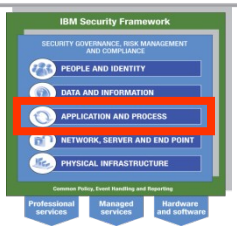
Table 3: Vendors with the Most Vulnerability Disclosures, 2009

Percentage of Vulnerability Disclosures Attributed to Top 10 Vendors
2009



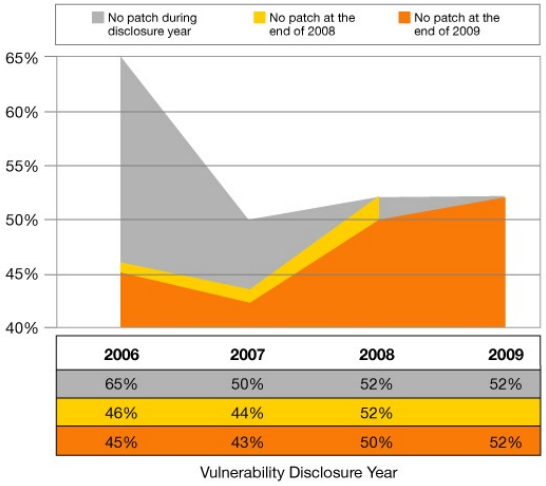
Source: IBM X-Force®

Patches Still Unavailable for Over Half of Vulnerabilities



- Over half (**52%**) of all vulnerabilities disclosed in 2009 had no vendor-supplied patches to remedy the vulnerability.
  - **45%** of vulnerabilities from 2006, **43%** from 2007 and **50%** from 2008 still have no patches available at the end of 2009.

Percentage of Vulnerabilities with Vendor-Supplied Patches by Vulnerability Disclosure Year
2006-2009



	2006	2007	2008	2009
No patch during disclosure year	65%	50%	52%	52%
No patch at the end of 2008	46%	44%	52%	
No patch at the end of 2009	45%	43%	50%	52%

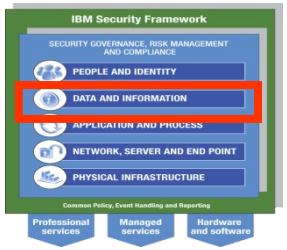
Vulnerability Disclosure Year

Source: IBM X-Force®

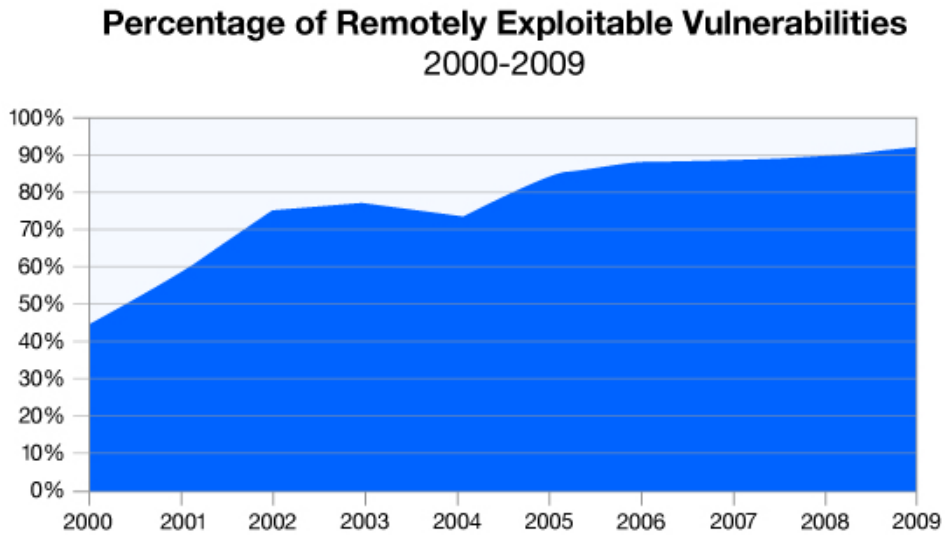
Vendor	Percent of 2009 Disclosures with No Patch	Percent of Critical & High 2009 Disclosures with No Patch
All Vendors–2009 Average	52%	60%
Linux	50%	53%
Oracle	40%	38%
Novell	27%	31%
IBM	25%	27%
Google	47%	25%
Apple	14%	22%
Microsoft	29%	15%
Sun	7%	8%
Symantec	18%	7%
HP	16%	5%
Adobe	4%	4%
Cisco	11%	1%
Opera	47%	0%
GNU	33%	0%
Mozilla	15%	0%
Rim	14%	0%

Table 4: Best and Worst Patchers, 2009

Remotely Exploitable Vulnerabilities On The Rise

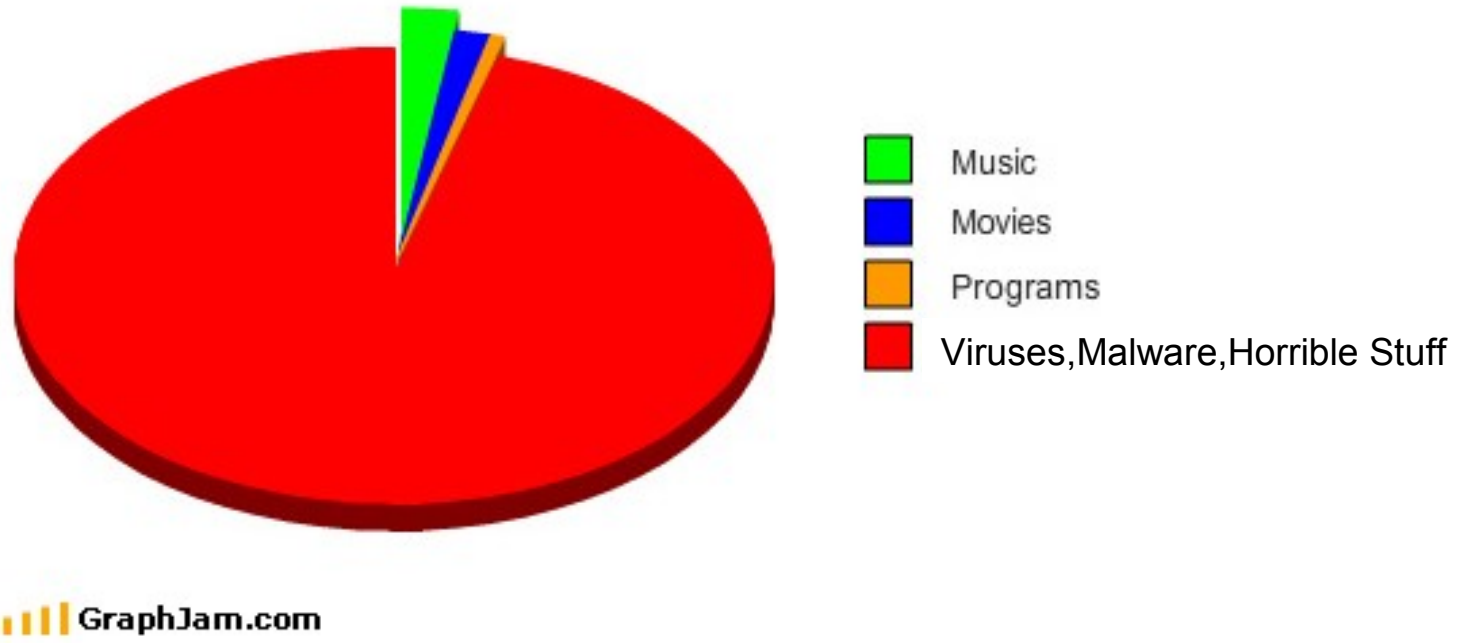


- In the past four years, remotely exploitable vulnerabilities have grown from **85%** to **92%** of all vulnerability disclosures.
  - These vulnerabilities are significant because they can be executed without physical access to a vulnerable system.

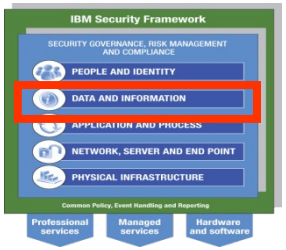


Source: IBM X-Force®

What People Download From Limewire

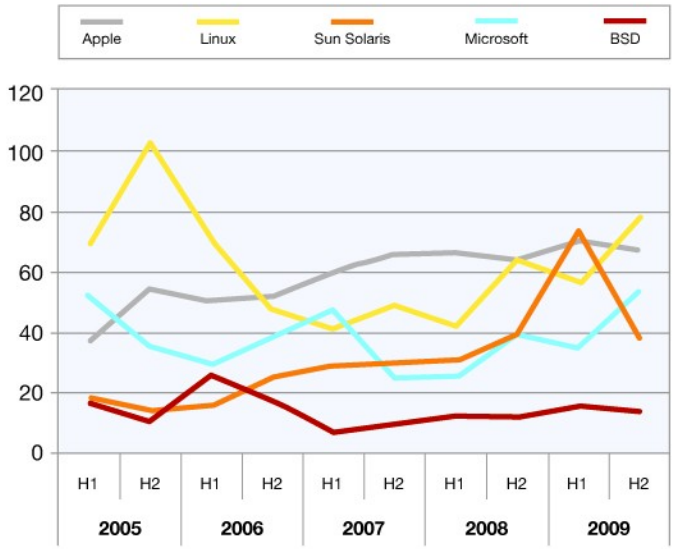


Most Vulnerable Operating Systems



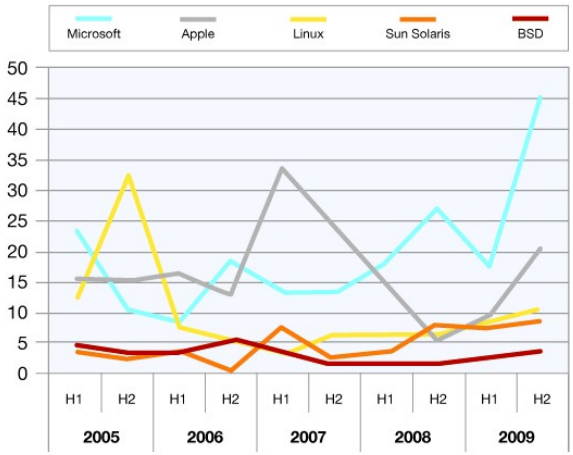
- In the second half of 2009, the number of new vulnerabilities for Linux and Microsoft took a sharp turn upwards while Sun Solaris drastically declined.

Vulnerability Disclosures Affecting Operating Systems
2005-2009



Source: IBM X-Force®

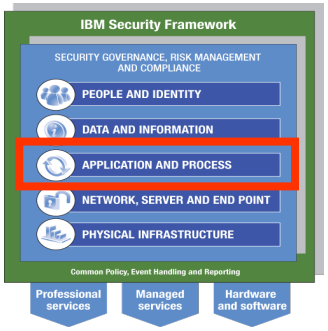
Critical and High Vulnerability Disclosures Affecting Operating Systems
2005-2009



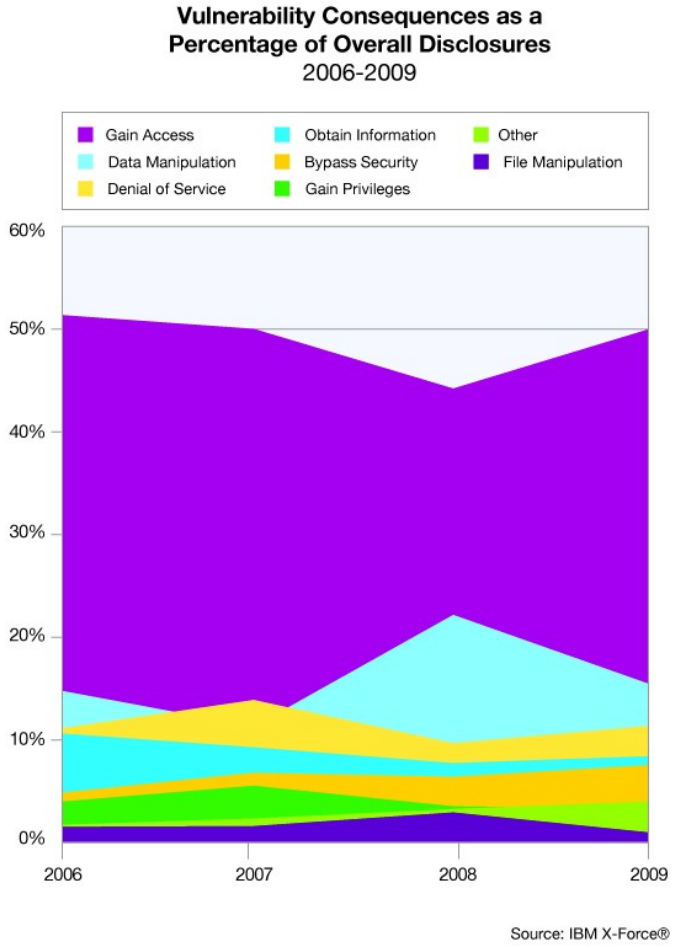
Source: IBM X-Force®

- BSD is in the number five slot, replacing IBM AIX who was fifth in 2008.
- For critical and high vulnerabilities, Microsoft takes first place. Apple is in second place.

2009 Attacker Motivation is to Gain Access and Manipulate Data

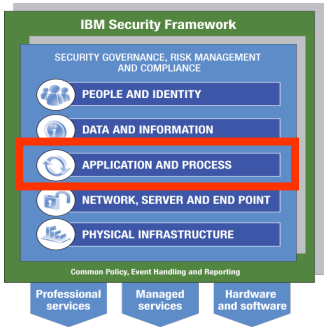


- "Gain access" remains the primary consequence of vulnerability exploitation.
  - Approaching the **50%** mark that was previously seen throughout 2006 and 2007.
- "Data Manipulation" took a plunge but still higher in comparison to 2006 and 2007.
- "Bypass Security" and "Denial of Service" is increasing.

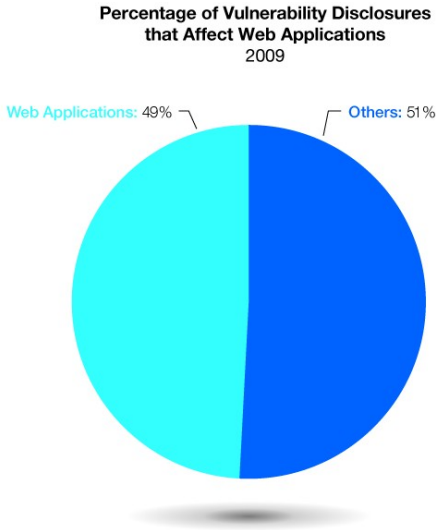


Source: IBM X-Force®

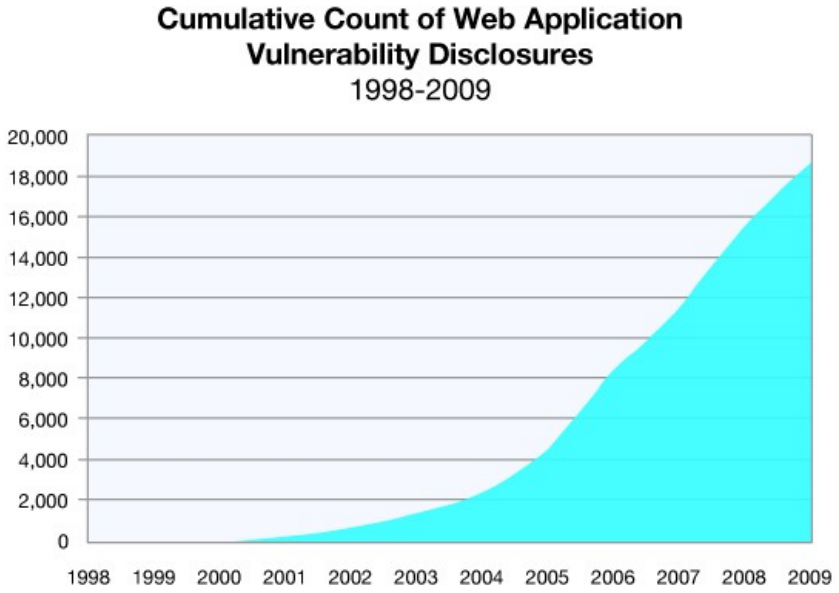
Web App Vulnerabilities Continue to Dominate



- **49%** of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting disclosures surpassed SQL injection to take the top spot.
- **67%** of web application vulnerabilities had no patch available at the end of 2009.



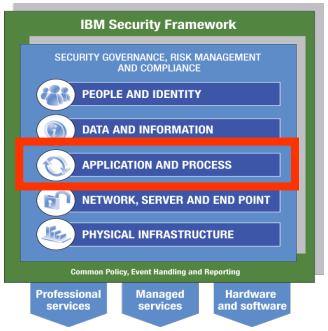
Source: IBM X-Force®



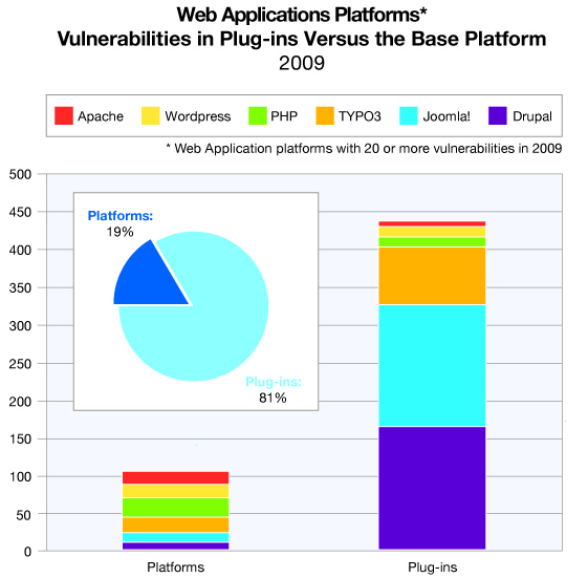
Source: IBM X-Force®

What can possibly happen?

Web App Plug-Ins Are Vulnerable



- **81%** of web application vulnerabilities affect plug-ins and not the base platform.
- **80%** or more of the vulnerabilities affecting plug-ins for Apache and Joomla! had no patch.

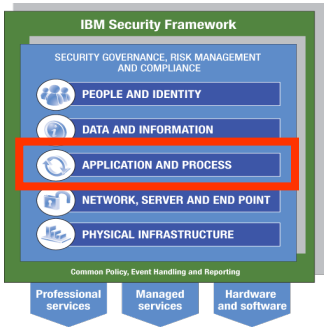


Source: IBM X-Force®

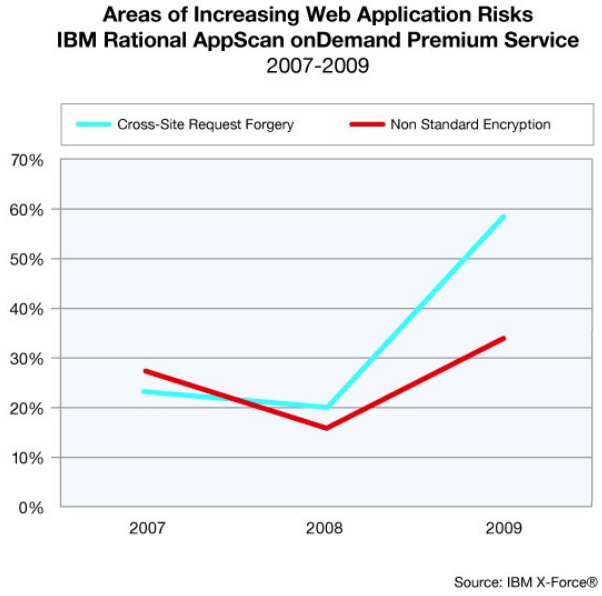
Platform	Percent of Vulnerabilities with No Patch	
	Base Platform	Plug-ins
Apache	23%	86%
Drupal	18%	13%
Joomla!	8%	80%
PHP	42%	15%
TYPO3	5%	51%
Wordpress	13%	57%

Table 8: Percentage of Web Application Platforms and Plug-in Vulnerability Disclosures without a Patch, 2009

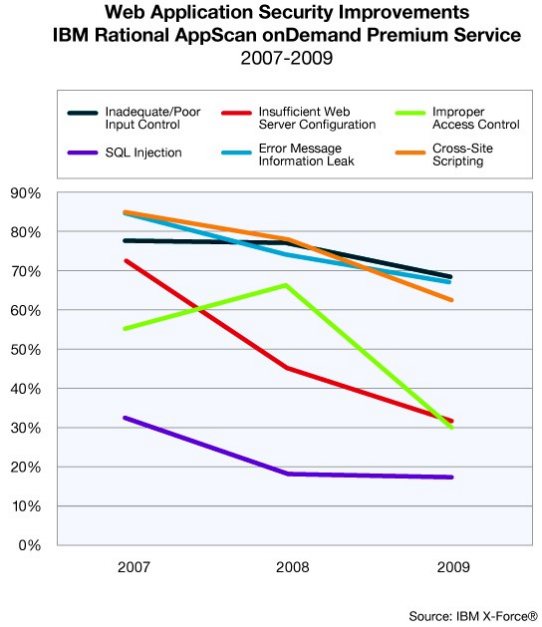
Real World Conclusions from Web App Assessments



- Cross-Site Request Forgery (CRSF) vulnerabilities increased from **22%** in 2007 to **59%** in 2009.
- SQL Injection vulnerabilities dropped from **33%** in 2007 to **18%** in 2009.
- Cross-Site Scripting (XSS) vulnerabilities dropped from **83%** in 2007 to **64%** in 2009.
- Inadequate Input control is the most prevalent developer-related issue, and the likelihood of finding it in 2009 is almost **70%**.



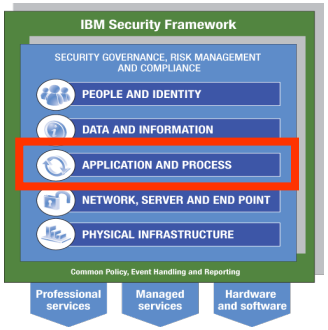
Source: IBM X-Force®



Source: IBM X-Force®

Most Prevalent Web Application Vulnerabilities by Industry

- CSRF findings are increasing in all verticals.
  - Highest in Telecommunication sector applications at **74%** and the lowest in retail & logistic applications at **16%**.
- SQL Injection is much more likely to occur in Information Technology (including "dot com") applications (**37%**) than in Financial Services applications (**8%**).
- XSS findings differ greatly from one industry to another: Telecommunications is the highest at **95%** and Financial Services is the lowest at **58%**.



Financial Services

Category	Avg # Vulns	% Likely to Occur
Improper Use of SSL	61.5	84%
Improper Access Control	3.2	76%
Error Message Information Leak	36.2	71%
Inadequate / Poor Input Control	12.0	61%
Cross-Site Scripting	11.3	58%
Information Disclosure	2.0	55%
Improper Application Deployment	2.6	50%

Telecommunications

Category	Avg # Vulns	% Likely to Occur
Cross-Site Scripting	91.5	95%
Inadequate / Poor Input Control	94.7	95%
Information Disclosure	30.1	84%
Error Message Information Leak	45.5	79%
Improper Application Deployment	3.1	79%
Cross-Site Request Forgery	5.3	74%

Retail and Logistics

Category	Avg # Vulns	% Likely to Occur
Improper Use of SSL	26.8	76%
Error Message Information Leak	15.0	74%
Cross-Site Scripting	21.2	68%
Inadequate / Poor Input Control	22.9	63%
Information Disclosure	5.1	63%
Insufficient Web Server Configuration	5.6	55%

Industrials

Category	Avg # Vulns	% Likely to Occur
Inadequate / Poor Input Control	35.8	72%
Error Message Information Leak	14.7	67%
Cross-Site Scripting	31.7	65%
Information Disclosure	17.3	58%
Cross-Site Request Forgery	7.7	58%

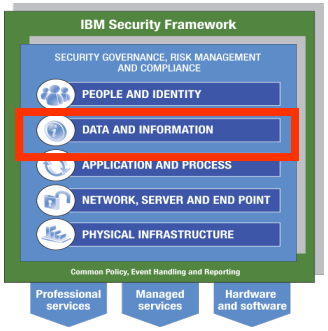
Information Technology

Category	Avg # Vulns	% Likely to Occur
Inadequate / Poor Input Control	47.5	95%
Cross-Site Scripting	14.6	89%
Improper Application Deployment	4.1	84%
Improper Access Control	2.5	84%
Error Message Information Leak	39.8	74%
Improper Use of SSL	15.8	58%
Information Disclosure	4.1	58%

Health, Medical and Education

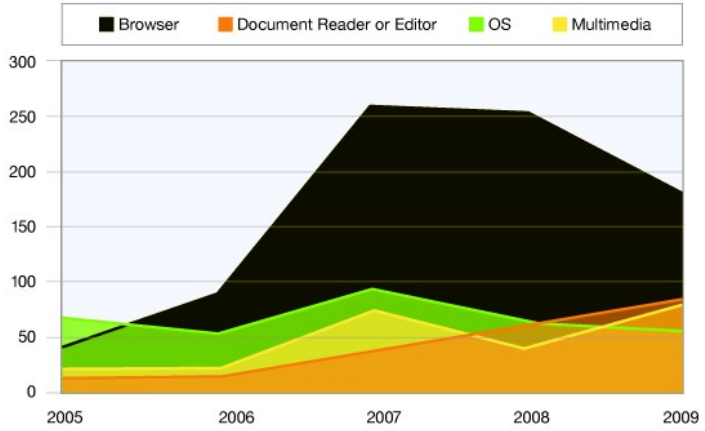
Category	Avg # Vulns	% Likely to Occur
Cross-Site Scripting	11.9	91%
Inadequate / Poor Input Control	19.7	82%
Information Disclosure	8.6	82%
Error Message Information Leak	9.7	73%
Insufficient Web Server Configuration	16.3	64%
Improper Use of SSL	30.2	55%
Improper Application Deployment	1.4	55%

Client-Side Vulnerabilities: Document and Multimedia Vulnerabilities are on the Rise



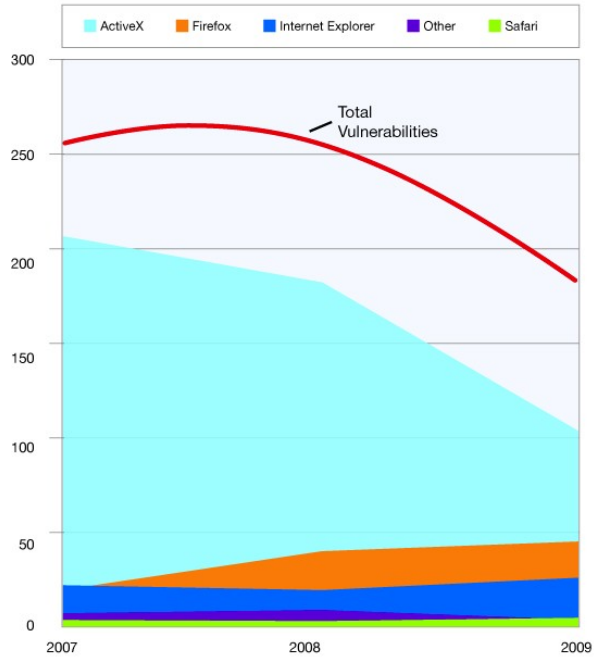
- Largest number of client-side vulnerabilities in 2009 affects Web browsers and their plug-ins.
- Document Reader and Multimedia vulnerabilities surpass OS vulnerabilities in 2009.

Top Client Categories – Changes in Critical and High Client Software Vulnerabilities
2005-2009



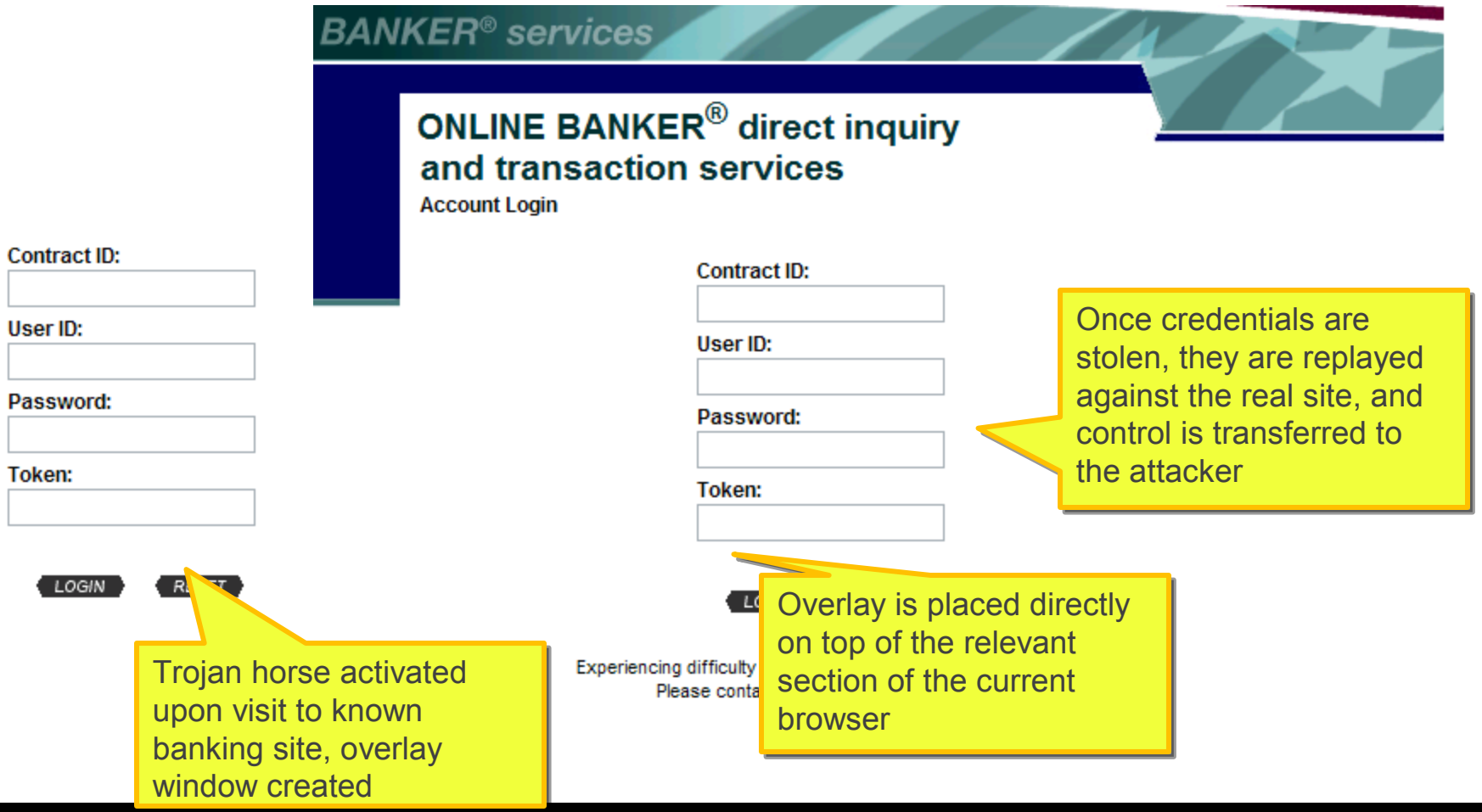
Source: IBM X-Force®

Critical and High Client Vulnerability Disclosures Affecting Browser-Related Software
2007-2009

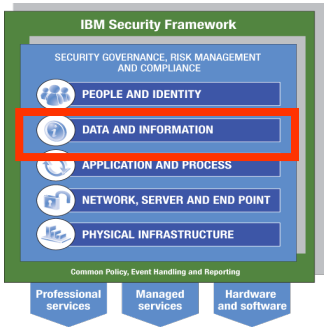


Source: IBM X-Force®

Trojan Window Overlay to Steal Token Information

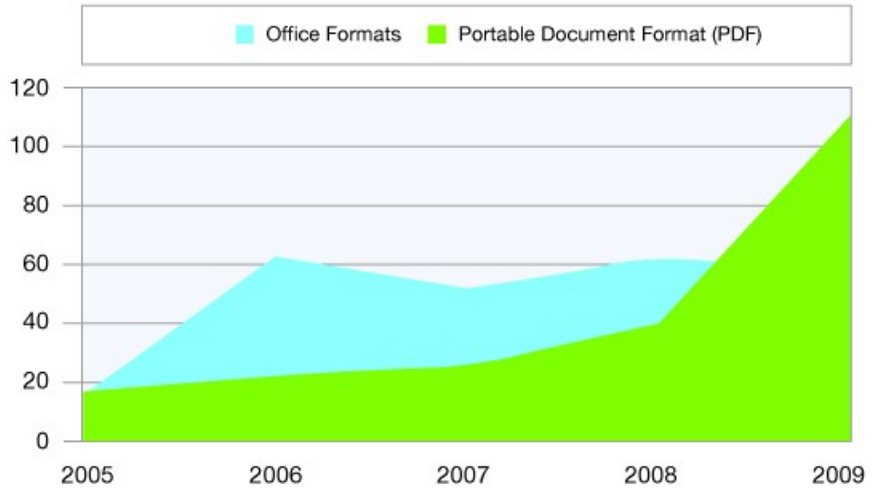


Vulnerabilities in Document Readers Skyrocket



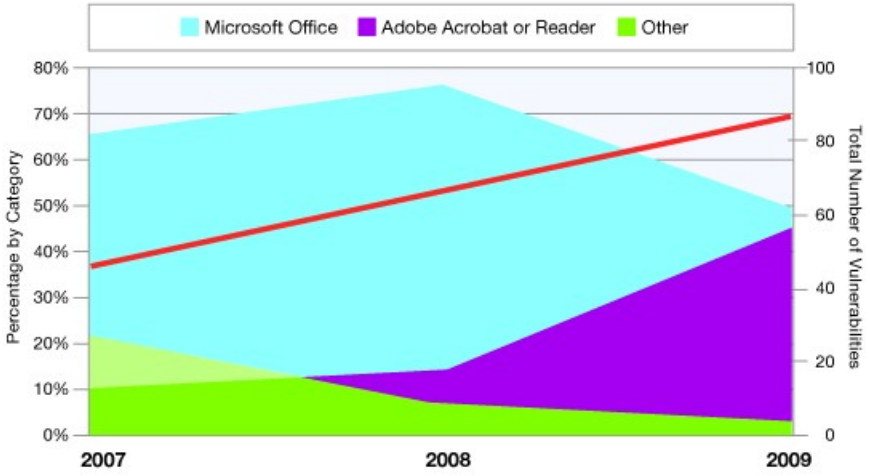
- Portable Document Format (PDF) vulnerabilities dominate in 2009.
- Microsoft Office document disclosures are on the decline while Adobe disclosures continue to rise.

Vulnerability Disclosures
Related to Document Format Issues
2005-2009



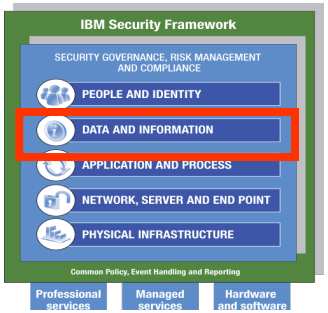
Source: IBM X-Force®

Critical and High Vulnerability Disclosures
Affecting Document Readers and Editors
2007-2009



Source: IBM X-Force®

Attackers Turn to Adobe Products to Launch Exploits



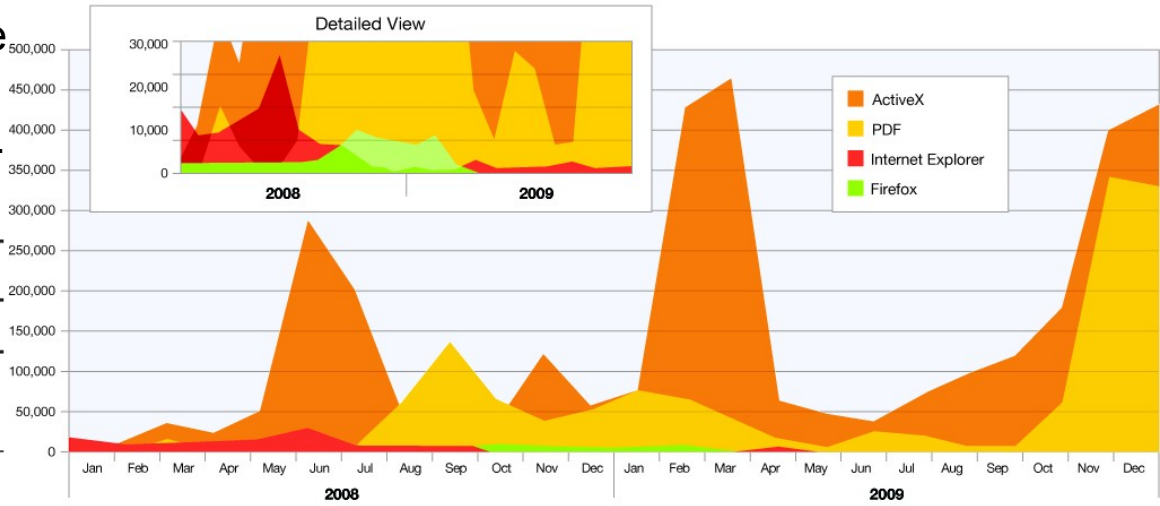
- Four of the top five web based exploits are related to Adobe products.
- Core browser vulnerabilities have taken a back seat to malicious PDFs and ActiveX vulnerabilities.

Top Five Web-Based Exploits

Rank	2009
1.	Microsoft Office Web Components Spreadsheet ActiveX (CVE-2009-1136)
2.	Adobe Acrobat and Reader Collab.CollectE-mailInfo (CVE-2007-5659)
3.	Adobe Acrobat and Reader util.printf() (CVE-2008-2992)
4.	Adobe Acrobat and Reader GetIcon() (CVE-2009-0927)
5.	Adobe Flash Player SWF Scene Count (CVE-2007-0071)

Table 11: Top Five Web-Based Exploits, 2009
Source: IBM X-Force Whiro Crawler

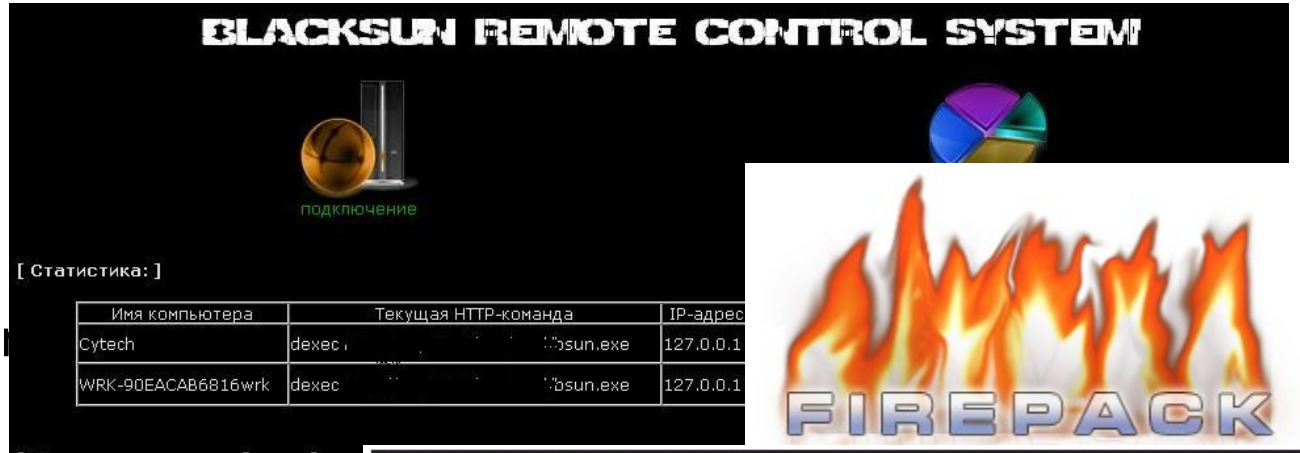
Browser and PDF Exploitation
Source: IBM Managed Security Services
2008-2009



Source: IBM X-Force®

Popular drive-by-download exploit packs

- WebAttacker2
- Mpack
- IcePack
  - Localized to Fren in May 2008
- Firepack
- Neosploit
- Black Sun
- Cyber Bot



Top Five Web Exploit Toolkits

Rank	2009 (Full Year)	2009 H2 (Second Half)
1.	Gumblar	Gumblar
2.	CuteQQ	CuteQQ
3.	Phoenix	JustExploit
4.	zoPack	Nuclear
5.	JustExploit	Elenore

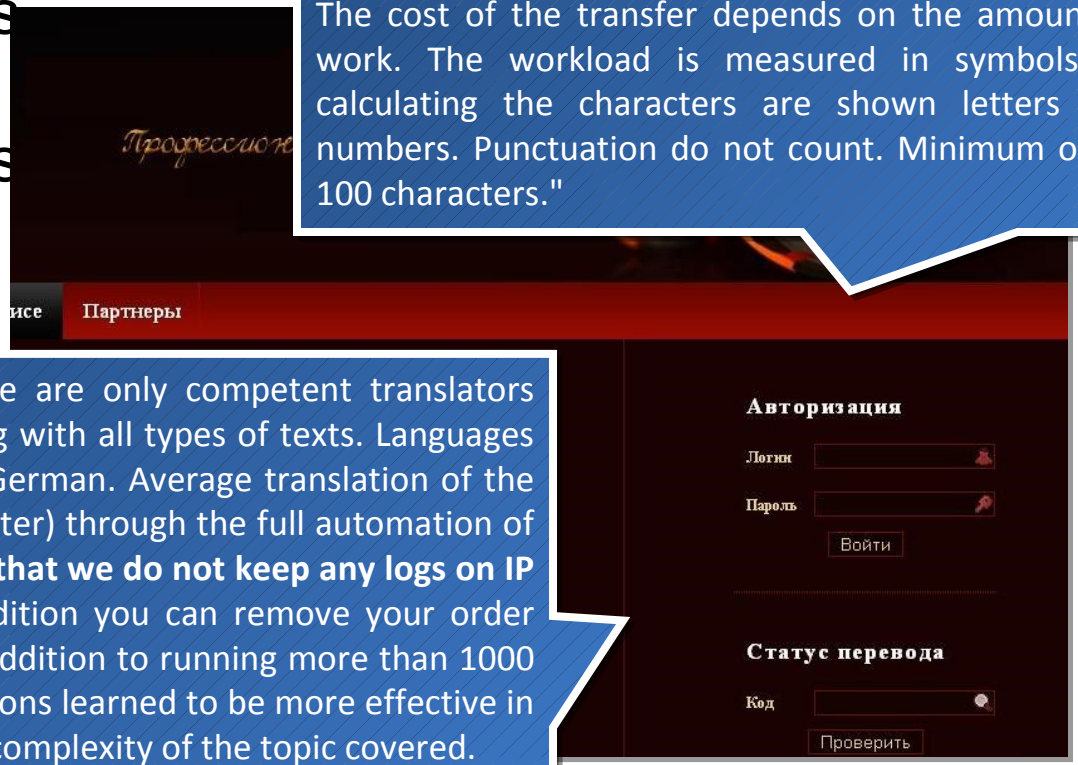
Table 12: Top Five Web Exploit Toolkits, 2009
Source: IBM X-Force Whiro Crawler

Localizing attacks

- Local language attack suppor
- Can be outsourced
- Translation services for spam/phishing/ malware campaigns

Prices and deadlines:
* Standard - the deadline is not more than 24 hours. Prices depend on the direction and guidance from the 'Order'.
* Term - work on your translation begins precedence. The price of the 50% more than the standard translation. Prices also depend on the direction and guidance from the 'Order'.

The cost of the transfer depends on the amount of work. The workload is measured in symbols. In calculating the characters are shown letters and numbers. Punctuation do not count. Minimum order 100 characters."



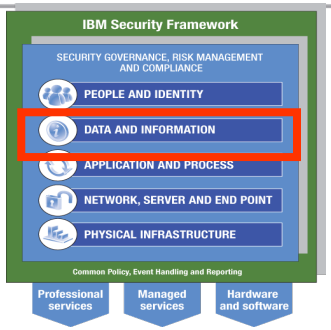
"We offer our services in translation. We are only competent translators profile higher education. Service is working with all types of texts. Languages available at this time of Russian, English, German. Average translation of the text takes up to 10 hours (usually much faster) through the full automation of the order and payment. **Just want to note that we do not keep any logs on IP and does not require registration.** In addition you can remove your order from the database after his execution. In addition to running more than 1000 translations already, we can use all the lessons learned to be more effective in our services. Prices vary depending on the complexity of the topic covered.

Localized social engineering

- What if the phisher wants to get more sophisticated?
- Third-party “help-desk” support
  - "talk cybercrime on behalf of you"
- Multiple languages supported
  - English (3 male voices and 2 female ones)
  - German (2 male voices and 1 female one)
  - Spanish (1 male voice and 2 female ones)
  - Italian (1 male voice and 1 female one)
  - French (1 male voice and 1 female one)

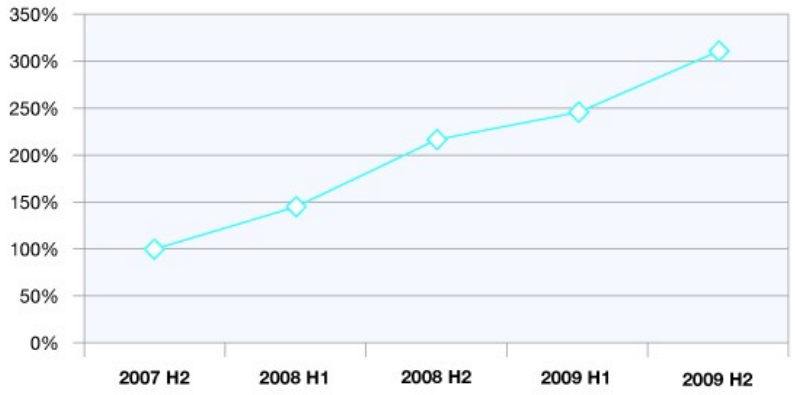
- $9 per call, dropping to $6 for repeat customers

“Bad” Web Content Tries to Evade Filters



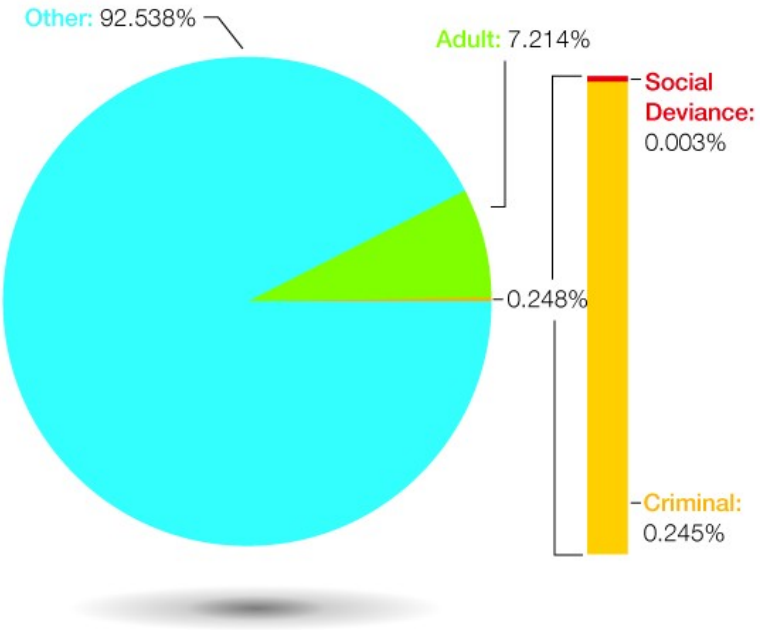
- **7.5%** of the Internet contains unwanted content such as pornographic or criminal Web sites.
- Anonymous proxies, which hide a target URL from a Web filter, have steadily increased to more than triple in number since 2007.

Volume Increases of Anonymous Proxy Web Sites
2007 H2-2009 H2



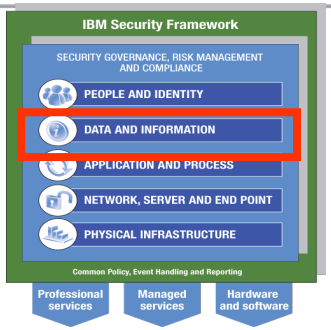
Source: IBM X-Force®

Content Distribution of the Internet
2009



Source: IBM X-Force®

Suspicious Web Pages and Files are on the Rise

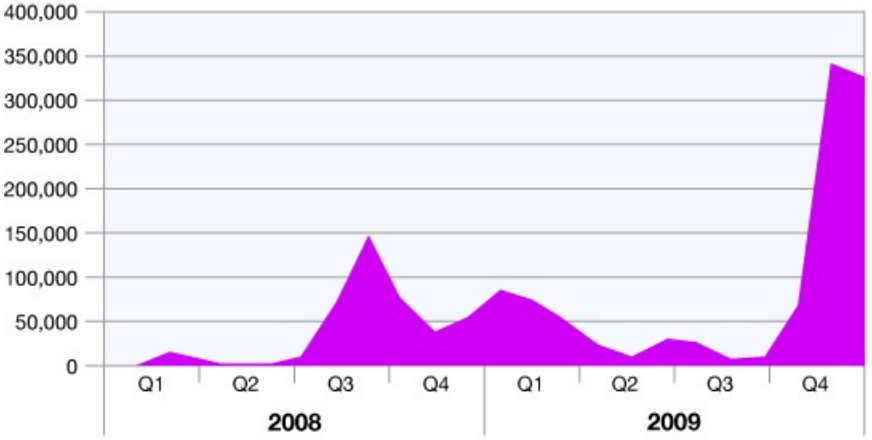


- The level of obfuscation found in Web exploits continues to rise.
- Exploit toolkit packages have started to include both malicious Adobe Flash and PDF files.
- Adobe PDF files saw increases in obfuscation complexity throughout 2009.

Obfuscated Web Pages and Files
Source: IBM Managed Security Services
2008-2009

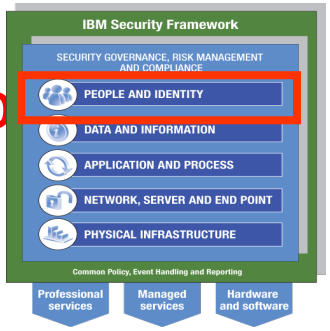
Source: IBM X-Force®

PDF Attacks
Source: IBM Managed Security Services
2008-2009



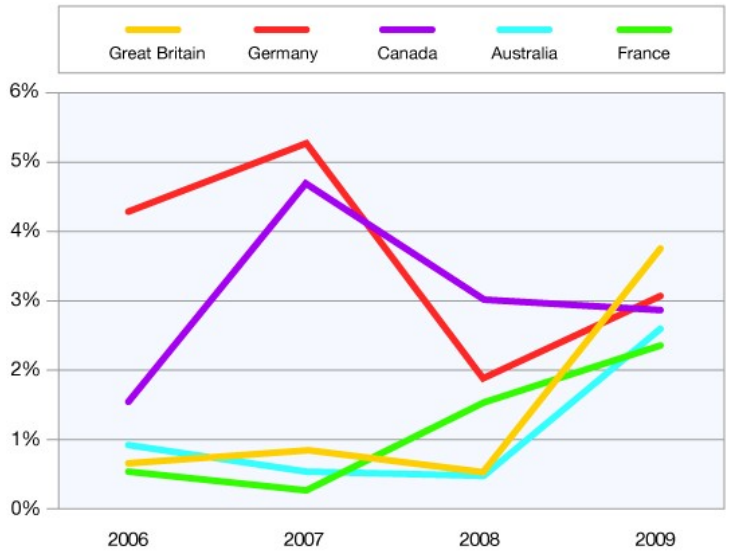
Source: IBM X-Force®

Malicious Web Links Increase by 345%



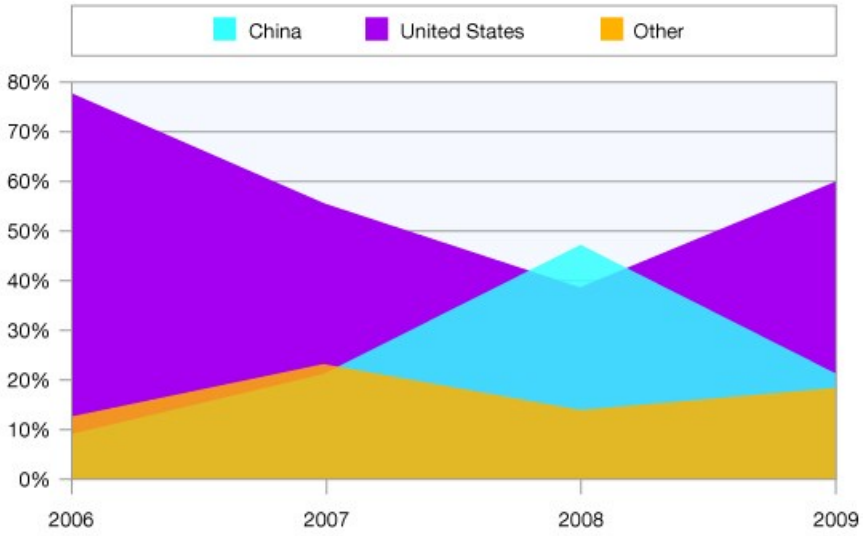
- United States and China continue to reign as the top hosting countries for malicious links.
- Many more second tier countries are jumping into this game.

Second-Tier Countries that Host Two Percent or More of All Malicious URLs
2006-2009



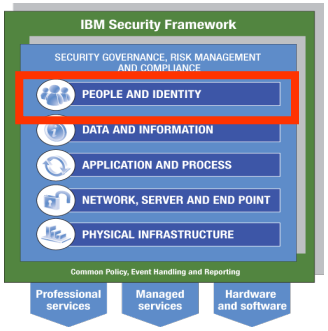
Source: IBM X-Force®

Countries Hosting the Most Malicious URLs
Source: IBM spam and URL filter database
2006-2009



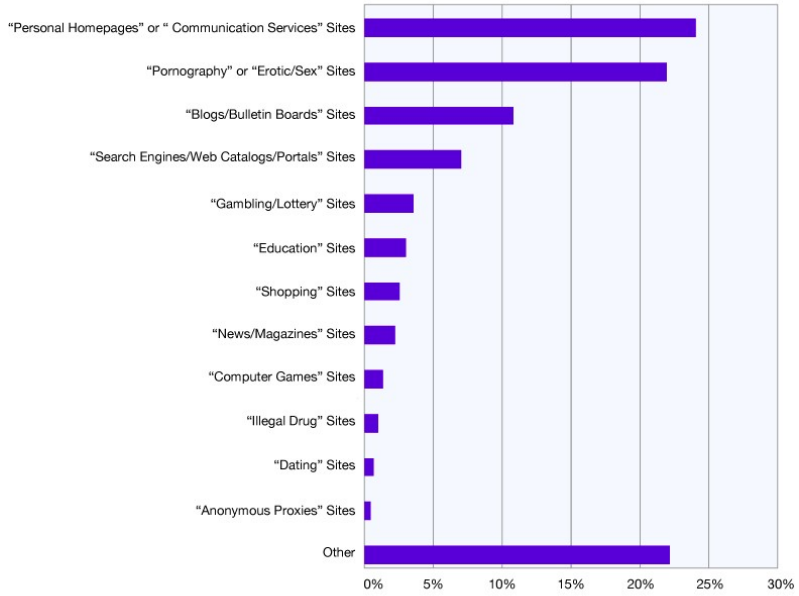
Source: IBM X-Force®

Websites Hosting Bad Links



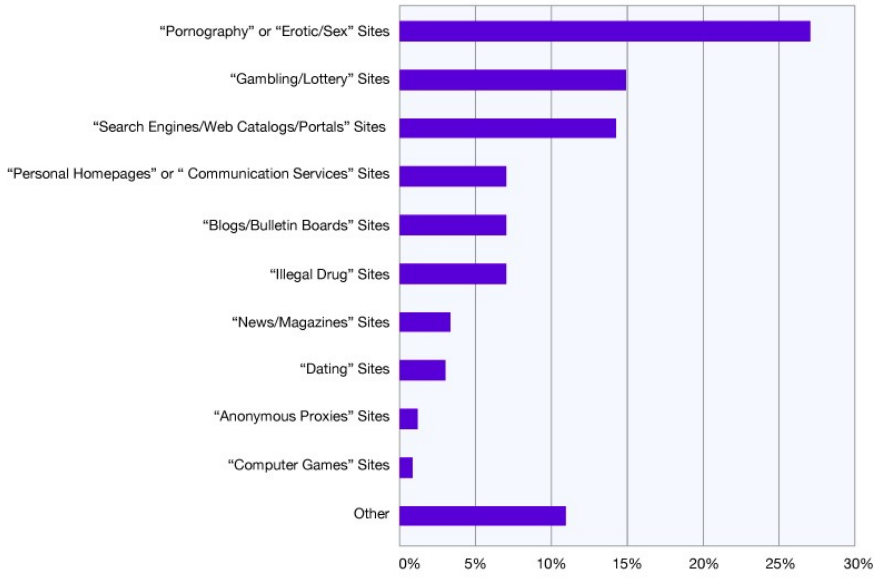
- Since the 1 half of 2009, Professional “bad” Web sites like pornography, gambling, or illegal drugs Web sites have increased their links to malware.
- Blogs and bulletin boards have also seen increases in malware links.

Top Web Site Categories Containing at Least One Malicious Link
2009 H2



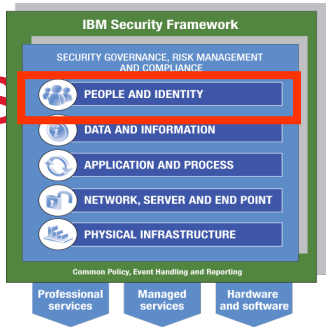
Source: IBM X-Force®

Top Web Site Categories Containing 10 or More Malicious Links
2009 H2

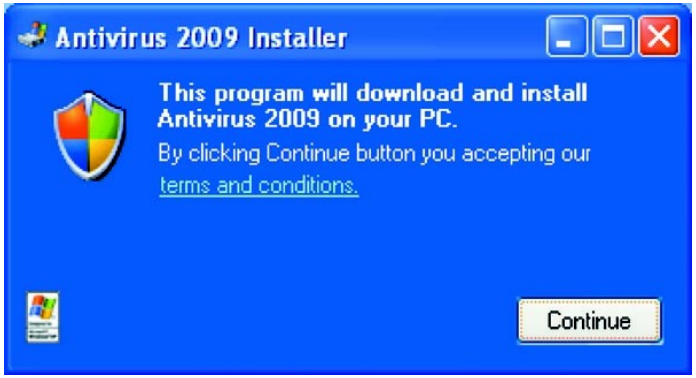


Source: IBM X-Force®

Socially Engineered Malware on the Ris

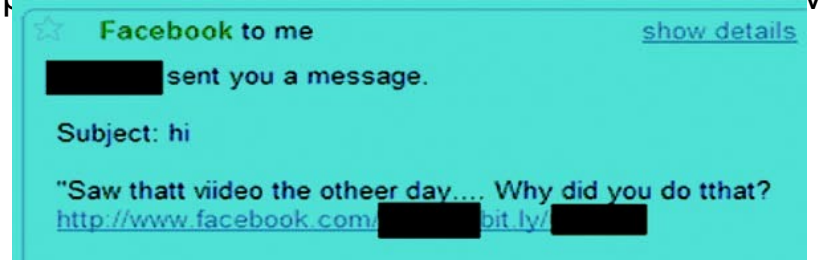


- Social networks represent a vehicle for malware authors to distribute their programs in ways that are not easily blocked. Examples include:
  - Antivirus 2009, which lures users into downloading a fake AV product.
  - The Koobface Worm which infiltrated Facebook, Myspace, and other social networking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



- These types of attacks are ongoing and increasing in intensity.

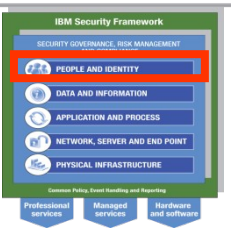
- Another upward trend is the use of software toolkits to deliver malware.



Dangerous Holiday Greeting

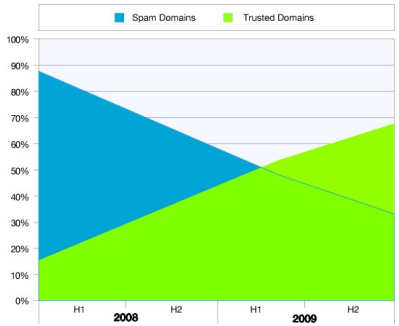
Source: f-secure.com

Spam Continues to Change to Avoid Detection



- **80%** of spam is classified as URL spam.
- Spammers continue to use “trusted” domains and “legitimate links” in spam messages to avoid anti-spam technologies.
- Brazil, the U.S., and India account for about 30 percent of worldwide spam in 2009.
  - In the second half of 2009, Vietnam appears in second place of spam-sending countries.

Top 10 Domains Used in Spam
Spam Domains vs. Trusted Domains
2008-2009



Source: IBM X-Force®

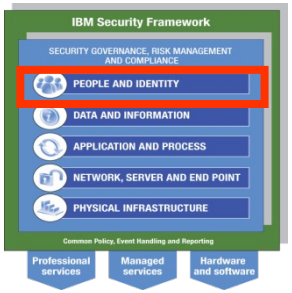
January 2009	February 2009	March 2009	April 2009	May 2009	June 2009
chat.ru	sexyhardy.com	rodale.com	interia.pl	yahoo.com	yahoo.com
thuspattern.com	aspirationask.com	menshealth.com	akamaitech.net	menshealth.com	googlegroups.com
powerinstrument.com	shoprespect.com	webmd.com	menshealth.com	icontact.com	webmd.com
cbsnews.com	msn.com	mkt41.net	ask.com	webmd.com	icontact.com
hereidea.com	yulesearching.com	interia.pl	webmd.com	earlytorise.com	mansellgroup.net
notdune.com	wordobservant.com	icontact.com	rodale.com	doctorspreferred.com	ranmooon.com
methoddegree.com	assistingoriginal.com	akamaitech.net	go.com	mansellgroup.net	signgras.com
chithigh.com	tarecahol.cn	msn.com	yahoo.com	healthcentral.com	rannew.com
chitlink.com	integrityprove.com	about.com	yimg.com	menshealth.fr	blueheav.com
boughtprosperity.com	approvaltruthful.com	rodalenews.com	behaviorright.com	trendsmag.com	rangreat.com

Table 16: Most Common Domains in URL Spam, 2009 H1

July 2009	August 2009	September 2009	October 2009	November 2009	December 2009
yahoo.com	yahoo.com	magshine.com	mediapix.ru	mediapix.ru	imageshack.us
webmd.com	blurblow.com	yahoo.com	yahoo.com	4freeimagehost.com	flickr.com
wallmotion.com	nyavekep.cn	google.com	cmeqoher.cn	imagechicken.com	yahoo.com
nyavekep.cn	blurpack.com	webmd.com	webmd.com	ipicture.ru	photolava.com
msn.com	blurnight.com	magcloude.com	google.com	topmiddle.com	pixfarm.net
pfizerhelpfulanswers.com	blurgreat.com	magroof.com	icontact.com	imageshack.us	mediapix.ru
akamaitech.net	by.ru	maghat.com	fuxehmg.cn	inselpix.com	live.com
icontact.com	livefilestore.com	cmeqoher.cn	blingdisc.com	flickr.com	webmd.com
livefilestore.com	ally.com	nyavekep.cn	by.ru	commoncatch.com	picturebay.net
skyeclean.com	bankofamerica.comally.com		groundmons.com	yahoo.com	pixiurl.com

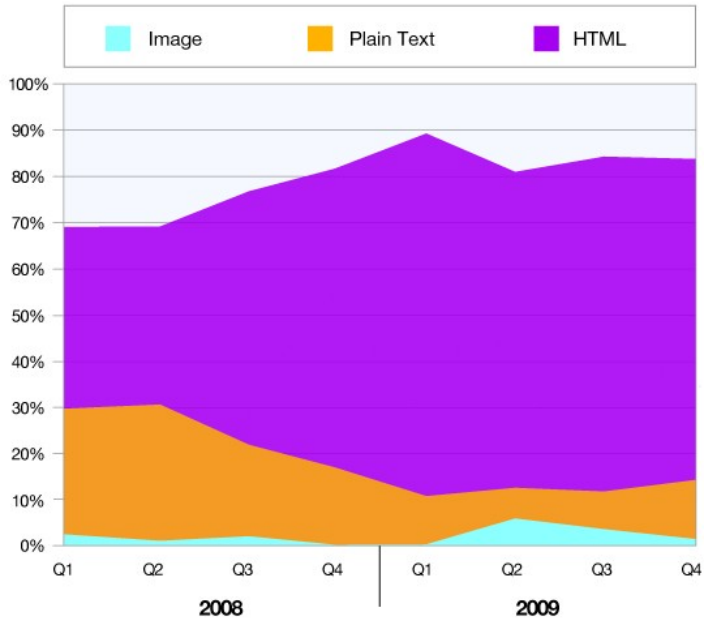
Table 17: Most Common Domains in URL Spam, 2009 H2

HTML Spam Recovers



- Spam volume increased through 2009.
- Image-based spam declined in the second half of 2009 and HTML-based spam recovered.

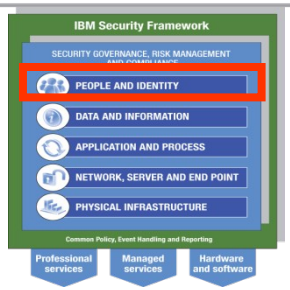
Types of Spam
2008-2009



Source: IBM X-Force®

Changes in Spam Volume
April, 2008 - December, 2009

Source: IBM X-Force®

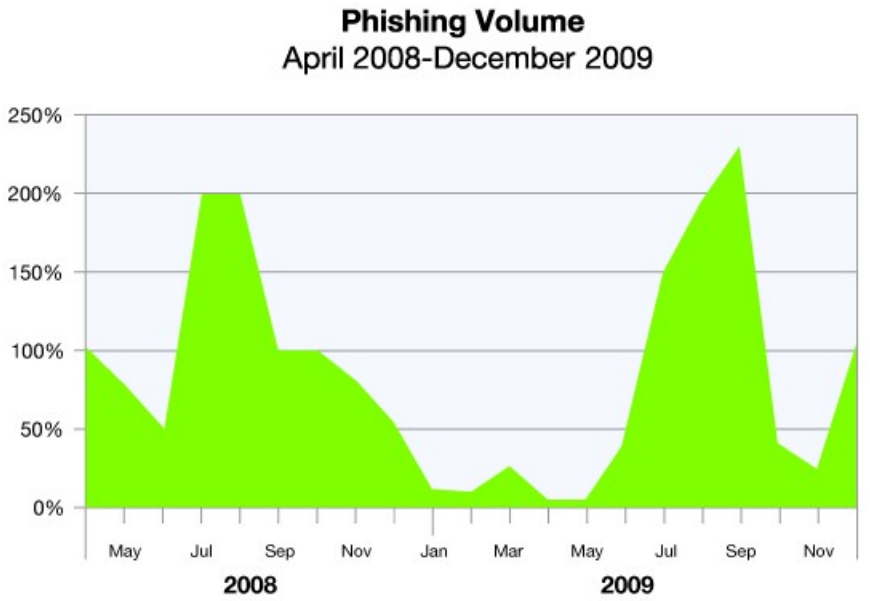


Phishing Attacks Increase Dramatically

- Contrary to the 1st half of 2009, phishers came back with a vengance in the 2nd half of 2009.
- Country of Origin also changed dramatically:
  - Spain and Italy took top slots in 2008, but both have completely dropped from the top ten for 2009.
  - The top sender is Brazil, runner-up is the USA and third place goes to Russia, who was not even in the top ten last year.
- Top subject lines are back
  - Top 10 subject lines represent more than 38% of all phishing e-mails.
  - In 2008 the top subject lines made up only 6.23%.

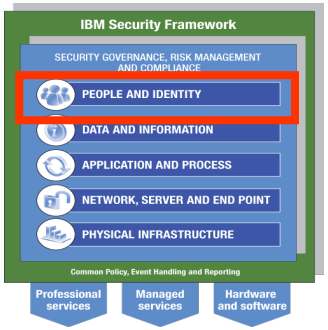
Subject Line	%
Notice of Underreported Income	17.09%
Attention! Votre compte PayPal a ete limite!	4.28%
Update Your Account	3.78%
GMAC Bank is now Ally Bank	2.57%
Ally Bank (former GMAC Bank) customer form	2.27%
Instructions for Ally Bank (former GMAC Bank) customer	2.27%
For attention of Ally Bank (former GMAC Bank) customer	2.26%
New version of Ally Bank (former GMAC bank) customer form has been released	2.03%
Important Information Regarding Your Limited Account.	1.25%
American Express Online Form	0.68%

Table 24: Most Popular Phishing Subject Lines 2009



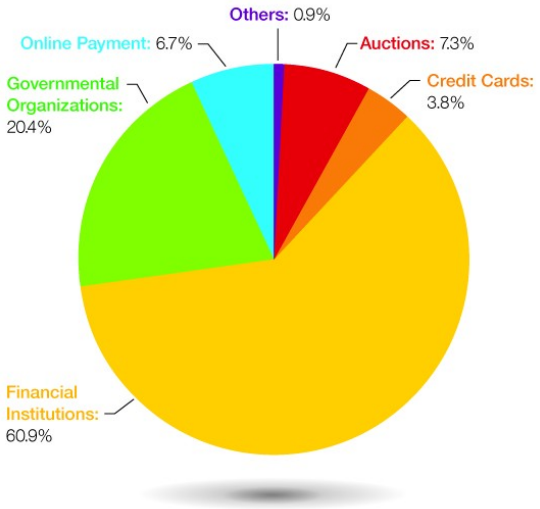
Source: IBM X-Force®

Phishing Targets Financial & Government Organizations



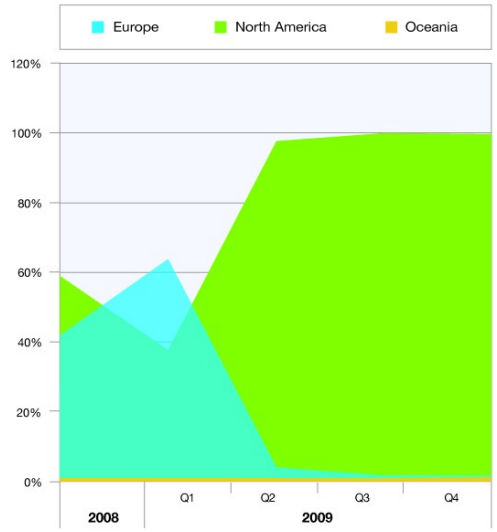
- **60.9%** of phishing is targeted at the financial industry vs. **90%** in 2008.
- Over **95%** of all financial phishing targets in 2009 are located in North America.
  - During the 4 quarter of 2009, **0.3%** of all financial phishing emails were targeted to Australia or New Zealand, making them bigger targets than all of Europe (**0.2%**).
- **20.4%** of phishing emails were targeted at government organizations.

Phishing Targets by Industry
2009



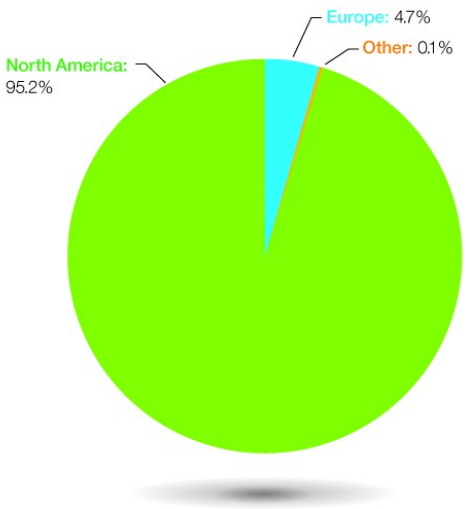
Source: IBM X-Force®

Financial Phishing by Geographical Location
2008-2009



Source: IBM X-Force®

Financial Phishing by Geographical Location
2009



Source: IBM X-Force®


H&M

STATOIL

ØRESUNDSBRON

Danfoss

Arla

Säkerhetspolisen
Vi skyddar Sverige och demokratin

NB NORGES BANK

POLITI

FÖRSVARSMAKTEN

MAX

DnB NOR


VELUX

Skatteetaten

RESURS
BANK


Sonu Ericsson


Jernbaneverket

Arrive

Danske Spil

LEO

LEO Pharma

investor

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

MARATHON

Marathon
Petroleum Norge AS


EDB

steria

Cloetta

RADIOMETER


NORSK TIPPING

TeleComputing®
- making IT easier

TelgeEnergi

For More IBM X-Force Security Leadership

X-Force Trends Report

The IBM X-Force Trend Statistics Report provides statistical information about all aspects of threats that affect Internet security,. Find out more at http://www-935.ibm.com/services/us/iss/xforce/midyearreport/

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