Trend and Risks

IBM Internet Security Systems (ISS)

Vlatko Košturjak, IBM ISS - EMEA

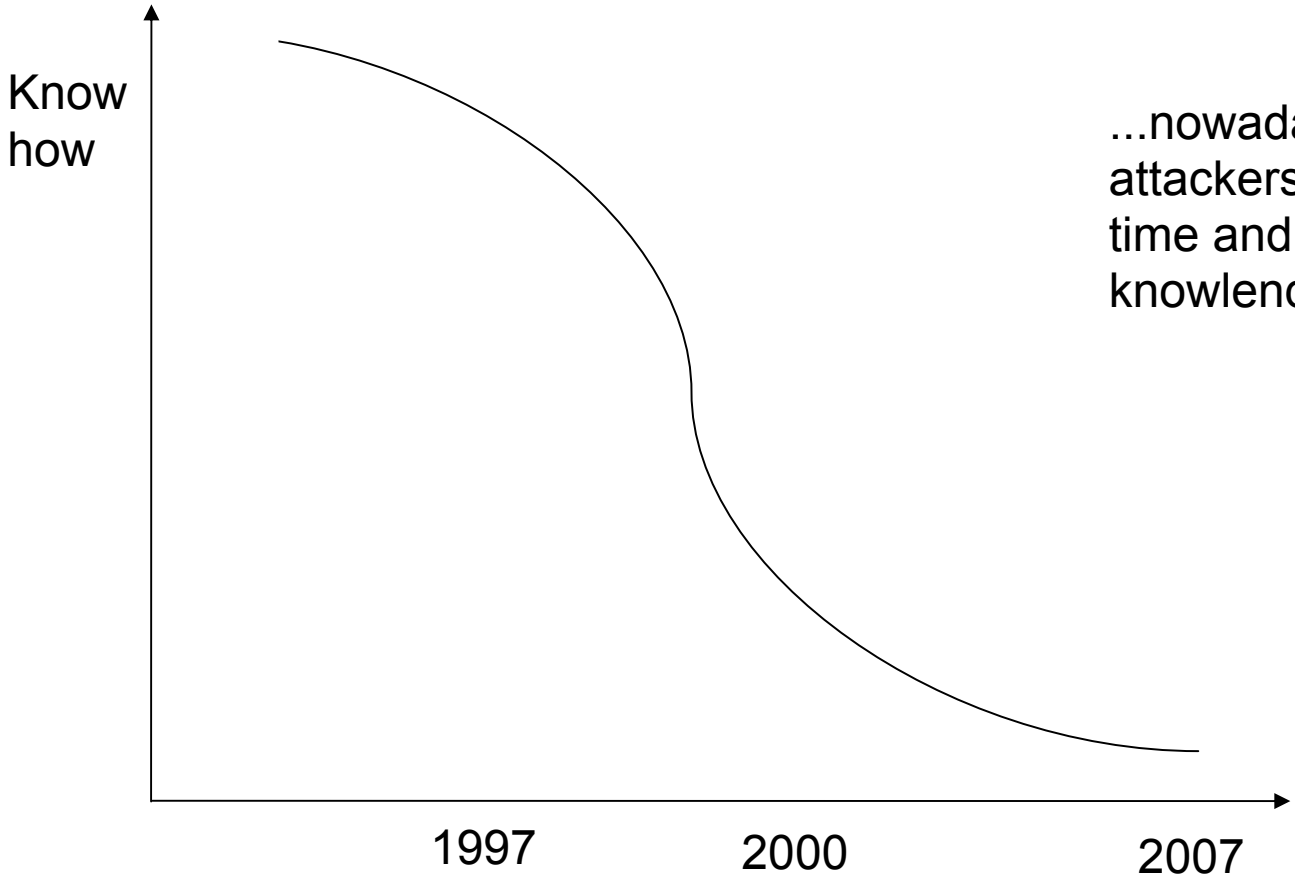
Agenda

- Few facts
- IBM ISS X-Force
- IBM ISS X-Force Trend & Risks Report / Threat report
  - Vulnerability Disclosures
  - Economics of Attacker Exploitation
  - Top ten vendor list for disclosures
  - Patches unavailable
  - Browser exploitation
  - Spam
  - Phishing
  - Malware
- Questions and Answers

Facts

- You're defending yourself from world wide criminals
- Law doesn't work across borders, attackers do
- No difference in attacking someone locally or 1000 miles away
- All tools are available
- ...

Knowledge & Attacker



...nowadays, attackers need less time and less knowlendge...

IBM Global Security Reach

8 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 4 Billion+ Events Per Day

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

X-Force R&D -- Unmatched Security Leadership

The mission of the IBM Internet Security Systems™ 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

10B	analyzed Web pages & images
150M	intrusion attempts daily
40M	spam & phishing attacks
43K	documented vulnerabilities

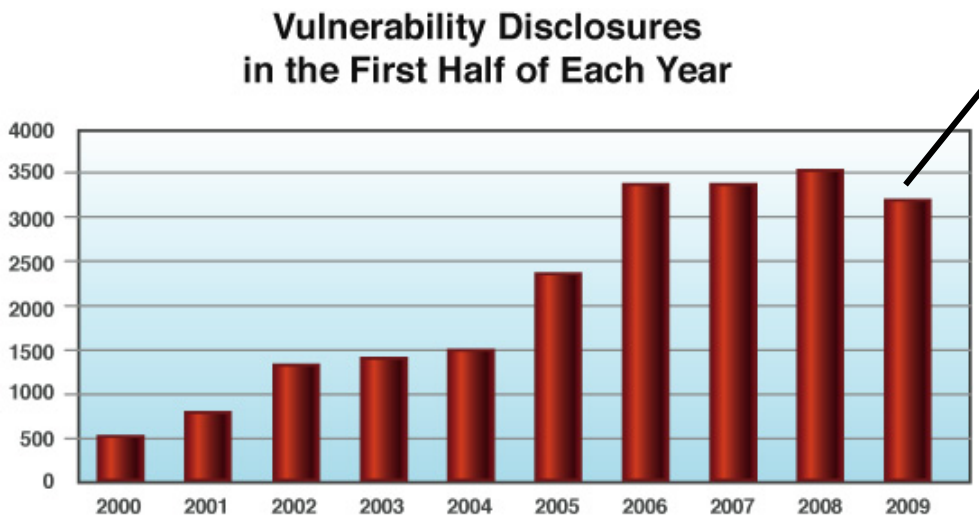
Millions of unique malware samples

Provides Specific Analysis of:

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

Looks Can Be Deceiving: Vulnerability Disclosures Decline but Exploitation Increases

- Declines in some of the largest categories of vulnerabilities
- Slowing disclosure rate is due to the disappearance of the low-hanging fruit from currently researched categories and existing applications
- Exploits targeting these vulnerabilities are increasing, especially SQL injection and ActiveX controls.



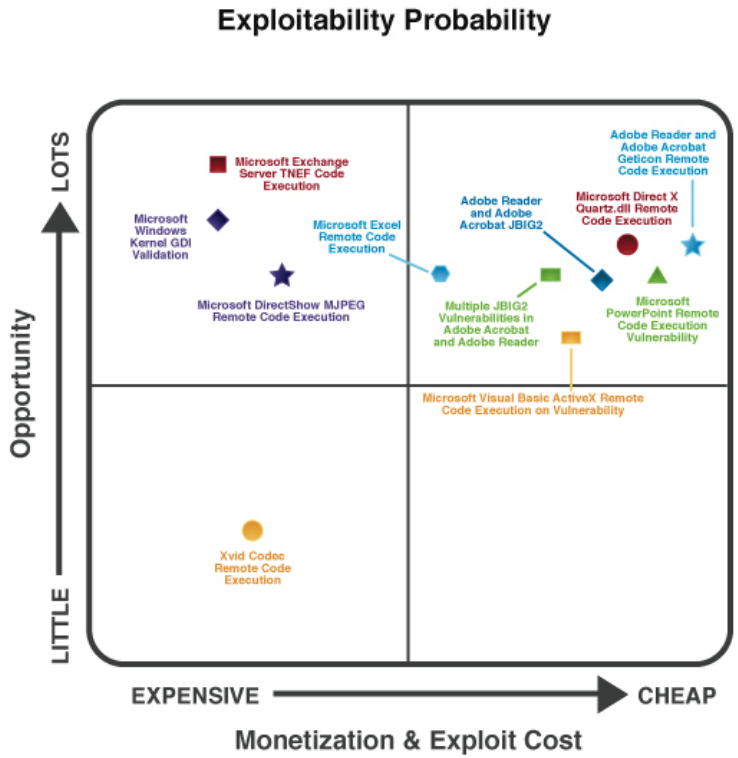
- High vulnerabilities are down **6%** YOY
- Medium vulnerabilities are up to **62%** of the vulnerabilities (8% YOY increase)

YOY = year over year

source: IBM X-Force®

The Economics of Attacker Exploitation

- Economics continue to play heavily into the exploitation probability of a vulnerability
- Recent Document Reader vulnerabilities impacting office documents and PDFs are very profitable and easily executable

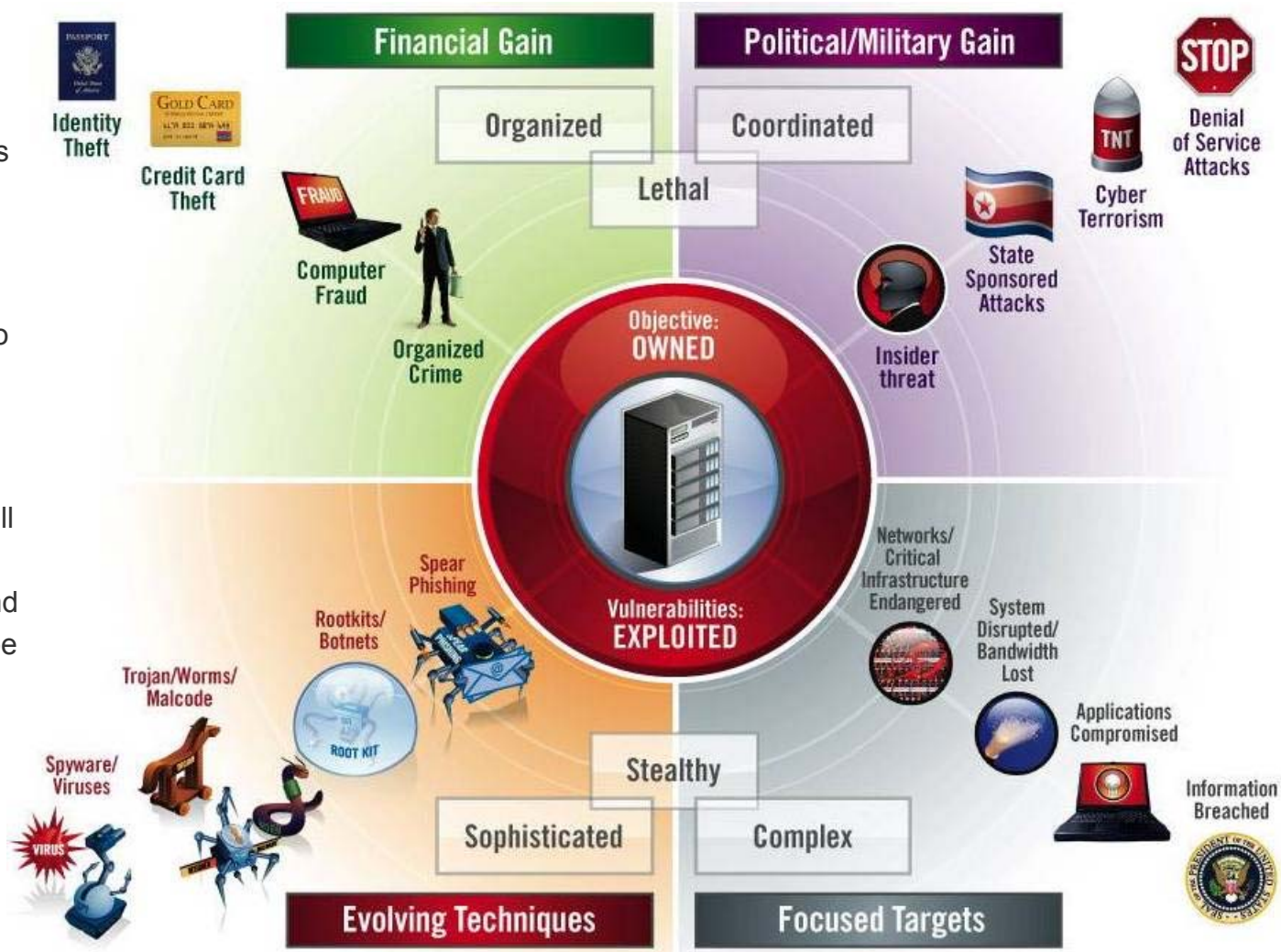


source: IBM X-Force®

The Economics of Attacker Exploitation

Threat Evolution:

- A flat world has brought about an unprecedented amount of criminals and cons
- Attackers keep ROI in mind as well, and constantly evolve their wares in order to re-purpose it for the next flood of attacks
- High profile vulnerabilities will still be the vehicles for new attacks, however, the low and slow attack vectors cannot be ignored
- The economics of exploitation must be taken into consideration to better prioritize risk



Microsoft, Apple and Sun Top Vendor List for Disclosures

- Top ten vendors account for **24%** of all disclosed vulnerabilities, up from 19% in 2008

2009 H1		
Ranking	Vendor	Disclosures
1.	Apple	3.8%
2.	Sun	3.6%
3.	Micrsoft	3.1%
4.	Oracle	2.7%
5.	IBM	2.5%
6.	Drupal	2.0%
7.	Mozilla	1.8%
8.	Cisco	1.8%
9.	Linux	1.5%
10.	Joomla!	1.2%

2008 (Full Year)		
Ranking	Vendor	Disclosures
1.	Microsoft	3.16%
2.	Apple	3.04%
3.	Sun	2.19%
4.	Joomla!	2.07%
5.	IBM	2.00%
6.	Oracle	1.65%
7.	Mozilla	1.43%
8.	Drupal	1.42%
9.	Cisco	1.23%
10.	TYPO3	1.23%

Table 2: Vendors with the Most Vulnerability Disclosures

- Microsoft dropped to #3 after holding the top spot since 2006
- Apple moved up to the #1 spot

My vendor not on this list? :)

Are those vendors taking security seriously? :(

Application & Processes:

Patches Still Unavailable for Half of Vulnerabilities

Vendor	Disclosures	Unpatched	% Unpatched
Joomla!	40	32	80%
Apple	122	22	18%
Microsoft	100	17	17%
Drupal	65	9	14%
Mozilla	59	8	14%
TYPO3	24	3	13%
Cisco	57	5	9%
Novell	40	2	8%
HP	40	3	8%
Sun	117	5	4%

*Vendors with twenty or more disclosures in 1H 2009

**IBM Disclosures 82, Unpatched 3, % Unpatched 3.7%

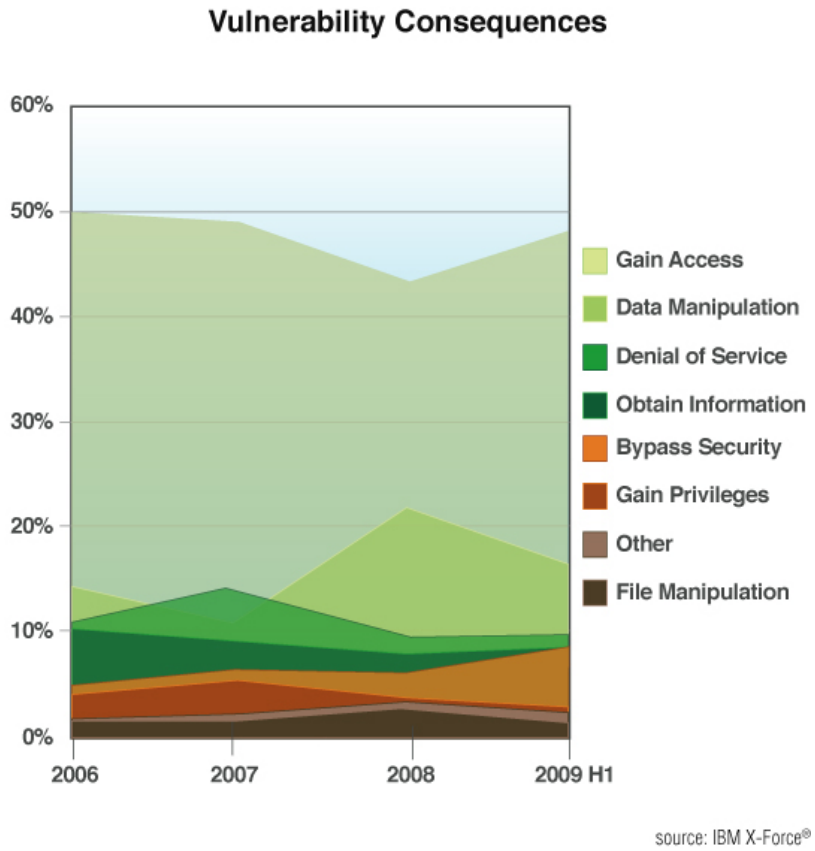
- Nearly half **(49%)** of all vulnerabilities disclosed in the first half of 2009 had no vendor-supplied patches to remedy the vulnerability

- Top 10 categories of operating systems account for **89%** of all operating system vulnerability disclosures and **93%** of all critical and high operating system disclosures in the first half of 2009.

Operating System	Percentage of Critical and High	Percentage of All OS Vulnerabilities
Microsoft	39%	14%
Apple	18%	24%
Sun Solaris	14%	26%
Linux	14%	20%
IBM AIX	7%	3%
BSD	2%	4%
Others	7%	11%

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 is increasing

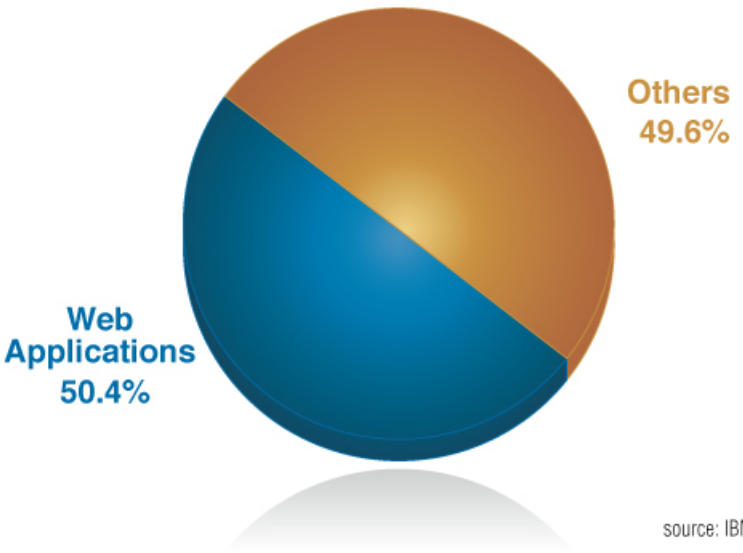


Application & Processes:

Web App Vulnerabilities Continue to Dominate

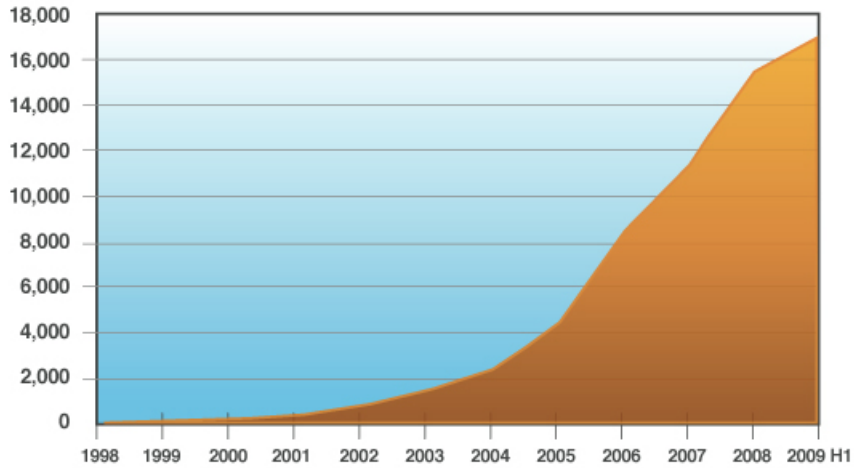
- **50.4%** of all vulnerabilities are Web application vulnerabilities
- SQL injection and Cross-Site Scripting are neck and neck in a race for the top spot

Web Application Vulnerabilities
as a Percentage of All Disclosures in 2009 H1



source: IBM X-Force®

Vulnerability Disclosures Affecting Web Applications
Cumulative, year over year

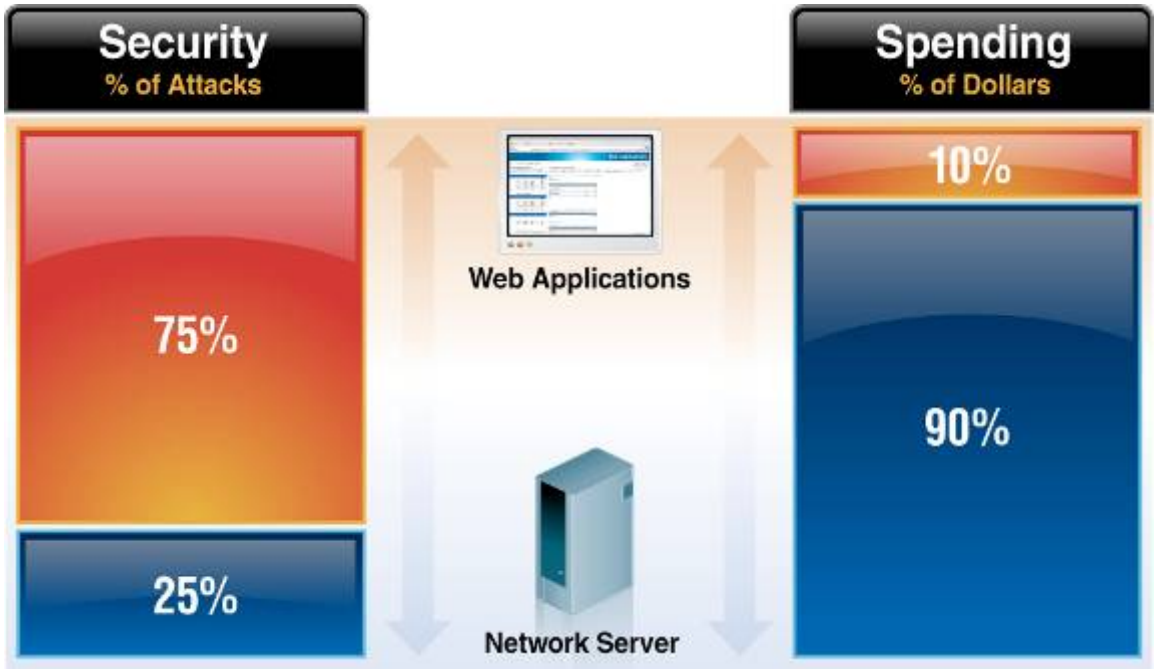


source: IBM X-Force®

Application & Processes:

Web App Vulnerabilities Continue to Dominate

Security and Spending are Unbalanced

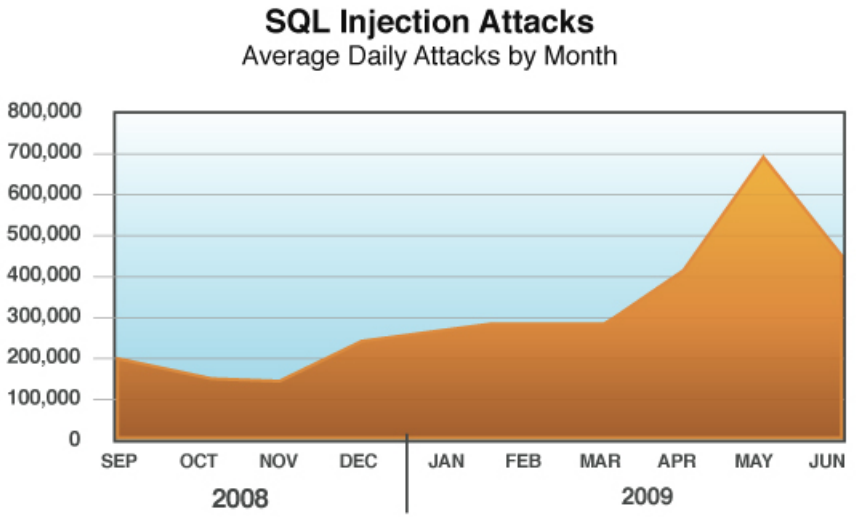


"The cleanup cost for fixing a bug in a homegrown Web application ranges anywhere from $400 to $4,000 to repair, depending on the vulnerability and the way it's fixed."
-Darkreading.com

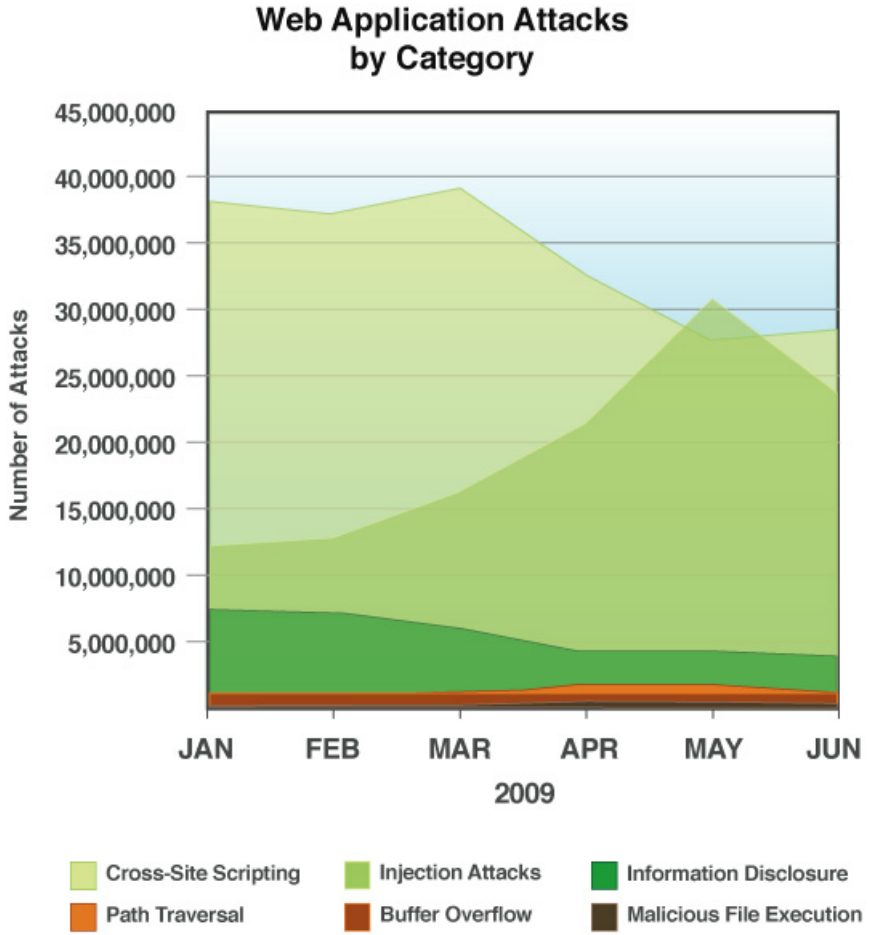
Application & Processes:

Cross Site Scripting and Injection Attacks Continue to Dominate

- **90%** of injection attacks are attributed to SQL-related attacks
- Automated toolkits continue to flourish in 2009
- SQL injection attacks continue to grow up **50%** in Q1 2009 vs. Q4 2008 and nearly doubling in Q2 vs. Q1



source: IBM X-Force®

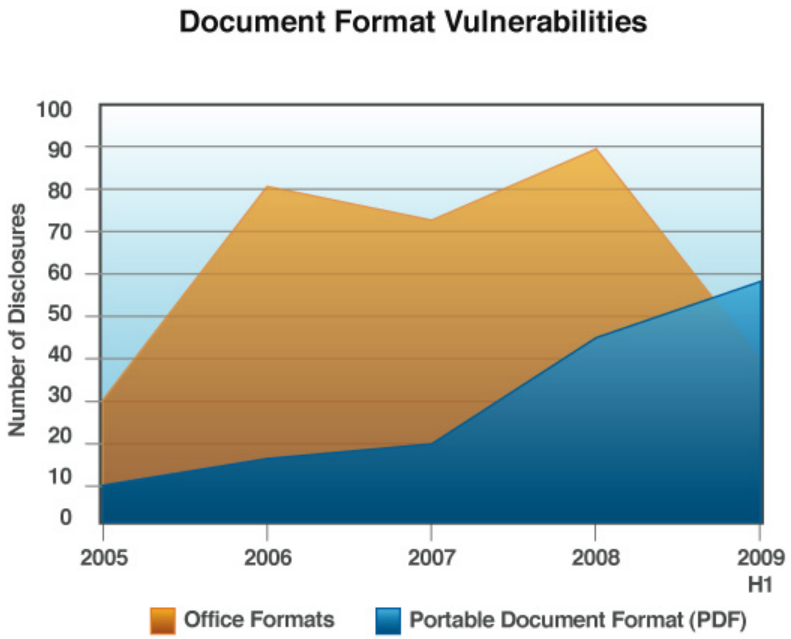


source: IBM X-Force®

Data & Information:

Vulnerabilities in Document Readers Skyrocket

- Portable Document Format (PDF) vulnerabilities disclosed in the first half of 2009 has already surpassed disclosures from all of 2008.
- PDF disclosures traded places with Office document disclosures to take the top spot.



source: IBM X-Force®

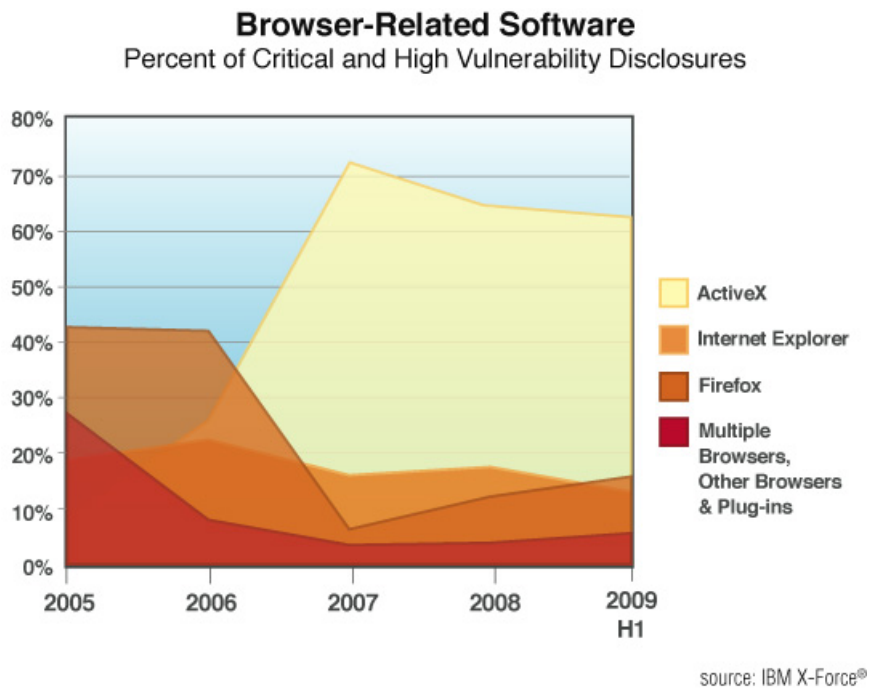
Points to Consider:

- Users trust .PDF more than .EXE
- PDF exploits becoming a popular method of attack

Browser Exploitation Prevention

- **The Web browser is the universal application**
- Attackers know that it delivers the best ROI

- **BEP protects against web browser exploitation regardless of the vulnerability**
- Approximately 20 signatures protecting against hundreds of vulnerabilities in multiple browsers
- Protects against both shellcode and obfuscated exploits
- Most IPS technology can't do either



Data & Information:

Decline in Disclosures Does Not Impact Exploitation

- Decline in ActiveX disclosures does not appear to be making an impact on exploitation.
- Three of the five most popular exploits are ActiveX controls.

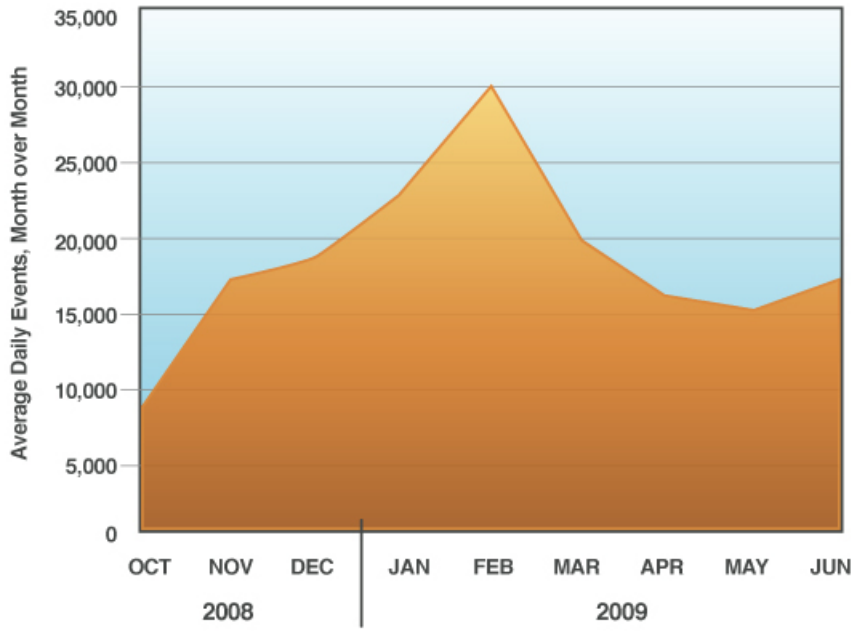
First time that a PDF exploit is in the top 5 list.

Most Popular Exploits

Rank	2008 H2	2009 H1
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)	Microsoft Snapshot Viewer ActiveX (CVE-2008-2463)
3.	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)	Adobe Acrobat and Reader Collab.CollectEmailInfo (CVE-2007-5659)
4.	RealPlayer IERPCtl ActiveX (CVE-2007-5601)	Microsoft IE7 DHTML Object Reuse (CVE-2009-0075)
5.	Apple QuickTime RSTP URL (CVE-2007-0015)	RealPlayer IERPCtl ActiveX (CVE-2007-5601)

Vulnerable ActiveX Usage and Attack Attempts

Source: ISS Managed Security Services

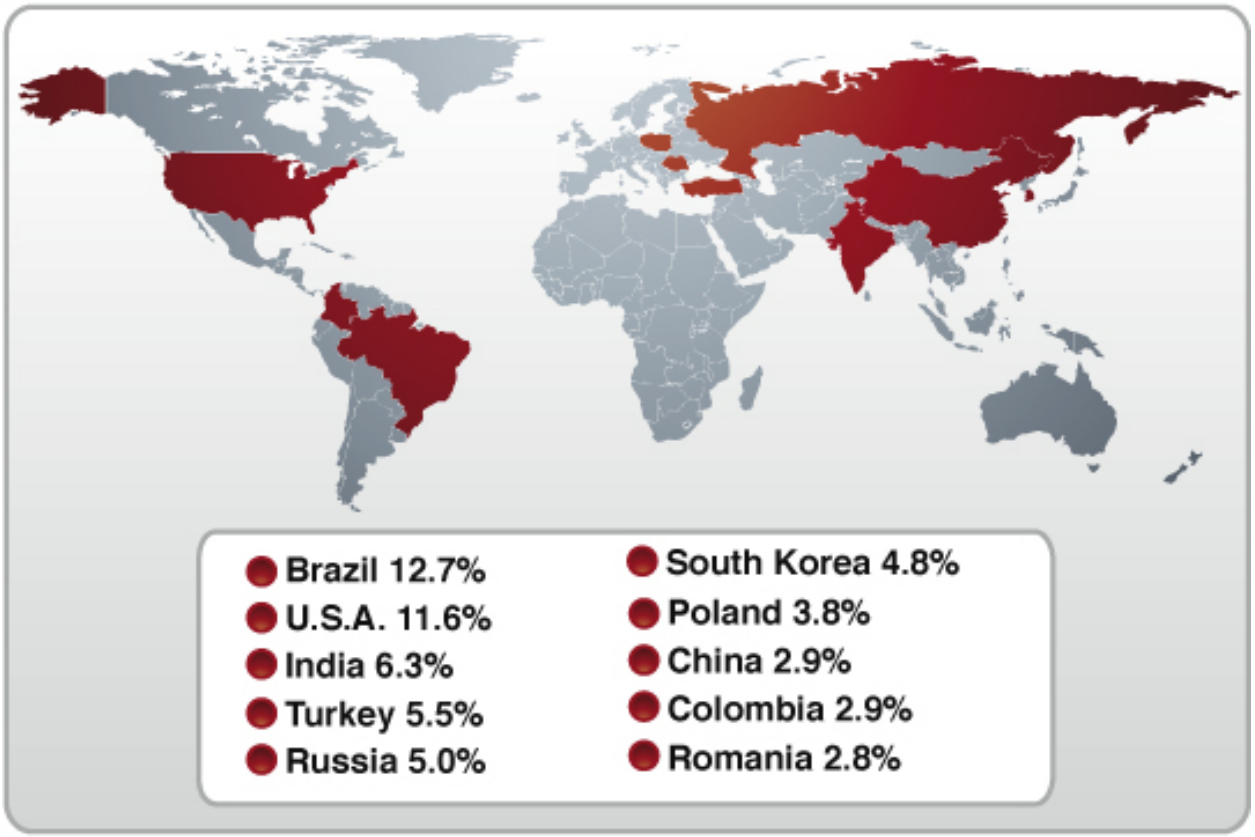


source: IBM X-Force®

Spam Senders

Geographical Distribution of Spam Senders

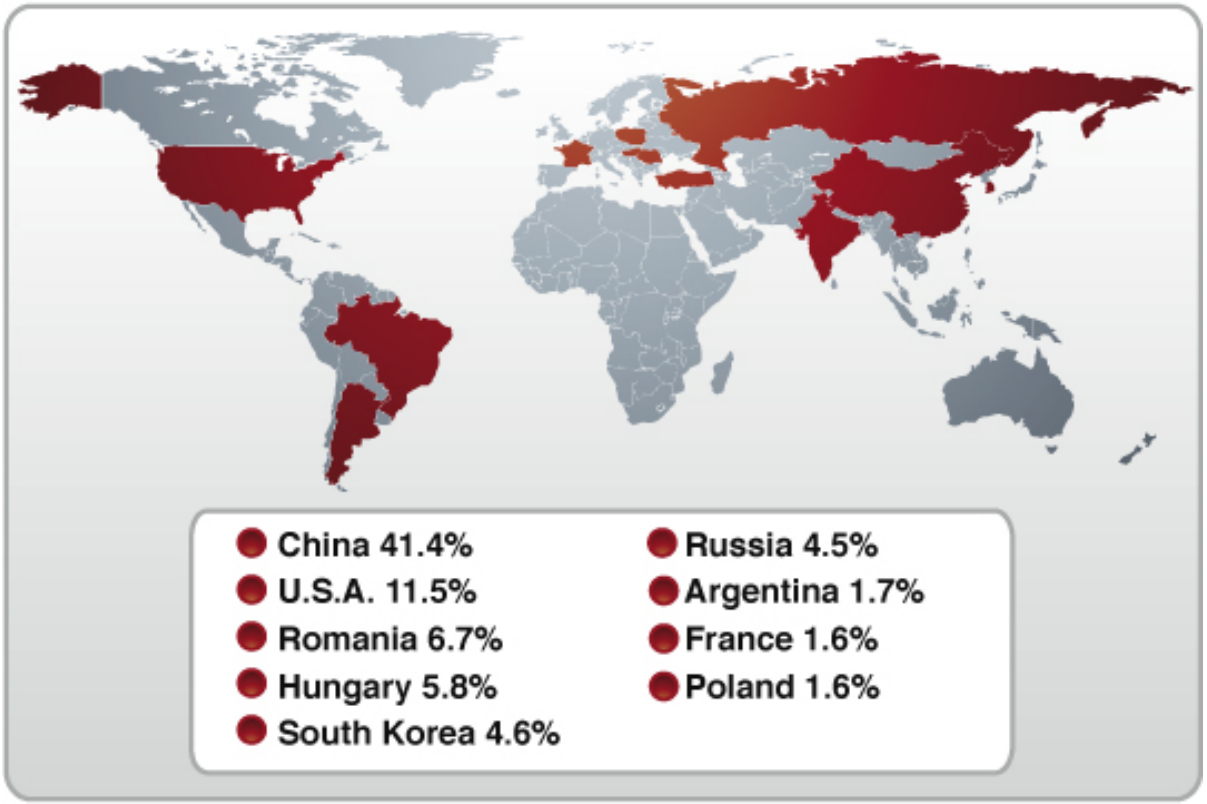
2009 H1



source: IBM X-Force®

SPAM URLs

Geographical Distribution of Spam URLs



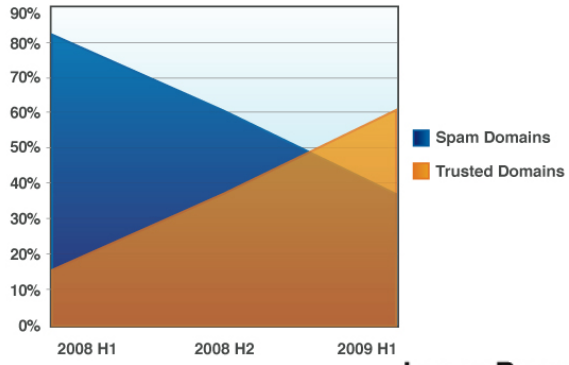
source: IBM X-Force®

People & Identity:

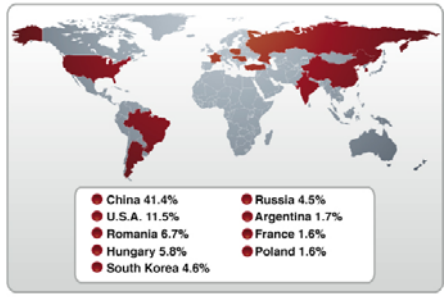
Spam Continues to Change to Avoid Detection

- Spam is up approximately **40%** in 2009
- **60%** of spam classified as URL spam
- Using “trusted” domains and “legitimate links” continues to help avoid anti-spam technologies
- Brazil, the U.S., and India account for about **30**
  of worldwide spam
- Image-based Spam has returned

Top Ten Domains Used in Spam
Spam Domains Versus Trusted Domains



Geographical Distribution of Spam URLs

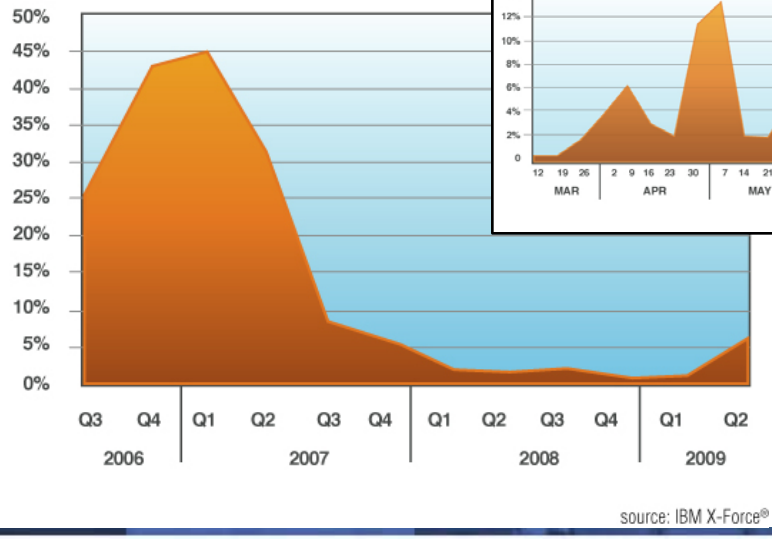


source: IBM X-Force®

Most Common Domains in URL Spam, 2009 H1

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

Image-Based Spam
2006 Q3-2009 Q2



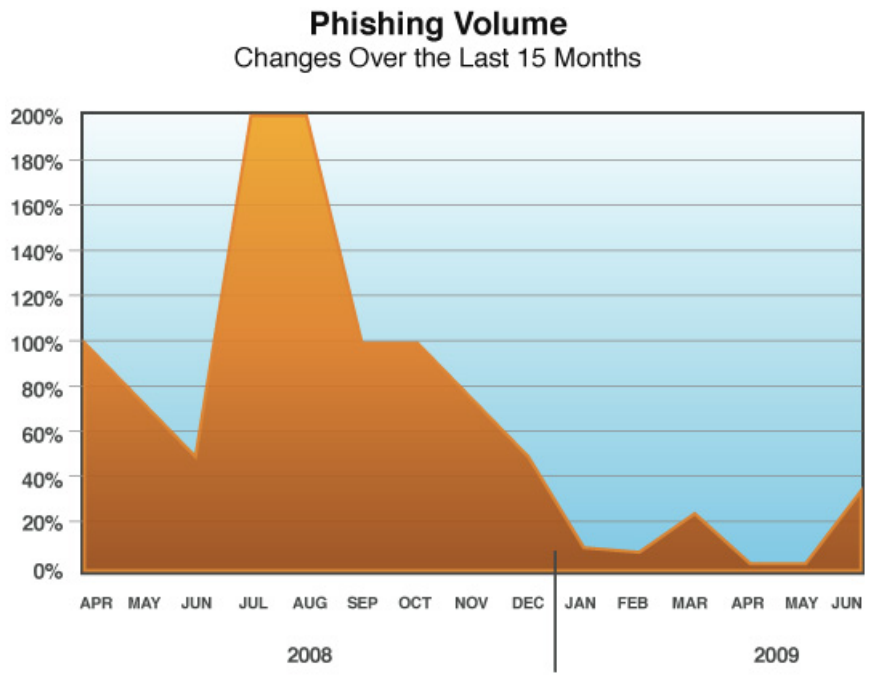
source: IBM X-Force®

People & Identity:

Phishing Attacks Decline Dramatically

- Phishing attacks decline to only 0.1% of the spam volume, driven down by a sharp decline in financial phishing (66% of all phishing vs. 90% in 2008)
- Attacks against online payment institutions remain steady

Subject Line	%
Attention! Votre compte PayPal a ete limite!	24.05%
Important Information Regarding Your Limited Account.	7.02%
PayPal® Account Review Department	2.06%
Account Security Measures	1.35%
Citibank Alert: Additional Security Requirements	1.33%
Important Information Regarding Your Account.	0.89%
Online Account Security Measures	0.53%
PayPalŽ Account Review Department	0.5%
Paypal Account Update	0.44%
Security alert	0.27%



source: IBM X-Force®

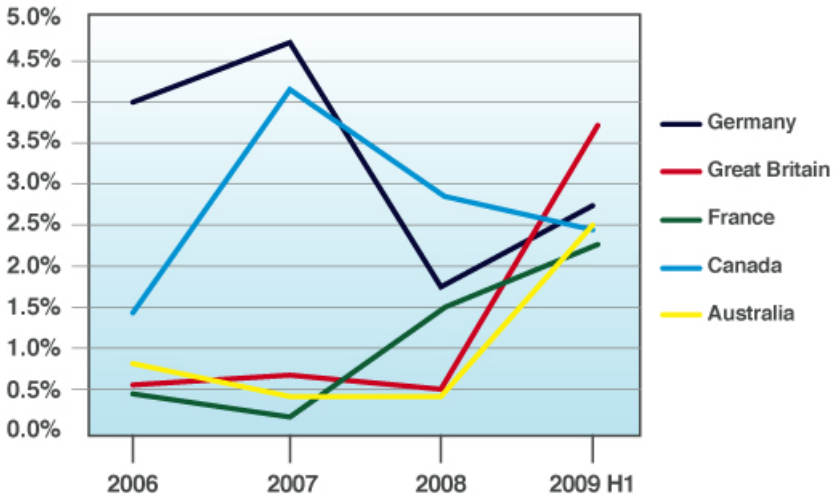
People & Identity:

Malicious Web Links Increase by 508%

- United States and China continue to reign as the top hosting countries for malicious links
  - Japan makes the top three at 8%
- Many more second tier countries are jumping into this game
  - Countries hosting at least one malicious URL jumped by **80%** in comparison to 2008

Malicious URLs by Second-Tier Hosting Countries

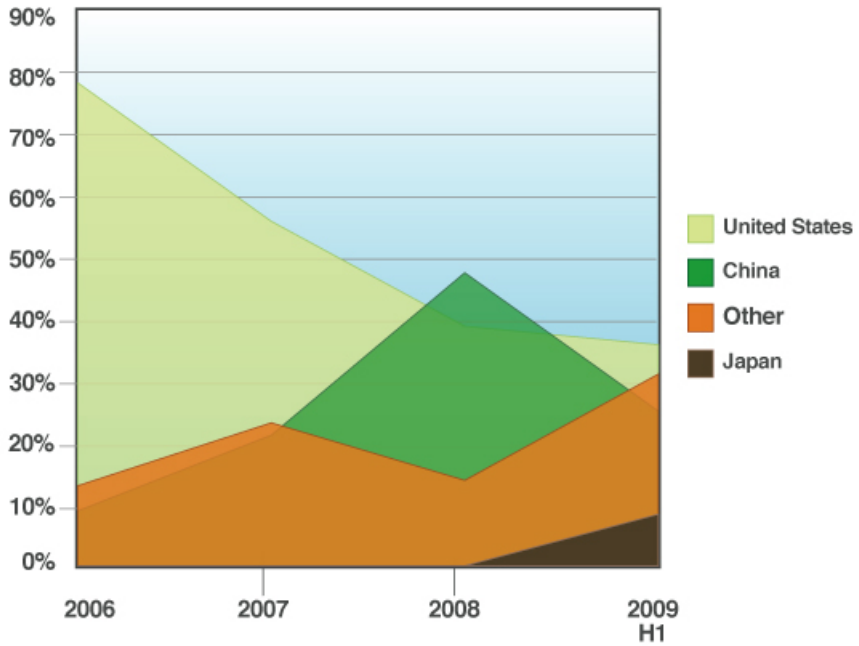
Source: ISS Cobion Crawler, 2006-2009 H1



source: IBM X-Force®

Malicious URLs by Top-Tier Hosting Countries

Source: ISS Cobion Crawler, 2006-2009 H1

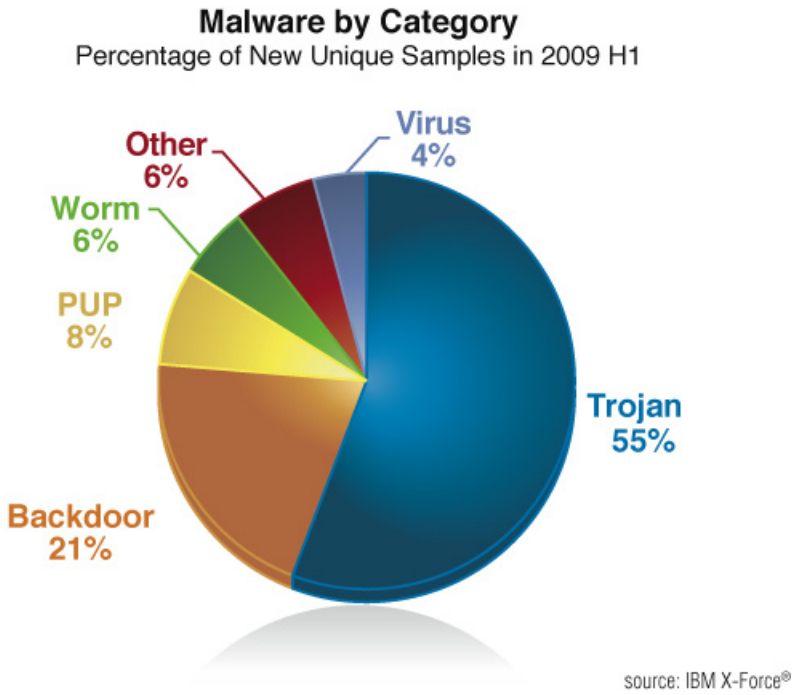


source: IBM X-Force®

People & Identity:

Majority of New Malware Are Trojans

- Trojans increased by nine percentage points, up from 46% in 2008
- Large number of new malware is generated by publicly-available toolkits
- Level of sophistication seen in 2009 malware was unprecedented
  - Techniques to propagate, mutate and hide indicate attackers have the finances and the expertise to outsmart those that can't keep up



Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

Price : 99$ (United State Dollar)

Silver Edition

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/*Vista*
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements on clipboard and save them

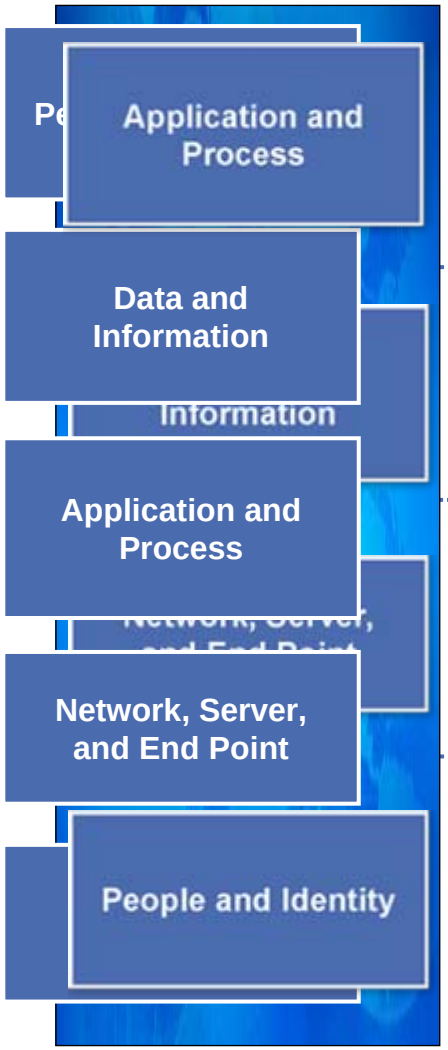
Price : 179$ (United State Dollar)

Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/*Vista*
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249$ (United State Dollar)

Report Summary:
Attacks Continue Across all Security Domains



- **3,240** new vulnerabilities were discovered in the first half of 2009, representing a decrease in comparison to 2008
- Largest categories of new vuln disclosures, SQL injection and ActiveX exploits, are slowing although exploitation remains strong
- **50.4%** of all vulnerabilities are Web application vulnerabilities

- Attackers have turned to hiding exploits in malicious documents that are hosted on Web sites or sent to victims through email (like spam)
- Portable Document Format (PDF) vulnerabilities disclosed in the first half of 2009 have already surpassed disclosures from all of 2008

- New malicious Web links increased by **508%** in comparison to the first half of 2008
- Attackers are exploiting trusted Web sites to fool users into clicking their malicious links
- Trojans make up **55%** of all Malware. Information-stealing Trojans are largest category

- Although URL spam (email with links to the spam content) are still the predominant type of spam, image-based spam has started to make a comeback.
- **66%** of phishing is targeted at the finance industry, **31%** targeted at online payment institutions

Few things to consider...

- Microsoft Windows AutoRun
- Secure Socket Layer (SSL)
  - SSLsniff
  - SSLstrip
  - MD5 collision – CA keys compromise
  - Zero-byte certificate attack
  - ...
- Social engineering attacks
  - Last time your employees had education?

Microsoft Security Advisory (967940)

Update for Windows Autorun

Published: February 24, 2009

source: IBM X-Force®

Questions and Answer?
Or assessments?

<vlatko.kosturjak@hr.ibm.com>