

Pulse

Comes to You



IBM

Managing the World's Infrastructure

X-Force® Trends and Strategy

IBM Internet Security Systems (ISS)

Filip Schepers

Technical Sales - South West Europe

Loïc Guézo

Technical Sales Leader – France

CISSP® - Lead Auditor ISO/IEC 27001:2005

24 Juin 2009

© 2009 IBM Corporation

IBM Security Strategy

Powered by X-Force

IBM Internet Security Systems Protection Platform

The most advanced and complete security architecture
ever developed —delivering preemptive security

- Integrated security intelligence
- Comprehensive suite of professional security services
- Platform and service extensibility
- Correlation and integration of multiple data sources
- Underlying “best-in-breed” appliances
- 24/7 outsourced security management
- Improved system uptime and performance without a large investment in technology or resources



Protection Platform

IBM global security reach



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



Only IBM Security is backed by the IBM X-Force® research team



X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force 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

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

9.1B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
40K documented vulnerabilities
Millions of unique malware samples

Provides Specific Analysis of:

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

Converging threats force a change in our security mindset – and technology

- Thus protection technology effectiveness is reliant on truly researching new approaches *and must be a focus!!*



Evolving Technologies The Rewards (and Risk) of Innovation



"We have put so many security products into our systems that the complexity of the sum of those security products has become itself part of the problem."

– Dan Geer

Keynote Speaker
Source Boston Conference
March 2008

- New technologies require new forms of protection – and can be “disruptive”
- Security systems themselves carry data

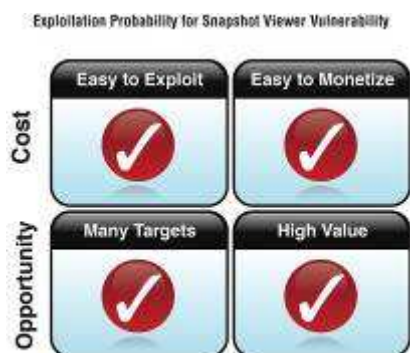
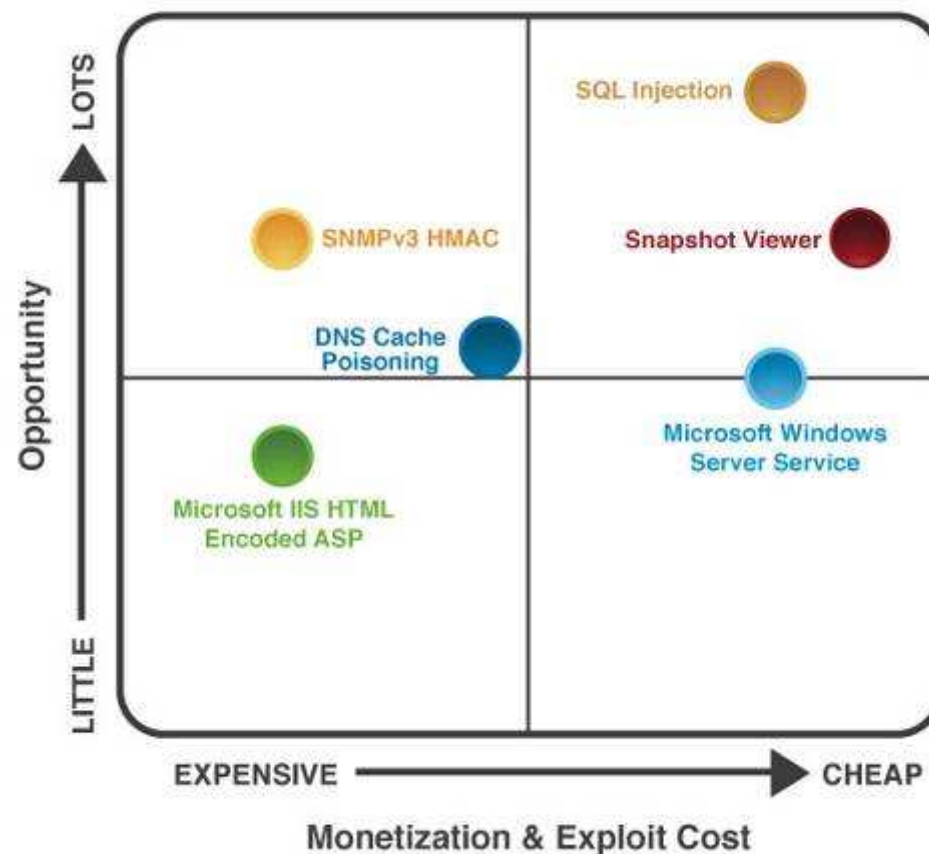
X-Force[®] Trends and Strategy

IBM Internet Security Systems (ISS)

The Economics of Attacker Exploitation

- Economics play heavily into the exploitation probability of a vulnerability
 - Serious computer criminals need a ROI
 - Exploits must be easy to exploit with a high payoff, upper right hand quadrant of the Exploitability Probability Quadrant
- Security industry must learn to incorporate criminal motivations into security response procedures
 - CVSS scored 'critical' vulnerabilities may not be as critical as they seem
- The Snapshot Viewer vulnerability is a good example of very profitable and easily executable attack

Exploitability Probability Quadrant



source: IBM X-Force®

Report Summary -- Attacks Continue Across all Security Domains

People and Identity

Data and Information

Application and Process

Network, Server, and End Point

■ Vulnerabilities

- Vulnerabilities have reached a high plateau in 2008, with 53% not having any vendor-supplied patches
- Apple & Linux top the most vulnerable operating systems
- 54.9% of all vulnerabilities are Web application vulnerabilities, and 75% of those have no patches available
- Mass endpoint exploitation is happening through browser vulnerabilities, malicious movies and documents like Adobe PDF files

■ Web-Based Security Threats

- Number of malicious Web sites in the 4th quarter of 2008 alone surpassed the total number seen in all of 2007
- China surpassed US for the first time in hosting most malicious Web sites
- Web applications have become the Achilles heel of corporate IT security
- SQL injection is the most predominant type of Web application vulnerability

■ Spam & Phishing

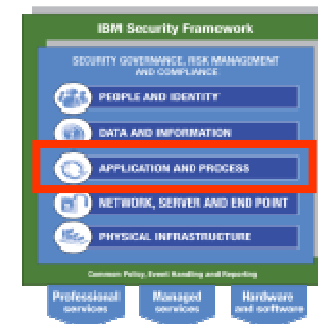
- Simple spam (text or URL) replaced complex (PDF, image) spam in 2008
- More than 97% of spam sites are only up for a week or less
- URL spam is now coming from well known & trusted domains (blogspot, doubleclick, google)
- More than 90% of phishing is targeted at the finance industry

■ Malware

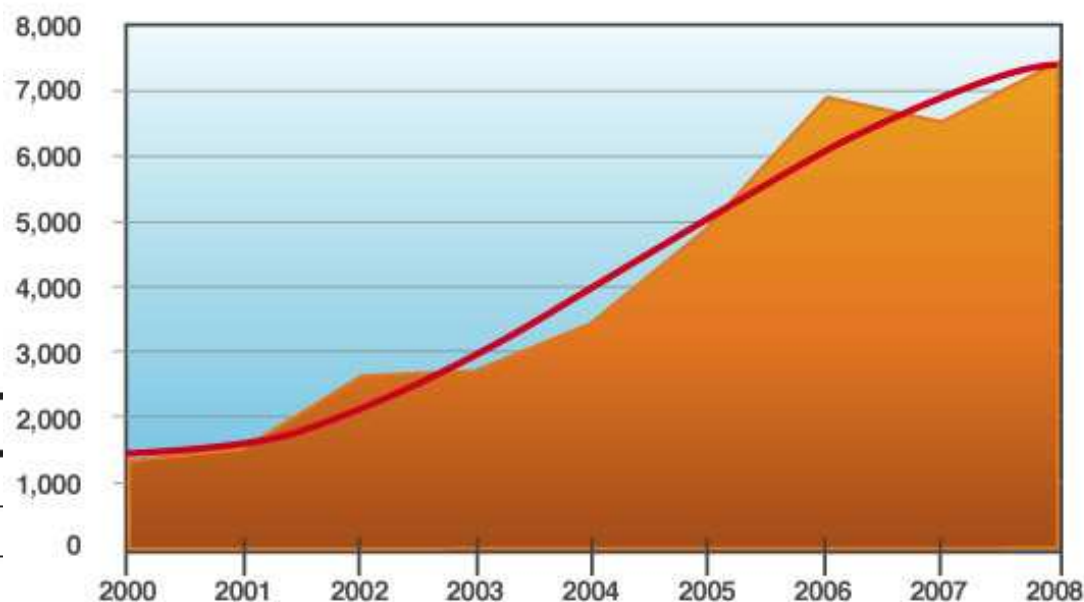
- Trojans make up 46% of all Malware, with information-stealing as the most prevalent

Vulnerabilities are at a High Plateau

- **13.5%** increase from 2007, totaling 7,406 new vulnerabilities
 - From 2001-2006 the average annual growth was **36.5%**, from 2006-2008 growth tapered to **2%**
 - Vulnerability disclosures appear to be reaching a permanently high plateau
- June 2008 was the highest month for disclosures (692)
 - Busiest week statistics are below
 - Tuesday remains busiest day of the week for disclosures due to multiple vendor-released advisories



Vulnerability Disclosures
2000 – 2008

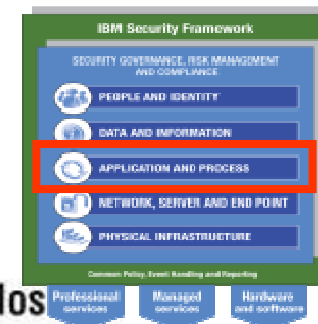


source: IBM X-Force®

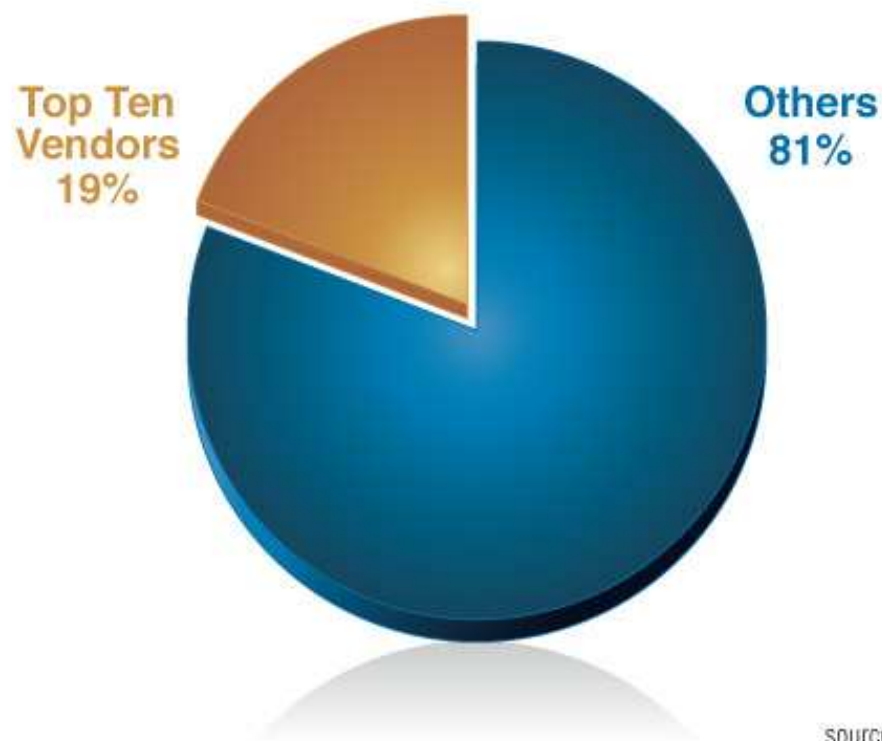
Year	Busiest Week for Vulnerability Disclosures
2000 – 2005	Week before Christmas
2006	Week before Thanksgiving
2007	Summer
2008	Week before Christmas

Web Application Vendors Rise in Prominence

- Top ten vendors listed below comprise **19%** of all vulnerability disclosures
 - New vendors this year are Joomla!, Drupal, Typo3, and Mozilla
 - Open source Web Content Management System (CMS) vendors written in PHP enter the list



Percentage of Vulnerability Disclosures Attributed to Top Ten Vendors

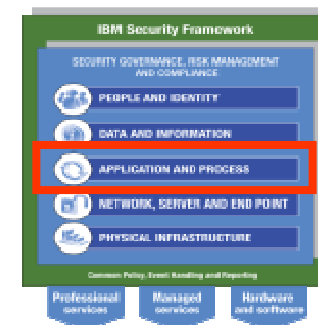


Ranking	Vendor	Disclosures
1.	Microsoft	3.16%
2.	Apple	3.04%
3.	Sun	2.19%
4.	Joomla!	2.07%
5.	IBM	2.00%
6.	Oracle	1.65%
7.	Mozilla	1.43%
8.	Drupal	1.42%
9.	Cisco	1.23%
10.	TYPO3	1.23%

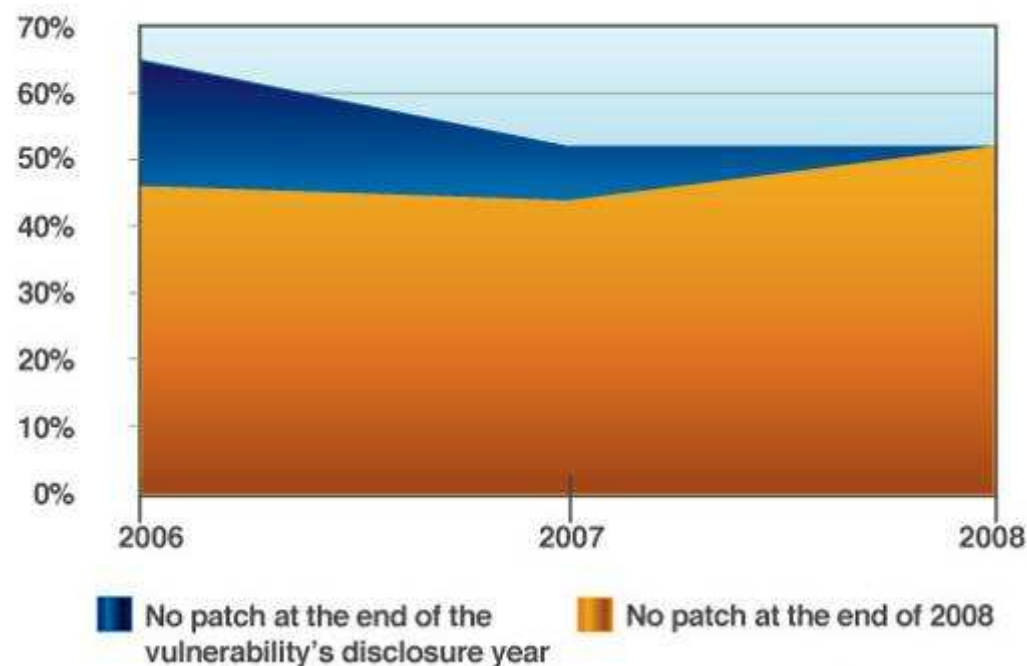
source: IBM X-Force®

Vendors not Patching Vulnerabilities

- **53%** of all vulnerabilities disclosed in 2008 had no vendor-supplied patches to remedy the vulnerability
 - **44%** of vulnerabilities from 2007 and **46%** from 2006 still have no patches

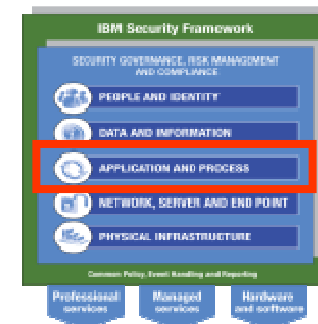


Percentage of Vulnerabilities with Vendor-Supplied Patches
by Vulnerability Disclosure Year, 2006 – 2008



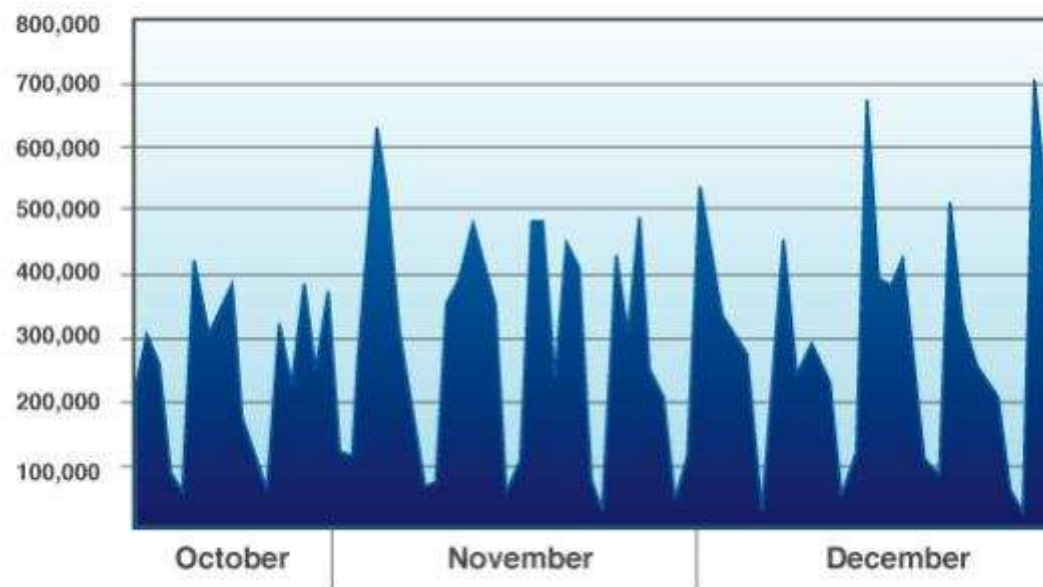
source: IBM X-Force®

Good Web Sites Using Bad ActiveX Controls



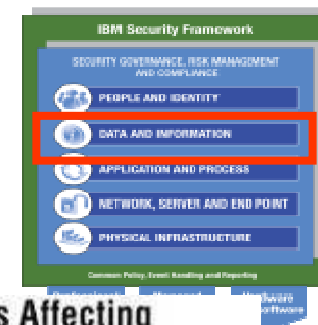
- Vulnerable ActiveX is the #2 web-related exploit used by real attackers
- Updated browsers can mitigate the problem
 - Very few people always have their browser consistently patched
- Good Web sites, frequently using old or unaudited code, request that users load these known vulnerable ActiveX controls
- Examples of bad ActiveX controls found on good Web sites:
 - Aurigma ImageUploader 4.1
 - BusinessObjects RptViewerAX
 - Macrovision InstallShield InstallScript One-Click Install
 - Macrovision InstallShield Update Service Web Agent
 - Microsoft MDAC RDS Dataspace
 - Microsoft WebViewFolderIcon

Vulnerable ActiveX Control Usage and Exploitation



source: IBM X-Force®

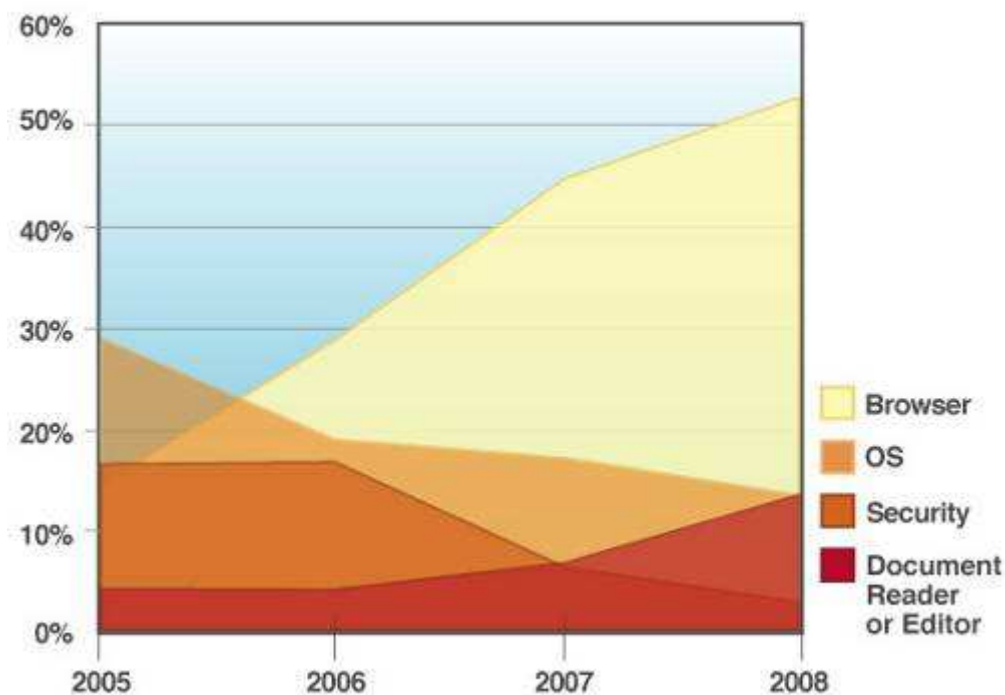
Hackers Target Unpatched PCs



- PC vulnerabilities decreased overall for the first time in 2008, although some categories increased
 - Document readers & editors increased **162%**
 - Multimedia applications were up by **127%**

- Web Browser vulnerabilities make up **52%**
 - Hackers rely on users not patching browsers

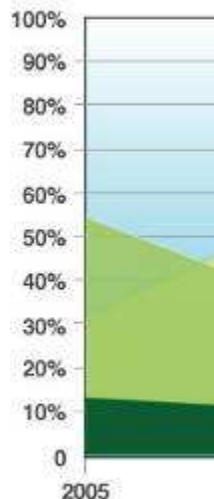
Critical and High Vulnerability Disclosures Affecting Client-Side Applications by Application Category, 2005 – 2008



source: IBM X-Force®

Exploits

- Pre-package management
 - It is not known if it actually works
- 89% of public exploit day or before 2008
 - Up from 10% in 2005



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 detected 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 detected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/Vista
- Webcam streaming is available with this version
- Realtime Screen viewing (controlling is disabled)
- Notifies changements on clipboard and save them

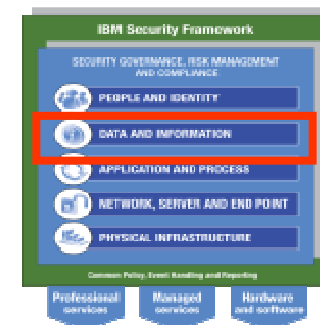
Price : 179\$ (United State Dollar)



Gold Edition

- 6 months (unlimited) or 9 months (maximum 3 times) replacement warranty if it gets detected 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)

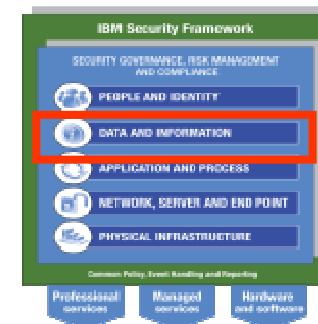
Price : 249\$ (United State Dollar)



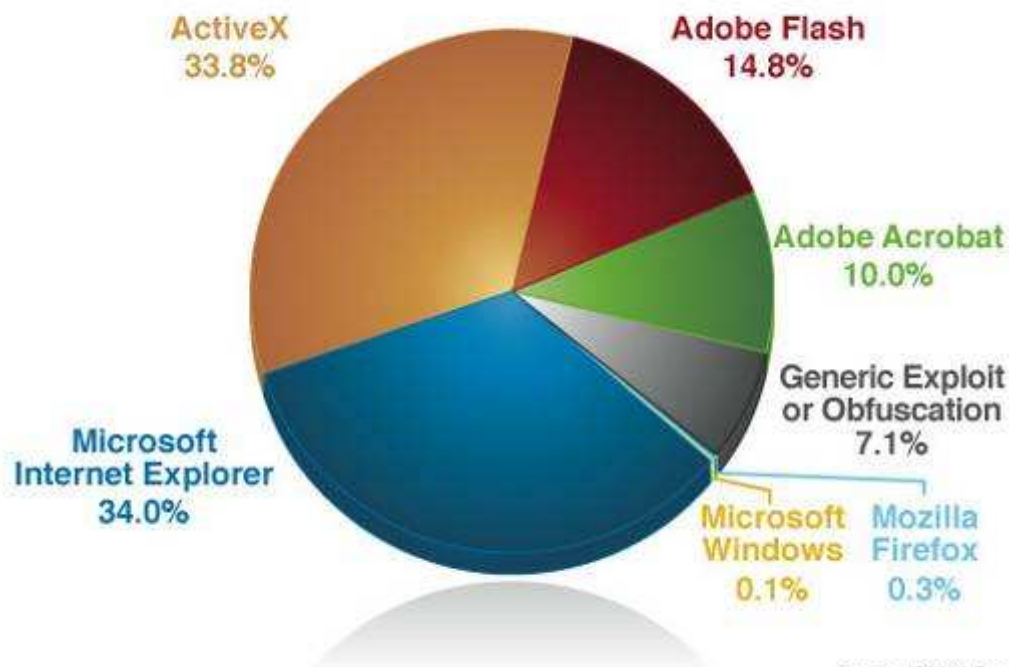
H2 (Second Half)
DD
k (and variants)
exploit
do (and variants)
H2 (Second Half)
Microsoft MDAC RDS Dataspace
ActiveX (CVE-2006-0003)
Microsoft WebViewFolderIcon ActiveX
(CVE-2006-3730)
Internet Explorer "createControlRange"
ActiveX (CVE-2005-0055)
Windows Media Player IERPCtl ActiveX
(CVE-2007-5601)
QuickTime RSTP URL
(CVE-2007-0015)

Exploits Hide in Documents like PDFs

- In addition to browser and ActiveX, exploits hiding in documents (like PDFs) became much more significant in the last quarter of 2008
- In 2008 China surpassed the US as being the largest source of malicious Web sites

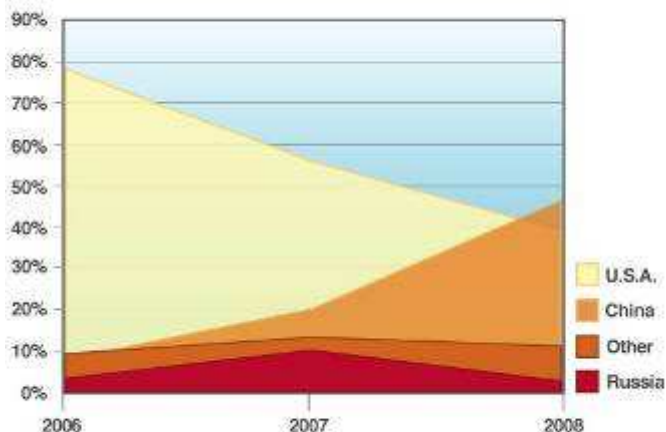


Malicious Website Exploits by Affected Application
ISS Cobion Crawler, 2008 Q4



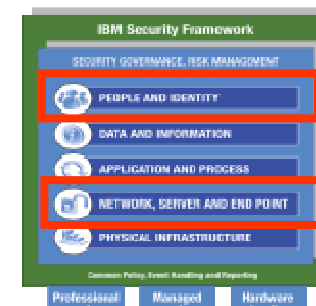
source: IBM X-Force®

Malicious URLs by Hosting Country
ISS Cobion Crawler, 2006 – 2008



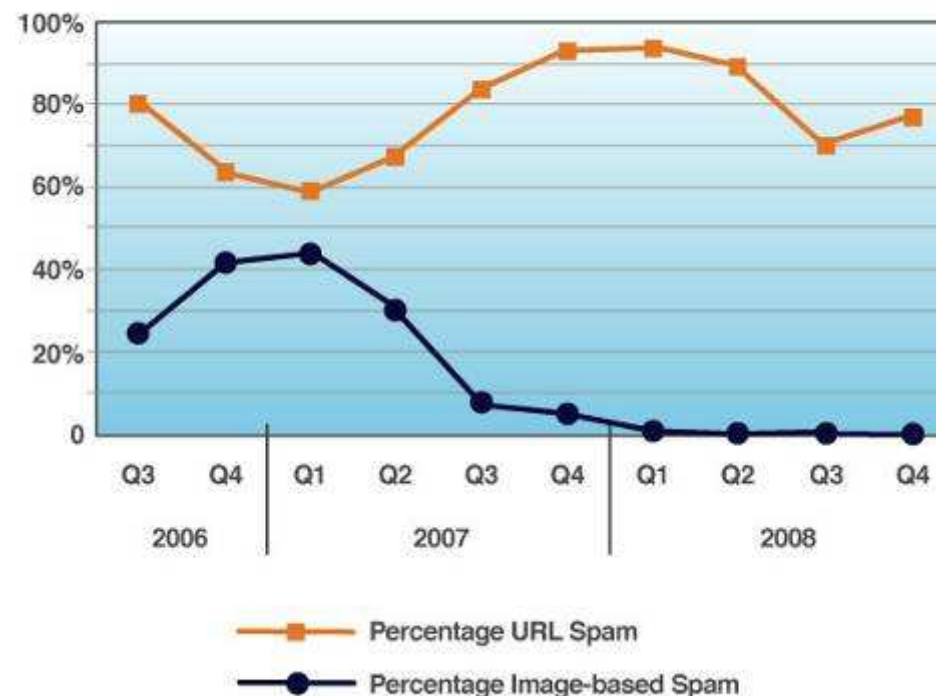
source: IBM X-Force®

Spam Changes to Avoid Detection



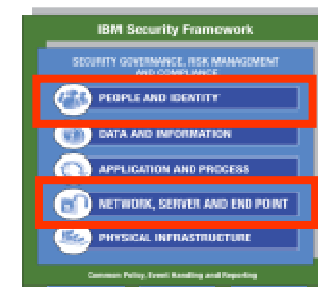
- URL spam that evades anti-spam technologies is on the rise
 - URL spam includes a simple link to a Web site that delivers a spam message to a victim
 - Its simplicity makes it difficult to detect
- More than **97%** of spam URLs are put up and taken down within a week or less
 - Compared to spam URLs remaining up for longer than a month in 2006
- URL spam is now coming from well known and trusted domains like blogspot, doubleclick and google
 - Using “trusted” domains and “legitimate links” continues to help avoid anti-spam technologies
 - Targeted news Websites include cnn.com, msn/msnbc.com, and bbc.co.uk

Percentage of Image-based Spam and URL Spam



source: IBM X-Force®

Phishers Narrow in on Targets

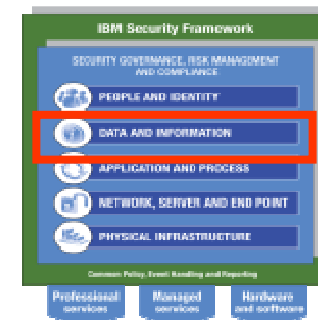


- Phishing is **5%** of the overall spam volume
- Phishers are becoming more granular in their targets
 - In 2007 the top subject lines represented more than 40% of all phishing emails
 - In 2008 the top subject lines made up only **6.23%**
- 2008 saw a trend in engaging the user to perform an action
 - Rather than having a generic subject like “security alert,” the phishers attempt to engage the user into doing something, such as fixing an account that has been suspended or updating account information

2007 Subject Lines	%
<empty subject line>	22.21%
Account Security Measures!	3.86%
Important Notice – E*TRADE FINANCIAL Corp	3.21%
Important Notice!	2.01%
Volksbanken Raiffeisenbanken AG: 02/11/2007	1.94%
Security Measures!	1.82%
Citibank Account Security!	1.77%
Citibank Bank Notice!	1.75%
Citibank Account Security Measures!	1.74%
Volksbanken Raiffeisenbanken AG: 14/11/2007	1.32%

2008 Subject Lines	%
PayPal® Account Review Department	1.47%
PayPal Security Department	0.97%
PayPal Abuse Department.	0.63%
PayPal Account Security Measures	0.60%
Volksbanken Raiffeisenbanken	0.48%
PayPal Account Suspension	0.47%
Restore Your Barclays Account	0.44%
Read carefully - Important Notification	0.40%
Update Your Billing Information.	0.39%
Read carefully - Important Notification!	0.38%

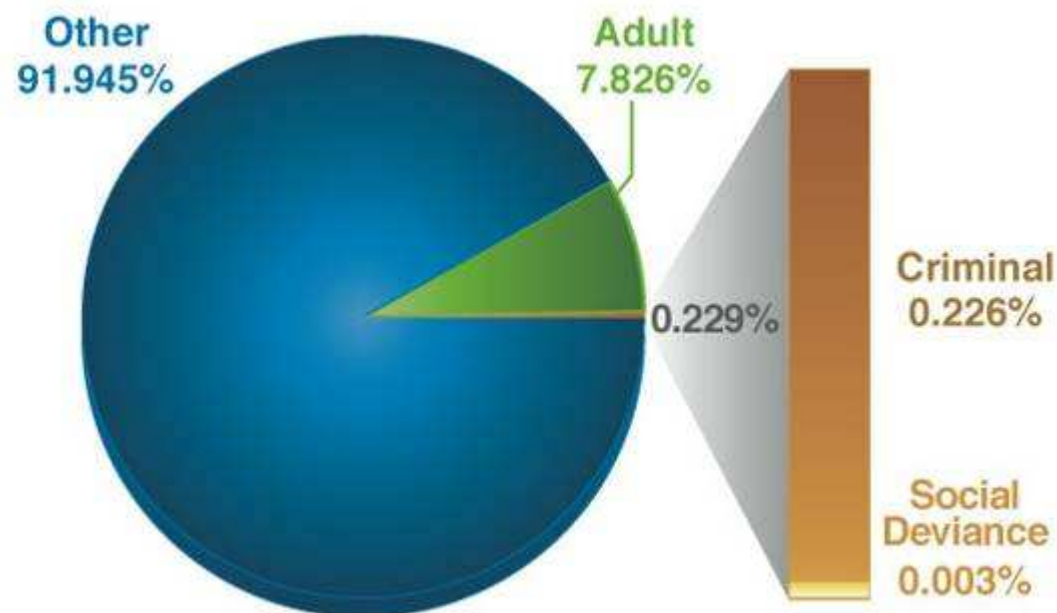
“Bad” Web Content Tries to Evade Filters



- **8%** of the Internet contains unwanted content such as pornographic or criminal Web sites
 - The US distributes more than 50% of all adult, criminal and socially deviant Web sites

- Anonymous Web proxies, that hide a target URL from a Web filter, more than doubled from 2007 to 2008

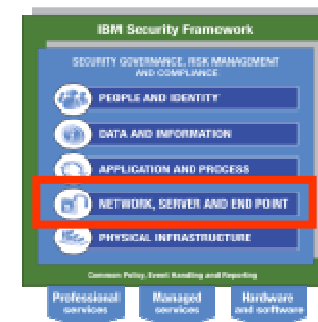
Content Distribution of the Internet
2008



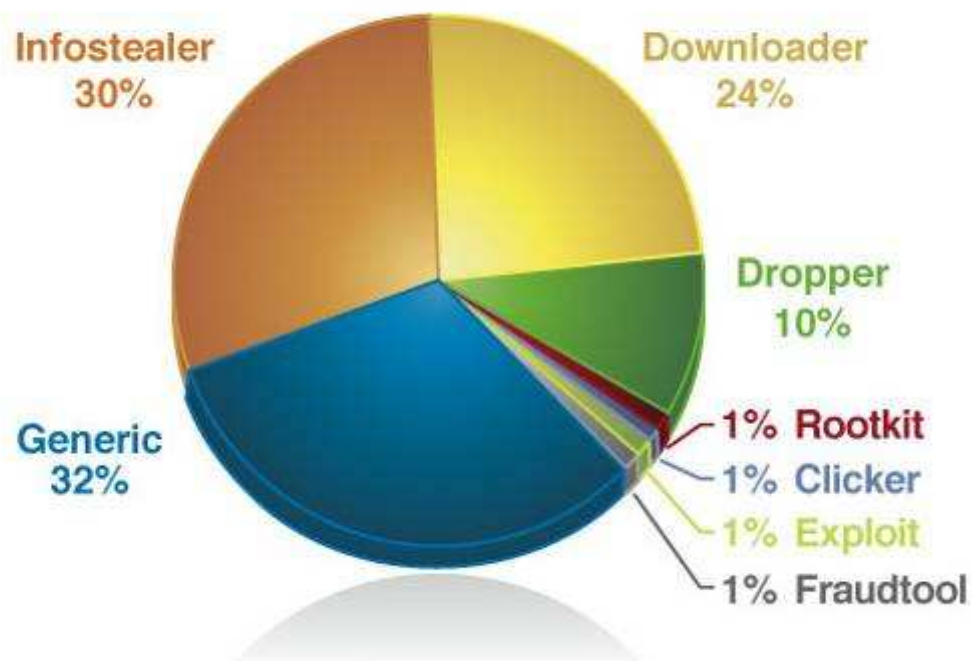
source: IBM X-Force®

Information Stealing Trojans are Increasing

- Trojans make up **46%** of all Malware
- Infostealers & Downloaders are the most common subcategories
 - Both have increased in prevalence in 2008
 - Increase of attackers aiming to spy and steal information from users
 - 38% of Infostealer Trojans target online games
 - 18% of Infostealer Trojans target online banking
- Attackers continue to use multi-component/multi-stage strategies to download or drop additional malware components after a system is compromised



Trojans by Category 2008



source: IBM X-Force®

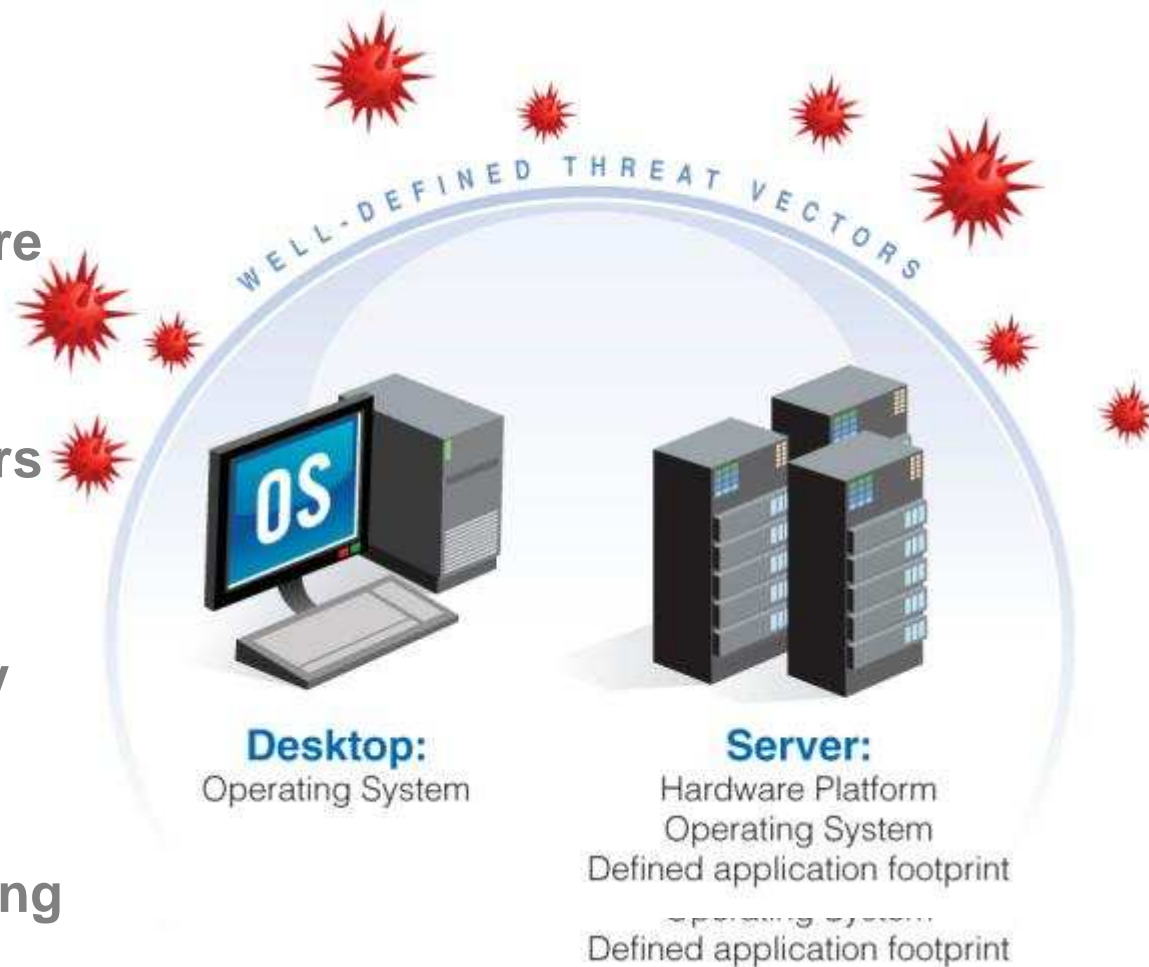
Web Application Vulnerability Landscape

The Web Ecosystem

The Security Landscape of Old

Traditional Infrastructure was easier to protect . . .

- Concrete entities that were easy to understand
- Attack surface and vectors were very well-defined
- Application footprint very static
- Perimeter defense was king



The Changing Security Landscape of Today

“Webification” has changed everything . . .

- Infrastructure is more abstract and less defined
- Everything needs a web interface
- Agents and heavy clients are no longer acceptable
- Traditional defenses no longer apply

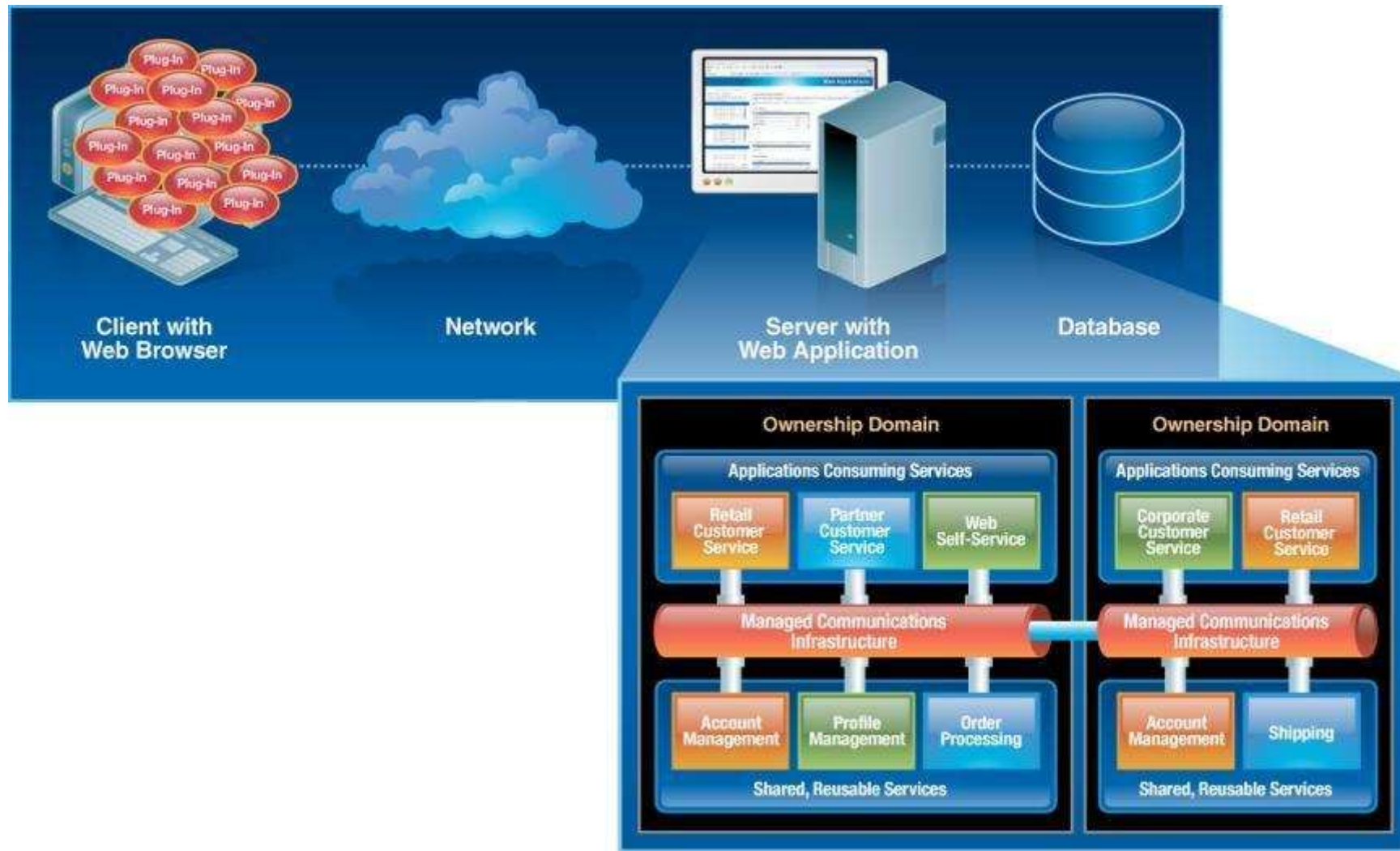


The Web Ecosystem (simple view)

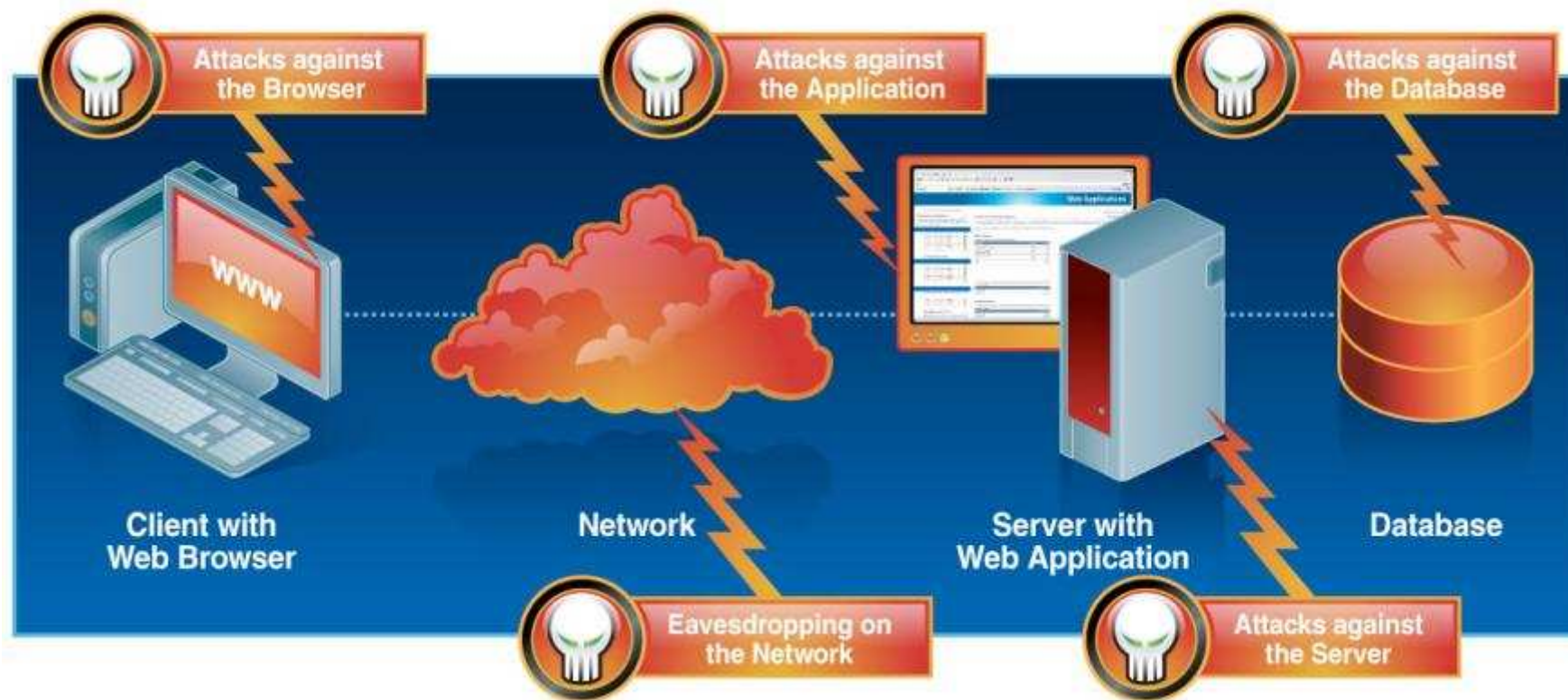
- Client with a Web browser renders the content for a user
- Network transports content between the server and the client
- Server with the Web application performs the required action
- Database stores information



The Web Ecosystem (complex view)



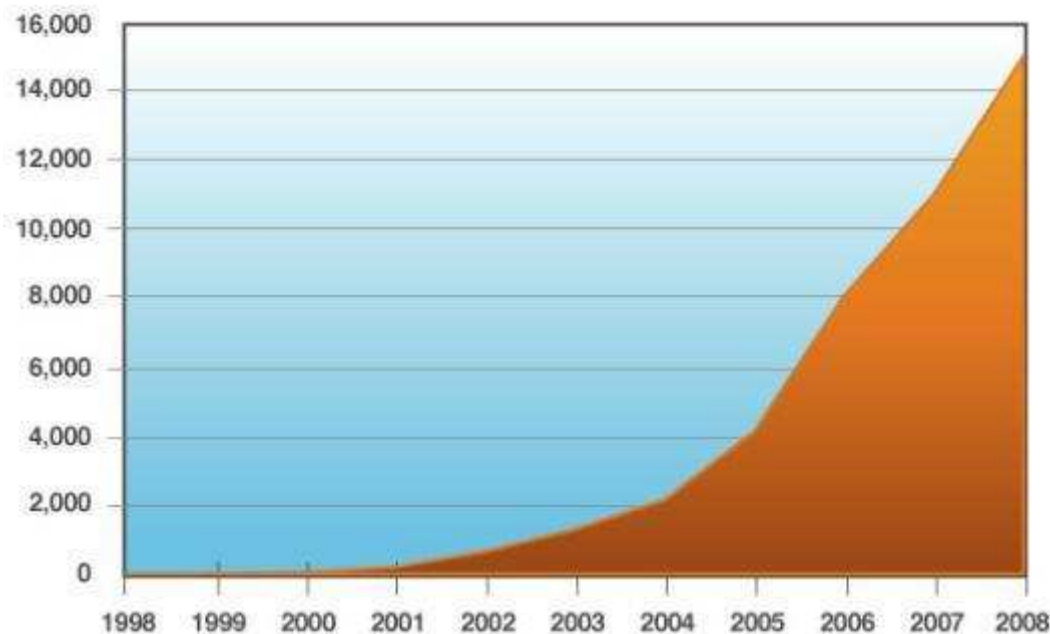
Attack Vectors



Growth of Web Application Vulnerabilities

- SQL injection vulnerability disclosures more than doubled in comparison to 2007
- The number of active, automated attacks on web servers was unprecedented

Cumulative Count of Web Application Vulnerabilities
1998 – 2008



source: IBM X-Force®

2008 Web Threats Take Center Stage

- Web application vulnerabilities
 - Represent largest category in vulnerability disclosures (55% in 2008)
 - 74% of Web application vulnerabilities disclosed in 2008 have no patch to fix them
 - Excluding home-built applications

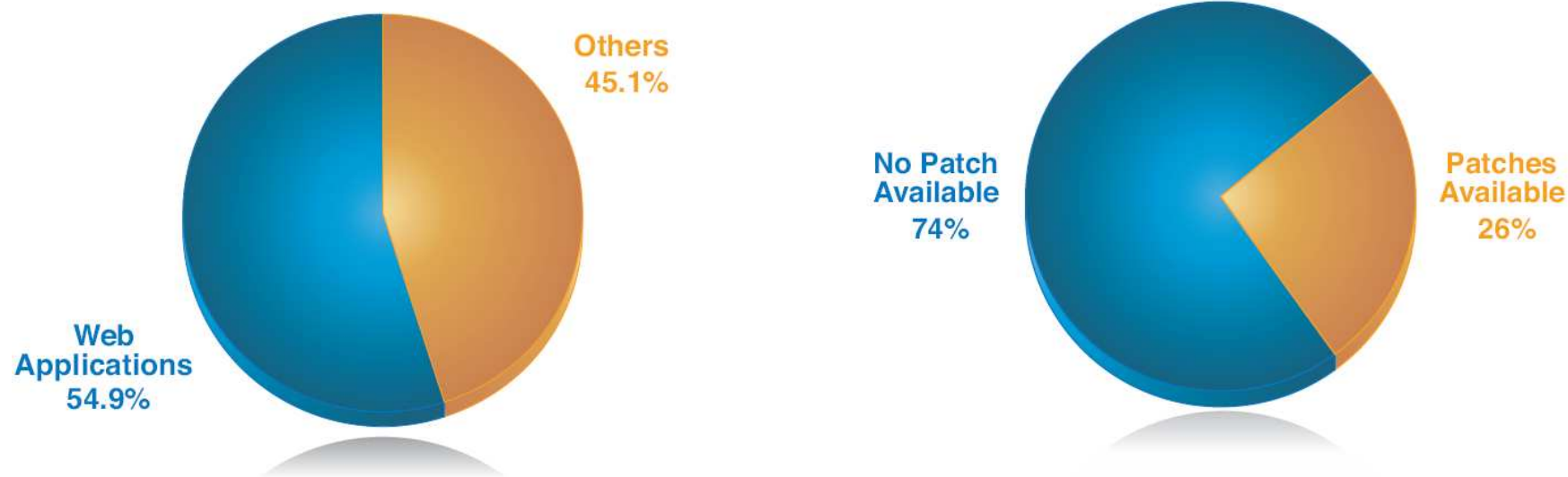


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

Exploitation is Rampant

- Exploitation of SQL injection skyrocketed in 2008
 - Increased by 30x from the midyear to the end of 2008



Figure 20: Initial SQL Injection Attacks Monitored by IBM ISS Managed Security Services, May – June 2008

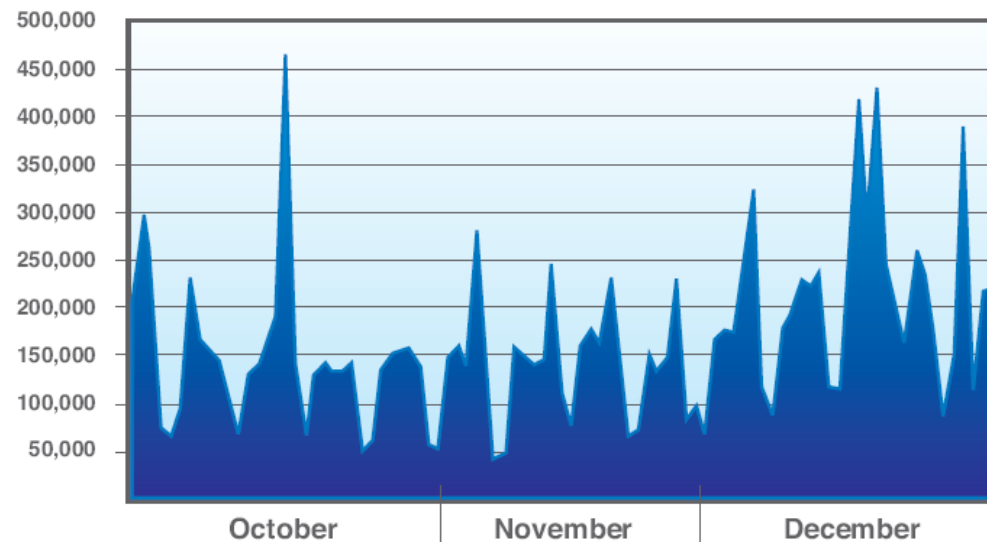


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

Reality: Security and Spending Are Unbalanced



75% of All Attacks on Information Security are Directed to the Web Application Layer

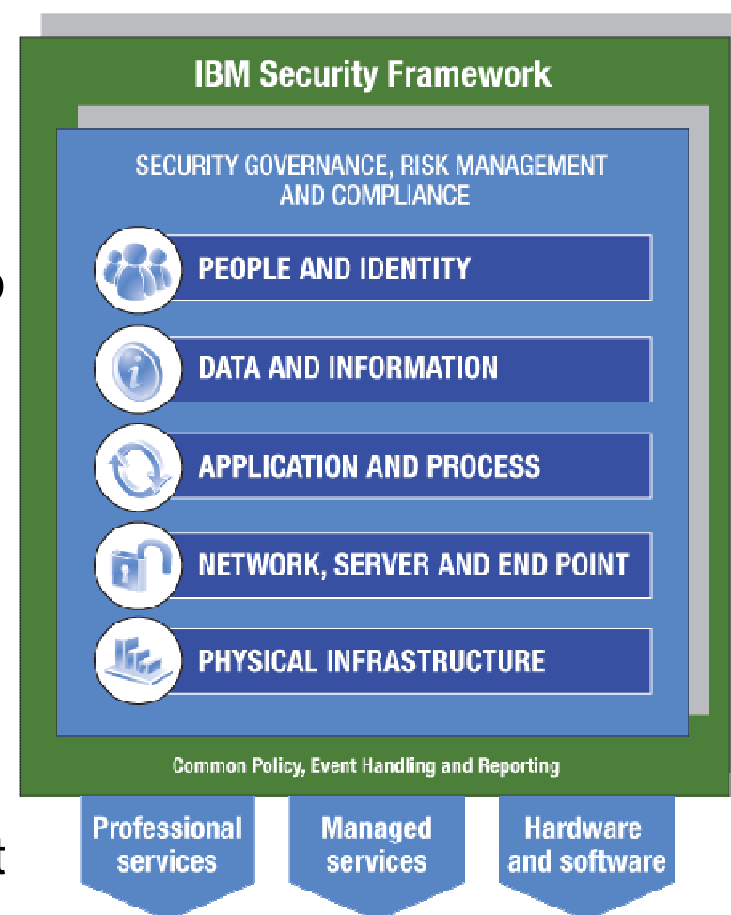
2/3 of All Web Applications are Vulnerable ****Gartner**

The Conundrum

- How security professionals and businesses prioritize risk and threats haven't changed with the overall landscape
- Businesses and professionals still tend to prioritize risk against an outdated traditional infrastructure viewpoint
- Businesses and professionals still tend to implement security solutions that focus on traditional threats and vectors
- Big blind spots
 - Browsers and web applications are still largely ignored or prioritized below other infrastructure from a security perspective

X-Force 2008 Trends – Summary

- Vulnerabilities are at a high plateau
- Secure Web presence has become the Achilles heel of corporate IT security
- Mass endpoint exploitation is happening not only through browser vulnerabilities, but also through malicious movies and documents like Adobe PDF files
- Successful exploitation typically leads to the installation of information-stealing Trojans
 - The most prevalent malware category
- China hosts the most malicious Web sites, surpassing the US for the first time in 2008
- The McColo takedown had the single largest impact on spam all year



X-Force 2008 Trends – Mapping to IBM Portfolio



Risk	IBM Security Solutions
Vulnerabilities	<ul style="list-style-type: none"> - IBM ISS Intrusion Prevention System (IPS) products: Proventia Network IPS, Proventia Server, RealSecure Server Sensor, Proventia Desktop & Proventia Multifunction (MFS) - IBM ISS Managed Protection Services for IPS - Tivoli Security Information and Event Manager (TSIEM)
Web Application Vulnerabilities	<ul style="list-style-type: none"> - Web application IPS security for Network, Server and MFS (April marketing launch) - Managed Protection Services for IPS - Rational Appscan for assessment , Rational Appscan Enterprise - Tivoli Security Information and Event Manager, Tivoli Security Policy Manager
PC Vulnerabilities including Malicious Web Exploits	<ul style="list-style-type: none"> - IBM ISS Intrusion Prevention System (IPS) product lines (see above list under vulnerabilities) - Managed Protection Services for IPS, - Managed Security Services for Web Security - Proventia Web Filter
Spam	Mail security offerings: <ul style="list-style-type: none"> - Proventia Network Mail / Lotus Protector - Proventia Multifunction System (MFS) - Managed Security Services for Mail Security
Unwanted Web Content	<ul style="list-style-type: none"> - Proventia MFS, Proventia Web Filter - Managed Security Services for Web Security
Malware	<ul style="list-style-type: none"> - Proventia Desktop and MFS - Managed Security Services for Mail and Web Security - Proventia Network Mail / Lotus Protector - Proventia Web Filter



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/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>



X- Force Threat Analysis Service

Stay up-to-date on the latest threats customized for your environment: <http://www-935.ibm.com/services/us/index.wss/offering/iss/a1026943>

Qui contacter à IBM – ISS France ?		Adresse e-mail	Téléphones
ISS France leader	Thomas STOLTZ	thomas_stoltz@fr.ibm.com	01 49 05 92 37 / 06 70 01 22 92
Sales Manager	Philippe BEAUCHAMP	philippe_beauchamp@fr.ibm.com	01 49 05 86 86 / 06 84 64 02 41
Technical Manager	Loïc GUEZO	lguezo@fr.ibm.com	01 49 05 71 97 / 06 72 83 40 27
Marketing	Marie-Odile Triquet	Triquet-libeau@fr.ibm.com	01 49 05 85 21 / 06 72 79 81 54
Relation partenaires	Florence BRISSET	florence.brisset@fr.ibm.com	01 49 05 82 54 / 06 74 69 03 74
Services managés	Dominique LYON	dlyon@fr.ibm.com	01 49 05 84 35 / 06 75 09 58 74
Secteur Public	Alexandre PISANI	alexandre.pisani@fr.ibm.com	01 49 05 63 97 / 06 84 95 19 62
Secteur Indus / COM	Valentin JANGWA	VJANGWA@fr.ibm.com	01 49 05 38 28 / 06 15 09 69 49
Secteur Distribution	Christian QUADRADO	christian.quadrado@fr.ibm.com	01 49 05 09 62 / 06 73 98 24 26
Secteur FSS / Insurance	Catherine CHAPPOT	catherine_chappot@fr.ibm.com	06 07 919 330
Secteur Genral Business	Jean-Claude MAZIERES	jeanclaude.mazieres@fr.ibm.com	01 49 05 08 70 / 06 84 64 08 76
Secteur Indus / CSI	Sébastien GELOT	sebastien.gelot@fr.ibm.com	01 49 05 87 83 / 06 76 45 73 86

Thank
You

