2009 IBM ISS X-Force®
Mid-Year Trend & Risk Report

IBM Internet Security Systems (ISS)

Andrew Luetje
ISS Solutions Specialist
816-679-2885
andrewlu@us.ibm.com

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

Report Summary:
Attacks Continue Across all Security Domains

Application and Process

- **3,240** new vulnerabilities were discovered in the first half of 2009, a **8%** decrease over 2008, but SQL injection and Active X exploitations are on the rise.
- **50.4%** of all vulnerabilities are Web application vulnerabilities
- "Gain access" remains the primary consequence of vulnerability exploitation

Data and Information

- Portable Document Format (PDF) vulnerabilities disclosed in the first half of 2009 has already surpassed disclosures from all of 2008
- US regains top spot in hosting the most malicious Web sites

Network, Server, and End Point

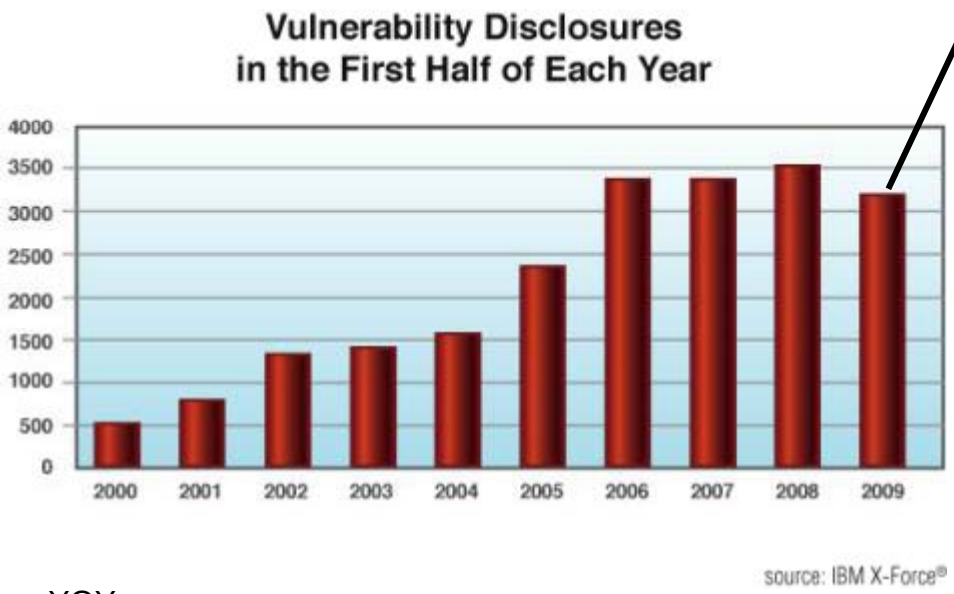
- Trojans make up **55%** of all Malware
- Information-stealing Trojans are the most prevalent malware category
- New malicious Web links increased by **508%** in comparison to the first half of 2008.

People and Identity

- URL spam (simple, one-liner text-based spam) that evades anti-spam technologies emerged in early 2008, continues to be the predominant type, coming from well known & trusted domains (blogspot, doubleclick, google)
- **66%** of phishing is targeted at the finance industry, **31%** targeted at Online Payment Institution

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
- Exploitations targeting these vulnerabilities are increasing especially SQL injection and ActiveX controls.

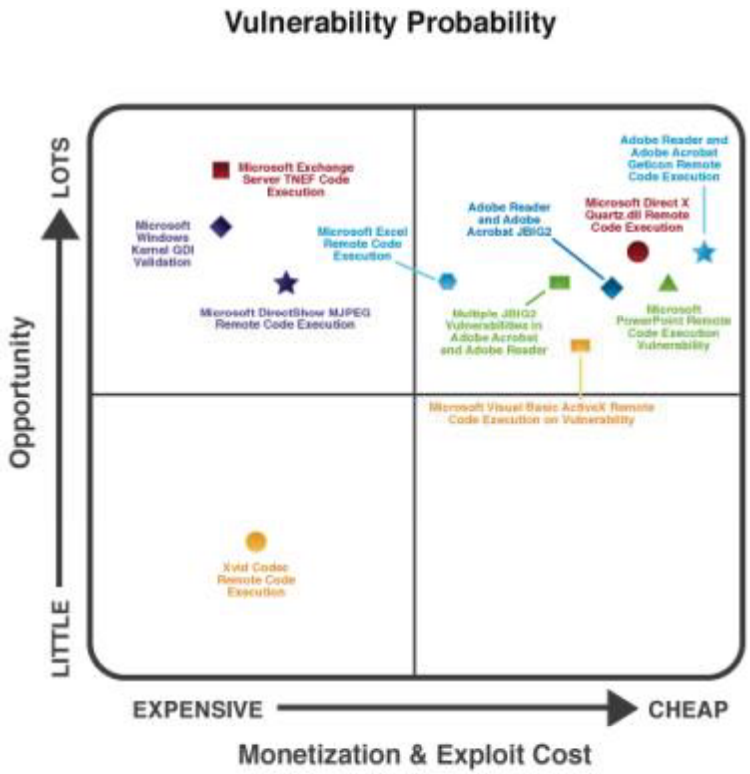


- High vulnerabilities are down **6%** YOY
- Medium vulnerabilities are up to **62%** of the vulnerabilities (8% YOY increase)

YOY = year over year

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

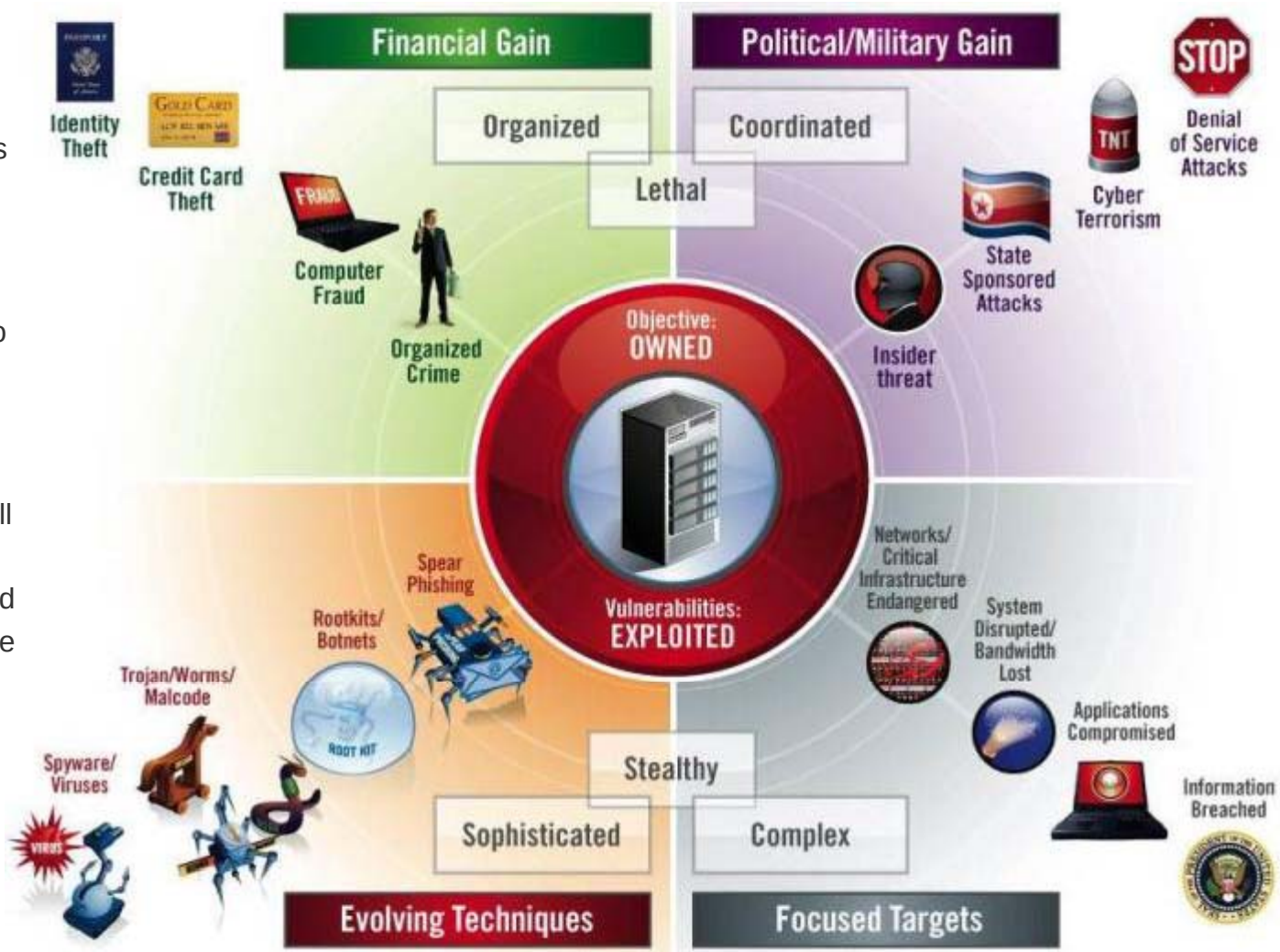


source: IBM X-Force®

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

Customers should also be concerned about vendors 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%

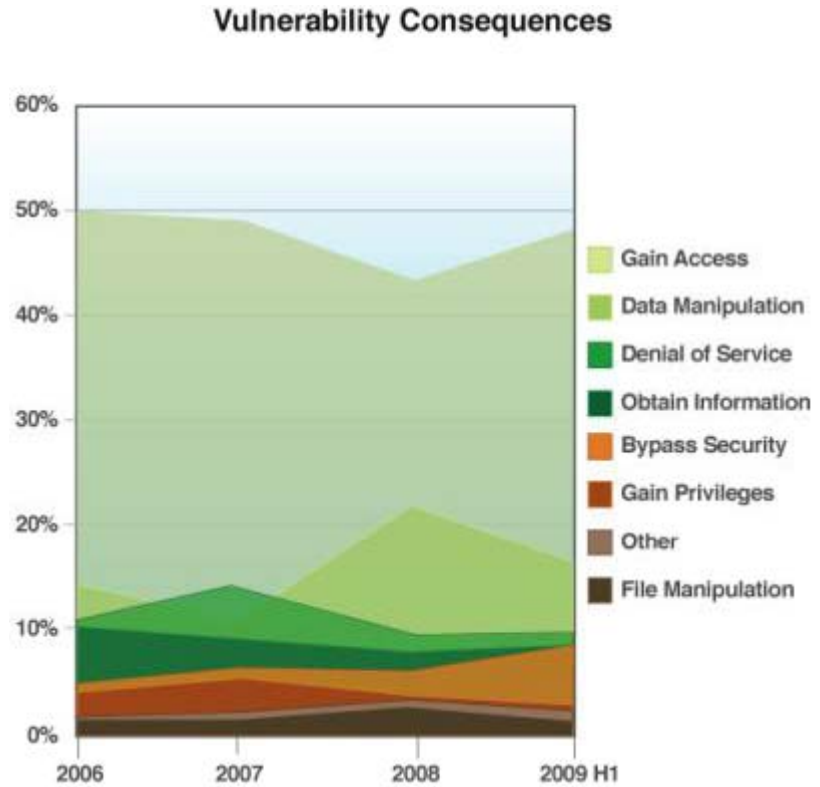
- Nearly half **(49%)** of all vulnerabilities disclosed in the first half of 2009 had no vendor-supplied patches to remedy the vulnerability

- 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



source: IBM X-Force®

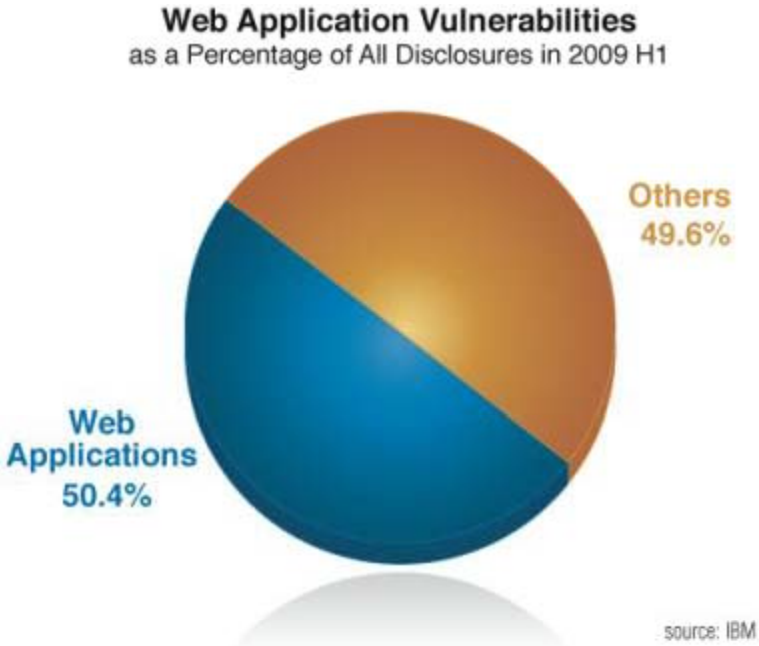
Questions to Ask:
- Are you confident that an attacker can not gain access to your system?
- Is your private data secure?

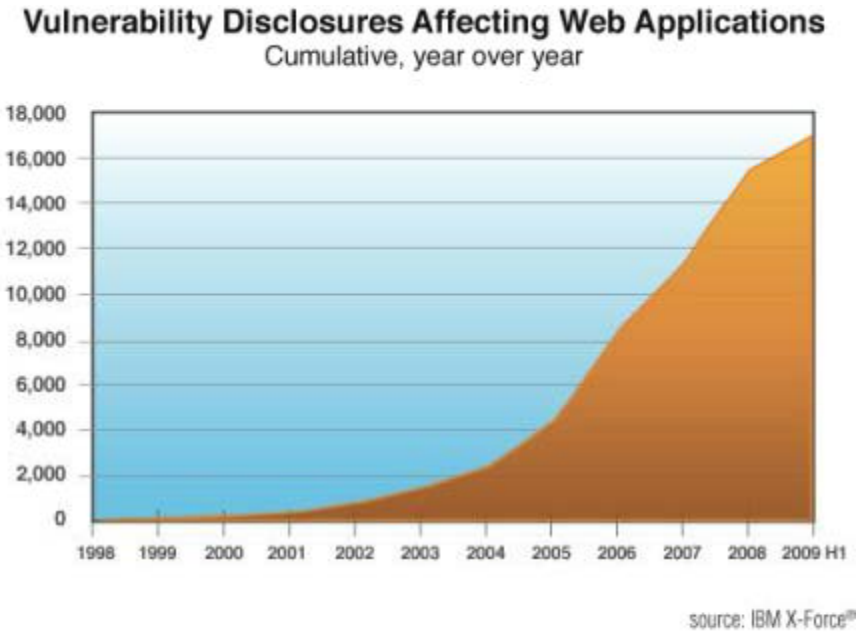
IBM Security Offerings:
- IBM Proventia Network, Server and Endpoint Intrusion Detection and Prevention products and services
- IBM Web Application Security
- IBM ISS Data Security products and services

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



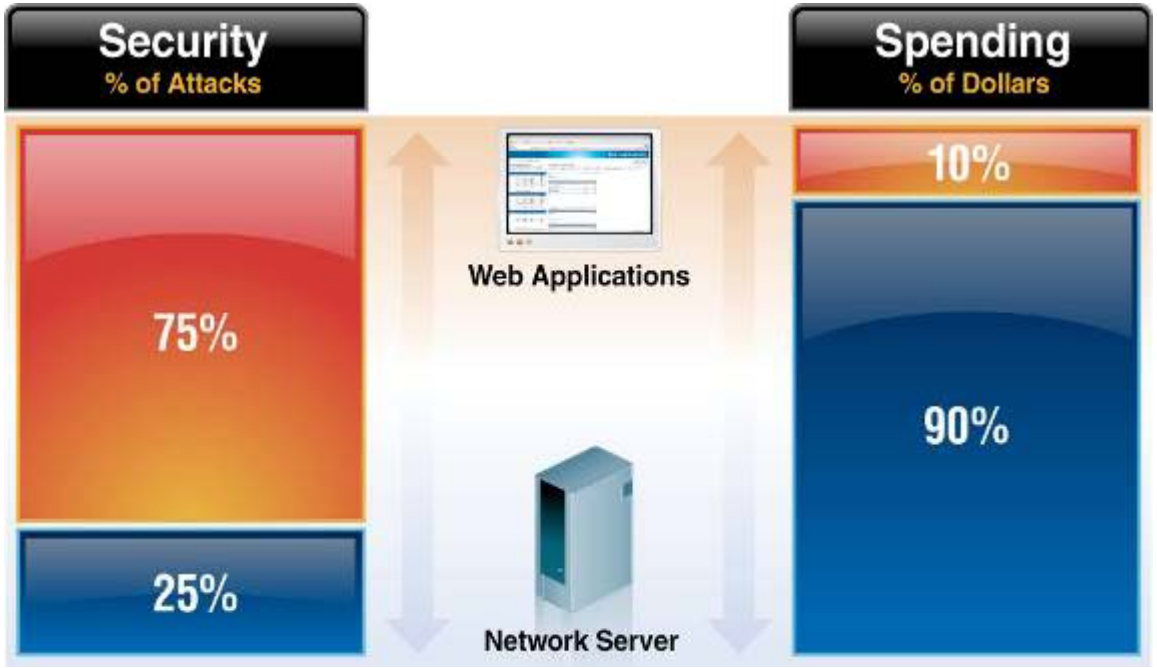


Application & Processes:

Web App Vulnerabilities Continue to Dominate

Security and Spending are Unbalanced

Average website has 7 cross site vulnerabilities

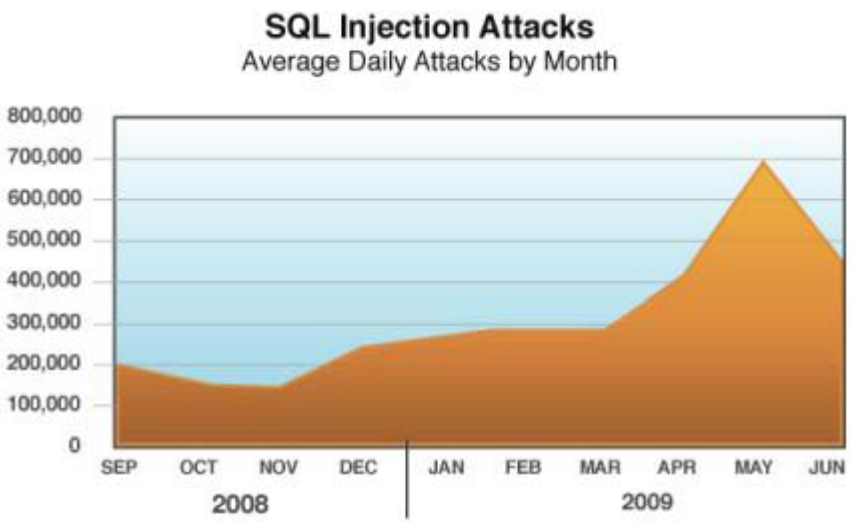


"The cleanup cost for fixing a bug in a homegrown Web application ranges anywhere from $400 to $4,000 to repair, depending on the vulnerability and the way it's fixed."
-Darkreading.com

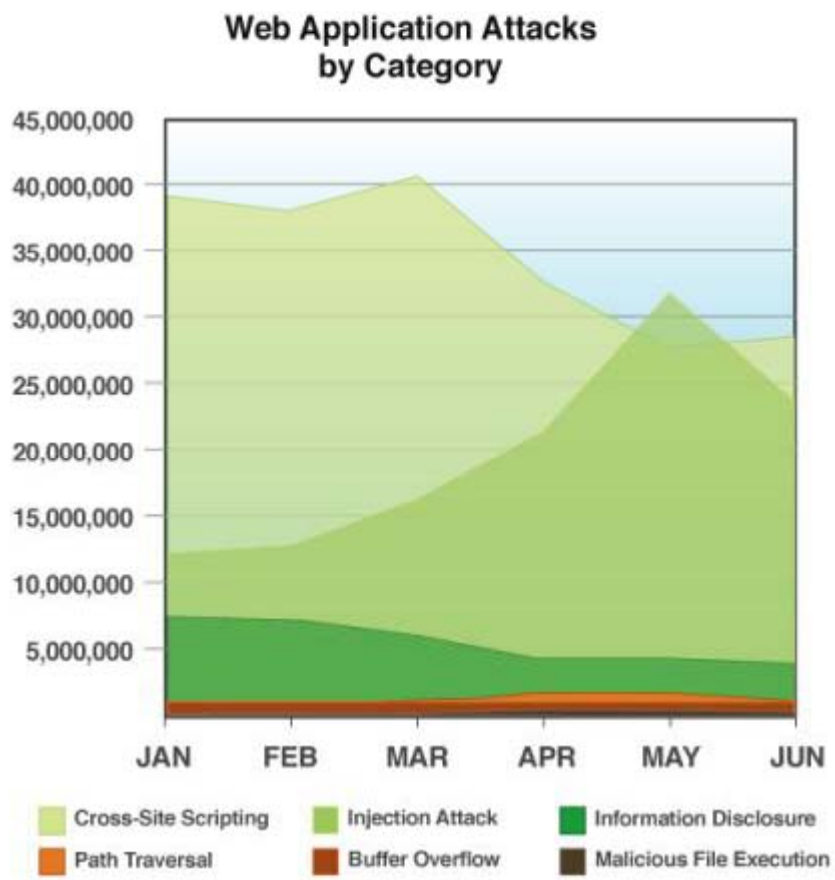
Application & Processes:

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®

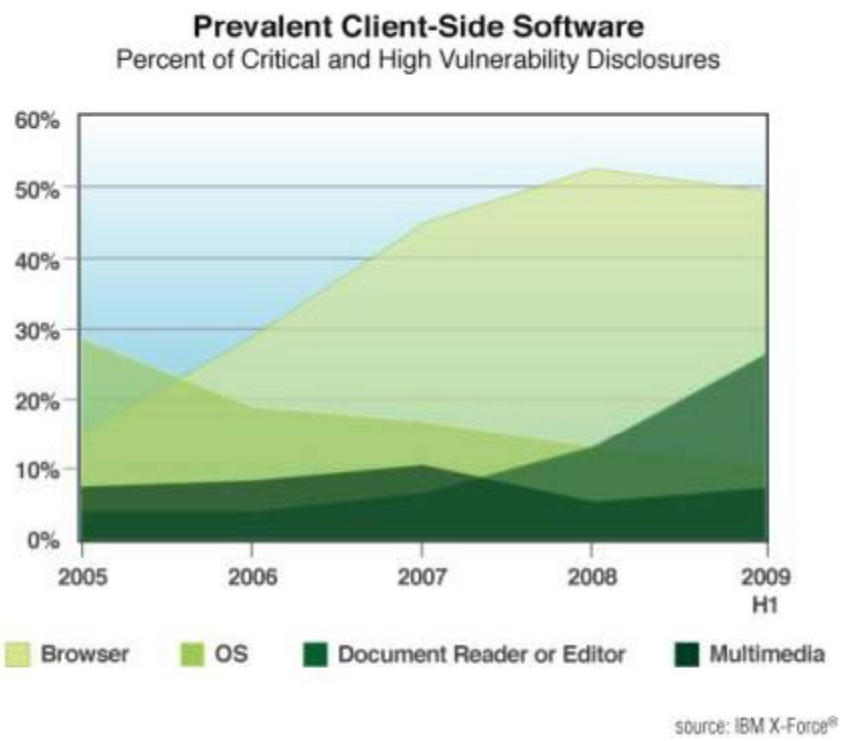
SQL Injection Attack Tools

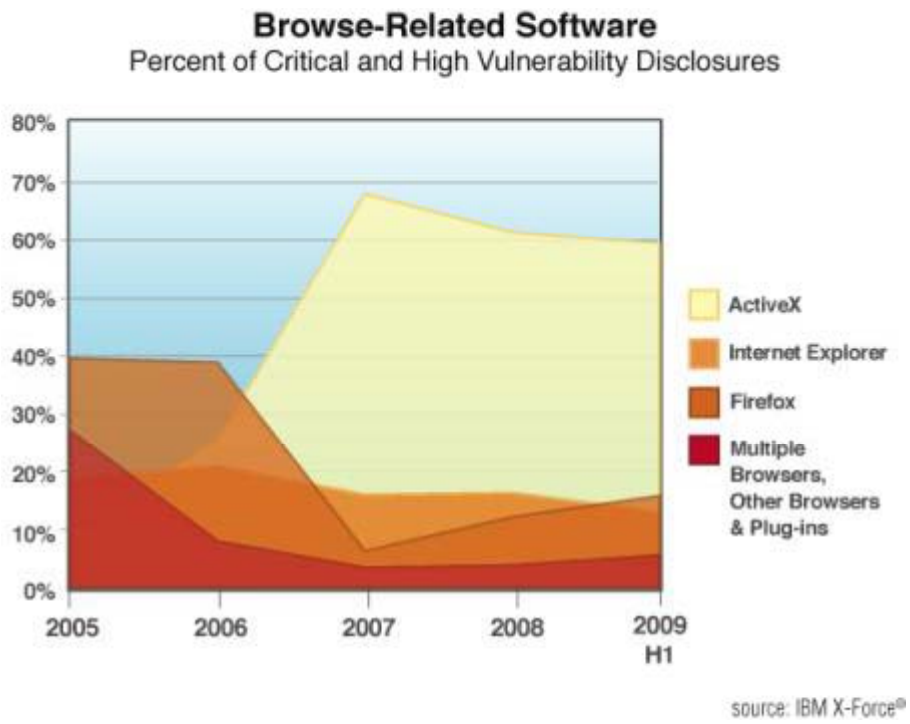
* Automatic page-rank verification
* Search engine integration for finding "vulnerable" sites
* Prioritization of results based on probability for successful injection
* Reverse domain name resolution
* etc.

Data & Information:

Client-Side Vulnerabilities – Firefox Surpasses Internet Explorer

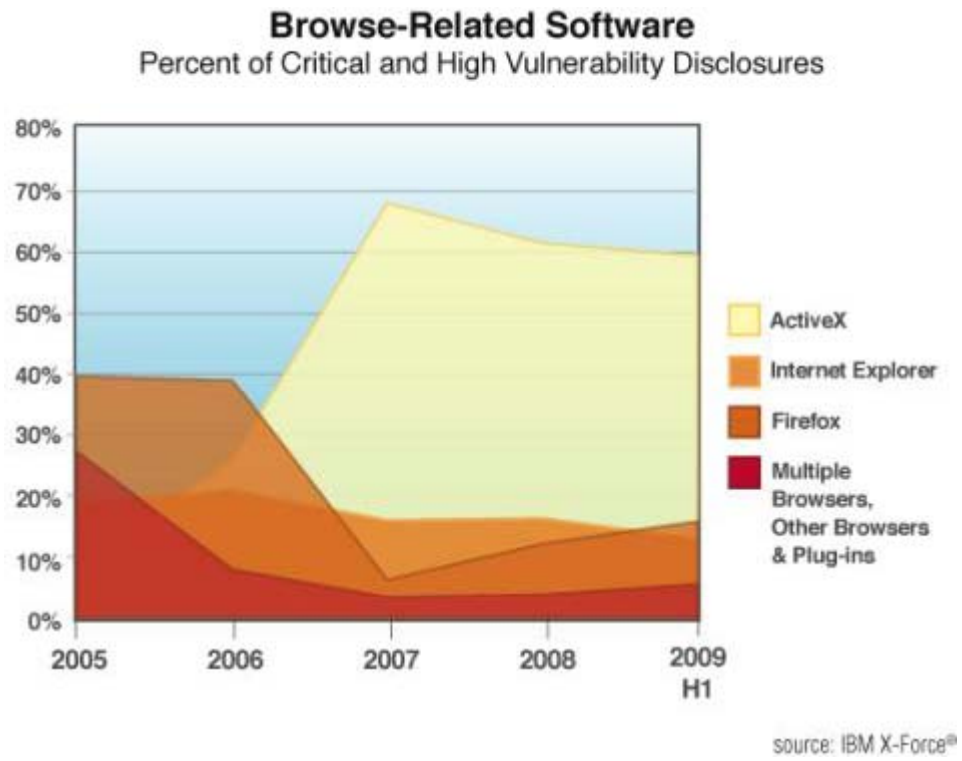
- Largest number of client-side vulnerabilities in the first half of 2009 affects Web browsers and their plug-ins
- Mozilla Firefox surpasses Microsoft Internet Explorer for the 1st time.





Browser Exploitation Prevention (BEP)

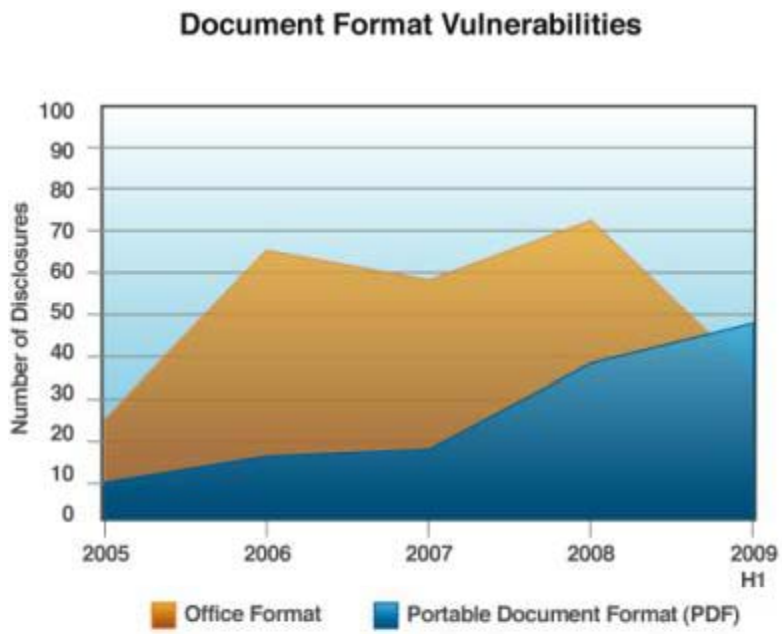
- **The Web browser is the universal application**
  - Attackers know that it delivers the best ROI
- **BEP protects against web browser exploitation regardless of the vulnerability**
  - Approximately 20 signatures protecting against hundreds of vulnerabilities in multiple browsers
  - Protects against both shellcode and obfuscation based exploits
  - Most IPS technology can't do either



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

Data & Information:

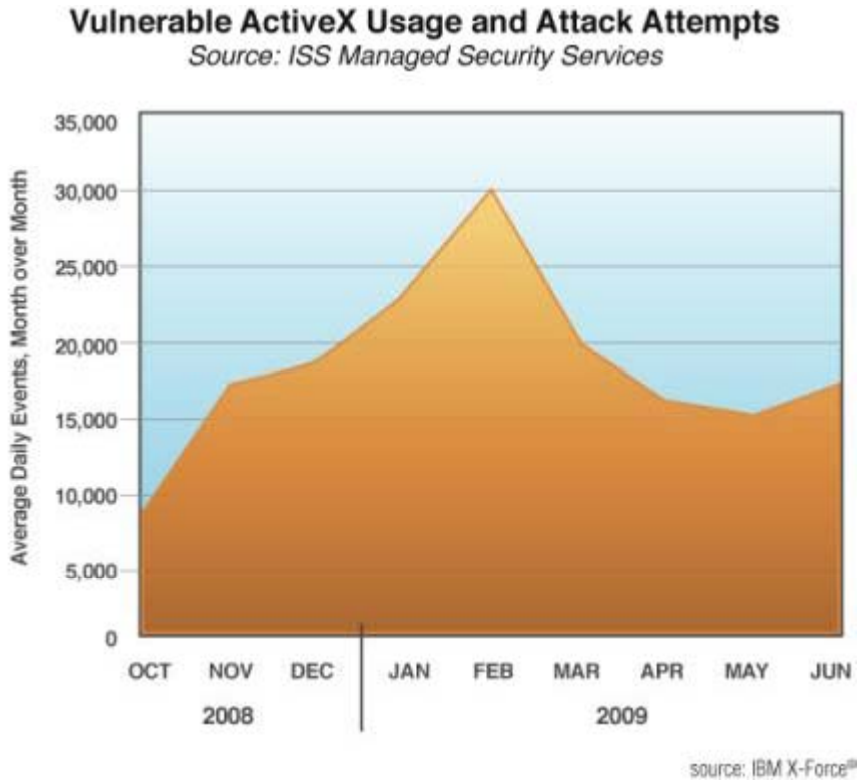
Decline in Disclosures Does Not Impact Exploitation

- 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

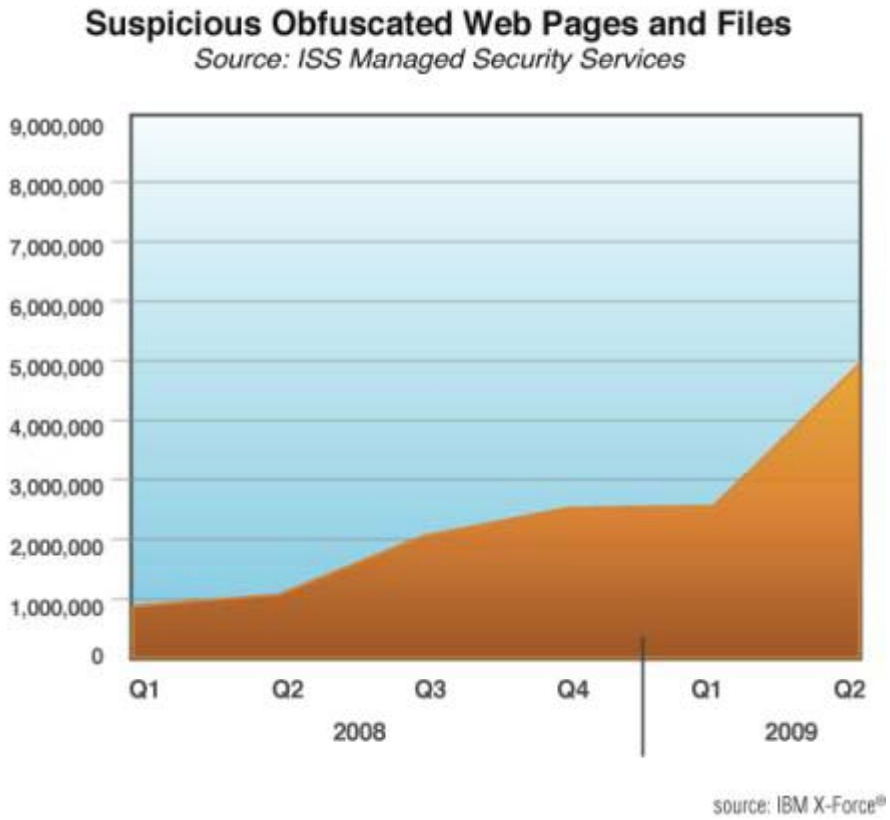
Rank	2008 H2	2009 H1
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)	Microsoft Snapshot Viewer ActiveX (CVE-2008-2463)
3.	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)	Adobe 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)



Data & Information:

Suspicious Web Pages and Files are on the Rise

- The level of obfuscation found in Web exploits, and, especially, PDF files continues to rise
- Some of these techniques are being passed to malicious multimedia files as well
- From Q1 to Q2 alone, the amount of suspicious, obfuscated content nearly doubled



People & Identity:

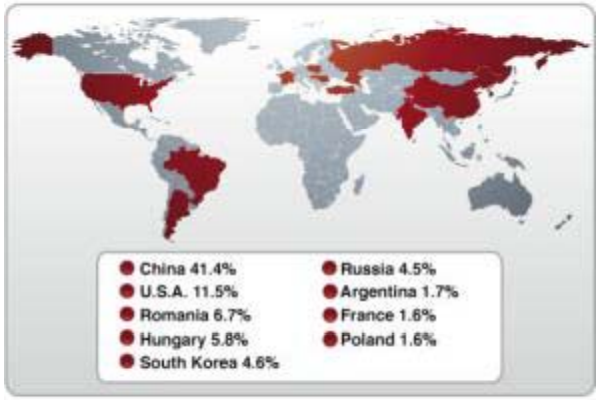
Spam Continues to Change to Avoid Detection

- 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

Most Common Domains in URL Spam, 2009 H1

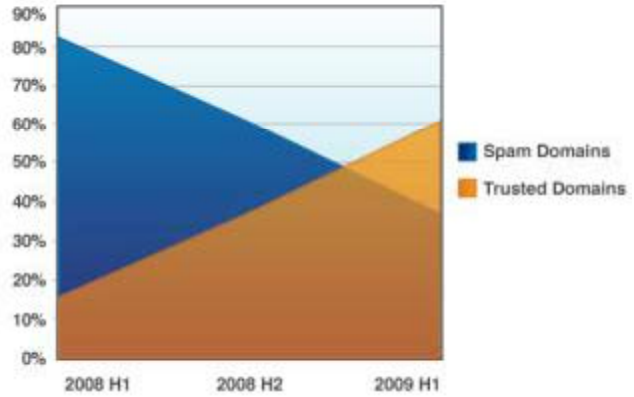
January 2009	February 2009	March 2009	April 2009	May 2009	June 2009
chat.ru	sexyhardy.com	rodale.com	interia.pl	yahoo.com	yahoo.com
thuspattern.com	aspirationask.com	menshealth.com	akamaitech.net	menshealth.com	googlegroups.com
powerinstrument.com	shoprespect.com	webmd.com	menshealth.com	icontact.com	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

Geographical Distribution of Spam URLs



source: IBM X-Force®

Top Ten Domains Used in Spam
Spam Domains Versus Trusted Domains



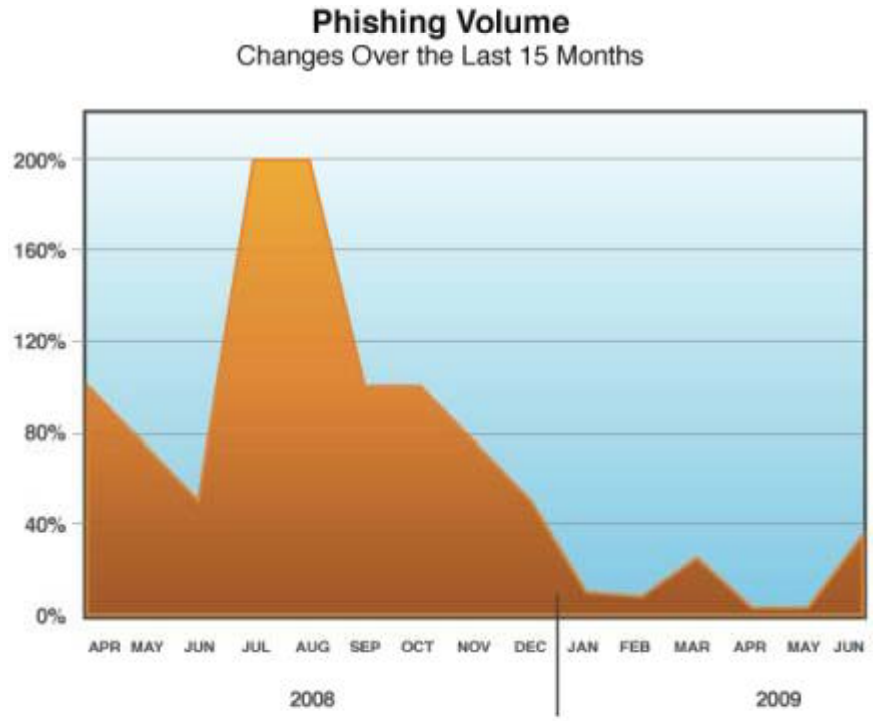
source: IBM X-Force®

People & Identity:

Phishing Attacks Decline Dramatically

- Phishing attacks decline to only **0.1%** of the spam volume
- Online Payment institutions Phishing attempts increased **24%** over last year
- Top subject lines are back
  - Top 10 most popular subject lines represent more than **38%** of all phishing e-mails
  - In 2008 the top subject lines made up only **6.23%**

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%



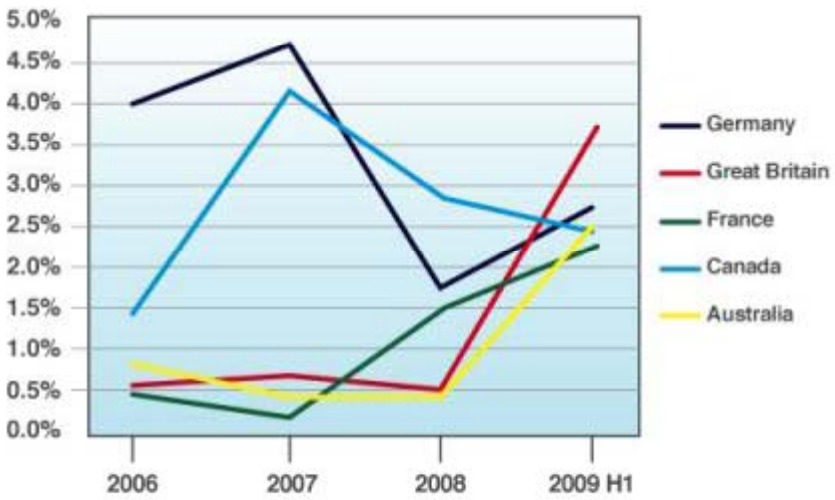
source: IBM X-Force®

People & Identity:

Malicious Web Links Increase by 508%

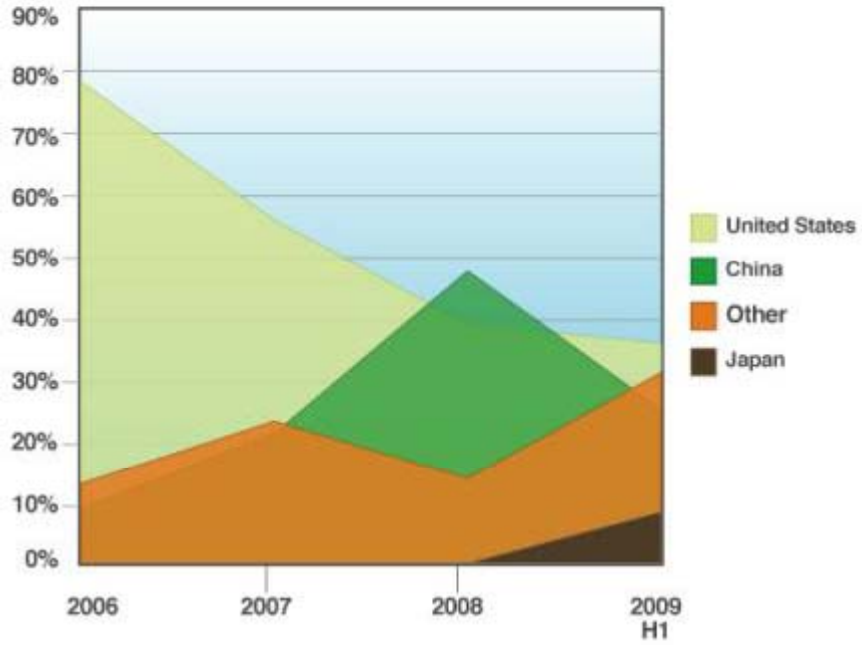
- United States and China continue to reign as the top hosting countries for malicious links
  - Japan makes the top three at 8%
- Many more second tier countries are jumping into this game
  - Countries hosting at least one malicious URL jumped by **80%** in comparison to 2008

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

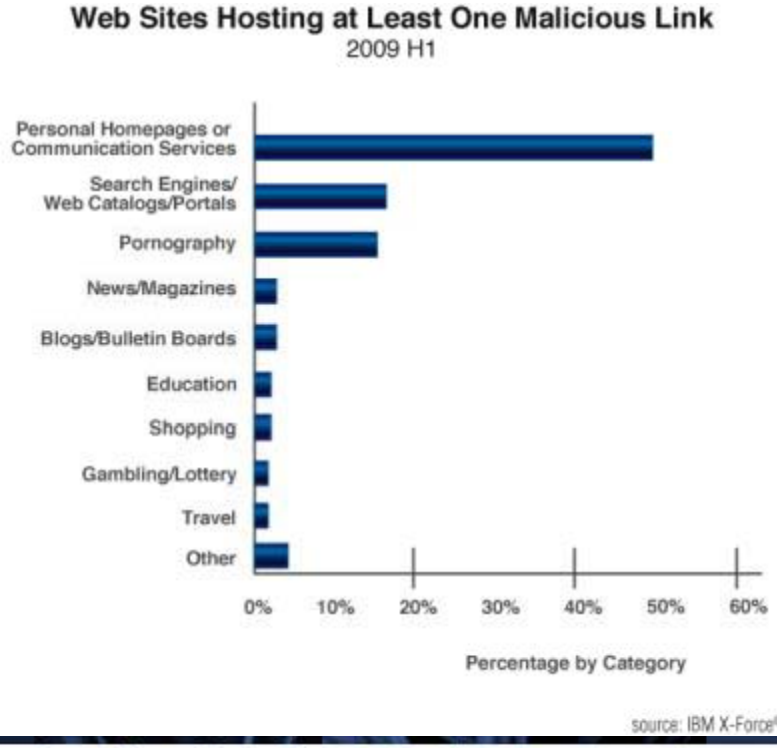


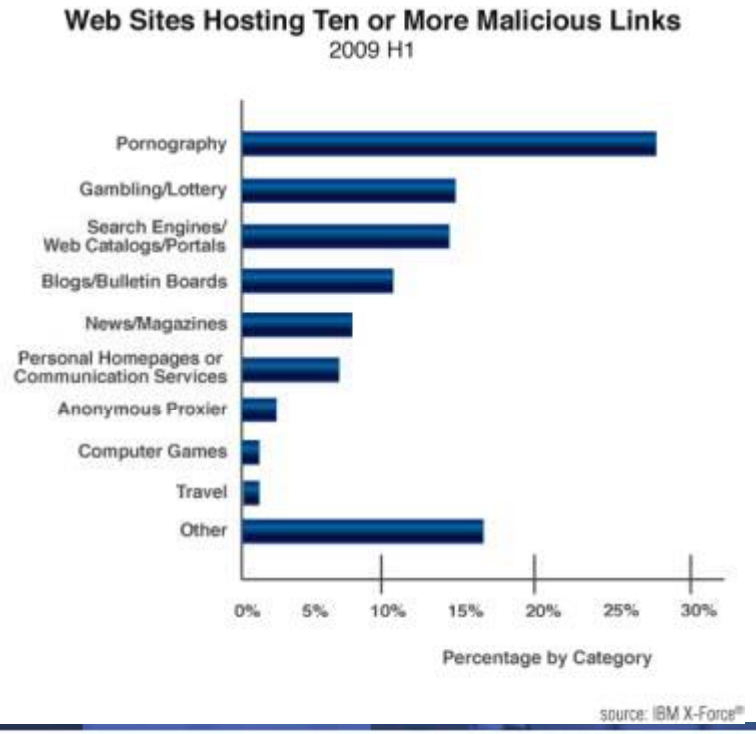
source: IBM X-Force®

People & Identity:

Good Websites Hosting Bad Links

- Personal homepages (typically hosted by communication service company domains) account for approximately half of all the domains hosting at least one malicious link
- Hosts that have 10 or more, pornography accounts for nearly **28%** and gambling accounts for more than **14%**

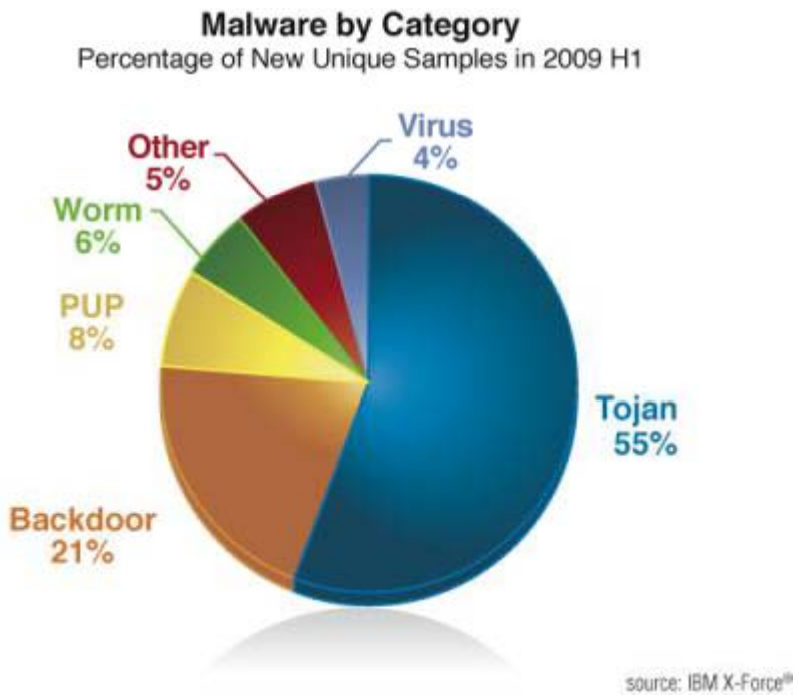




People & Identity:

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

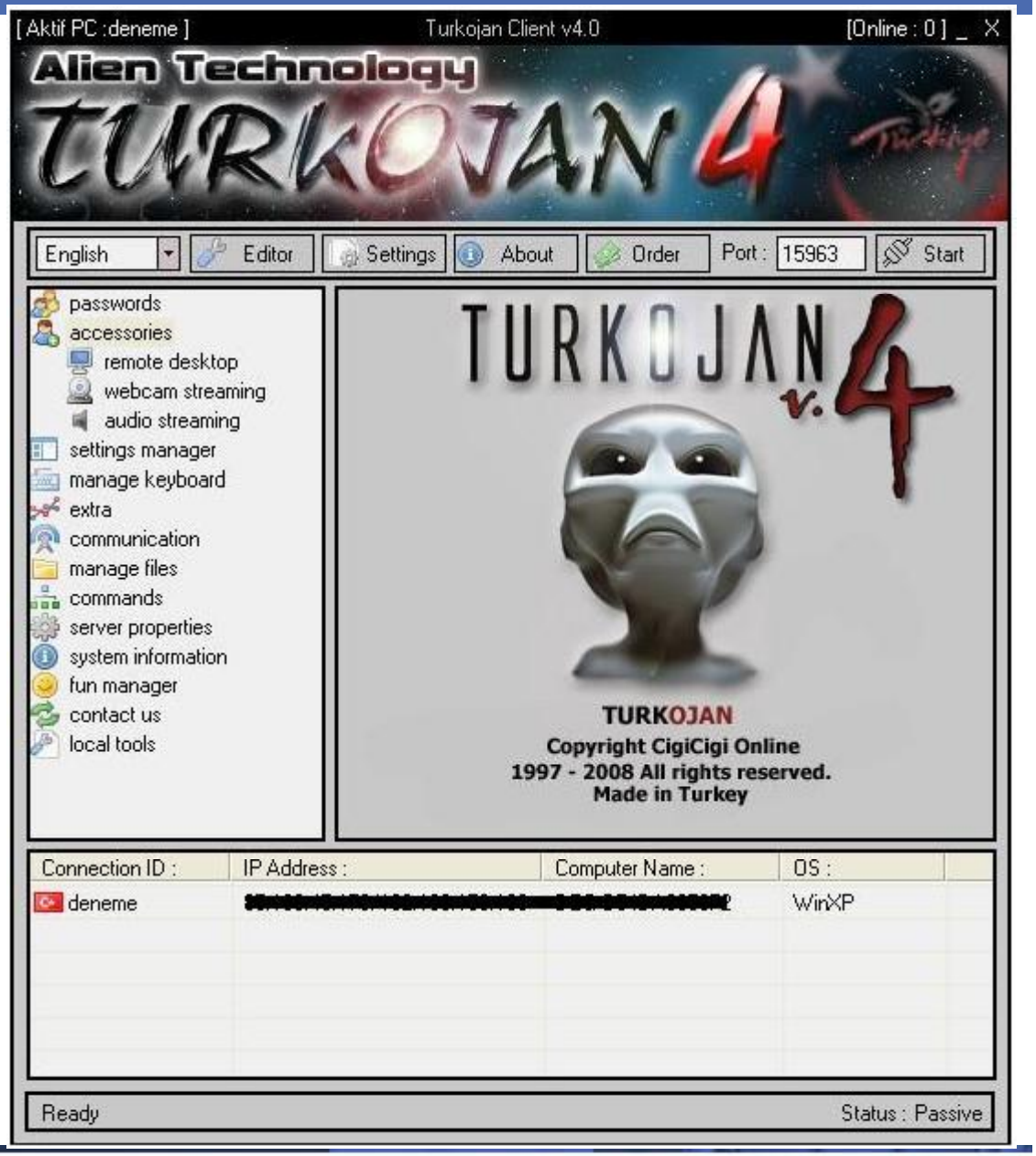


Trojan Creator Kits

Constructor/Turkojan (from Turkey)

V.4 New features

- Remote Desktop
- Webcam Streaming
- Audio Streaming
- Remote passwords
- MSN Sniffer
- Remote Shell
- Advanced File Manager
- Online & Offline keylogger
- Information about remote computer
- Etc..



Trojan Creator Kits

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)

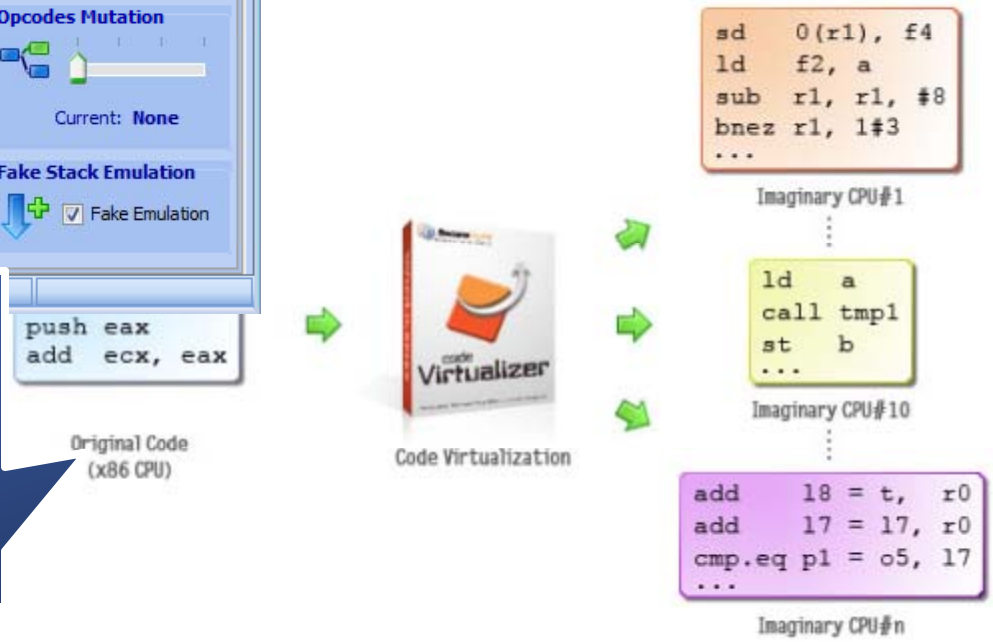
Price : 249$ (United State Dollar)

Commercial Anti-debugging Tools for Malware Authors

Code Virtualizer will convert your original code (Intel x86 instructions) into Virtual Opcodes that will only be understood by an internal Virtual Machine.

Code Virtualizer can protect your sensitive code areas in any x32 and x64 native PE files (like executable files/EXEs, system services, DLLs , OCXs , ActiveX controls, screen savers and device drivers).

Code Virtualizer can generate multiple types of virtual machines with a different instruction set for each one. This means that a specific block of Intel x86 instructions can be converted into different instruction set for each machine, preventing an attacker from recognizing any generated virtual opcode after the transformation from x86



Malware Quality Assurance

Check to see if the DIY malware can defeat commercial AV?

Balance: 20$ | Logged as: test | Se

Logged as : test
AccountType: PayPerMonth
Balance: 20$

FreeChecks Per Month: 0
FreeChecks Left: 0
PayPerMonth : 40$
PayPerCheck : 1$

CreationDate : 2008-02-04 17:56:57
Last Visit Date: 2008-02-05 01:36:35
Last Check Date: 2008-02-05 00:58:09

Balance: 20$ | Logged as: test | Service Load:

Scanning Finished

Antivirus	Version	DatabaseVersion	Result
Antivir	2.1.11-49	2008-02-04	TR/Agent.3638
ArcaVir	1.0.5	2008-02-04	---
Avast	1.0.8	2008-02-03	---
AVG	7.5.50	2008-02-04	Trojan horse Downloader.Small.BIY
BitDefender	7.60825	2008-02-04	Generic.Malware.dld!!.3E3550AE
ClamAv	0.91.2	2008-02-04	---
DrWeb	4.44.0.10150	2008-02-03	DLOADER.Trojan
eScan	2.0.8	2008-02-02	---
F-Prot	6.2.1	2008-02-04	W32/Downloader.gen10
F-Secure	5.53	2008-02-04	---
Kaspersky	5.7.13	2008-02-04	---
McAfee	2.1.11-49	2008-02-01	Generic.ff trojan
Nod32	2.16-2	2008-02-04	---
Panda	9.04.03	2008-02-03	---
Sophos	4.25.0	2008-02-04	Virus 'Mal/DownLdr-F'
Symantec	1.0.3.8	2008-02-04	---
VBA32	3.12.2.5	2008-02-04	---
VirusBuster	1.3.4	2008-02-04	---

Additional information
FileName: lo.exe
FileSize: 3638 bytes
MD5: add5c5eadda0caa482bb4353ab3233eb
SHA1: 4ef7341ed4525a8ce2f20033cb2dd6dd84099694
TotalResults: 7/18

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

2009 X-Force Mid-Year Trend & Risk Report – IBM Offerings Portfolio

Area of Risk	IBM Security Solutions
Vulnerabilities	- IBM ISS Intrusion Prevention System (IPS) products: Proventia Network IPS, Proventia Server, RealSecure Server Sensor, Proventia Desktop & Proventia Network Multifunction Security (MFS) -IBM ISS Managed Protection Services for IPS - Tivoli Security Information and Event Manager (TSIEM)
Web Application Vulnerabilities	-Web application IPS security for Network, Server and MFS -- Managed Protection Services for IPS -Rational Appscan for assessment -Rational Ounce Labs for Source Code Testing -Rational Appscan Enterprise - Tivoli Security Information and Event Manager - Tivoli Security Policy Manager
PC Vulnerabilities including Malicious Web Exploits	- 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: - Proventia Network Mail / Lotus Protector - Proventia Multifunction System (MFS) - Managed Security Services for Mail Security
Unwanted Web Content	- Proventia MFS - Managed Security Services for Web Security - Proventia Web Filter
Malware	- Proventia Endpoint Secure Control and Proventia MFS - Managed Security Services for Mail and Web Security - Proventia Network Mail / Lotus Protector - Proventia Web Filter

THANK YOU!

Need to Know More?
Check out These Backup Materials

Glossary of Terms

Attack Technique	Description
Cross-site Scripting	Cross-site scripting vulnerabilities occur when Web applications do not properly validate user input from form fields, the syntax of URLs, etc. These vulnerabilities allow attackers to embed their own script into a page the user is visiting, manipulating the behavior or appearance of the page. These page changes can be used to steal sensitive information, manipulate the Web application in a malicious way, or embed more content on the page that exploits other vulnerabilities. The attacker first has to create a specially-crafted Web link, and then entice the victim into clicking it (through spam, user forums, etc.) The user is more likely to be tricked clicking the link, because the domain name of the URL is a trusted or familiar company. The attack attempt may appear to the user to come from the trusted organization itself, and not the attacker that compromised the organization's vulnerability.
SQL Injection	SQL injection vulnerabilities are also related to improper validation of user input, and they occur when this input (from a form field, for example), is allowed to dynamically include SQL statements that are then executed by a database. Access to a back-end database may allow attackers to read, delete, and modify sensitive information, and in some cases, execute arbitrary code. In addition to exposing confidential customer information (like credit card data), SQL injection vulnerabilities can also allow attackers to embed other attacks inside the database that can then be used against visitors to the Web site.
File Include	File include vulnerabilities (typically found in PHP applications) occur when the application retrieves code from a remote source to be executed in the local application. Oftentimes, the remote source is not validated for authenticity, which allows an attacker to use the Web application to remotely execute malicious code.
Other	This category includes some denial-of-service attacks and miscellaneous techniques that allow attackers to view or obtain unauthorized information, change files, directories, user information or other components of Web applications.

Attack Category	Description
Buffer Overflow attacks	This type of attack overflows a buffer with excessive data, which allows an attacker to run remote shell on the computer and gain the same system privileges granted to the application being attacked.
Cross-site Scripting attacks	This type of attack exploits the trust relationship between a user and the Web sites they visit.
Information Disclosure attacks	This type of attack is aimed at acquiring system specific information about a Web site including software distribution, version numbers, and patch levels. The acquired information might also contain the location of backup files or temporary files.
Injection attacks	This type of attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database, or change data on a Web site.
Malicious File Execution attacks (also known as file include attacks)	This type of attack allows an attacker to perform remote code execution, remote root kit installation, complete system compromise, and internal system compromise (on Windows systems) through the use of SMB file wrappers for the PHP scripting language.
Path Traversal attacks	This type of attack forces access to files, directories, and commands that are located outside the Web document root directory or CGI root directory.

Glossary of Terms

Consequence	Definition
Bypass Security	Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner
Data Manipulation	Manipulate data used or stored by the host associated with the service or application
Denial of Service	Crash or disrupt a service or system to take down a network
File Manipulation	Create, delete, read, modify, or overwrite files
Gain Access	Obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system
Gain Privileges	Privileges can be gained on the local system only
Obtain Information	Obtain information such as file and path names, source code, passwords, or server configuration details
Other	Anything not covered by the other categories

Category	Description
Virus	Propagates by infecting a host file
Worm	Self-propagates via e-mail, network shares, removable drives, file sharing or instant messaging applications
Backdoor	Provides functionality for a remote attacker to log on and/or execute arbitrary commands on the affected system
Trojan	Performs a variety of malicious functions such as spying, stealing information, logging key strokes and downloading additional malware
Potentially Unwanted Programs (PUP)	Programs which the user may consent on being installed but may affect the security posture of the system or may be used for malicious purposes. Examples are Adware, Dialers and Hacktools/"hacker tools" (which includes sniffers, port scanners, malware constructor kits, etc.)
Other	Unclassified malicious programs not falling within the other primary categories

Category	Description
Infostealer	Spies and/or steals information. This category includes password stealers, keystroke loggers and spyware.
Downloader	Downloads one or more malware components from a remote site and then installs them on the affected system.
Dropper	Drops and installs one or more embedded malware components onto an affected system.
Injector	Injects an embedded malware component into other another process. One purpose is for the embedded (and usually obfuscated) malware to evade antivirus detection. Another purpose is for the embedded malware to evade host-based firewalls by injecting it into a trusted process such as a browser or a system process.
FraudTool	Malware used to commit fraud. An example is malware that displays fake error or infection messages, and then entices the user to purchase fake tools or security software.
Clicker	Generates website traffic, the purpose of which is to generate revenue or other malicious purposes.
Rootkit	Components used by other malware in order to have the capability to hide themselves from the user and security software.
Exploit	Documents or media files containing exploit code.
Proxy	Allows a remote attacker to relay connection through the affected system in order to hide its real origin.
Other	Trojans that do not fall within the other subcategories.