



Sukhdev Singh
IBM ASEAN
CISSP
CISM
XFE



Certified Enterprise Architect (TOGAF®)



IBM **Security** Summit
IBM Security Solutions. Secure By Design.



U.S. and Pakistan Clash Over Payments for War on Terror

IN DEPTH Pages 14-15

OPINION:
Bailing Out
Tepeco the More
Honest Way
Page 11

THE WALL STREET JOURNAL.

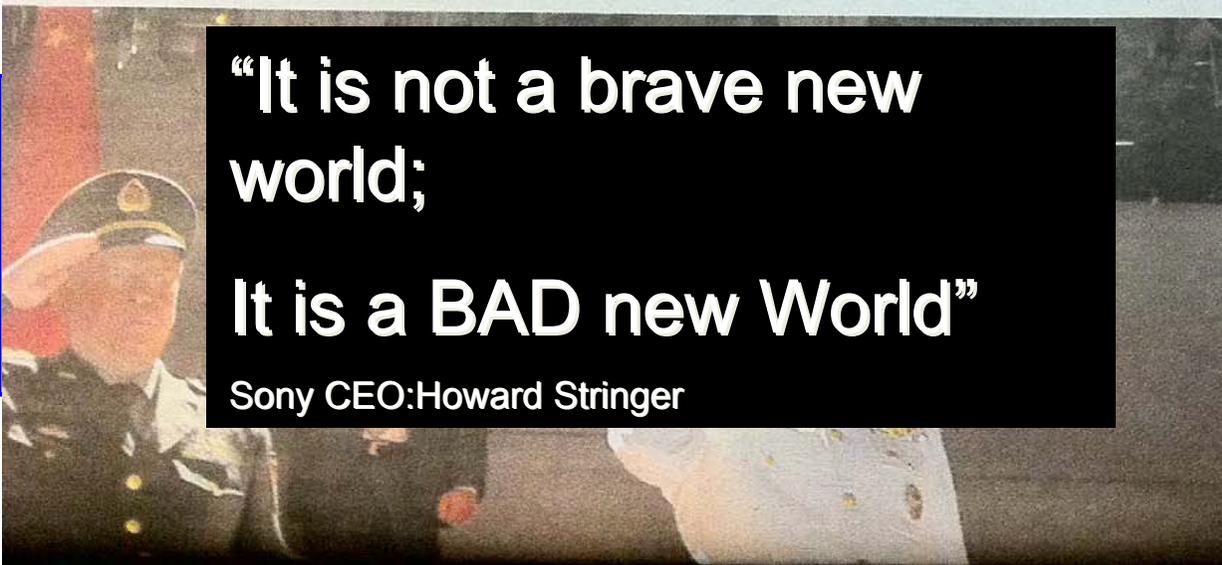
(India facsimile Vol. 2 No. 242)

ASIA

Wednesday, May 18, 2011

asia.wsj.com

ry Officials Visit U.S. in Effort to Thaw Relations



**“It is not a brave new world;
It is a BAD new World”**

Sony CEO: Howard Stringer

Sony Chief Cautions on Cybercrime

By DAISUKE WAKABAYASHI

TOKYO—Despite spending weeks to resolve a massive Internet security breach, Sony Corp. Chief Executive Howard

ing video and music network could lead the way to bigger problems well beyond Sony, or the gaming industry. He warned the attacks may one day target the global Internet

What is at Risk ?

- Interruption of business operations
(Lost Revenues)
- Decreased productivity due to additional strain placed on network resources
(Lost Revenues)
- Loss of confidential information
(Lost Competitive Advantage)
- Increased recruiting and staffing costs
(Lost Profits)



두통

Mission

To protect our customers from security threats on the Internet by developing a comprehensive knowledge of vulnerabilities and attack methodologies and applying that knowledge through effective protection technologies.

IBM X-Force Research and Development

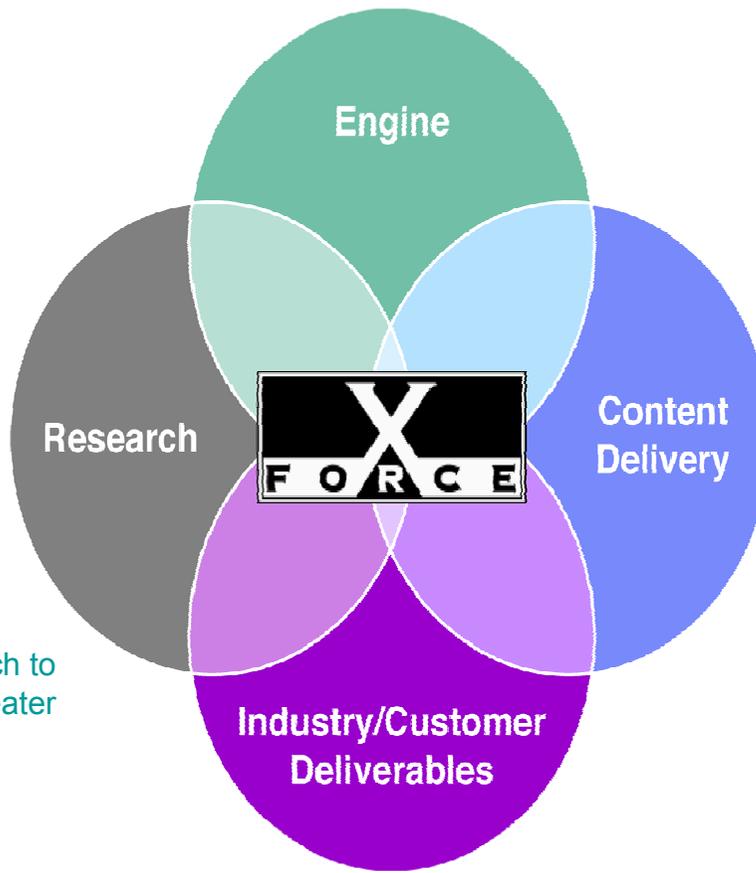
The world's leading enterprise security R&D organization

Engine

- Support content stream needs and capabilities
- Support requirements for engine enhancement
- Maintenance and tool development

Research

- Support content streams
- Expand current capabilities in research to provide industry knowledge to the greater IBM



Global security operations center (infrastructure monitoring)

Content Delivery

- Continue third party testing Dominance
- Execute to deliver new content streams for new engines

Industry/Customer Deliverables

- Blog, Marketing and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

X-Force R&D - Unmatched Security Leadership

The mission of the
IBM 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

14B analyzed Web pages & images

40M spam & phishing attacks

54K documented vulnerabilities

Billions of intrusion attempts daily

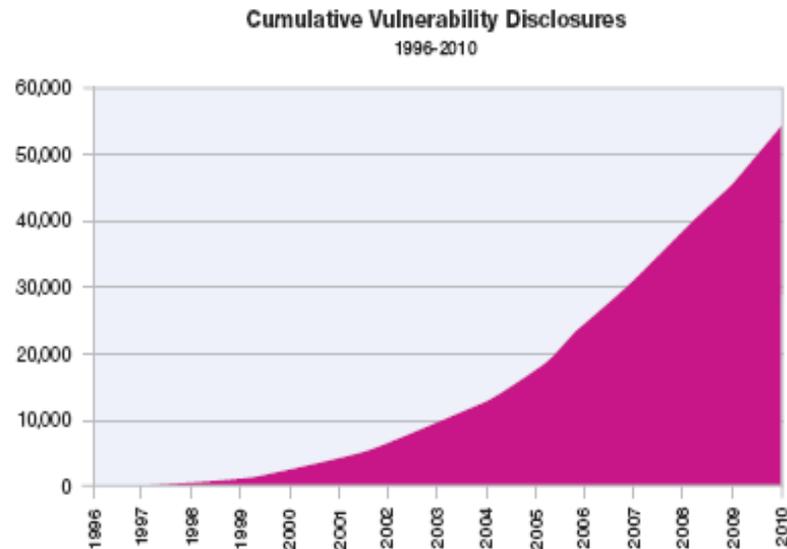
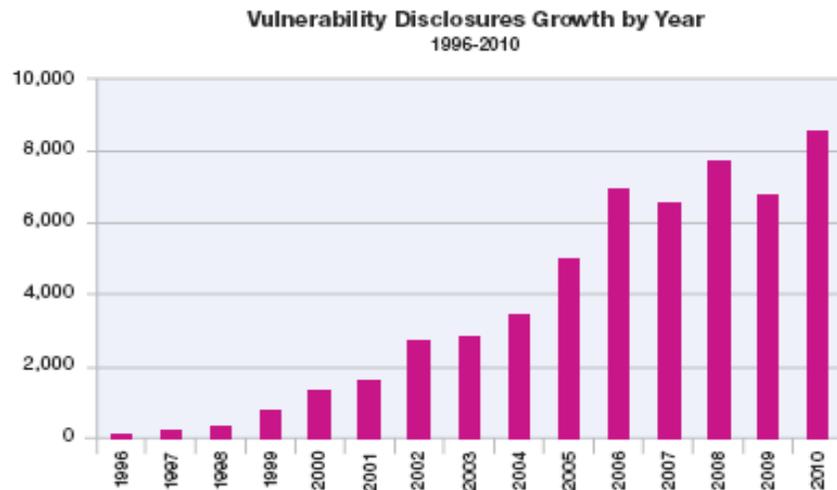
Millions of unique malware samples

Provides Specific Analysis of:

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

Vendors Reporting the Largest Number of Vulnerability Disclosures in History

- Vulnerability disclosures up **27%**.
 - Web applications continue to be the largest category of disclosure.
- Significant increase across the board signifies efforts that are going on throughout the software industry to improve software quality and identify and patch vulnerabilities.





Patches Still Unavailable for Many Vulnerabilities

- **44%** of all vulnerabilities disclosed in 2010 had no vendor-supplied patches to remedy the vulnerability.
 - Most patches become available for most vulnerabilities at the same time that they are publicly disclosed.
 - However some vulnerabilities are publicly disclosed for many weeks before patches are released.

Patch Release Timing – First 8 Weeks of 2010

| Patch Timeline | All | Top Vendors |
|----------------|------|-------------|
| Same Day | 3400 | 1814 |
| Week 1 | 192 | 34 |
| Week 2 | 55 | 11 |
| Week 3 | 57 | 12 |
| Week 4 | 33 | 7 |
| Week 5 | 27 | 7 |
| Week 6 | 22 | 4 |
| Week 7 | 17 | 3 |
| Week 8 | 16 | 8 |



Public Exploit Exposures Up in 2010

Public exploit disclosures up **21%** in 2010 versus 2009

- Approximately **14.9%** of the vulnerabilities disclosed in 2010 had public exploits, which is down slightly from the 15.7% last year
- However more vulnerabilities were disclosed this year, so the total number of exploits increased.
- The vast majority of public exploits are released the same day or in conjunction with public disclosure of the vulnerability.

Public Exploit Disclosure Timing by Weeks

2010

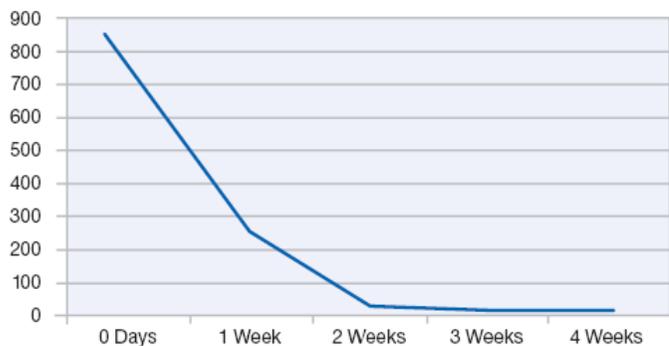


Figure 54: Public Exploit Disclosure Timing by Weeks – 2010

| Exploit Timing | 0 Days | 1 Week | 2 Weeks | 3 Weeks | 4 Weeks |
|----------------|--------|--------|---------|---------|---------|
| 0 Days | 854 | 270 | 18 | 9 | 9 |

Public Exploit Disclosures

2006-2010

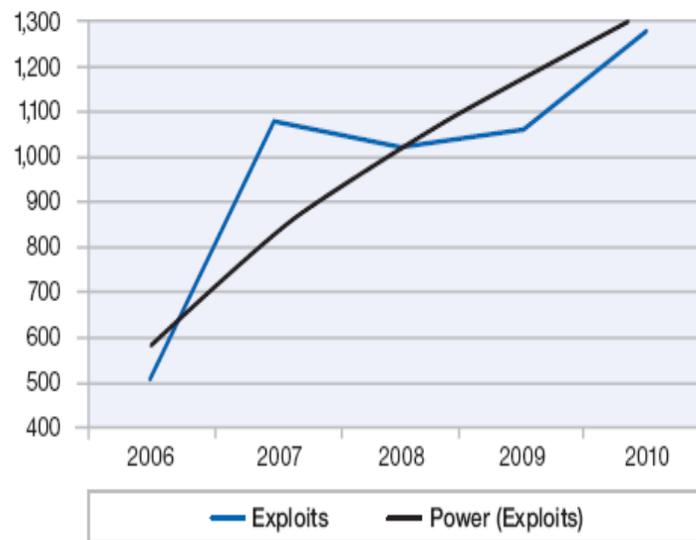


Figure 53: Public Exploit Disclosures – 2006-2010

| | 2006 | 2007 | 2008 | 2009 | 2010 |
|---------------------|------|-------|-------|-------|-------|
| True Exploits | 504 | 1078 | 1025 | 1059 | 1280 |
| Percentage of Total | 7.3% | 16.5% | 13.4% | 15.7% | 14.9% |

New exploit packs show up all the time

2 Weeks Ago #1

BleedingLife ◦
Junior Member

Join Date: Mar 2011
Posts: 2
Reputation: 0

Bleeding Life v2: RELOADED **Exploit Pack**



INTRODUCTION:

BleedingLife Exploit Pack was looked down upon in the beginning of its start. As time went on and users began to take a chance with this pack, they've eventually understood BL is no normal pack. With less exploits and a higher rate than other packs, BL has really made a name for itself. Now, BL has turned into a series. BL v1, BL v2, BL Mini-Java, BL Java Edition, BL Adobe Edition. And... Here before us, BL v2 Reloaded. If you want a low cost, high rate and great quality pack... Purchase BleedingLife v2 Reloaded!

EXPLOITS:

- [x] CVE-2008-2992
- [x] CVE-2010-0188
- [x] CVE-2010-0842
- [x] CVE-2010-1297
- [x] CVE-2010-2884
- [x] CVE-2010-3552
- [x] JavaSignedApplet (Requires user interaction but can be disabled.)
- [x] All exploits bypass ASLR and DEP where needed.

AVERAGE RATE:

- [x] BL v2 has an average rate between 30% - 40%
- [x] SS/Proof coming soon ...

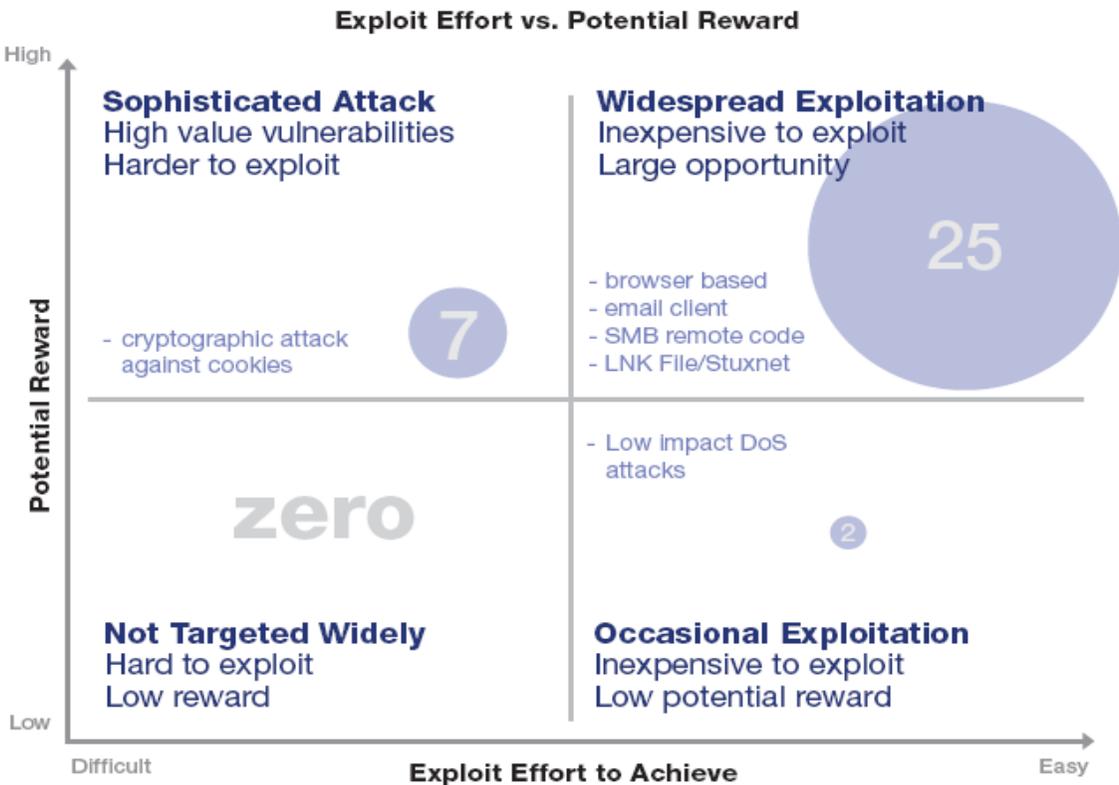
PAYMENT OPTIONS:

- [x] BleedingLife v2 Reloaded - \$400.00
- [x] FUD Update - \$50.00
- [x] Domain Change - \$50.00
- [x] Liberty Reserve & WebMoney ONLY!
- [x] Previous v2 Buyers - FREE Update!



Exploit Effort vs. Potential Reward

- Economics continue to play heavily into the exploitation probability of a vulnerability
- All but one of the 25 vulnerabilities in the top right are vulnerabilities in the browser, the browser environment, or in email clients.
- The only vulnerability in this category that is not a browser or email client side issue is the LNK file vulnerability that the Stuxnet worm used to exploit computers via malicious USB keys.





Top Attacks seen by X-Force in 2010

- Automated SQL Injection attacks
- Lateral scanning of the entire Internet for services with weak passwords
- The SQL Slammer worm was responsible for a huge amount of malicious traffic in 2010 but traffic levels dropped off significantly in March, 2011

| Rank | Event Name | Trend Line |
|------|-------------------------|---------------|
| 1 | SQL_SSRP_Slammer_Worm | Down |
| 2 | SQL_injection | Down |
| 3 | PsExec_Service_Accessed | Slightly Up |
| 4 | SSH_Brute_Force | Slightly Down |
| 5 | JScript_CollectGarbage | Up |
| 6 | HTTP_Unix_Passwords | Slightly Up |
| 7 | SMB_Mass_Login | Down |
| 8 | SMB_Empty_Password | No Change |
| 9 | SQL_Empty_Password | Up |

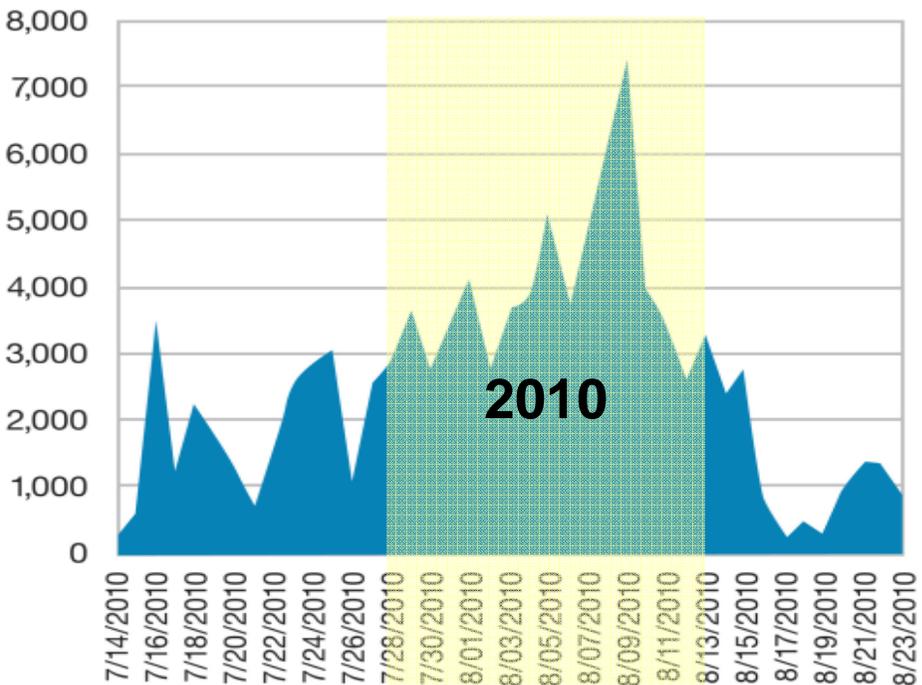
Table 1: Top MSS high volume signatures and trend line



SQL Injection Attacks

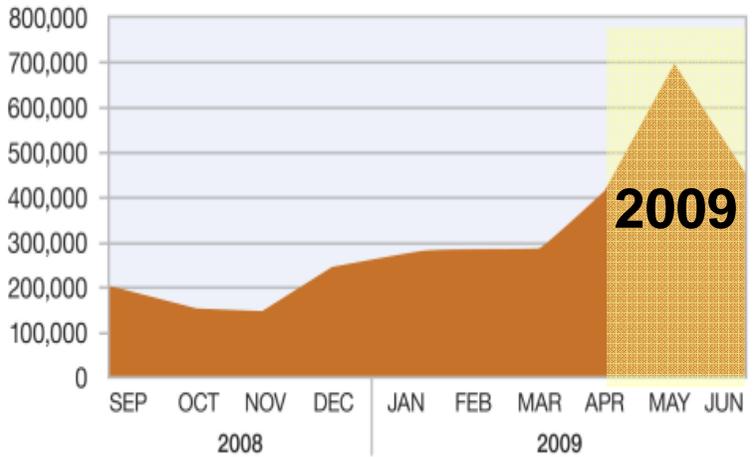
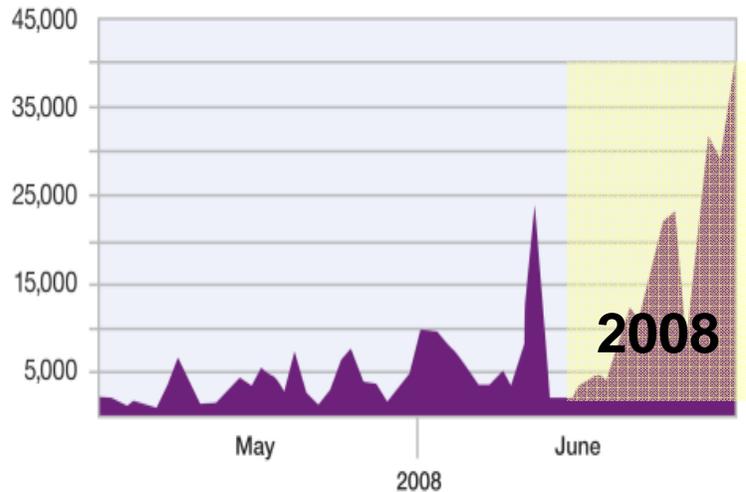
- During each of the past three years, there has been a globally scaled SQL injection attack some time during the months of May through August.
- The anatomy of these attacks is generally the same: they target .ASP pages that are vulnerable to SQL injection.

SQL_Injection_Declare_Exec Activity



Source: IBM X-Force®

SQL Injection Attacks Monitored by IBM Managed Security Services

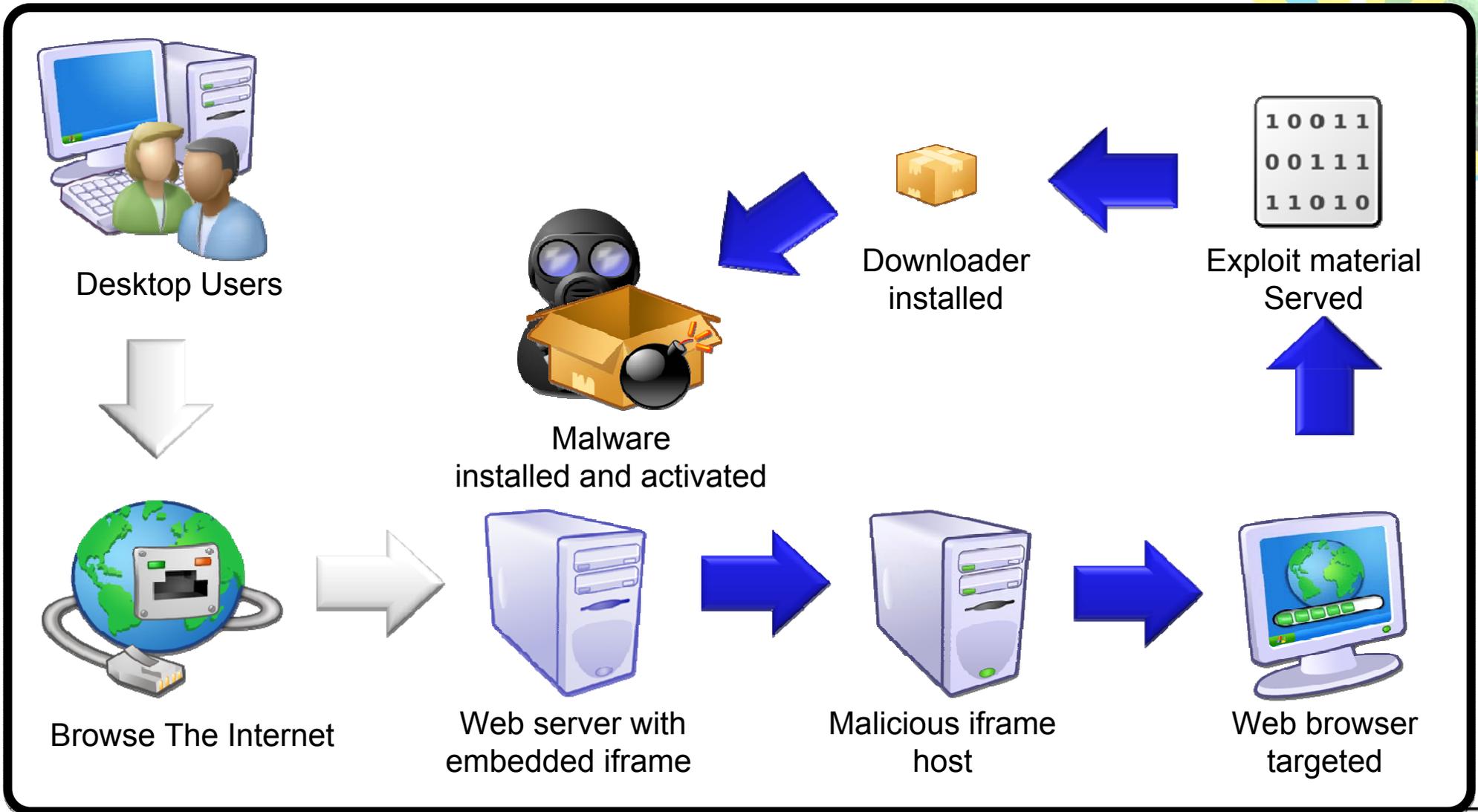


Source: IBM X-Force®





The drive-by-download process





SQL Injection Attack Tools

地址: 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=10 转到 停止 刷新 后退 前进

网页 图片 地图 资讯 视频 博客 更多 登录 信息

Google 高级搜索 搜索帮助 | Google

网页 约: 搜索结果 包含以下全部的字词 inurl:asp id 100 项结果

小提示: 包含以下的完整字句 包含至少一个下列字词

云南海泰贵金属是一家专业从事贵金属系列产品: 贵金属化合物、贵金属载体催化剂、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

- * 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.

S. 扫描页面漏洞 I. 仅扫描地址栏 I. 停止扫描 Q. 强行终止

安全漏洞 | 服务器错误

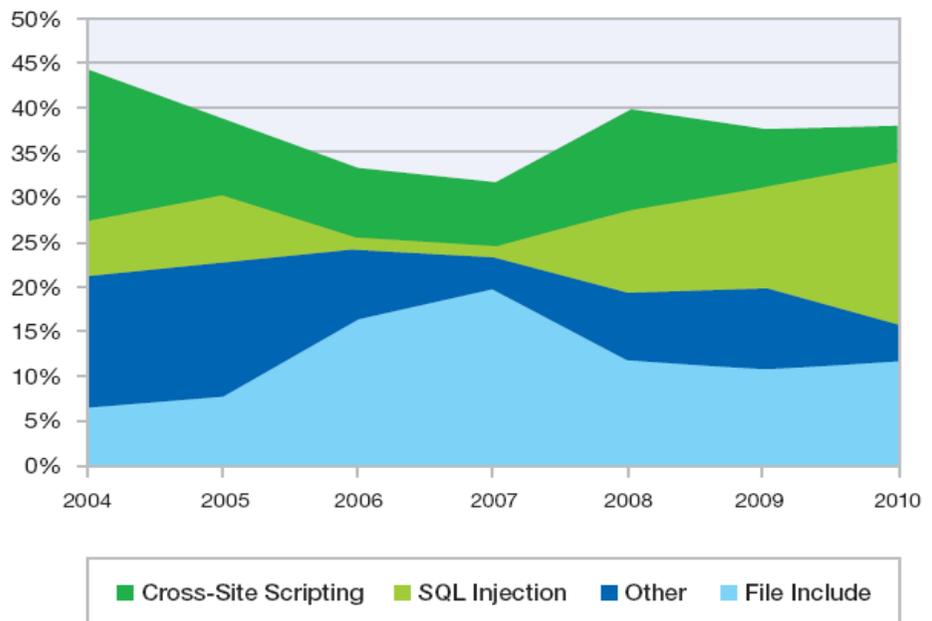
| 完整URL | 响应时间 | 可利用度 | 确定漏洞方式 | 注入方式 | 注入类型 | 数据库 | 页面标题 | 错误指纹 |
|---|------|------|-------------------|------|------|-----|-------------|-------------|
| http://www.cn/info.asp?id=6 | 1609 | 6 | aND 8=8 + aND 8=3 | AND | 数字型 | 未探测 | 康馨催乳公司 催乳 # | |
| http://www.bertech.com/shownews.asp | 5281 | 5 | 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.asp | 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?id=6 | 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_y | 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.asp | 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/zfmr.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- | |



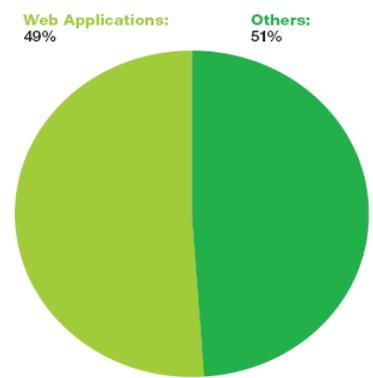
Web App Vulnerabilities Continue to Dominate

- Nearly half (**49%**) of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL

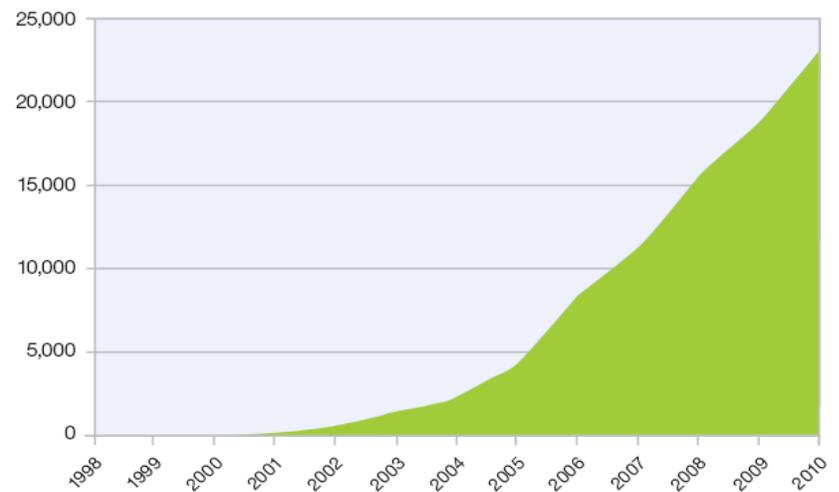
Web Application Vulnerabilities by Attack Technique
2004-2010



Web Application Vulnerabilities
as a Percentage of All Disclosures in 2010



Cumulative Count of Web Application Vulnerability Disclosures
1998-2010

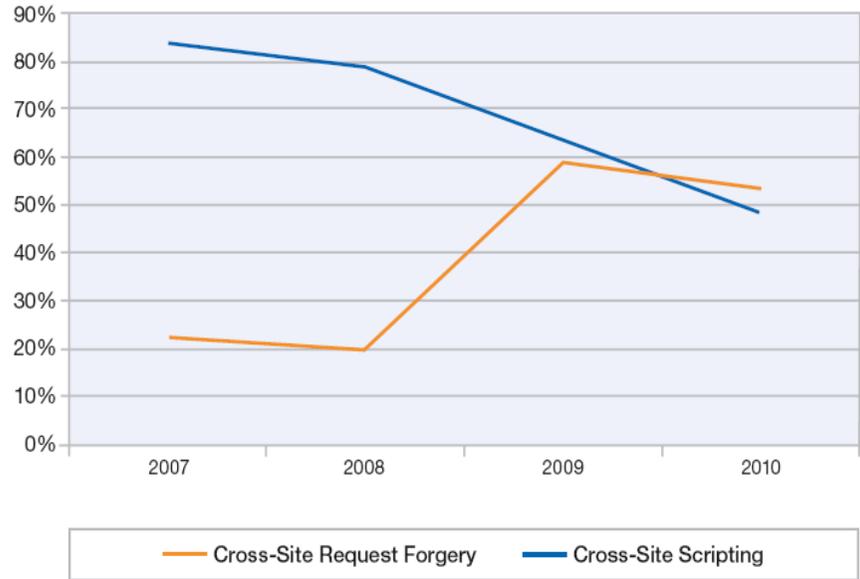


Real World Conclusions from Web App Assessments

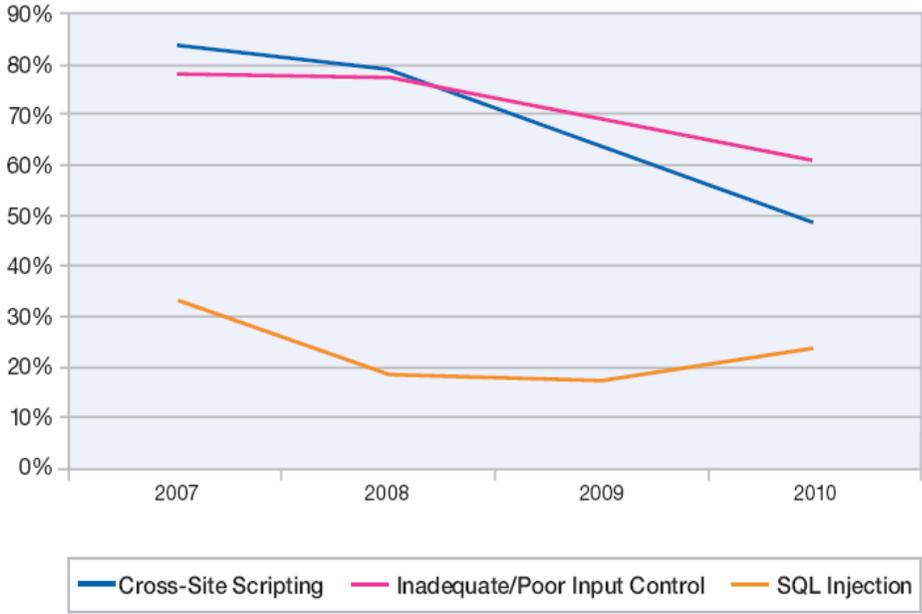


- In 2010, for the first time, we now find that Cross-Site Request Forgery (CRSF) vulnerabilities are more likely to be found in our testing than Cross-Site Scripting (XSS) vulnerabilities.
- XSS and SQL injection are both attributed directly to a lack of input control. The likelihood of finding it in 2010 is more than **60%**.

Cross-Site Request Forgery vs. Cross-Site Scripting Vulnerabilities
IBM® Rational® AppScan® OnDemand Premium Service
2007-2010



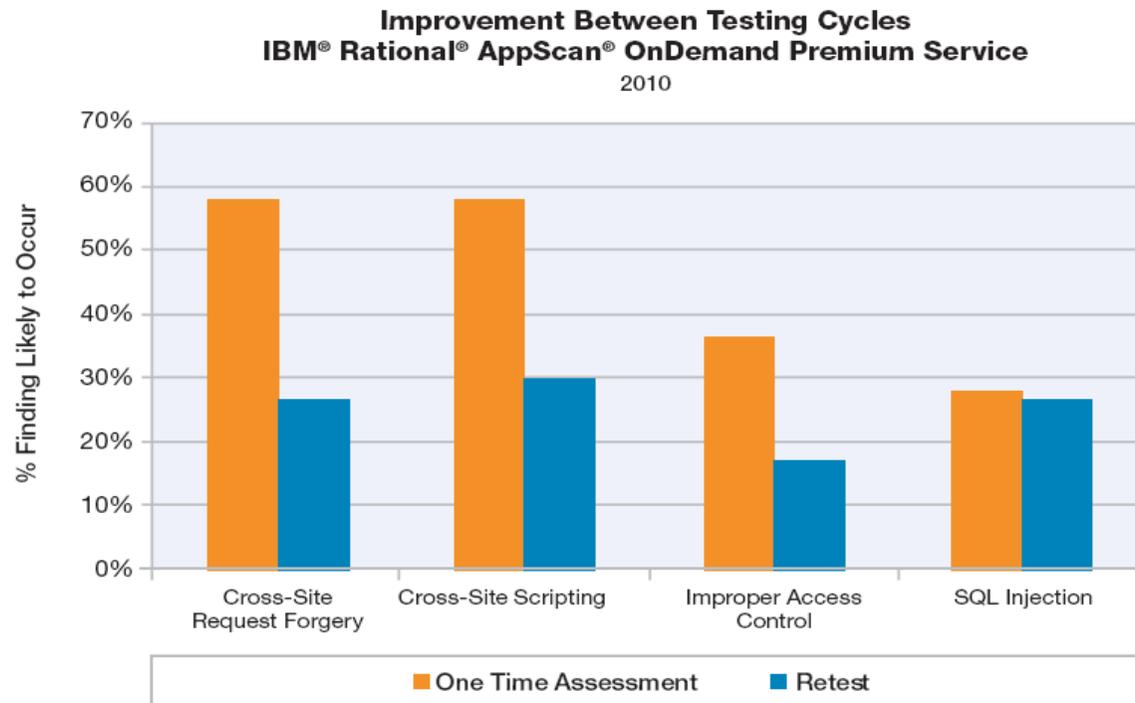
Annual Trends for Web Application Vulnerability Types
IBM® Rational® AppScan® OnDemand Premium Service
2007-2010





Improvement Between Application Testing Cycles

- There is a significant decline in the likelihood of finding application vulnerabilities in a retest.
- In many cases this reduction is more than half that of the original.
- Demonstrates the importance of testing applications but also follow up and mitigation.



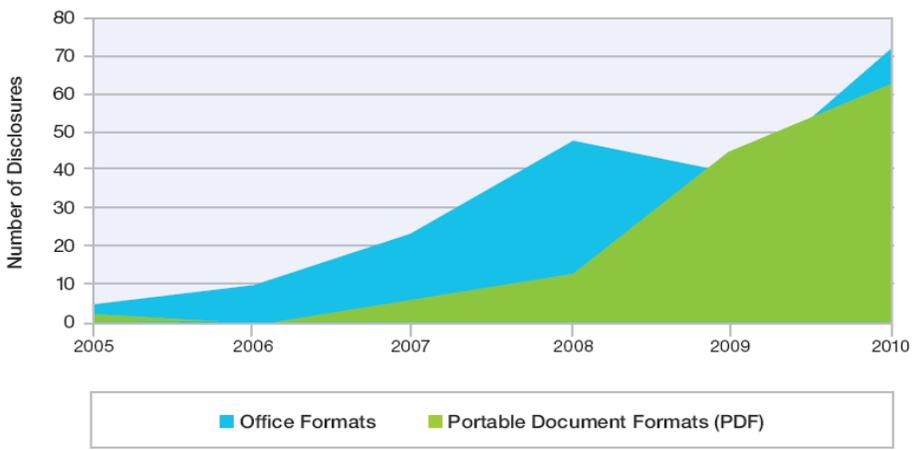
Note: Charts show which vulnerabilities were 50% or more likely to appear in a Web assessment for each industry



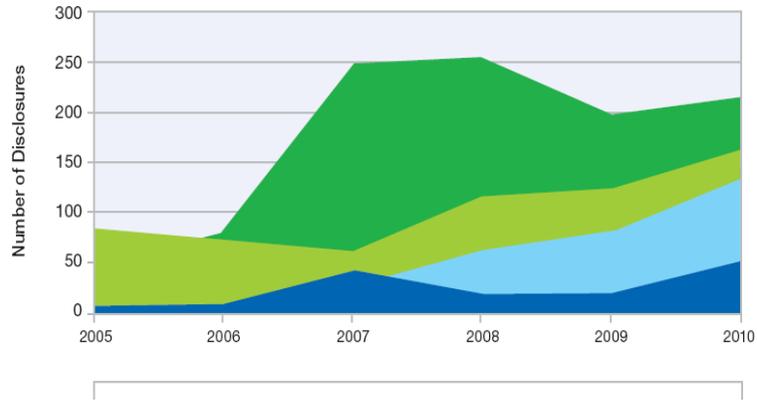
Client-Side Vulnerabilities: Web Browser, Document Reader & Multimedia Player Vulnerabilities Continue to Impact End Users

- Web browsers and their plug-ins continue to be the largest category of client-side vulnerabilities.
- 2010 saw an increase in the volume of disclosures in document readers and editors as well as multimedia players.

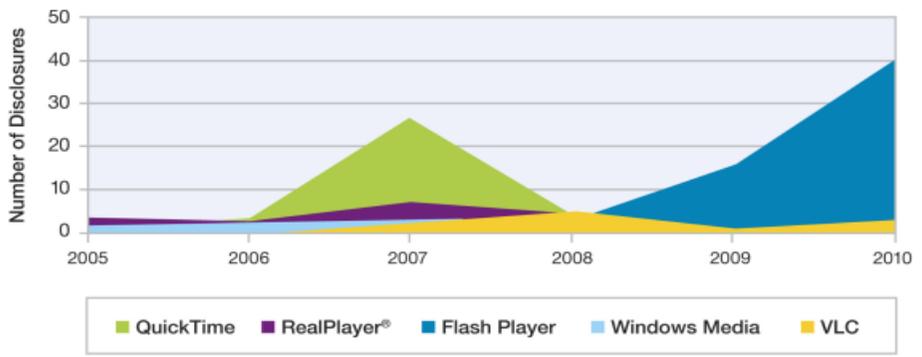
Vulnerability Disclosures Related to Critical and High Document Format Issues
2005-2010



Top Client Categories
Changes in Critical and High Client Software Vulnerabilities



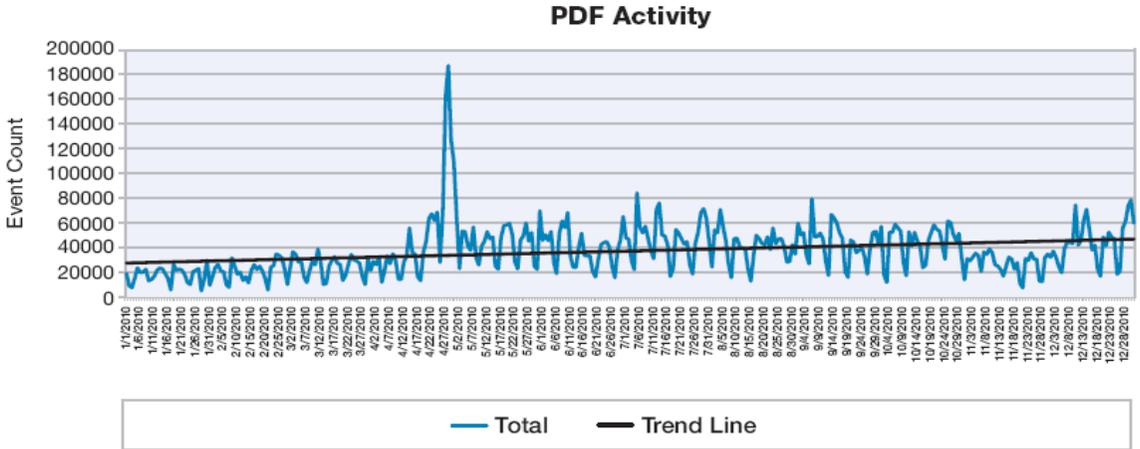
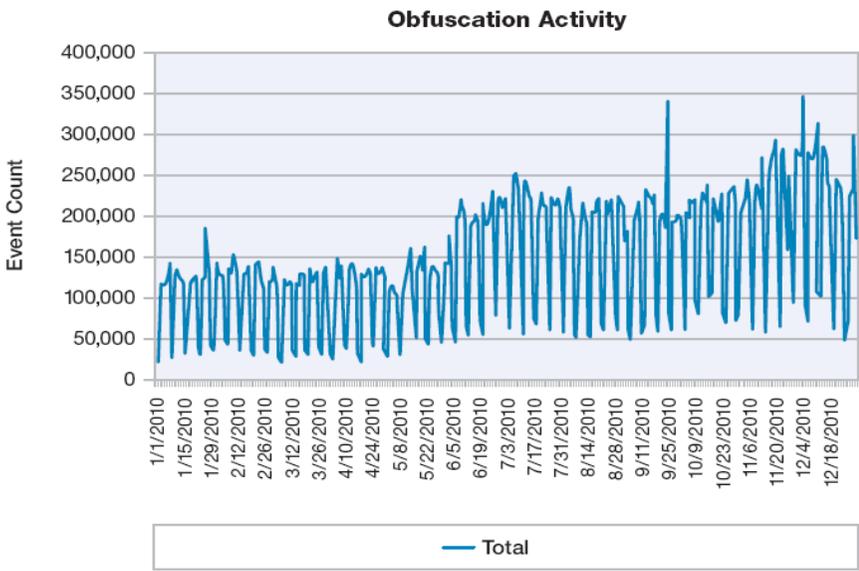
Critical and High Vulnerability Disclosures Affecting Multimedia Software
2005-2010



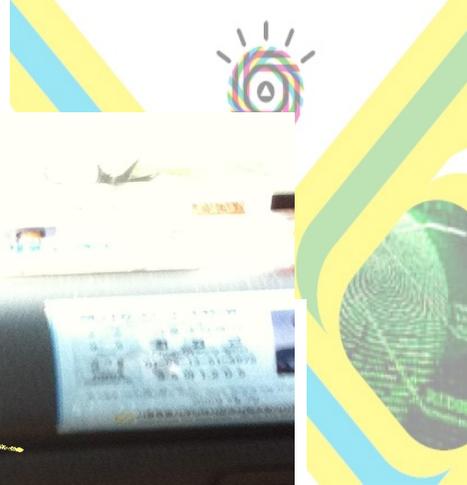
Suspicious Web Pages and Files



- Obfuscation activity continued to increase during 2010.
- Attackers never cease to find new ways to disguise their malicious traffic via JavaScript and PDF obfuscation.
 - Obfuscation is a technique used by software developers and attackers alike to hide or mask the code used to develop their applications.



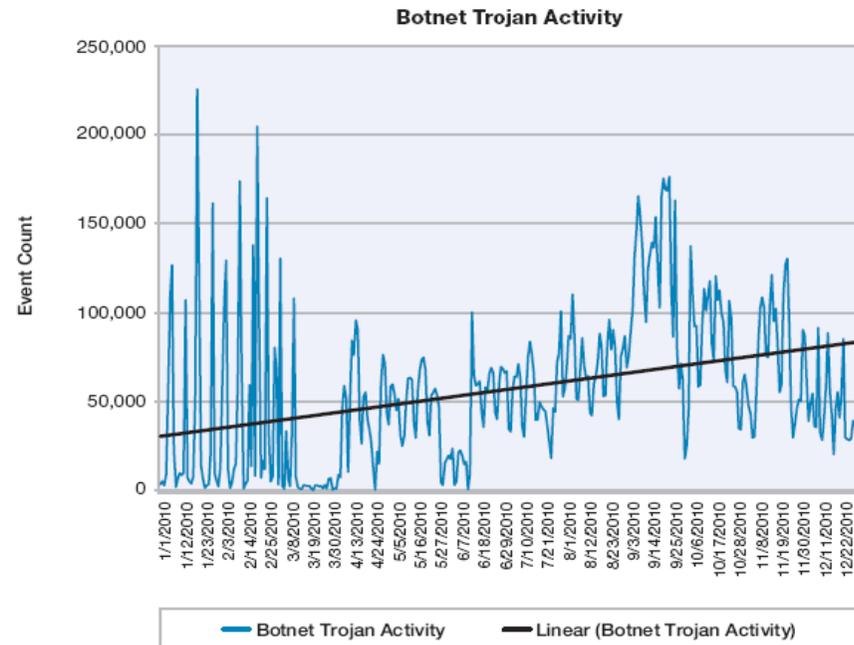
Proliferation of Mobile Devices Raises Security Concerns





Bot Network Activity on the Rise in 2010

- Trojan Bot networks continued to evolve in 2010 by widespread usage and availability.
- Zeus (also known as Zbot and Kneber) continue to evolve through intrinsic and plugin advances.
- Various bot networks based on Zeus were responsible for millions of dollars in losses over the last few years.
- Microsoft led operation resulted in the takedown of a majority of Waldec botnet in late February.
 - Communication between Waledac's command and control centers and its thousands of zombie computers was cut off in a matter of days.
- Much of the other activity seen is Zeus.



Zeus Crimeware Service



Member slots filled: 3 / 30

[Q] What is
[A] is a mix between the ZeuS Trojan and MalKit, A browser attack t
computer and start logging all outgoing connections.

[Q] How much does it cost?
[A] Hosting for costs \$50 for 3 months. This includes the following:

- Fully set up ZeuS Trojan with configured FUD binary.
- Log all information via internet explorer
- Log all FTP connections
- Steal banking data
- Steal credit cards
- Phish US, UK, and RU banks
- Host file override
- All other ZeuS Trojan features
- Fully set up MalKit with stats viewer inter graded.
- 10 IE 4/5/6/7 exploits
- 2 Firefox exploits
- 1 Opera exploit
- Admin area to view statistics

[Q] Can i see a demo?
[A] Yes you can, there is a demo set up [here](#) (Comming soon)

Methods of payment:

- Moneybookers.com
- LibertyReserve.com
- WesternUnion
- Alertpay

Zeus :: Logs search

Information:
Profile:
GMT date:
GMT time:

Statistics:
Summary

Botnet:
Online bots
Remote commands

Logs:
→ Search
Search with template
Uploaded files

Logout

Hosting for costs **\$50 for 3 months.**
This includes the following:

- # Fully set up ZeuS Trojan with configured FUD binary.
- # Log all information via internet explorer
- # Log all FTP connections
- # Steal banking data
- # Steal credit cards
- # Phish US, UK and RU banks
- # Host file override
- # All other ZeuS Trojan features
- # Fully set up MalKit with stats viewer inter graded.
- # 10 IE 4/5/6/7 exploits
- # 2 Firefox exploits
- # 1 Opera exploit“

We also host normal ZeuS clients for \$10/month.
This includes a fully set up zeus panel/configured binary

MassInfect
plorer, FireFox, Opera - 2008

| Hosts | Infects |
|-------|---------|
| 3 | 0 |
| 7 | 0 |
| 3 | 0 |
| 3 | 0 |
| 2 | 0 |
| 1 | 0 |
| 1 | 0 |
| 1 | 0 |
| 1 | 0 |
| 1 | 0 |
| 8 | 0 |
| 1 | 0 |
| 5 | 0 |
| 1 | 0 |

Reset
Grabbed data
Protected Storage
IE history
Other

Search

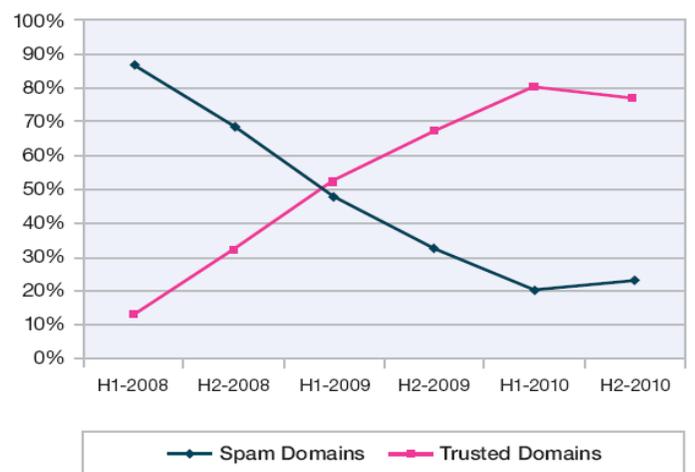




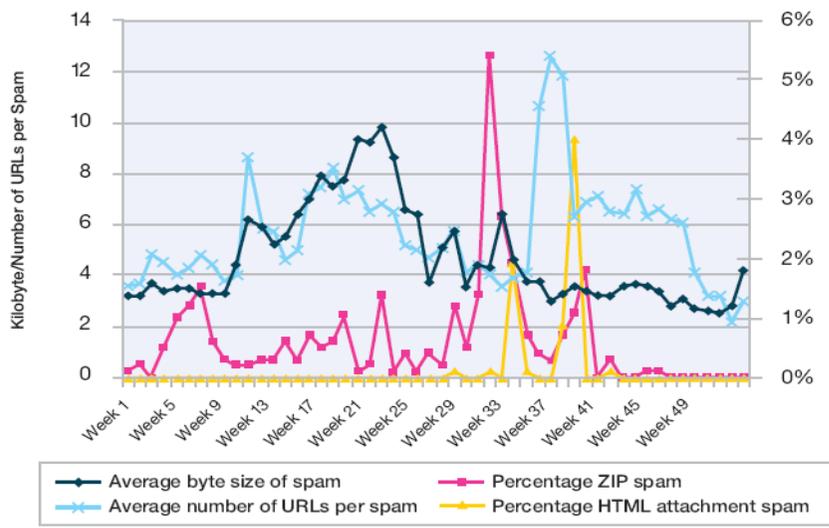
Spammers Focus on Content Rather than Volume

- Spammers made a continuous effort in 2010 to regularly change technical contents of spam messages rather than increasing volume.
 - Moving from random text spam combined with random URLs, ZIP Attachments, HTML attachments, to significantly increasing the average byte size of spam.
 - The amount of URL spam using well-known and trusted domain names declined slightly in the 2nd half of 2010, for the first time in more than two years.

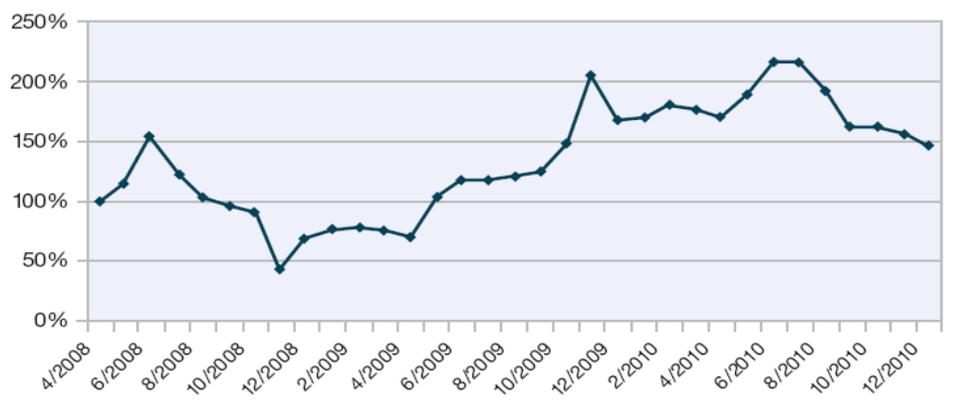
Top Ten Domains Used in Spam
Spam Domains vs. Trusted Domains
H1-2008 to H2-2010



Major Content Trends in Spam
2010 per week



Changes in Spam Volume
April 2008 to December 2010



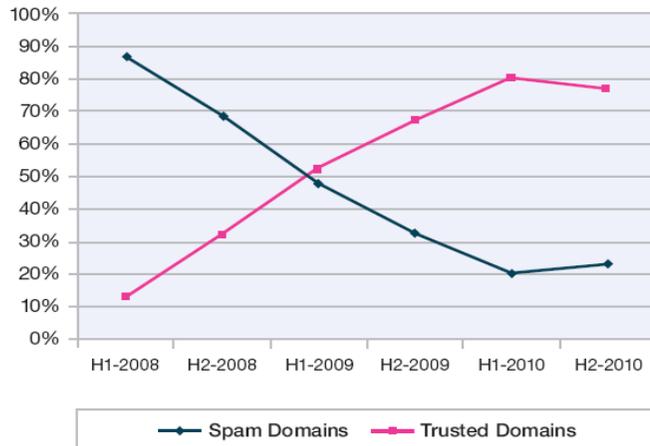
Spam Continues to Change to Avoid Detection



- **90%** of spam is classified as URL spam.
- Spammers continue to use “trusted” domains and “legitimate links” in spam messages to avoid anti-spam technologies.
- US, India, Brazil, and Vietnam were the top four spam-sending countries, accounting for nearly one-third of worldwide spam.

— The US once again takes the

**Top Ten Domains Used in Spam
Spam Domains vs. Trusted Domains
H1-2008 to H2-2010**



| Rank | January 2010 | February 2010 | March 2010 | April 2010 | May 2010 | June 2010 |
|------|-------------------|-------------------|-------------------|-------------------|-------------------|---------------|
| 1. | flickr.com | radikal.ru | livefilestore.com | livefilestore.com | imageshack.us | imageshack.us |
| 2. | imageshack.us | imageshack.us | imageboo.com | imageshack.us | imageshost.ru | imageshost.ru |
| 3. | radikal.ru | livefilestore.com | radikal.ru | imageshost.ru | myimg.de | pikucha.ru |
| 4. | livefilestore.com | flickr.com | imageshack.us | imgur.com | xs.to | imgur.com |
| 5. | webmd.com | live.com | googlegroups.com | myimg.de | imgur.com | mytasvir.com |
| 6. | picsochka.ru | imageboo.com | live.com | xs.to | tinypic.com | mojoimage.com |
| 7. | live.com | capalola.biz | akamaitech.net | icontact.com | livefilestore.com | myimg.de |
| 8. | superbshore.com | feetorder.ru | gonestory.com | tinypic.com | icontact.com | twimg.com |
| 9. | tumblr.com | laughexcite.ru | bestanswer.ru | live.com | googlegroups.com | icontact.com |
| 10. | fairgreat.com | hismouth.ru | wrotelike.ru | binkyounet.net | images-amazon.com | twitter.com |

| Rank | July 2010 | August 2010 | September 2010 | October 2010 | November 2010 | December 2010 |
|------|-----------------|----------------|--------------------------|---------------------|----------------------|-----------------------|
| 1. | imageshack.us | yahoo.com | the.com | businessinsider.com | rolex.com | pfizer.com |
| 2. | icontact.com | the.com | of.com | migre.me | msn.com | viagra.com |
| 3. | the.com | icontact.com | msn.com | 4freeimagehost.com | bit.ly | msn.com |
| 4. | myimg.de | feetspicy.com | pfizerhelpfulanswers.com | bit.ly | pfizer.com | rolex.com |
| 5. | of.com | of.com | and.com | postimage.org | co.cc | bit.ly |
| 6. | imgur.com | ratherwent.com | bit.ly | imgur.com | royalfoote.com | product45h.com |
| 7. | by.ru | and.com | in.com | pfizer.com | royalbelie.com | newpfizermed5k.com |
| 8. | and.com | facebook.com | yahoo.com | viagra.com | royalreleasable.com | xmages.net |
| 9. | in.com | in.com | a.com | uploadgeek.com | luxurystorewatch.com | cordfork.com |
| 10. | tastymighty.com | a.com | x-misc.com | vipplayerq.com | basincook.com | onlinepfizersoft2.com |

Table 3: Most common domains in URL spam, 2010

| Country | % of Spam |
|---------|-----------|
| USA | 10.9% |
| India | 8.2% |
| Brazil | 8.1% |
| Vietnam | 5.4% |
| Russia | 5.2% |

| Country | % of Spam |
|----------------|-----------|
| United Kingdom | 4.4% |
| Germany | 3.7% |
| South Korea | 3.3% |
| Ukraine | 3.0% |
| Romania | 2.9% |

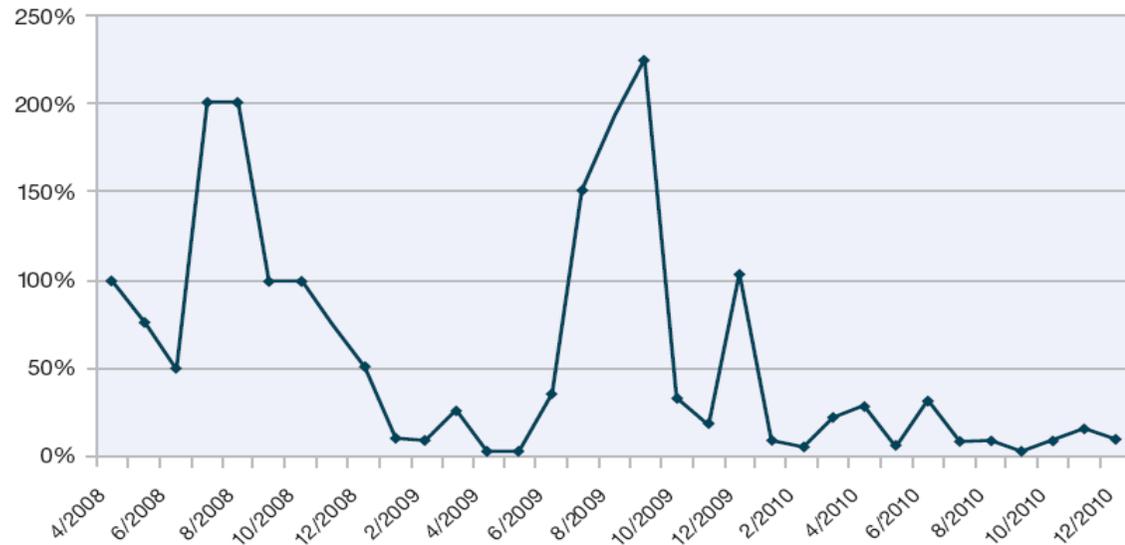
Table 5: Geographical Distribution of Spam Senders – 2010



Phishing Attacks Continue to Decline

- In 2010, Phishing emails slowed and the volume did not reach the levels seen at the end of 2009.
- India is the top sender in terms of phishing volume, while Russia is in second place, and Brazil holds third place.
 - Newcomers in the top 10 are Ukraine, Taiwan, and Vietnam, while Argentina, Turkey, and Chile disappeared from this list.
- Over time popular subject lines continue to drop in importance.
 - By 2010, the top 10 most popular

Phishing Volume Over Time
April 2008 to December 2010



| Country | % of Phishing |
|---------|---------------|
| India | 15.5% |
| Russia | 10.4% |
| Brazil | 7.6% |
| USA | 7.5% |
| Ukraine | 6.3% |

| Country | % of Phishing |
|-------------|---------------|
| South Korea | 4.7% |
| Colombia | 3.0% |
| Taiwan | 2.2% |
| Vietnam | 2.2% |
| Poland | 1.8% |

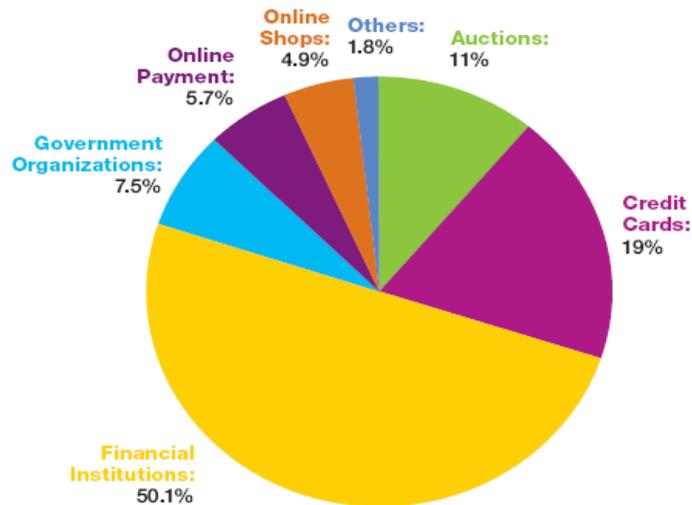
Table 7: Geographical Distribution of Phishing Senders – 2010

Phishing Targets Financial & Credit Card Industries

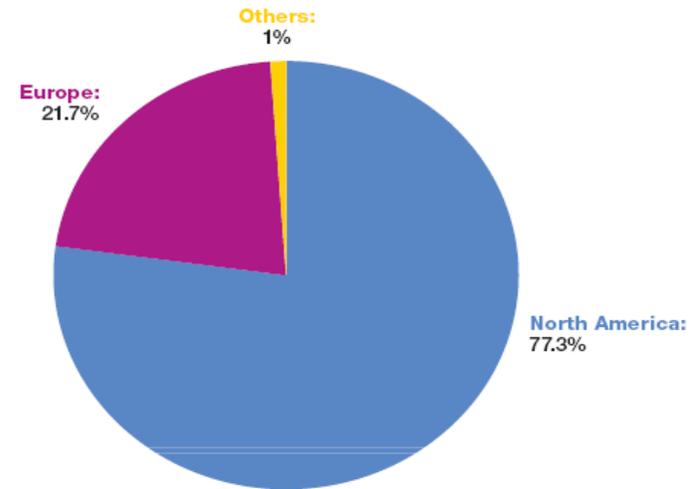


- **50.1%** of phishing is targeted at the financial industry vs. **60.9%** in 2009.
- **77%** of all financial phishing targets in the 2010 are located in North America vs. **95%** in 2009.
 - **22%** of financial phishing targets are located in Europe
- **19%** of phishing emails were targeted at credit cards

Phishing Targets by Industry
2010



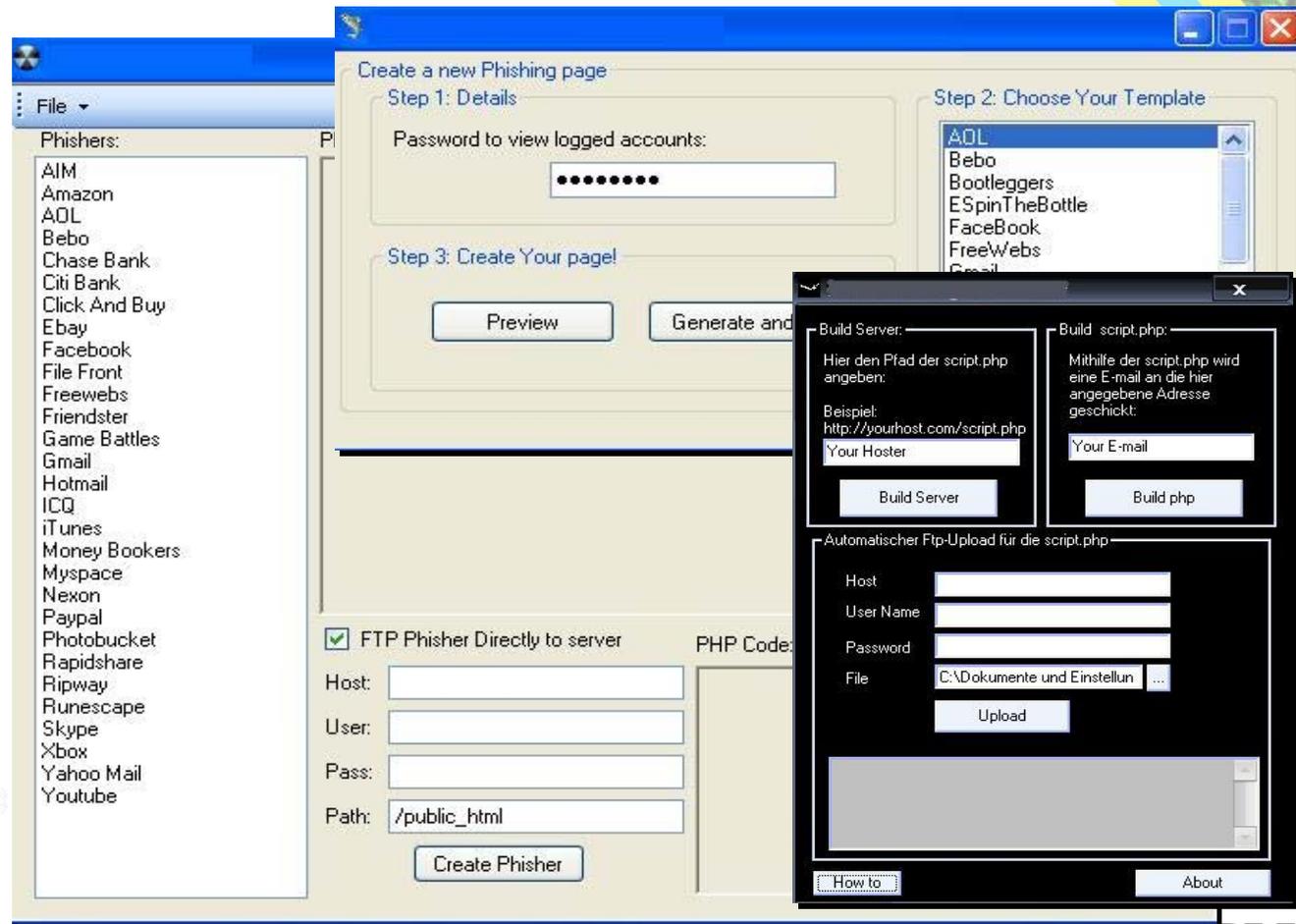
Financial Phishing by Geographical Location
2010



Phishing Tools

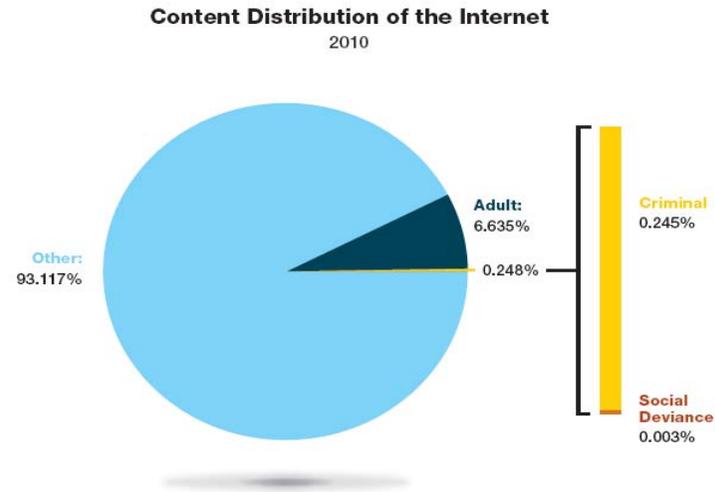
| | | |
|----------------------|-------|---------------|
| aol.data | 23 KB | DATA File |
| aol.phish | 1 KB | PHISH File |
| bebo.data | 69 KB | DATA File |
| bebo.phish | 1 KB | PHISH File |
| bootleggers.data | 5 KB | DATA File |
| bootleggers.phish | 1 KB | PHISH File |
| ESpinTheBottle.data | 60 KB | DATA File |
| ESpinTheBottle.phish | 1 KB | PHISH File |
| facebook.data | 25 KB | DATA File |
| facebook.phish | 1 KB | PHISH File |
| freewebs.data | 20 KB | DATA File |
| freewebs.phish | 1 KB | PHISH File |
| gmail.data | 21 KB | DATA File |
| gmail.phish | 1 KB | PHISH File |
| hi5.data | 78 KB | DATA File |
| hi5.phish | 1 KB | PHISH File |
| hotmail.data | 26 KB | DATA File |
| hotmail.phish | 1 KB | PHISH File |
| live.data | 85 KB | DATA File |
| live.phish | 1 KB | PHISH File |
| livelogin.data | 11 KB | DATA File |
| livelogin.phish | 1 KB | PHISH File |
| messblack.data | 53 KB | DATA File |
| messblack.phish | 1 KB | PHISH File |
| millersmiles.data | 20 KB | DATA File |
| millersmiles.phish | 1 KB | PHISH File |
| mobliffe.data | 7 KB | DATA File |
| mobliffe.phish | 1 KB | PHISH File |
| msndelchkr.data | 17 KB | DATA File |
| msndelchkr.phish | 1 KB | PHISH File |
| myspace.data | 50 KB | DATA File |
| myspace.phish | 1 KB | PHISH File |
| plugins | 1 KB | Text Document |
| rs.data | 5 KB | DATA File |
| rs.phish | 1 KB | PHISH File |
| WoW.data | 11 KB | DATA File |
| WoW.phish | 1 KB | PHISH File |

- Commercial phishing kits make it easy for a novice to start in the business

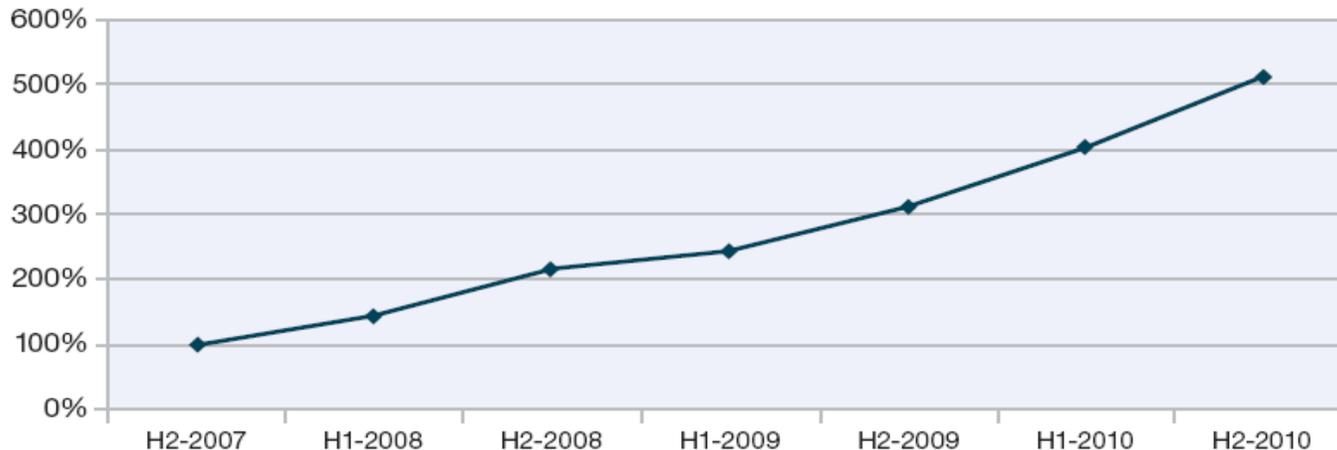


“Bad” Web Content Tries to Evade Filters

- Approximately **7%** of the Internet contains unwanted content such as pornographic or criminal Web sites.
- Anonymous proxies, which hide a target URL from a Web filter, have steadily increased more than quintupling in number since 2007.

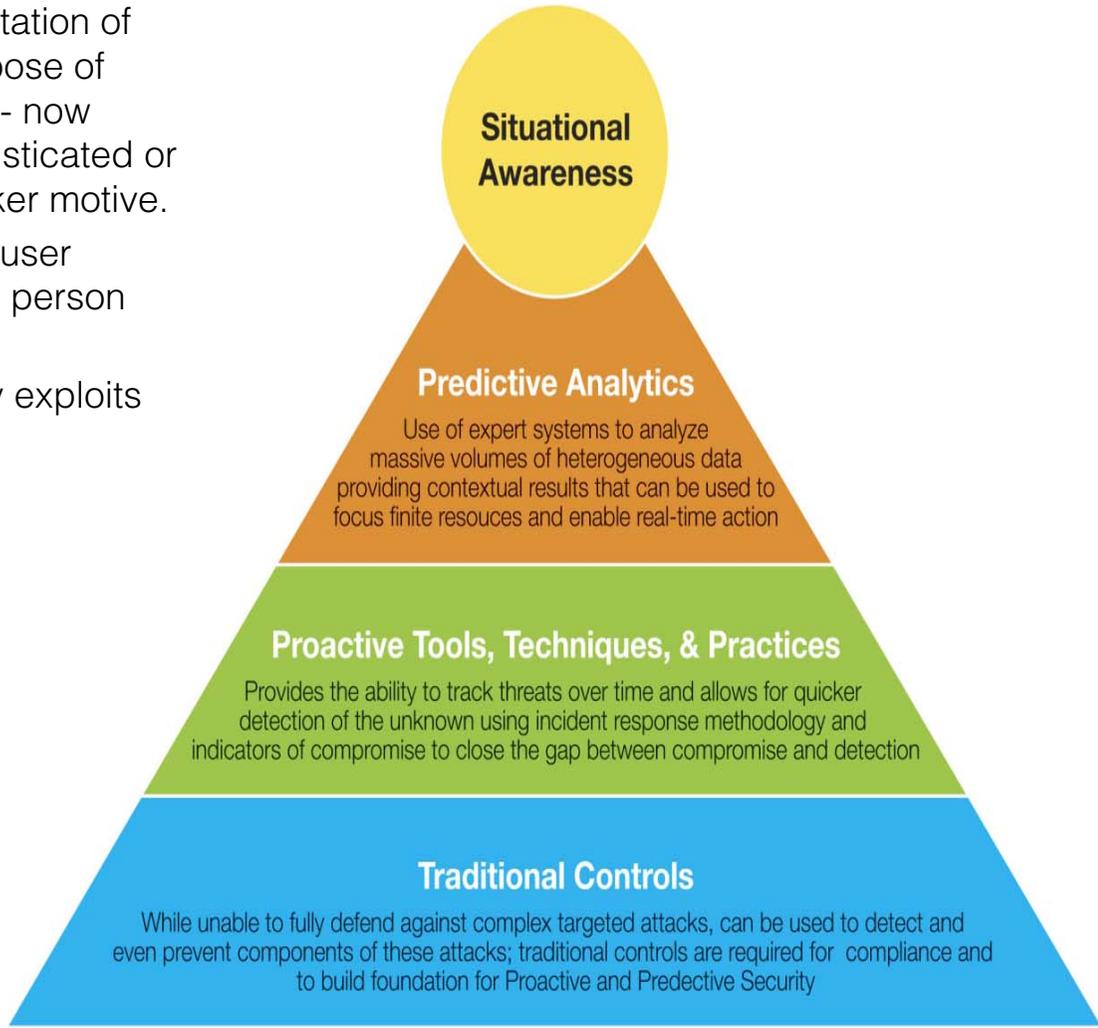


Volume Increases of Anonymous Proxy Websites
H2-2007 to H2-2010



Stuxnet and Advanced Persistent Threats (APT)

- APT previously thought to be exploitation of cyber-defense systems for the purpose of economic, political or military gain -- now associated with any targeted, sophisticated or complex attack regardless of attacker motive.
- Often a high-value target is an end-user system such as one that belongs to person who has access to sensitive data.
- Stuxnet took advantage of Zero day exploits with no work around or patch



Avoiding AV Technology – Malware Testing



ScanLix 1.0 [VirusScan]

C:\beta1.exe

| Antivirus | Posibles Infecciones |
|------------|----------------------|
| McAfee | Posible Virus: 1 |
| Kaspers... | Posible Virus: 1 |
| Shopos | viruses.....1 |
| F-Prot | Posible Virus: 0 |
| AntiVir | Posible Virus: 1 |
| Norton | Posible Virus: 0 |
| BitDefe... | Posible Virus: 1 |
| ClamWin | Posible Virus: 1 |
| Solo | Posible Virus: 1 |
| Nod32 | Posible Virus: 1 |

Resultado

| | |
|-------------------------------------|------------|
| <input checked="" type="checkbox"/> | Antiv... |
| <input checked="" type="checkbox"/> | Avast |
| <input checked="" type="checkbox"/> | AVG |
| <input checked="" type="checkbox"/> | BitDef |
| <input checked="" type="checkbox"/> | ClamW |
| <input checked="" type="checkbox"/> | DrWe |
| <input checked="" type="checkbox"/> | eTrus |
| <input checked="" type="checkbox"/> | Ewid |
| <input checked="" type="checkbox"/> | F-Pro |
| <input checked="" type="checkbox"/> | Ikaru |
| <input checked="" type="checkbox"/> | KAV |
| <input checked="" type="checkbox"/> | McAfe |
| <input checked="" type="checkbox"/> | NOD32 |
| <input checked="" type="checkbox"/> | Norm |
| <input checked="" type="checkbox"/> | Nort |
| <input checked="" type="checkbox"/> | Panda |
| <input checked="" type="checkbox"/> | PC-Cillin |
| <input checked="" type="checkbox"/> | Quick Heal |
| <input checked="" type="checkbox"/> | Solo |
| <input checked="" type="checkbox"/> | Sophos |
| <input checked="" type="checkbox"/> | VBA32 |

Bck/Bifrose.J
BKDR_BIFROSE.S
Backdoor.Bifrose.d
Backdoor.Bifrose.D
Troj/Bckdr-HEL
Backdoor.Win32.Bifrose.d

Scanear

tiempo: 99 seg

Multi AVs Fixer BETA - 21 Antivirus Supported - [iNs]

List of AVs can be Fixed :

- AVG Antivirus Free Edition
 - Fix
 - UnFix
 - Do It
- AntiVir Antivirus Free Edition
 - Fix
 - UnFix
 - Do It
- Ashampoo Antivirus
 - Fix
 - UnFix
 - Do It
- Avast 4 Antivirus
 - Fix
 - UnFix
 - Do It
- QuickHeal Antivirus
 - Fix
 - UnFix
 - Do It
- Norman Virus Control 5.90
 - Fix
 - UnFix
 - Do It
- Panda Antivirus 2008
 - Fix
 - UnFix
 - Do It

List of AVs can be Fixed :

- NOD 32 Antivirus
 - Fix
 - UnFix
 - Do It
- BitDefender Antivirus v8
 - Fix
 - UnFix
 - Do It
- Solo Antivirus 2008
 - Fix
 - UnFix
 - Do It
- Clam Win Antivirus
 - Fix
 - UnFix
 - Do It
- Kaspersky Antivirus 7.0.0.120
 - Fix
 - UnFix
 - Do It
- Trend Micro InterScan VirusWall v6
 - Fix
 - UnFix
 - Do It
- Sophos Antivirus 6.5.1
 - Fix
 - UnFix
 - Do It

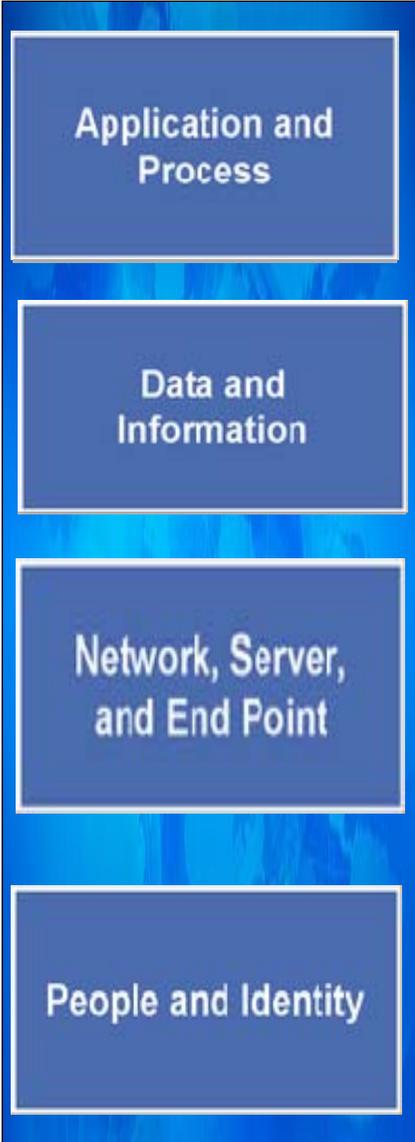
List of AVs can be Fixed :

- Dr. Web 4.44.1.01210
 - Fix
 - UnFix
 - Do It
- PCmav Antivirus 1.0.0
 - Fix
 - UnFix
 - Do It
- Norton AntiVirus 2008
 - Fix
 - UnFix
 - Do It
- McAfee Antivirus 10
 - Fix
 - UnFix
 - Do It
- The Shield Antivirus 2007
 - Fix
 - UnFix
 - Do It
- Rising AntiVirus Personal Edition
 - Fix
 - UnFix
 - Do It
- Sunbelt CounterSpy 2.5
 - Fix
 - UnFix
 - Do It

Go To Scan File



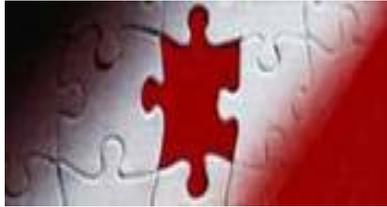
Report Summary -- Attacks Continue Across all Security Domains



- 2010 saw the largest number of vulnerability disclosures in history, up **27%**. This increase has had a significant operational impact for anyone managing large IT infrastructures. More vulnerability disclosures can mean more time patching and remediating vulnerable systems.
 - **49%** of the vulnerabilities disclosed in 2010 were web application vulnerabilities.
 - **44%** of all vulnerabilities disclosed had no vendor-supplied patches available at the end of 2010.
-
- Bot network activity continued to grow in 2010. Consolidation among Trojan botnets is expected to be an emerging trend.
 - The term “Advanced Persistent Threat” became an everyday part of the corporate security lexicon after high profile attacks on corporate enterprises by sophisticated, targeted attackers.
 - Anonymous proxy websites continue to increase in volume, quintupling since 2007.
-
- The SQL Slammer worm first surfaced in January 2003 and became known as one of the most devastating Internet threats of the past decade. This worm continued to generate a great deal of traffic on the Internet in 2010.
 - Obfuscation, whereby attackers attempt to hide their activities and disguise their programming, continued to increase over 2010 and shows no signs of waning.
 - SQL injection is one of the leading attack vectors seen in 2010 because of its simplicity to execute and its scalability to compromise large amounts of Web servers across the Internet.
-
- USA, India, Brazil, Vietnam, and Russia are the top five countries for spam origination in 2010.
 - The vast majority of spam, more than **90%**, is still classified as URL spam.
 - The amount of URL spam using well-known and trusted domain names declined slightly in the 2nd half of 2010, for the first time in more than two years.
 - In 2010, financial institutions continue to climb as the number one target for phishing attempts, representing **50%** of the targeted industries.



IBM X-Force Security Leadership



X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide 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>



감사합니다

Thank
YOU