




# Advanced Persistent Threats (APTs) Subversive Multi-Vector Threats (SMTs)

## What Does It Mean for Application Security

*OWASP - Austin*



Prepared by:  
Matthew Pour, CISSP  
Systems Engineer  
Blue Coat Systems

# Agenda

- APTs & SMTs at a Glance
- Vectors for Attacks
- High Value Targeting
- Evolving Protection Strategies
- Summary



# APTs & SMTs

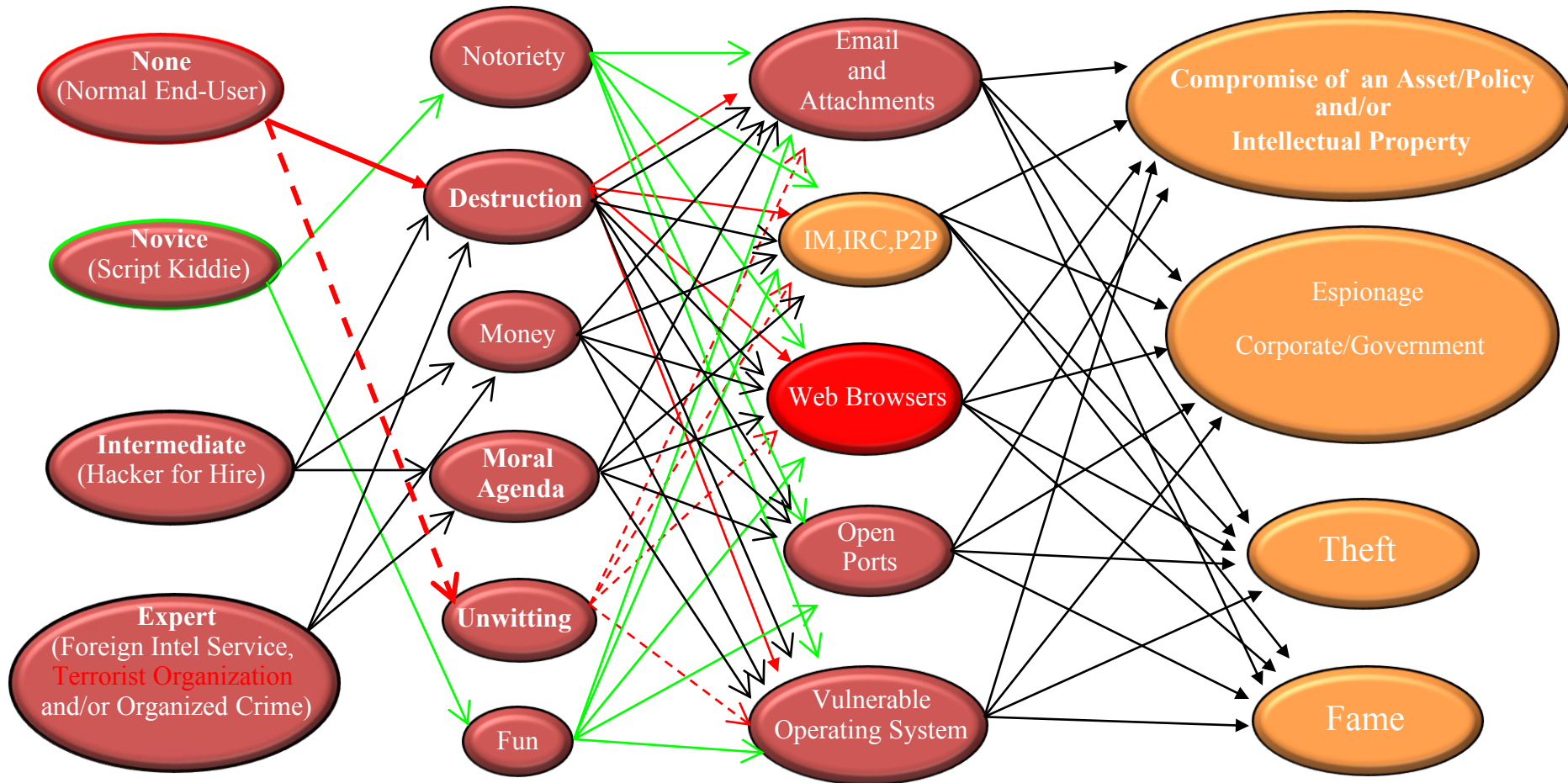
## APTs and SMTs

- Advanced Persistent Threat
  - Coined by Department of Defense
  - Events of Interest
- Subversive Multi-Vector Threat
  - Coined by Cassandra Security (ToorCon 11)

Non-Intentional Act - - - - -  
Intentional Act \_\_\_\_\_

## Classification of an Attacker

Expertise + Motivation + Attack Vector = Result

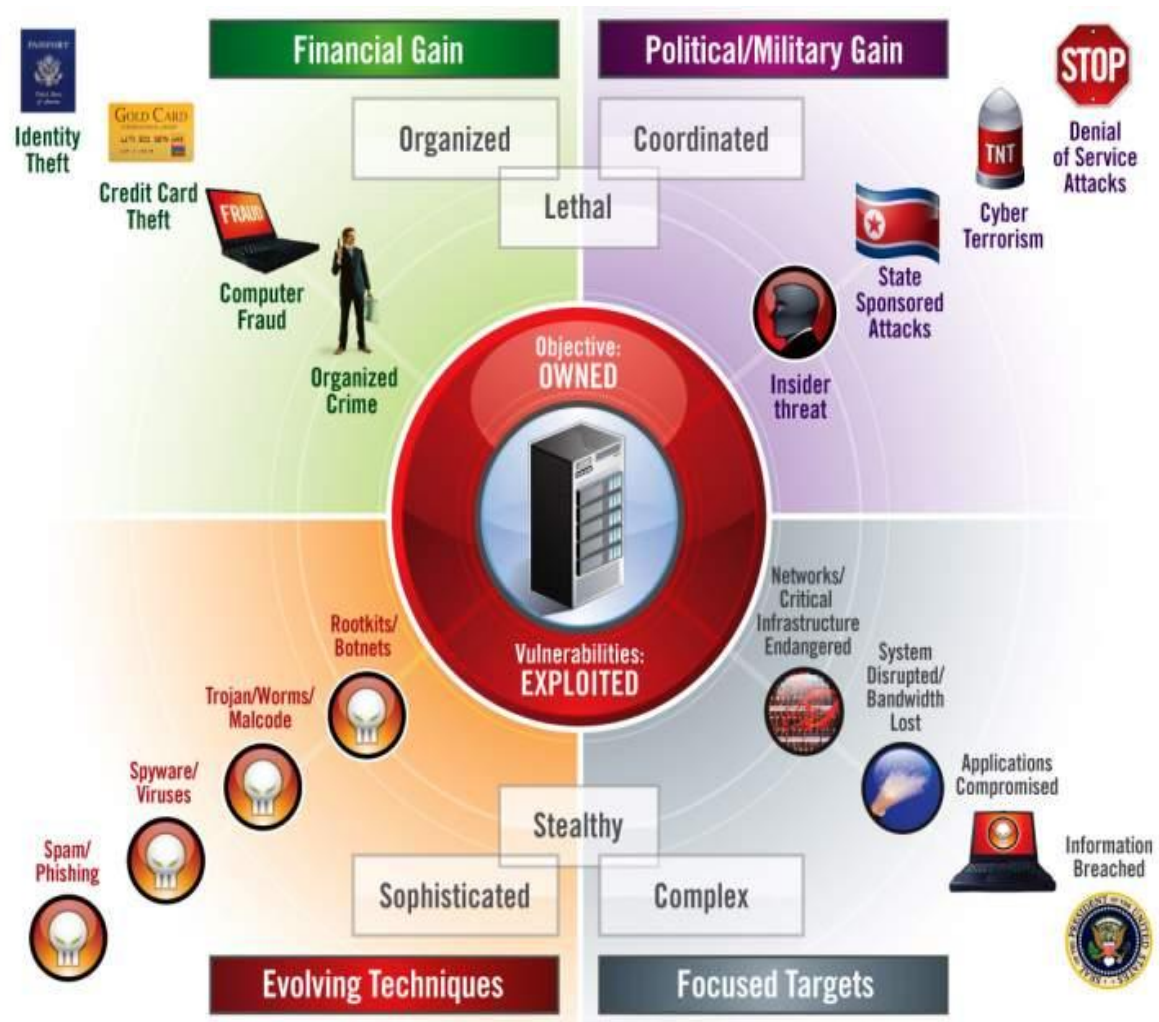




# Globalization and the Borderless Internet

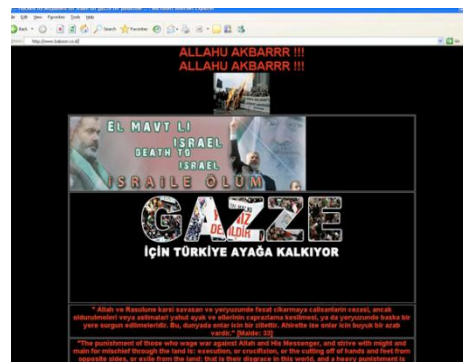
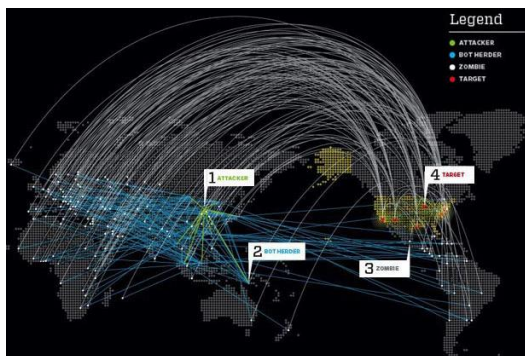
## • Threat Evolution:

- A flat world has brought about an unprecedented amount of criminals and cons
- In recent years the age of the worm has withered and application threats dominate
- 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



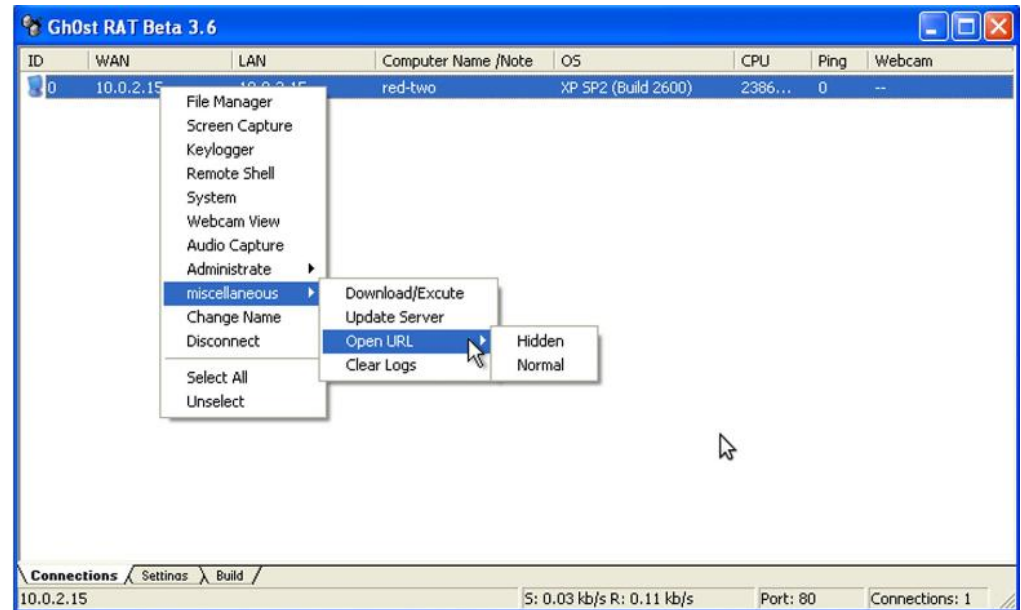
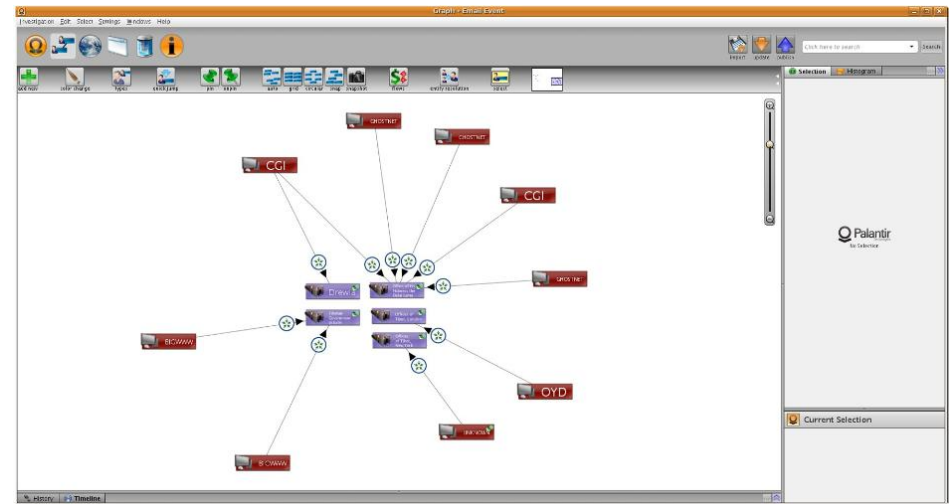
# Recent Examples of DDoS & Web Defacements

- Estonia Attacks
  - Parliament, ministries, banks, media targeted
- Georgia Attacks
  - Government Website's targeted
- Hamas Declares Cyber-war Against Israel
  - Israeli Political Organization targeted
- Moroccan Islamic Group
  - Israeli Bank Discount, news & weather sites attacked



# Ghost Net

- Ghost Net Forensics
  - Malware embedded in email
  - Spear Phishing
  - Drive by Malware
- Ghost RAT
  - Command & Control





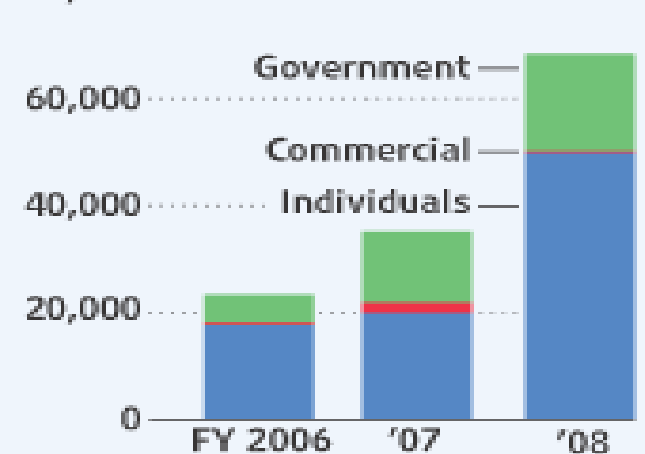
## Recent Examples of Corporate

- China vs. Google
- Marathon Oil
- Conoco Phillips
- Exxon Mobil



### Stealth Attacks

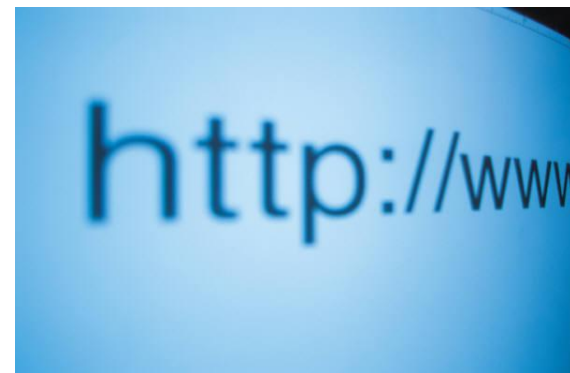
Number of reported cybersecurity breaches in the U.S., grouped by sector



Note: Fiscal year ends Sept. 30  
Source: Department of Homeland Security

# Recent Examples of Critical Infrastructure

- Insider Threat & Unauthorized Access
  - Computer system detecting pipeline leaks for three oil derricks off the Southern California coast disabled.
  - Queensland sanitation system – incident caused the release of millions of gallons of raw sewage
  - Laid Off Employee – plant temperature at risk
- Slammer Worm
  - Penetrated the network at Ohio's Davis-Besse nuclear power plant, disabling a safety monitoring system for nearly five hours.
- DDoS Attack on root name servers
  - Disabled the Internet for several hours

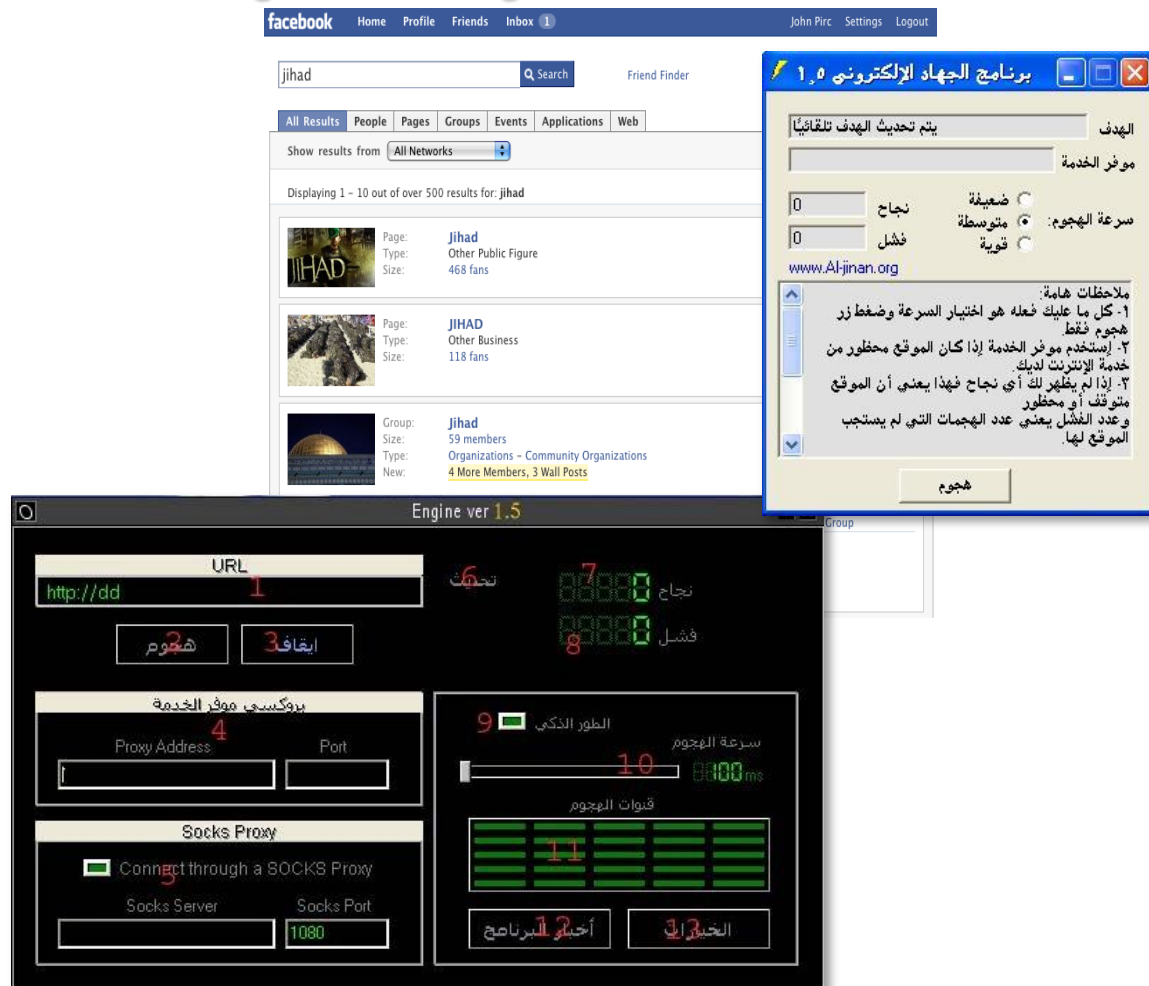


# Vectors of Attacks



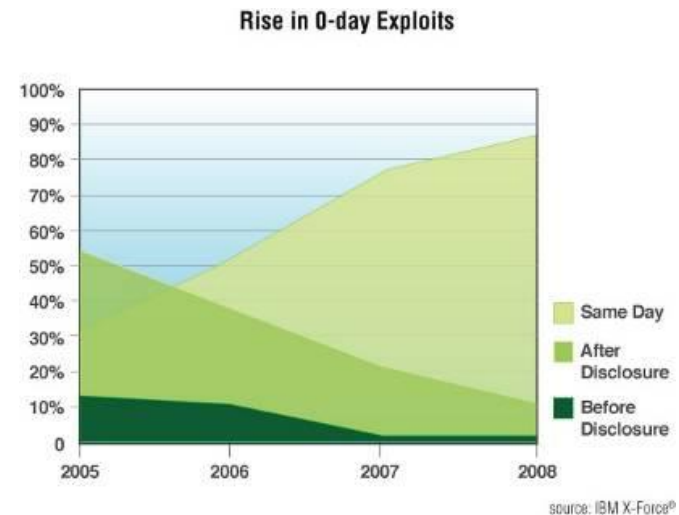
# The Cyber Jihad & “Common Cause” Attack Tools

- New social networks take up collective “arms” to target disliked organizations
- Largely bandwidth consumption orientated attacks
- Free tools to enable mass attacks
  - Multi-threaded HTTP GET Flooder
  - Similar to old ICMP PING flooders
- Open-source versions available for DIY authors and new “causes”



# Exploit code availability

- New browser and plug-in exploits are in high demand
  - 0-day exploit for IE/FF = \$25,000-\$75,000
  - Same-day exploit = \$2,000-\$30,000
  - Up to 3-days old exploit = \$5-\$500
- Drive-by-download exploit packs and support services increase spread of new exploits
  - Managed services and C&C distribution
  - New exploits can be propagated to thousands of sites/engines within seconds





# IcePack

- First appeared in July 2007
- **Two versions of IcePack**
- Basic Version “IcePack Lite Edition” (only has exploits for MS06-014 and MS06-006) and sold for \$30
- Advanced version “IcePack Platinum Edition”, sold for around \$400
- **Produced by “IDT Group” in Russian (now translated to English and French)**
- **/admin/license**
- Licensed on a per-website basis – “ERROR: Invalid License”

Contains Web browser optimized exploit pages

**/exploits/i.php**

Optimized for Internet Explorer  
Contains WinZip exploits,  
QuickTime overflow,  
MS06-057 WebViewFolderIcon,  
MS06-055 VML

**/exploits/movie.bin**

QuickTime overflow exploit

**/exploits/f.php**

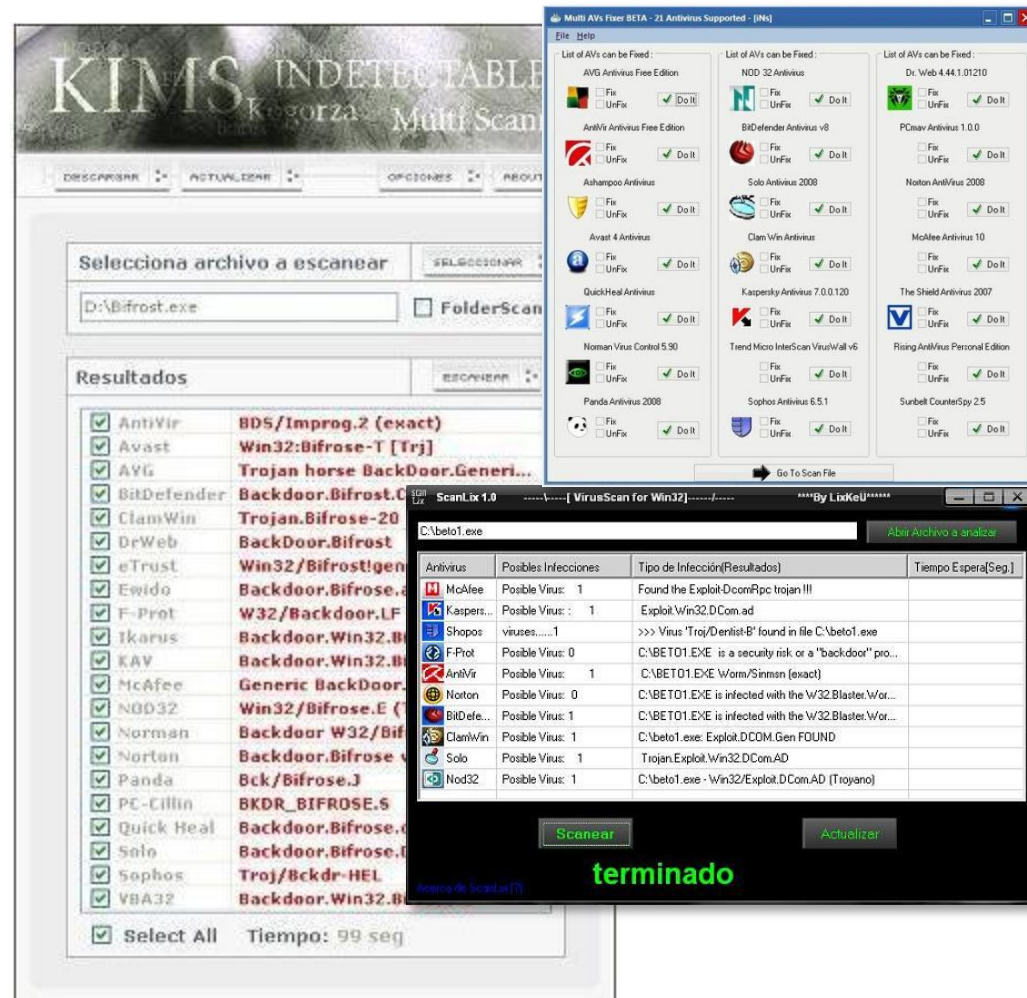
Firefox optimized version of MS06-006 exploit

**/exploits/o.php**

Opera optimized version of MS06-006 exploit

# Avoiding AV Technology – Malware Testing

- KIMS – English/Spanish
  - Requires attacker to install all the AV products themselves
- ScanLix
  - "install & forget" philosophy – just update from time to time.
  - ... see the different signature files being updated.
  - ...disadvantage is the limited number of engines it uses.



## Not Experienced...no problem

### Web-based portal bot-management

For a small fee, attackers can rent/purchase members of a larger botnet.

Online tools enable remote management and configuration of the botnet agents  
Portals include performance monitoring tools – how fast is the spam being sent, DDoS throughput, etc.



Bot traffic Statistics for [redacted] generated on 2008/08/09

Top 10 Countries:		Top 10 new countries today		Top 10 Countries order by bot's reports	
Country	Rating			Country	Rating
Russia	7099 56%			Russia	626089 59%
United States	1641 13%			United States	163156 15%
Germany	1504 12%			Germany	63896 6%
Netherlands	492 4%			Brazil	24697 2%
Ukraine	237 2%			Ukraine	20728 2%
Brazil	196 2%			Spain	19229 2%
United Kingdom	152 1%			Netherlands	13215 1%
Spain	138 1%			United Kingdom	11816 1%
Belgium	126 1%			Taiwan	11541 1%
Turkey	101 1%			Turkey	10173 1%
Totally: 80				Totally bot's reports: 1061892	



Hello,

Your last session: Tue Aug 5 06:16:31 2008

#### Active projects:

project	time end	price	bots	index time	size (mb)	action
[redacted]	14/1/2008	1	48 / 1	Tue May 13 00:18:43 2008	0.00	<a href="#">index</a>
[redacted]	6/8/2008	1	1048 / 10000	Tue Aug 5 17:00:52 2008	0.00	<a href="#">index</a>



# Anonymous Behavior



- Encryption - Secures Internet Connection
- Fast Speed - Not more then 30 Clients per server
- Compression - Rises your Connection Speed
- Compression - Less Traffic, Cheaper GPRS

**Commercial Anonymizing Service**

## SOCKS Jump Point

Many tools and services rely upon compromised hosts (typically botnet agents) to provide SOCKS proxies as anonymous exit/jump points.

Member information  
 Logged as: bill  
 Your tariff: V  
 Socks available: 250  
 Price per socks: Unlimited  
 Expiration date: 2008-02-19  
 Your balance: \$18.16 [Buy tariff](#)

Refresh Payment history Socks history IP Lookup Tunneling Exit

	IP / Host	Port	Country	State	City	Uptime
United States [131]	76.29.226.* / *.*,226.169	*****	United States	Alabama	Huntsville	11d 11h 38m
France [22]	68.39.115.* / *.*,comcast.net	*****	United States	New Jersey	Brick	4d 0h 28m
Germany [11]	75.128.253.* / *.*,253.14	*****	United States	Wisconsin	Madison	1d 23h 14m
Spain [11]	74.173.191.* / *.*,bellsouth.net	*****	United States	Florida	Miami	5d 2h 52m
Canada [10]	24.127.136.* / *.*,comcast.net	*****	United States	Pennsylvania	Bird In Hand	1h 22m
Sweden [10]	76.27.239.* / *.*,comcast.net	*****	United States	Oregon	Portland	7d 19h 3m
Italy [7]	76.83.213.* / *.*,rr.com	*****	United States	California	Palm Springs	2h 10m
United Kingdom [6]	76.213.157.* / *.*,sbcglobal.net					
Belgium [5]	206.74.70.* / *.*,70.15					
Austria [3]	67.184.149.* / *.*,comcast.net					
Other [2]	71.244.47.* / *.*,verizon.net					
Switzerland [2]	76.241.145.* / *.*,sbcglobal.net					
Greece [2]	70.230.254.* / *.*,sbcglobal.net					
Netherlands [2]	76.189.26.* / *.*,rr.com					
Denmark [1]	99.147.196.* / *.*,sbcglobal.net					
Hungary [1]						
Ireland [1]						
Israel [1]						
Norway [1]						
Russian Federation [1]						
Turkey [1]						

**Anonymous Proxies**  
 Volume of proxy services increasing year over year

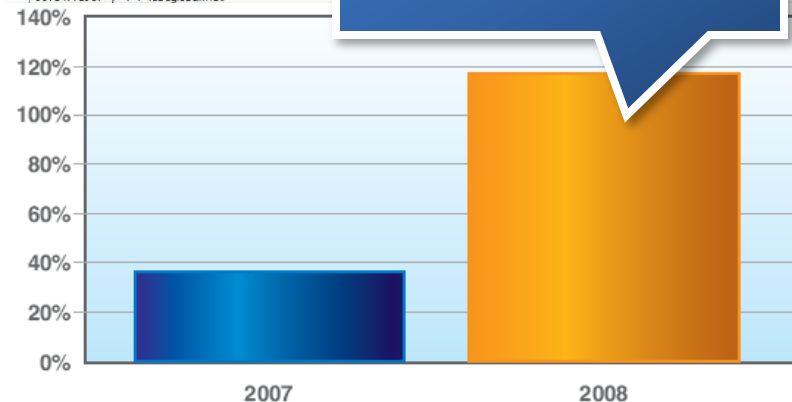


Figure 61: Year Over Year Increase of Anonymous Proxy Web Sites

# Localizing attacks

- Local language attack support
- Can be outsourced
- Translation services for spam/phishing/malware campaigns

## Prices and deadlines:

- \* Standard - the deadline is not more than 24 hours. Prices depend on the direction and guidance from the 'Order'.
- \* Term - work on your translation begins precedence. The price of the 50% more than the standard translation. Prices also depend on the direction and guidance from the 'Order'.

The cost of the transfer depends on the amount of work. The workload is measured in symbols. In calculating the characters are shown letters and numbers. Punctuation do not count. Minimum order 100 characters."

"We offer our services in translation. We are only competent translators profile higher education. Service is working with all types of texts. Languages available at this time of Russian, English, German. Average translation of the text takes up to 10 hours (usually much faster) through the full automation of the order and payment. **Just want to note that we do not keep any logs on IP and does not require registration.** In addition you can remove your order from the database after his execution. In addition to running more than 1000 translations already, we can use all the lessons learned to be more effective in our services. Prices vary depending on the complexity of the topic covered.



Авторизация

Логин

Пароль

Статус перевода

Код



# 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](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

Go Google 高级搜索 搜索帮助 | Google

网页 约有 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](http://www.cg160.com/userweb/company.asp?id=55442) - 22k - 网页快照 - 类似网页

检测: htt  
检测: htt  
检测: htt  
检测: htt  
检测: htt  
检测: htt  
检测: htt

- \* 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 T. 停止扫描 Q. 强行终止

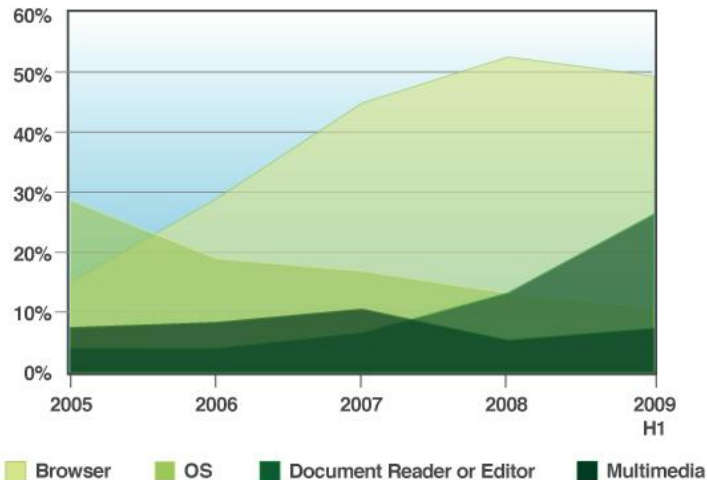
安全漏洞 服务器错误

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
<a href="http://www.cn/info.asp?id=6">http://www.cn/info.asp?id=6</a>	1609	6	aND 8=8 + aND 8=3	AND	数字型	未探测	康馨催乳公司 催乳 催	
<a href="http://www.bertech.com/shownews.asp?id=6">http://www.bertech.com/shownews.asp?id=6</a>	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	
<a href="http://www.bertech.com/ProductShow.asp?id=6">http://www.bertech.com/ProductShow.asp?id=6</a>	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	
<a href="http://www.ru.com/sinonews/list.asp?id=6">http://www.ru.com/sinonews/list.asp?id=6</a>	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, 80040e21,
<a href="http://www.gov.cn/qym/corporation.asp?id=6">http://www.gov.cn/qym/corporation.asp?id=6</a>	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, 80040e21,
<a href="http://www.com/00new/list.asp?id=6">http://www.com/00new/list.asp?id=6</a>	4610	5	aND 8=8 + aND 8=3	AND	数字型	未探测	上海假肢厂有限公司	
<a href="http://www.com.cn/products_list.asp?id=6">http://www.com.cn/products_list.asp?id=6</a>	4781	6	aND 8=8 + aND 8=3	AND	数字型	未探测	中怡数宽科技(苏州)	80040e21, 80040e21,
<a href="http://www.cha.com/CN/show.asp?id=112">http://www.cha.com/CN/show.asp?id=112</a>	5078	1	aND 8=8 + aND 8=3	AND	数字型	未探测	浪莎针织有限公司	
<a href="http://dg.com/zfbz/zfmr.asp?id=78">http://dg.com/zfbz/zfmr.asp?id=78</a>	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 Browsers are Complicated and Vulnerable

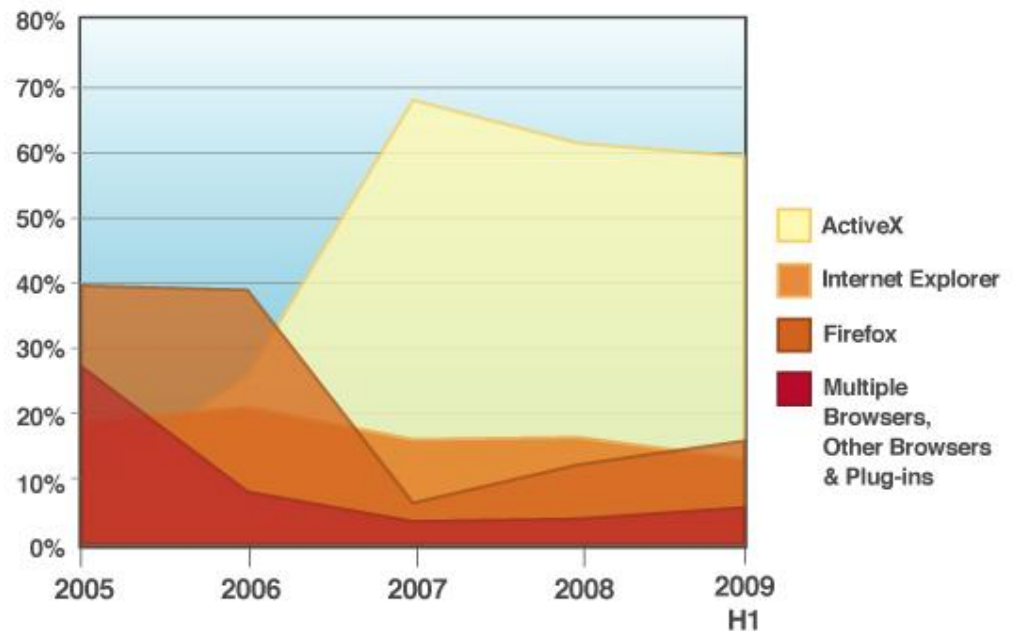
- **Largest number of client-side vulnerabilities in the first half of 2009 affects Web browsers and their plug-ins**
- **Mozilla Firefox surpasses Microsoft Internet Explorer for the 1<sup>st</sup> time.**

**Prevalent Client-Side Software**  
Percent of Critical and High Vulnerability Disclosures



source: IBM X-Force®

**Browse-Related Software**  
Percent of Critical and High Vulnerability Disclosures



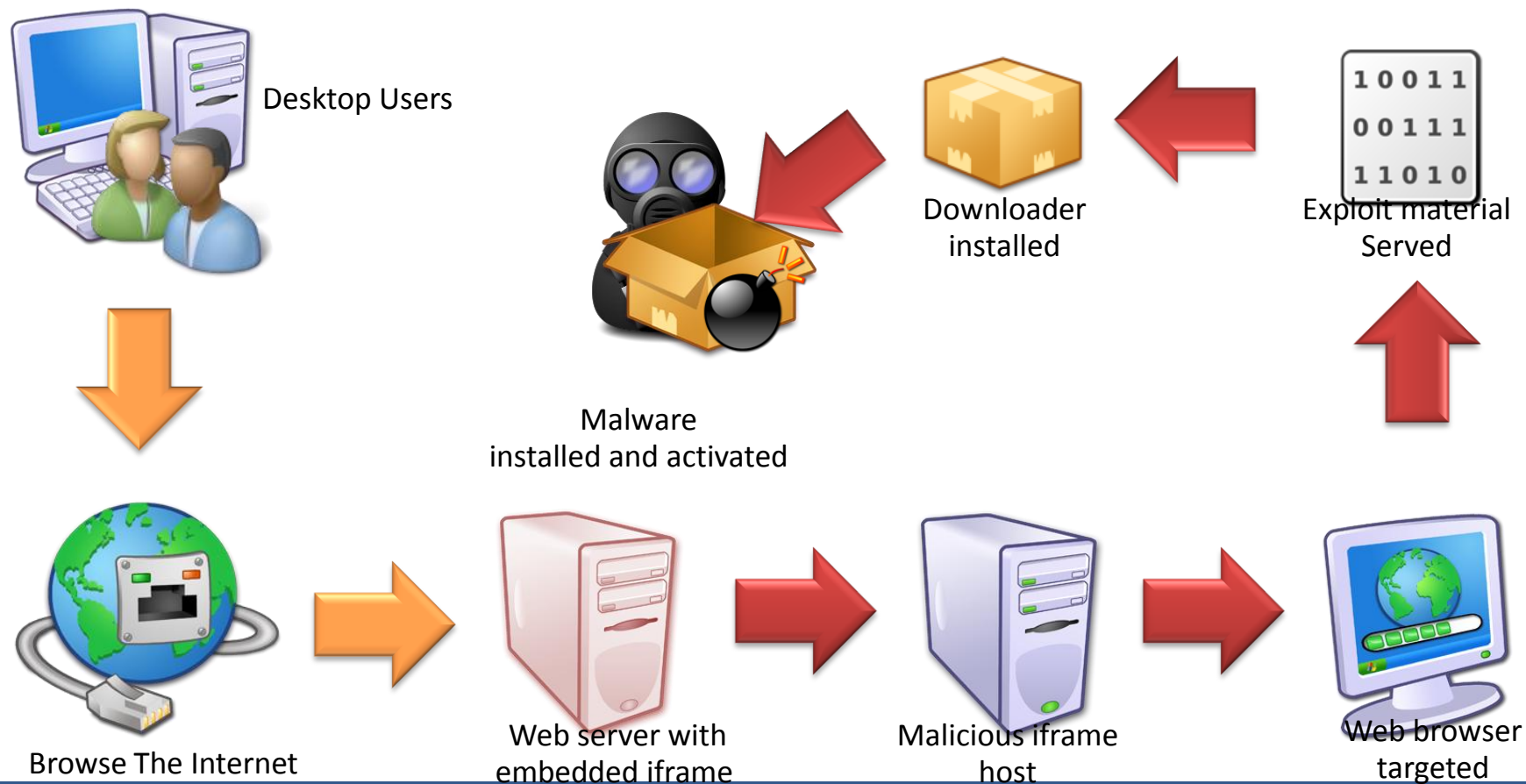
source: IBM X-Force®

# High Value Targets



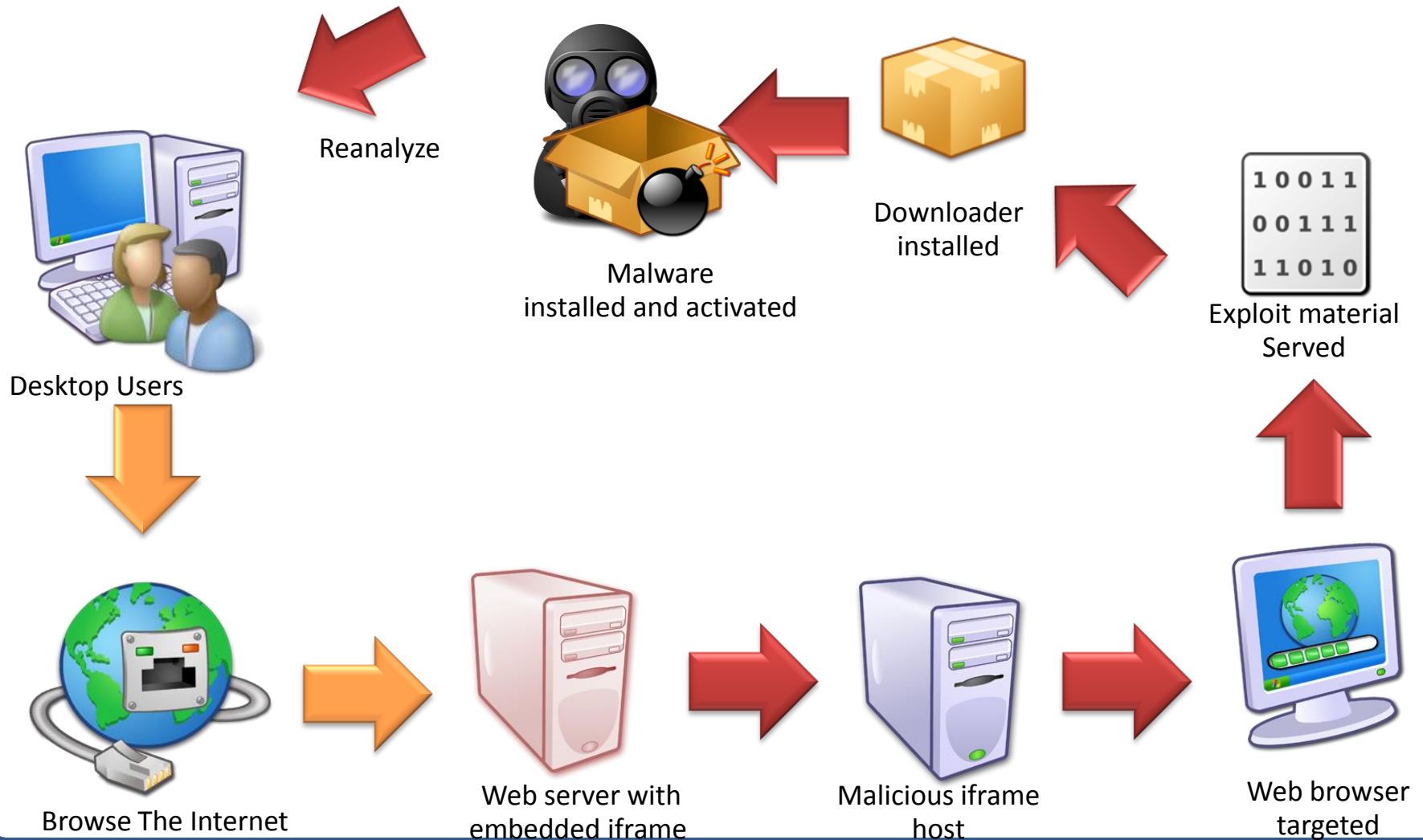
# The drive-by-download process

## Firewalls Exposed...





# Structured Attack





# Conficker – Technically sophisticated

- Well written code
  - Conficker.A signing key: 1024 bits
  - Conficker.B signing key: 4094 bits
  - No known remote code execution vulnerabilities
- Use of MD-6 by Ron Rivest
  - MD-6 was announced in October 2008
  - Included unexploitable vulnerability
  - Patched in Conficker.C
- Use of P2P Communications Protocol
  - Conficker A & B tried 500 daily domains
  - Conficker C tried 50,000
  - Unprecedented encoded P2P communications

# Conficker data transfer traffic from the first week of May, 2009

- Analysis Summary:
- P2P Message (All) : 12327
- P2P Message with FLAG\_CLIENT : 12327
- P2P Message with FLAG\_LOCAL : 0
- P2P Message with FLAG\_TCP : 1574
- P2P Message with FLAG\_LOCATION : 10753
- P2P Message with FLAG\_EXECDATA\_VAR : 35
- P2P Message with FLAG\_EXECDATA\_OFS : 0
- P2P Message with FLAG\_EXECDATA : 0
- P2P Message with FLAG\_SYSINFO : 186
- P2P Message with FLAG\_PEERINFO : 12157
- P2P Message with FLAG\_RESERVED1 : 0
- P2P Message with FLAG\_RESERVED2 : 0
- P2P Message with FLAG\_RESERVED3 : 0
- P2P Message with FLAG\_RESERVED4 : 0
- P2P Message with FLAG\_RESERVED5 : 0
- P2P Message with FLAG\_RESERVED6 : 0
- P2P Message with FLAG\_ENCODED : 12327

# Who did it and why?

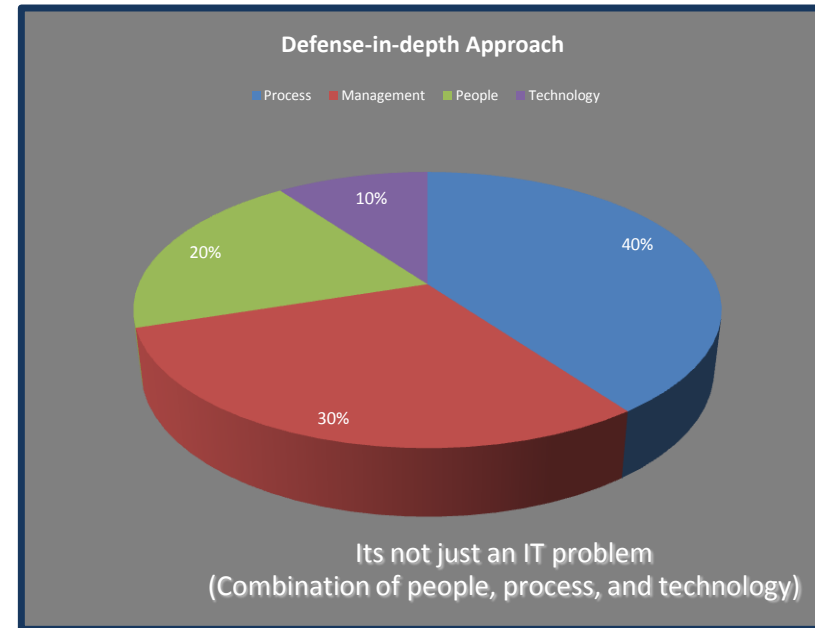
- Conficker A&B did not attack computers in Ukraine
- Isolated reports of malware appearing on Conficker.C nodes
  - Waldec
  - Rouge A/V
- Is there activity that no one has noticed?
- Are the botmasters biding their time?
  - For the Conficker Working Group to miss another domain or give up completely?
  - For another wormable vulnerability to be disclosed? MS09-050
  - For a political event?
- Have the botmasters been hit by a bus?

# Evolving Protection Strategies



## Best Practices

- Risk Management
- Incident Response
- Maturity Model
- Best Practices
  - Infraguard
  - OWASP
  - Information Sharing and Consortiums (ISACS)





## Protection Strategies – Defense in Depth

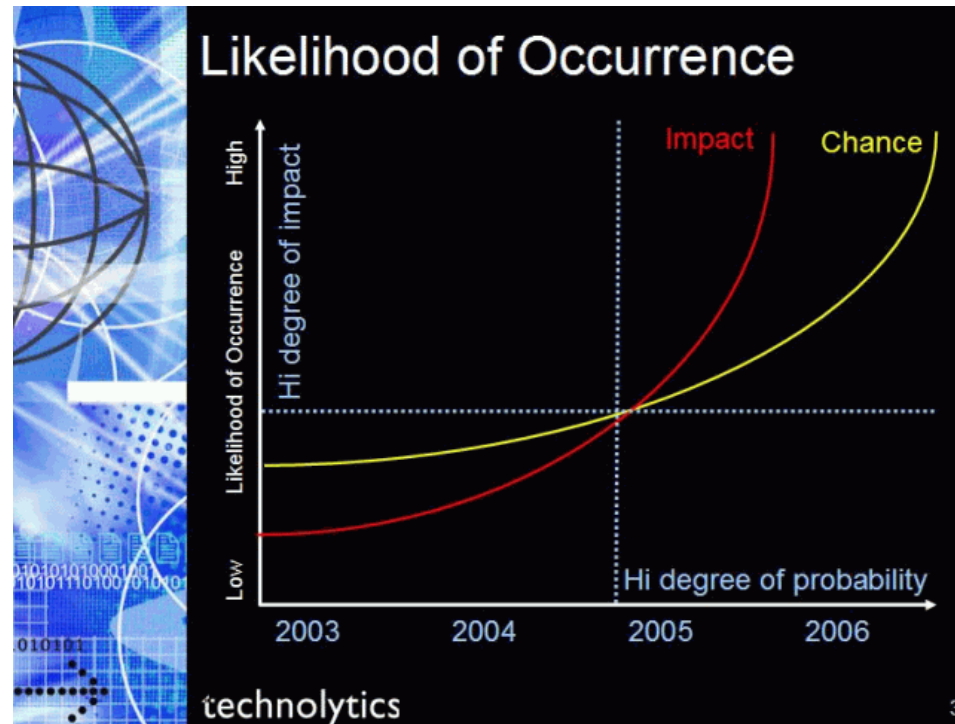
- SDLC
  - Assessment / Prevention
- Virtual Patching
  - Exploit protection from within the network
  - Provides coverage while software patches are deployed
- Deep Content Inspection
  - Network traffic and critical control protocols inspected for malicious and rogue commands
  - Complete Visibility



# Summary

## Summary

- APTS/SMTs
- Multiple Attack Vectors
- Evolution of the Threat
- Process/Technology



# Thank You!

Matthew Pour, CISSP  
matthew.pour@bluecoat.com