



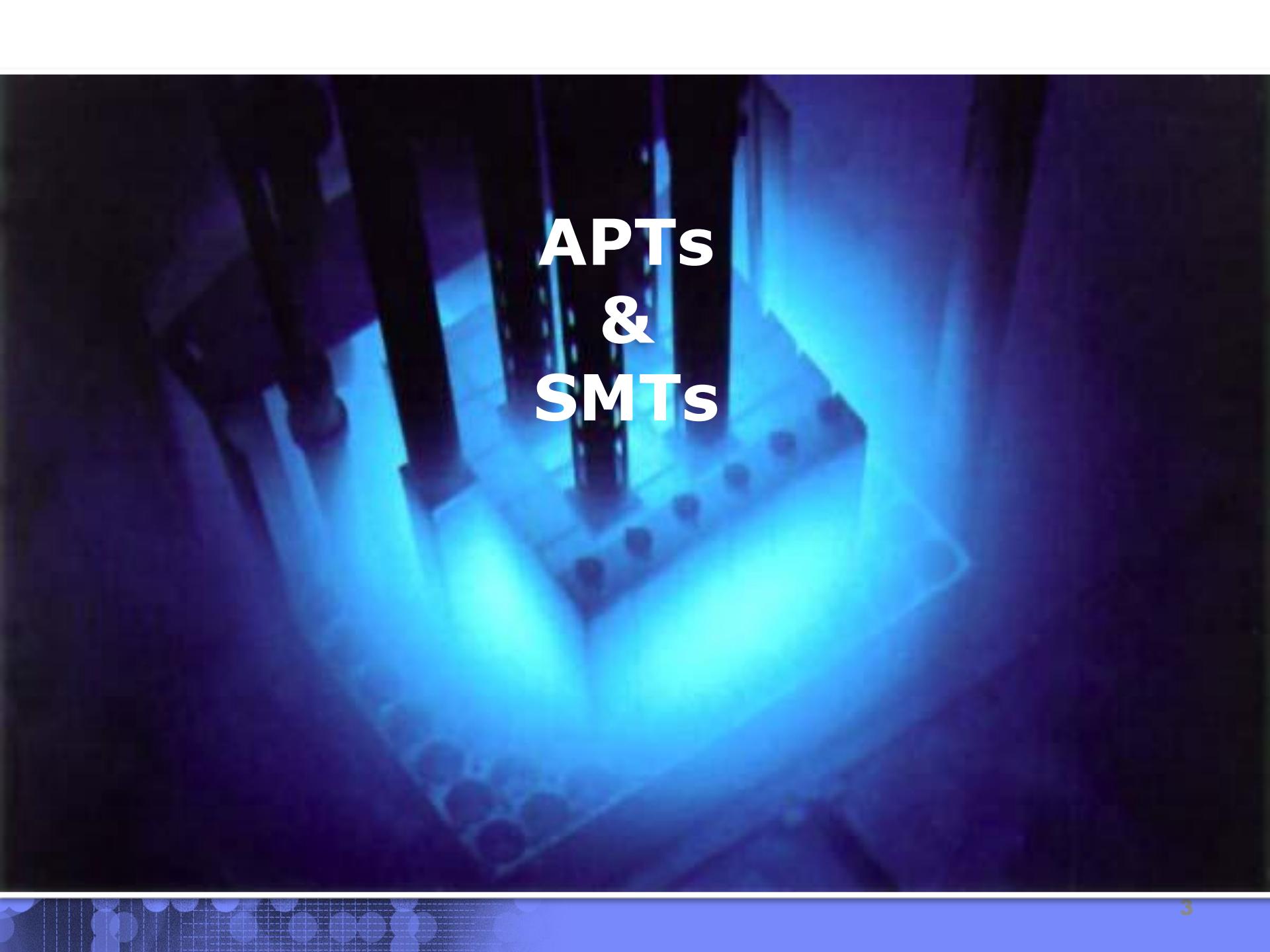
Advanced Persistent Threats (APTs) Subversive Multi-Vector Threats (SMTs)

What Does It Mean for Application Security

OWASP - Austin

Agenda

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



APTs & SMTs

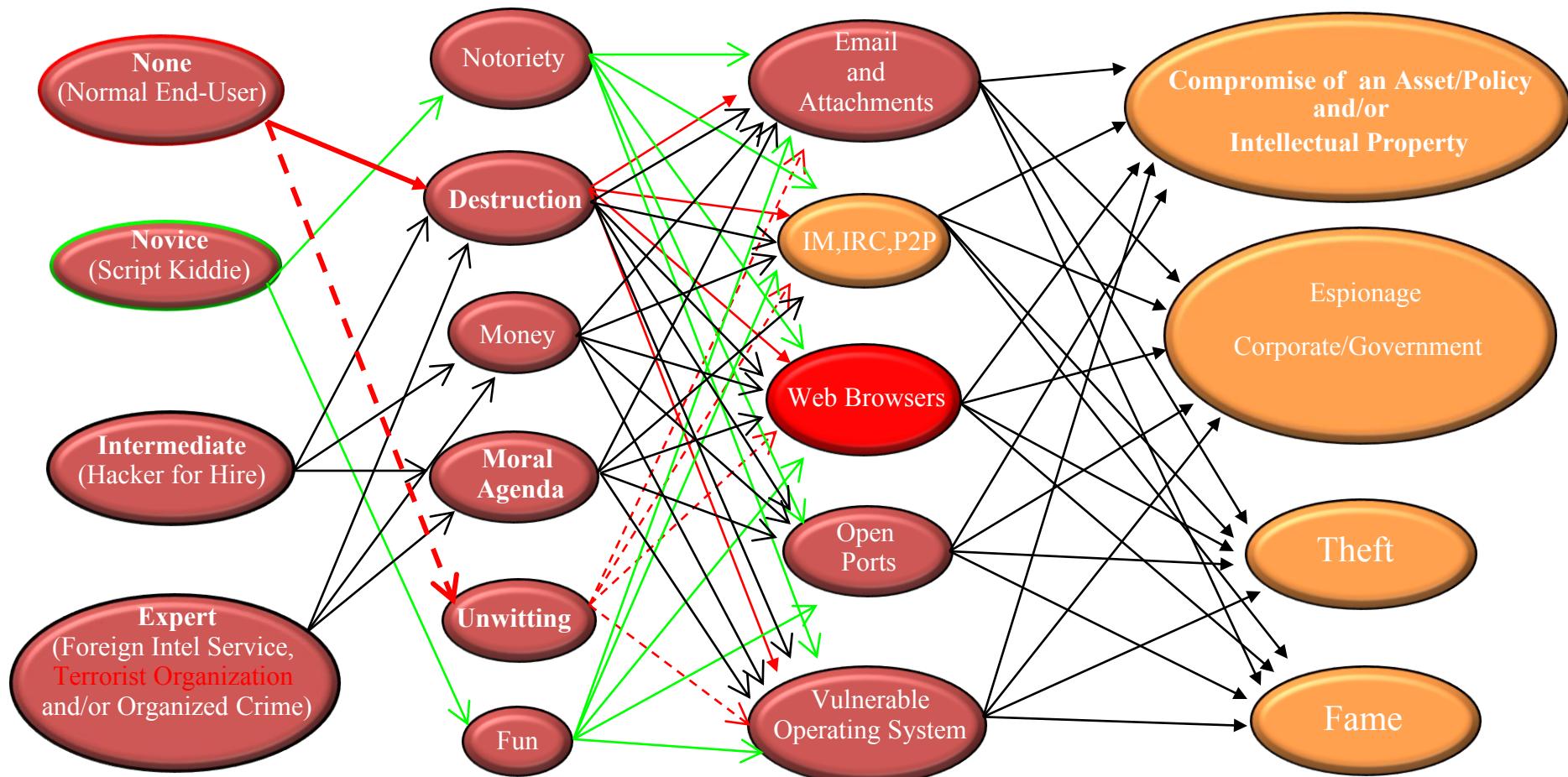
APTs and SMTs

- 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

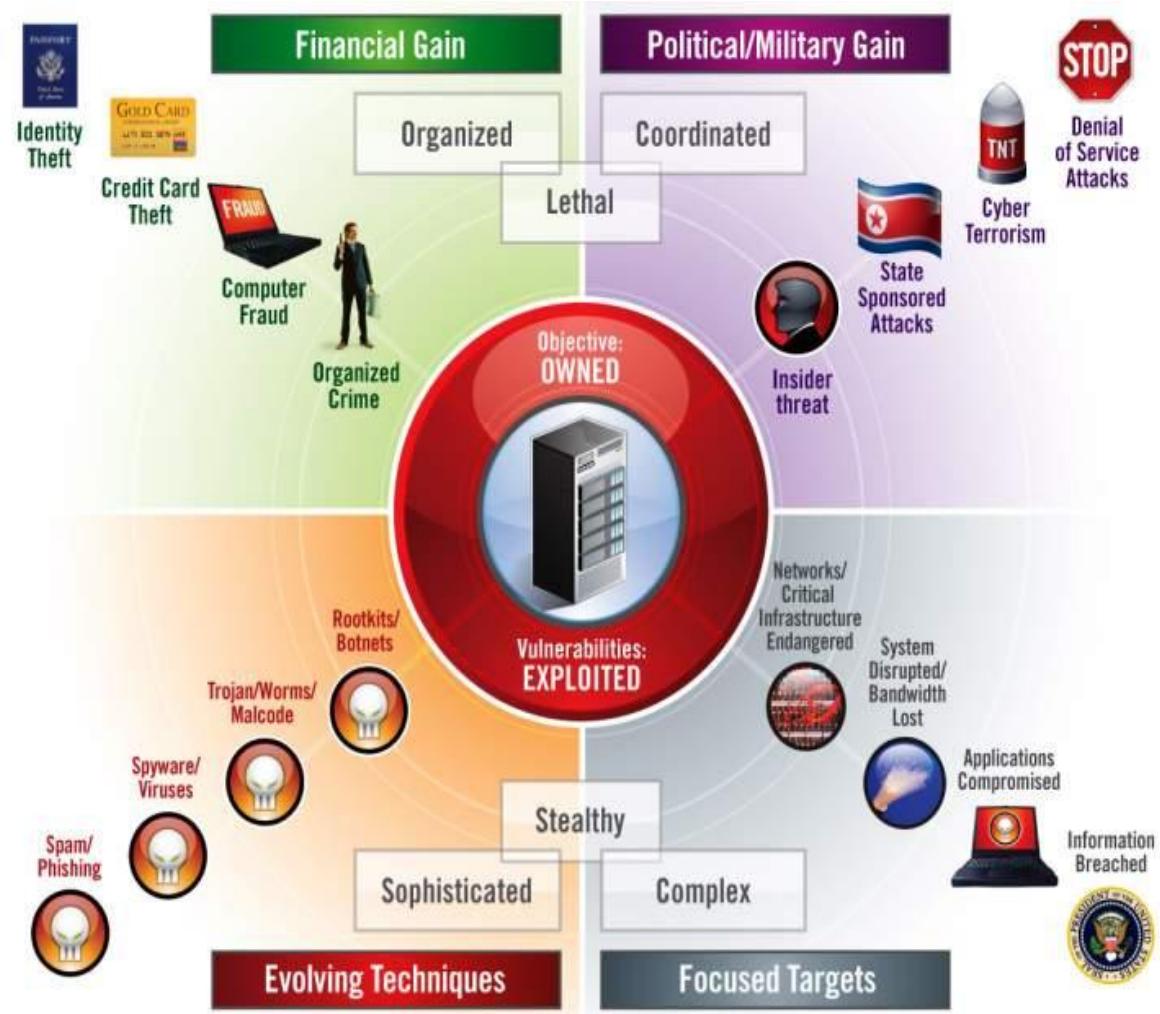
Expertise + Motivation + Attack Vector = Result



Globalization and the Borderless Internet

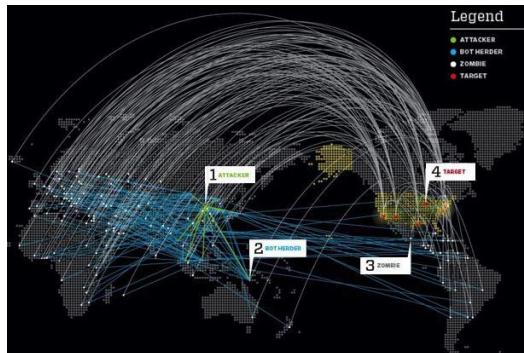
• Threat Evolution:

- 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



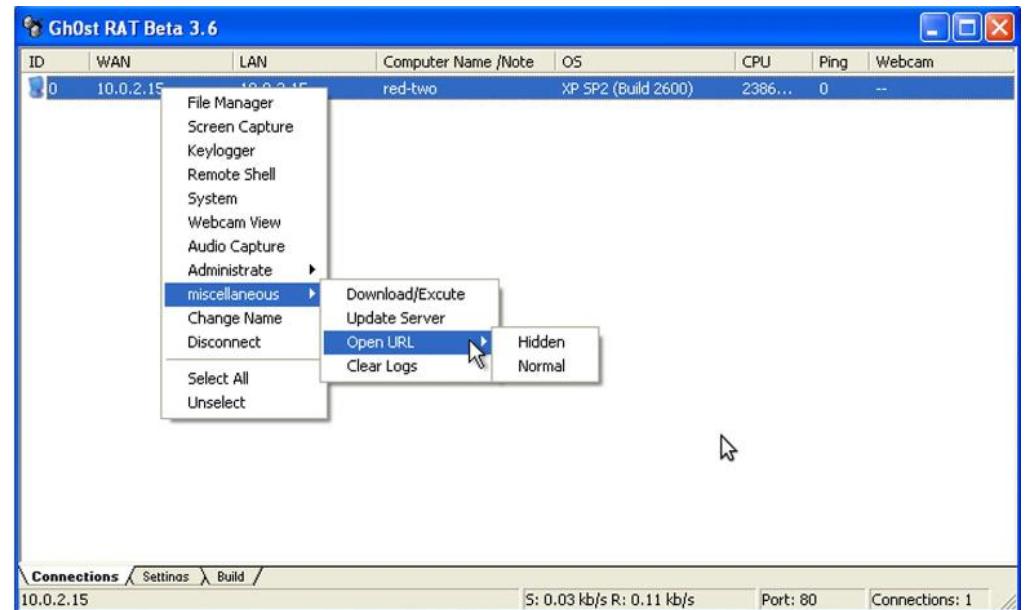
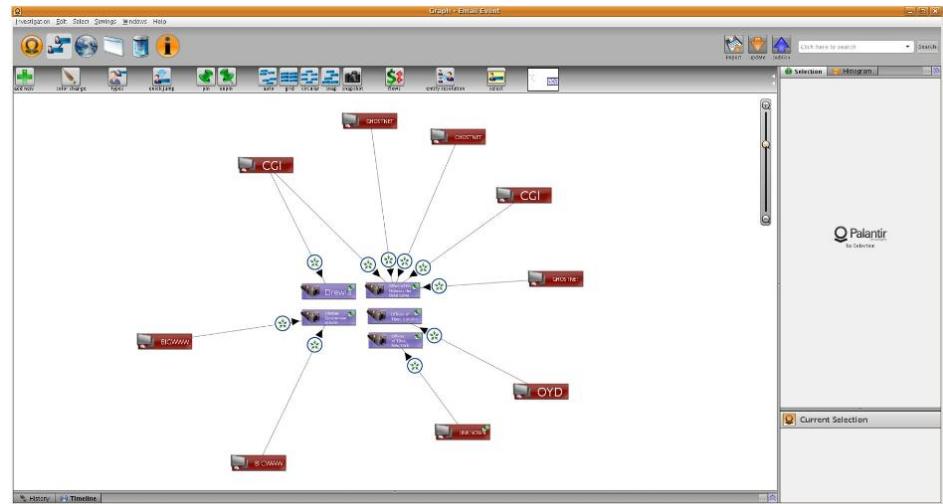
Recent Examples of DDoS & Web Defacements

- 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



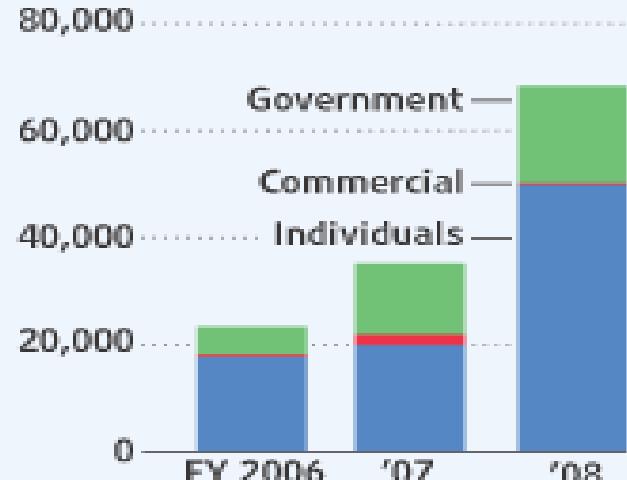
Recent Examples of Corporate

- 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

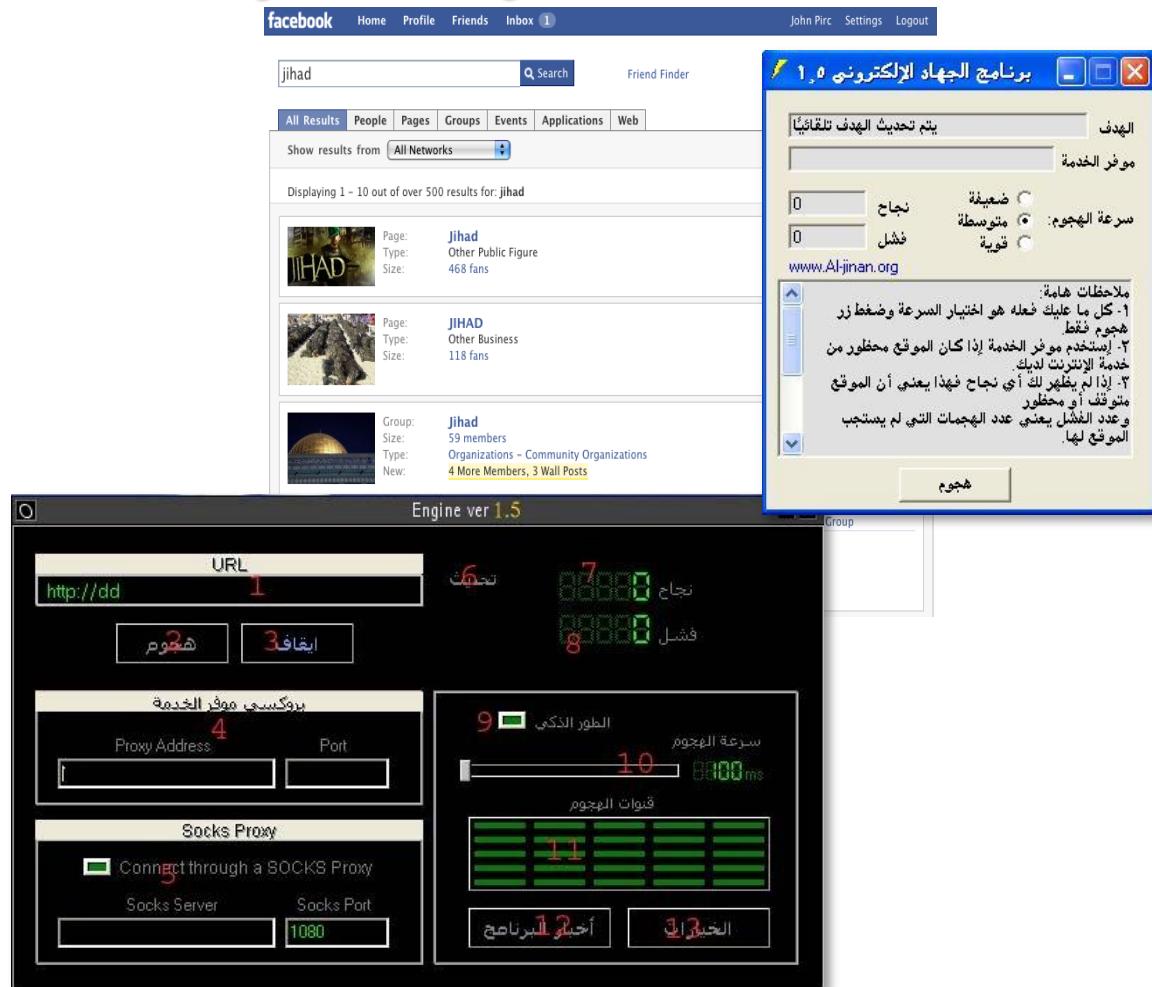
- Insider Threat & Unauthorized Access
 - Computer system detecting pipeline leaks for three oil derricks off the Southern California coast disabled.
 - Queensland sanitation system – incident caused the release of millions of gallons of raw sewage
 - Laid Off Employee – plant temperature at risk
- Slammer 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

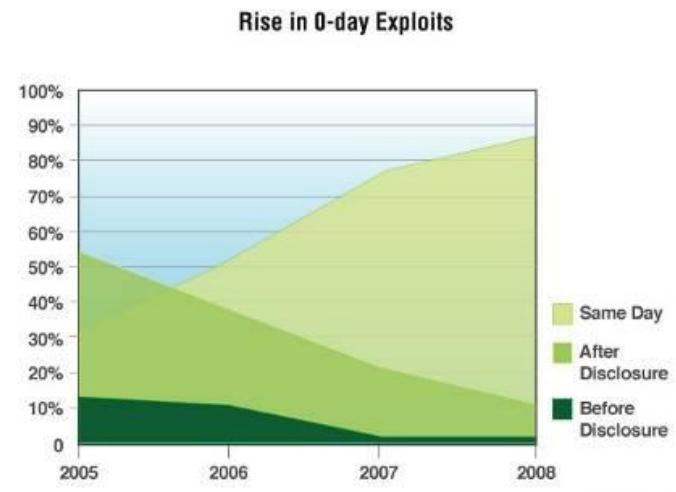
The Cyber Jihad & “Common Cause” Attack Tools

- 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

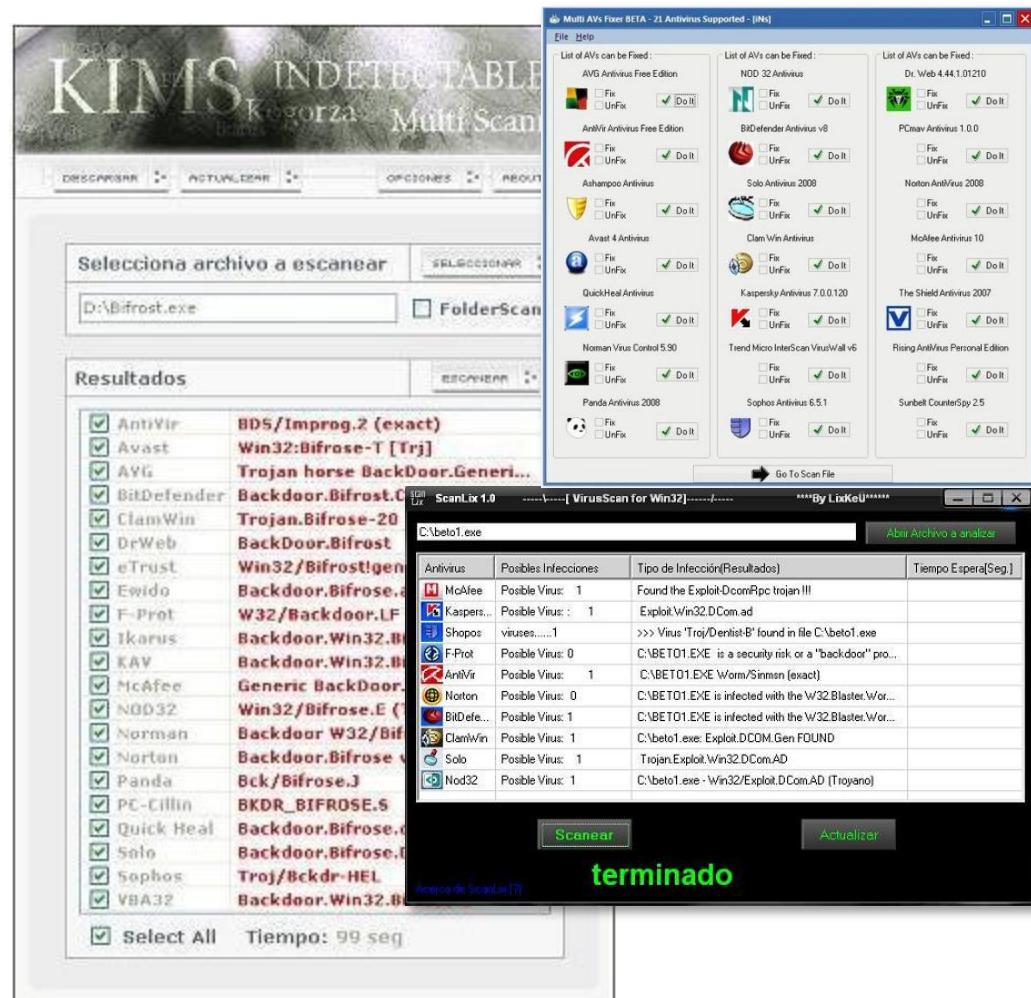
Firefox optimized version of MS06-006 exploit

/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

Country	Rating
Russia	7099 56%
United States	1641 13%
Germany	1504 12%
Netherlands	492 4%
Ukraine	237 2%
Brazil	196 2%
United Kingdom	152 1%
Spain	138 1%
Belgium	126 1%
Turkey	101 1%
Totally:	80

Top 10 new countries today

Country	Rating

Country Rating
totally: 0

Top 10 Countries order by bot's reports

Country	Rating
Russia	626089 59%
United States	163156 15%
Germany	63896 6%
Brazil	24697 2%
Ukraine	20728 2%
Spain	19229 2%
Netherlands	13215 1%
United Kingdom	11816 1%
Taiwan	11541 1%
Turkey	10173 1%
Totally bot's reports:	1061892

.. Professional Service ..

Мы не продаем безопасность -
мы ее обеспечиваем.

Обеспечивая безопасность -
предоставляем свободу!

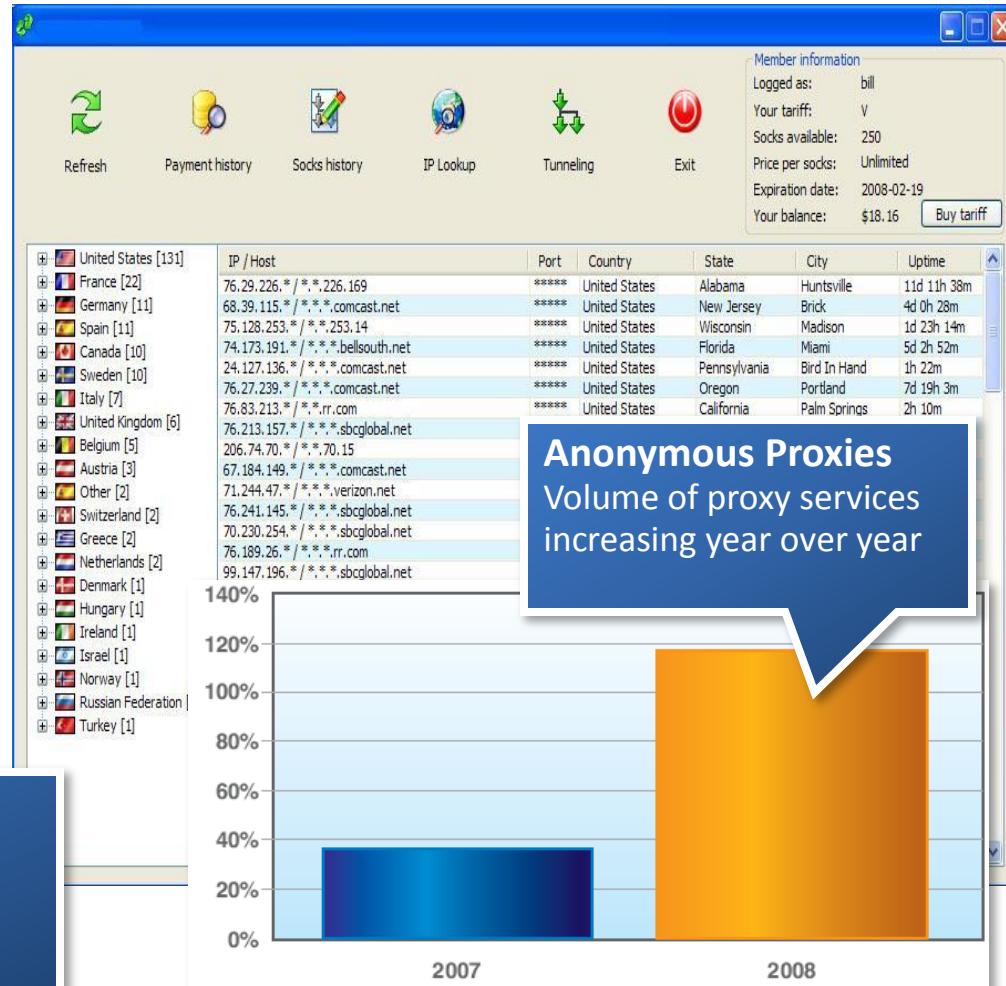
- ▶ Encryption - Secures Internet Connection
- ▶ Fast Speed - Not more than 30 Clients per server
- ▶ Compression - Rises your Connection Speed
- ▶ Compression - Less Traffic, Cheaper GPRS

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.

Anonymous Behavior



Localizing attacks

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



"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.

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."

Авторизация

Логин

Пароль

Статус перевода

Код

SQL Injection Attack Tools

地址: http://www.google.cn/search?as_q=inurl:asp id&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

包含以下全部的字词: inurl:asp id 100 项结果

包含以下的完整字句:

包含至少一个下列字词:

小提示:

搜索结果

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.

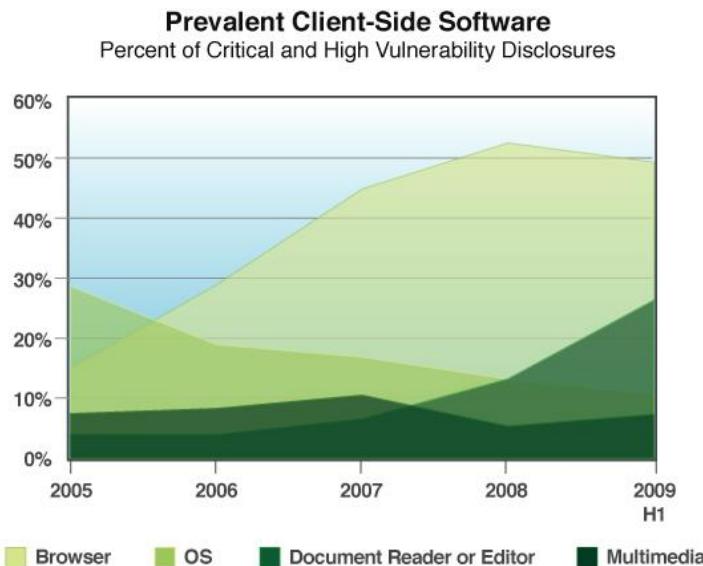
扫描页面漏洞 仅扫描地址栏 停止扫描 强行终止

安全漏洞 服务器错误

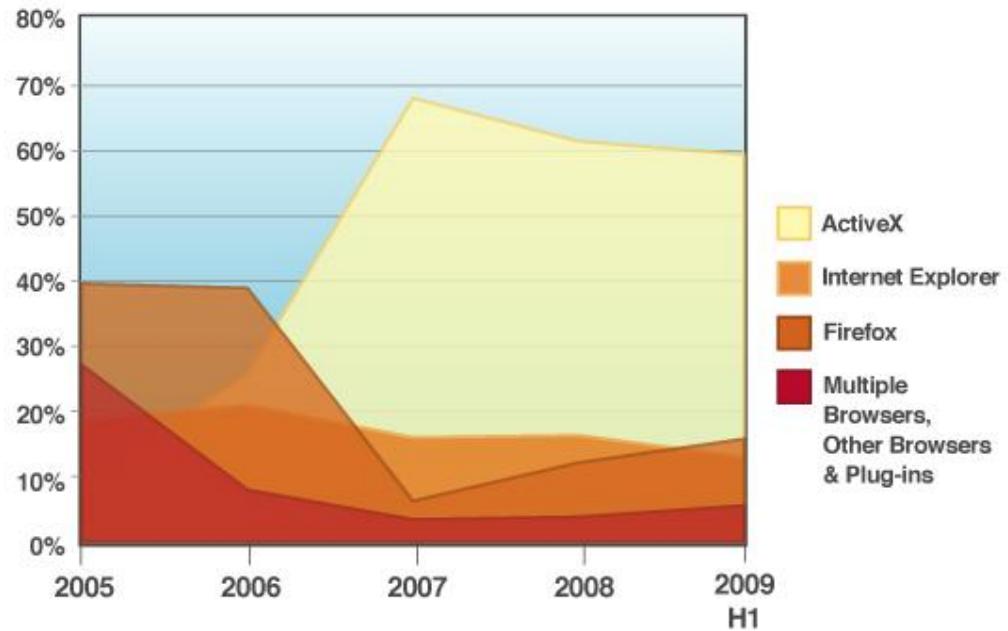
完整URL	响应时间	可利用度	确定漏洞方式	注入方式	注入类型	数据库	页面标题	错误指纹
http://www.cn/info.asp?id=6	1609	6	aND 8=8 + aND 8=3	AND	数字型	未探测	康馨催乳公司 催乳	80040e21,;
http://www.bertech.com/shownews.asp?5281	5281	5	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.bertech.com/ProductShow.6796	6796	5	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.u.com/sinonews/list.asp?i438	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/qym1/corporation_y2672	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=644610	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	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=1125078	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-	

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 1st time.**



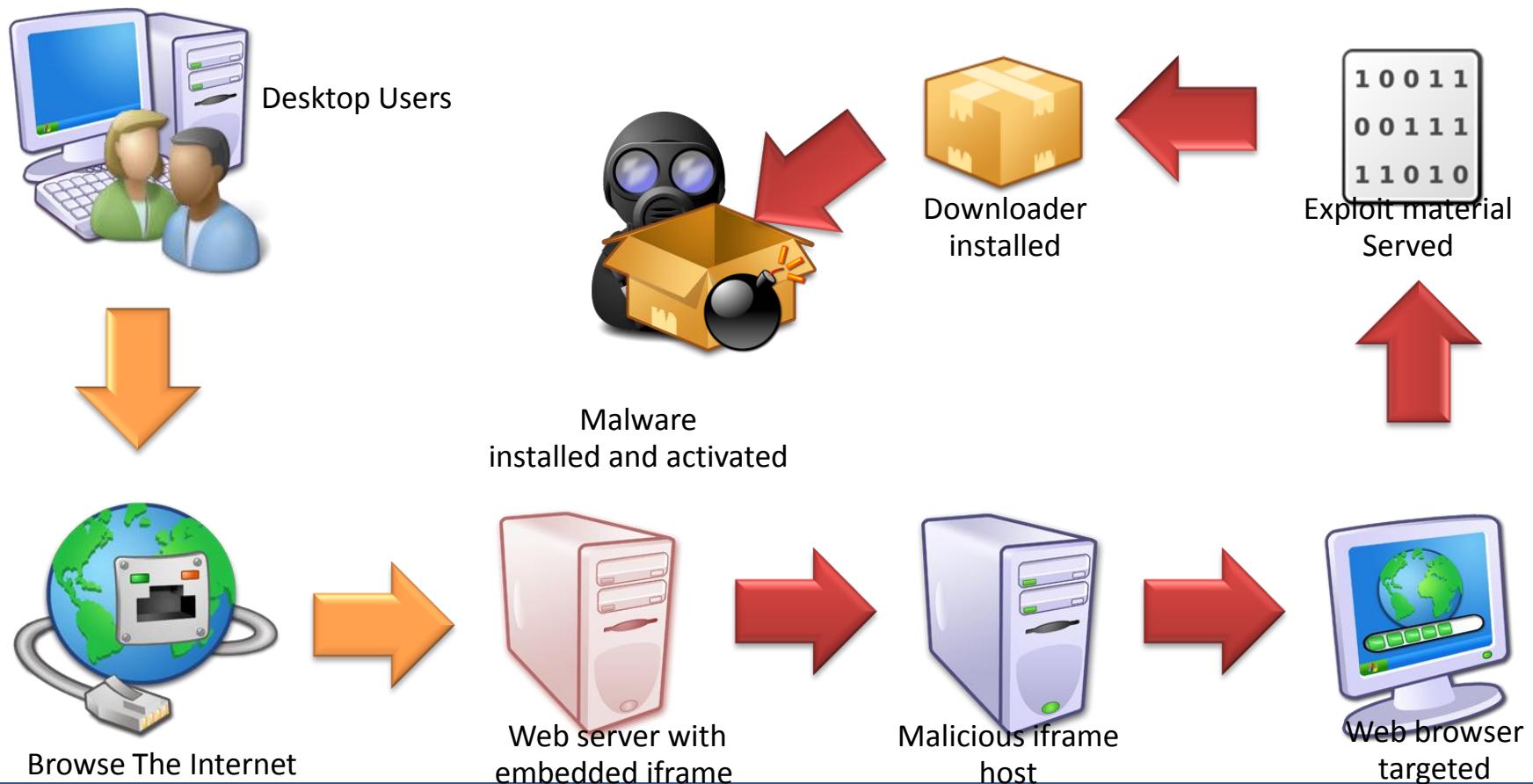
Browse-Related Software
Percent of Critical and High Vulnerability Disclosures



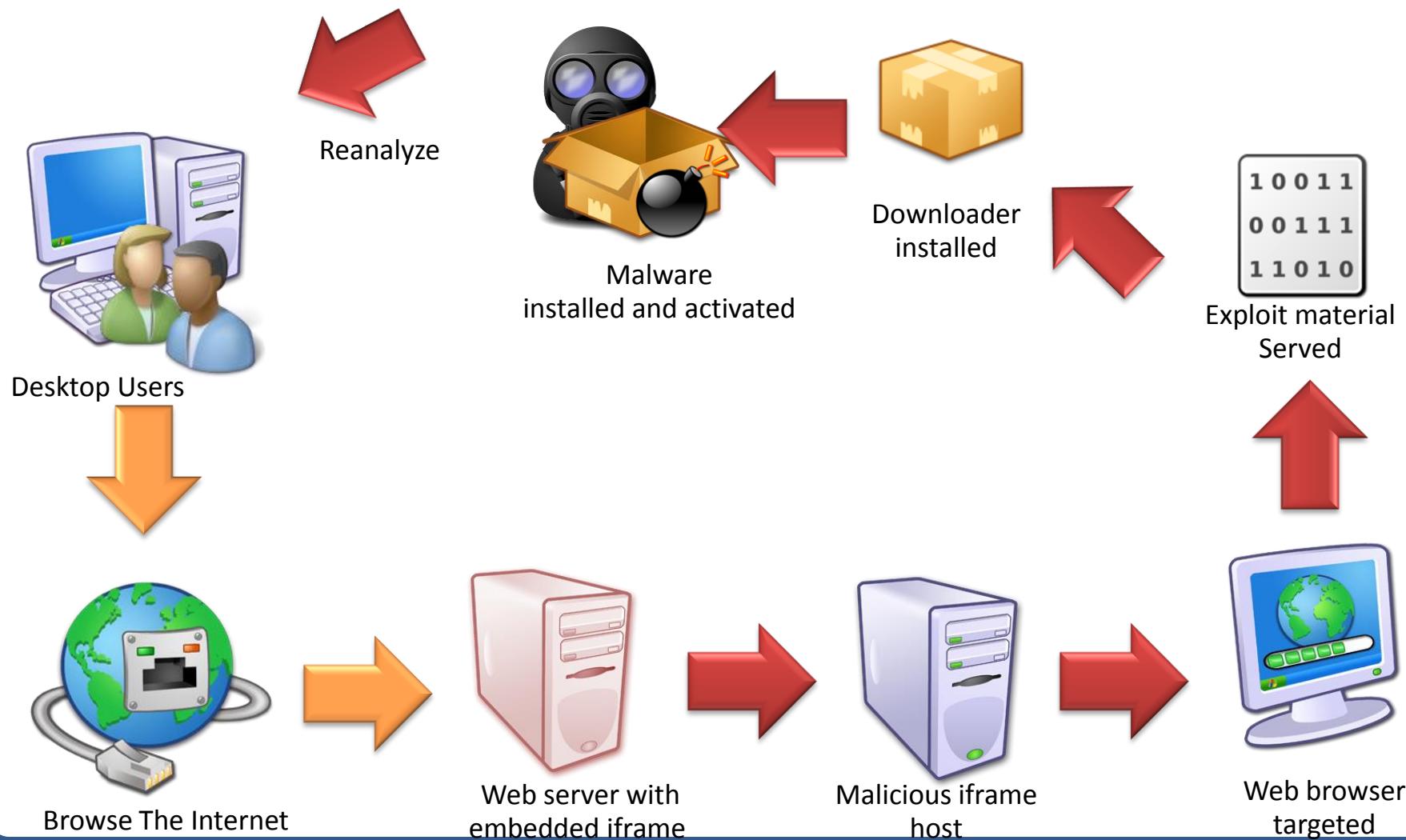
High Value Targets

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

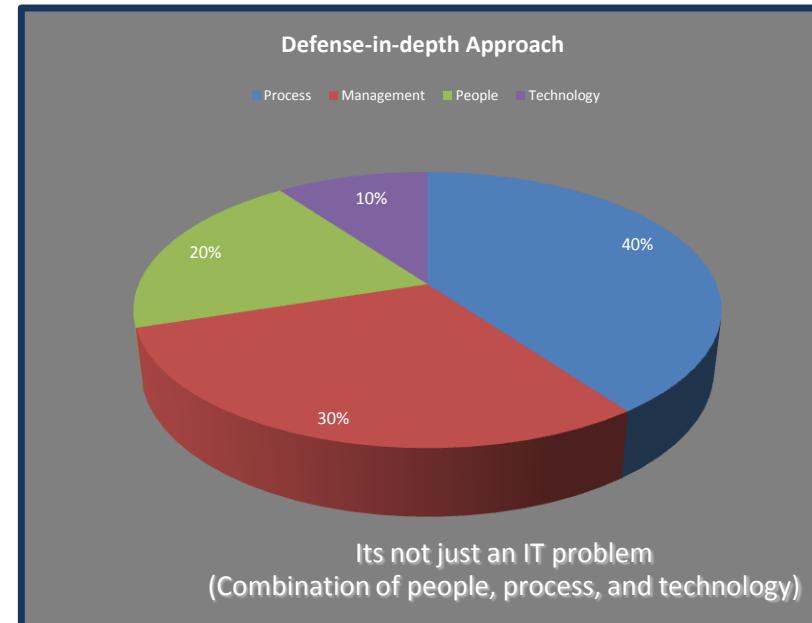
Who did it and why?

- 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

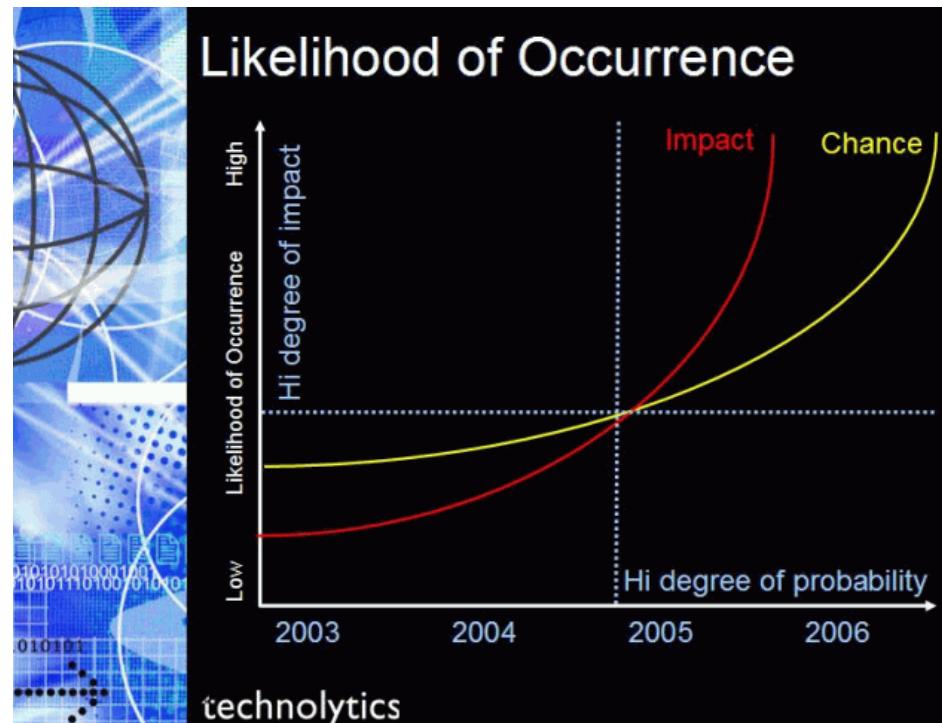
- SDLC
 - Assessment / Prevention
- Virtual Patching
 - Exploit protection from within the network
 - Provides coverage while software patches are deployed
- Deep Content Inspection
 - Network traffic and critical control protocols inspected for malicious and rogue commands
 - Complete Visibility



Summary

Summary

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



Thank You!

Matthew Pour, CISSP
matthew.pour@bluecoat.com