ACTIVE DEFENSE

DAVI OTTENHEIMER

DAVID WILLSON

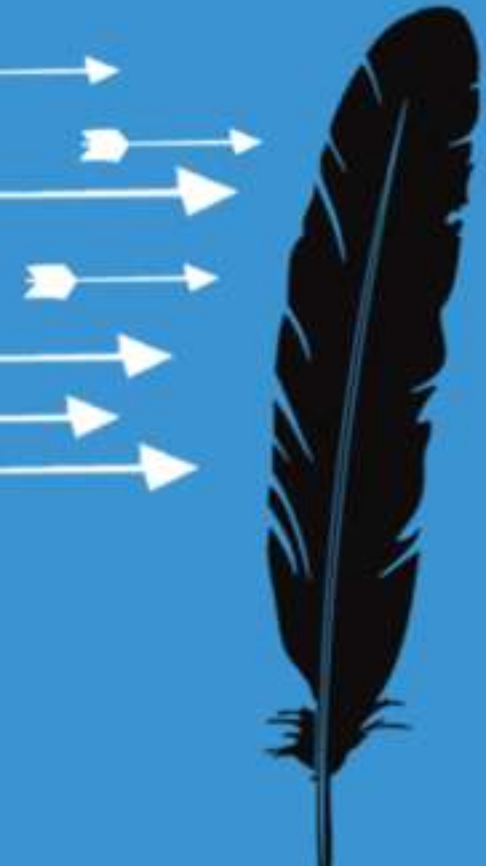
Session ID: HT-302

Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

Agenda

- Emerging Attacks
- Current Defenses
- How to Build an Active Defense



Attacks

A Study of Attacks

- Motive
- Means
- Opportunity

Attack - Motive

- Of MICE and MEECES
  - Money
  - Entertainment
  - Ego
  - Cause
  - Entrance to Social Groups
  - Status

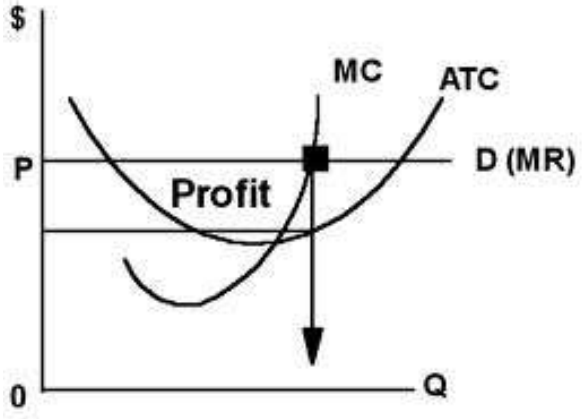
Hackers are stepping up the intensity of their attacks, moving from "disruption" to "destruction" of key computer systems.

- General Keith Alexander, NSA Director and Commander of US Cyber Command

http://phys.org/news/2012-10-hackers-shifting-destruction-cyber-chief.html
http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf

Attack - Motive

- (Anti)collaborative
- Collaborative
- Hyper-Collaborative

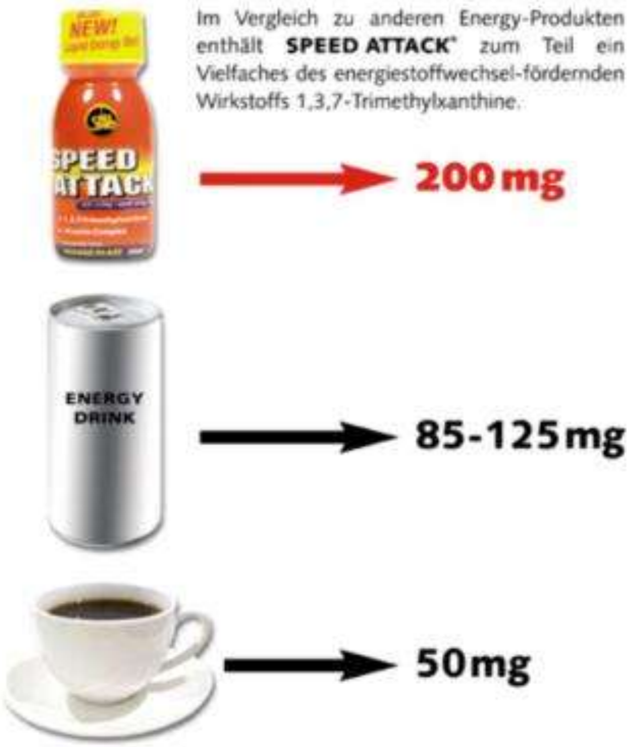


h@ctivism

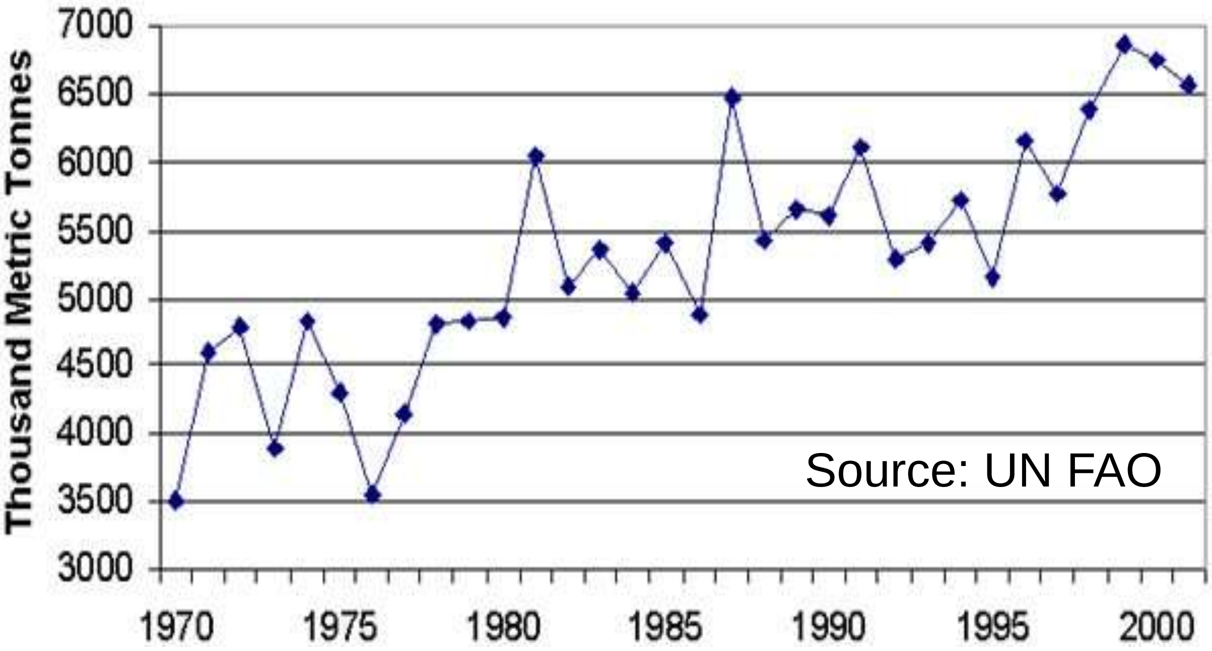
Attack - Means

- Getting easier all the time

Commodification of caffeine



Im Vergleich zu anderen Energy-Produkten enthält **SPEED ATTACK**® zum Teil ein Vielfaches des energiestoffwechsel-fördernden Wirkstoffs 1,3,7-Trimethylxanthine.



Source: UN FAO

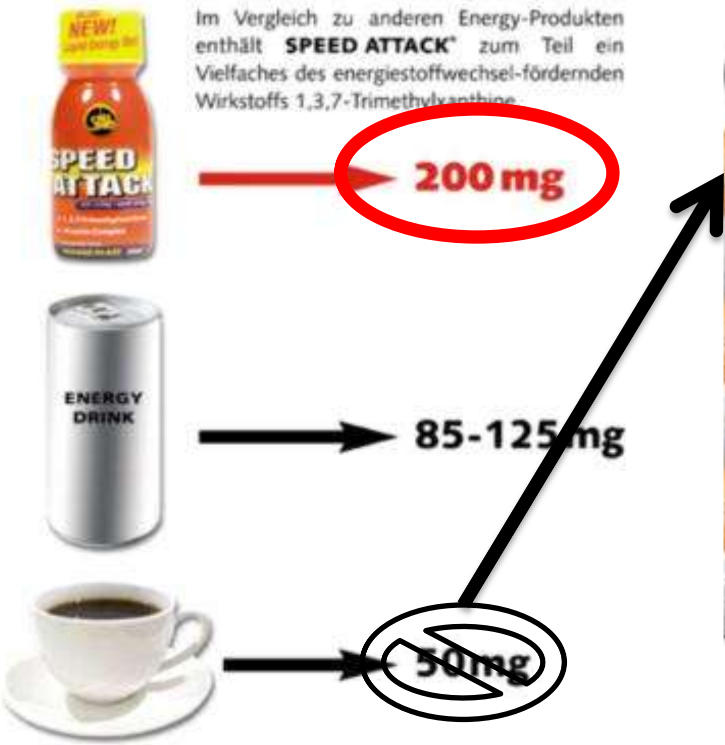
Global Coffee Consumption

http://www.fao.org/docrep/006/Y4343E/y4343e05.htm

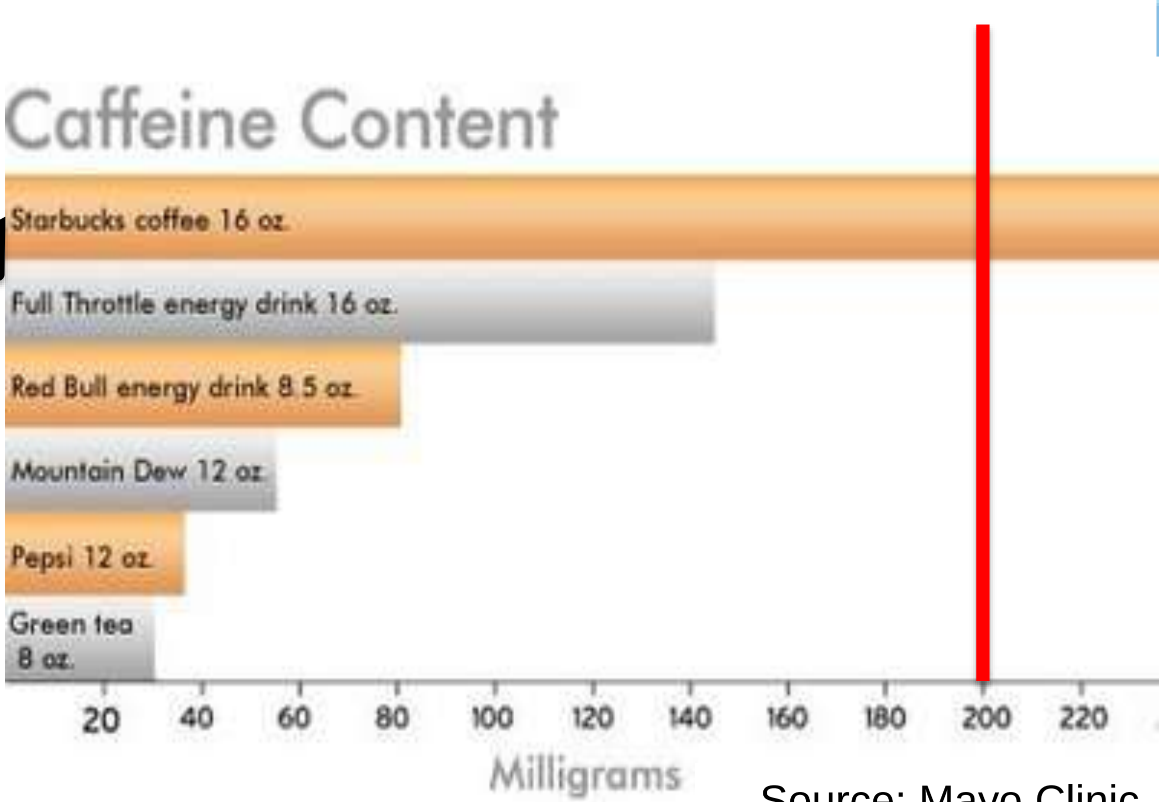
Attack - Means

- May be hidden…

Commodification of caffeine



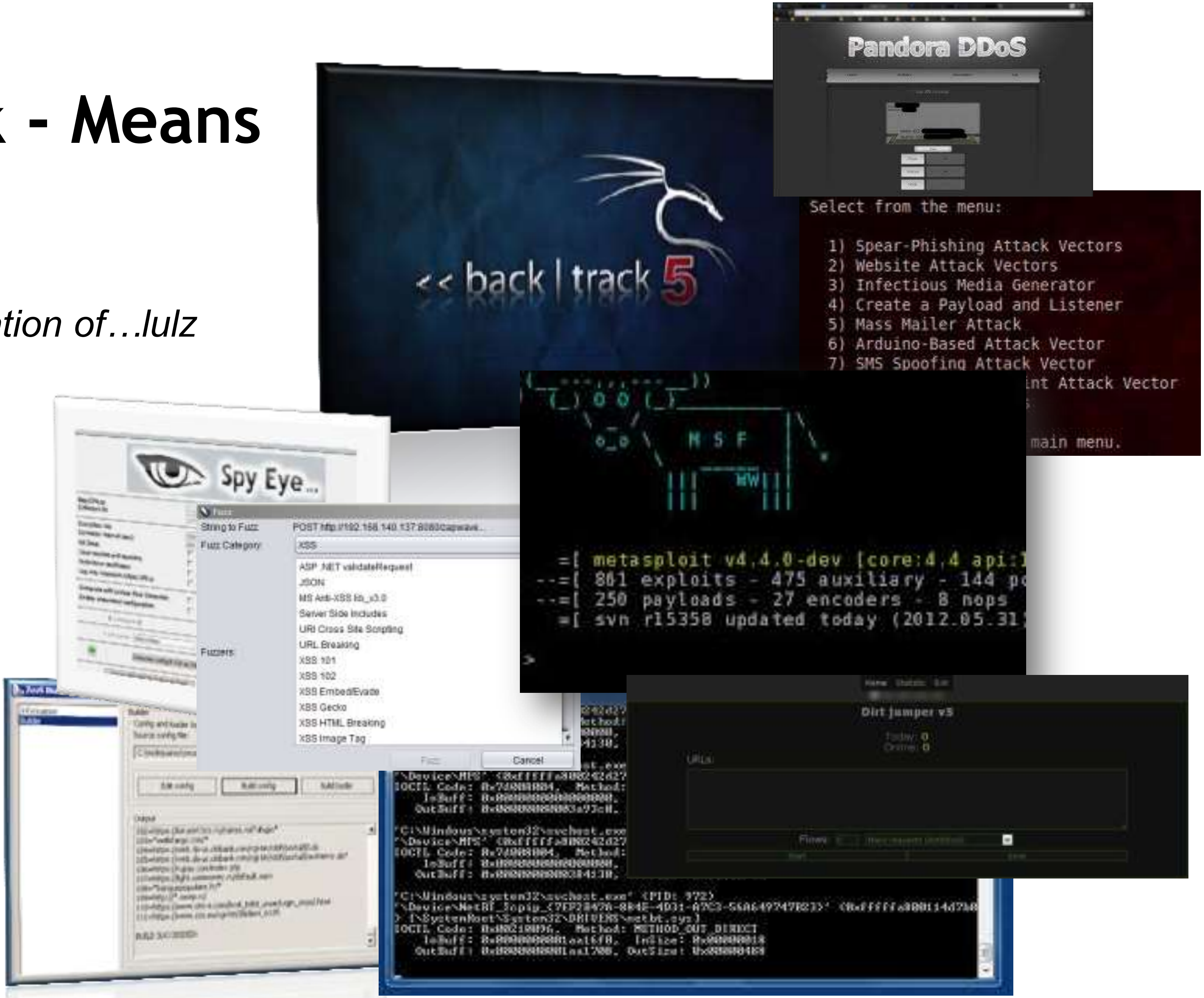
Im Vergleich zu anderen Energy-Produkten enthält **SPEED ATTACK**® zum Teil ein Vielfaches des energiestoffwechsel-fördernden Wirkstoffs 1,3,7-Trimethylxanthine.



Source: Mayo Clinic

Attack - Means

Commodification of…lulz



```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
                          int Attack Vector

                          main menu.
```

String to Fuzz: POST http://192.168.140.137:8080/capwave...

Fuzz Category: XSS

Fuzzers:
ASP .NET validateRequest
JSON
MS Anti-XSS lib_v3.0
Server Side Includes
URI Cross Site Scripting
URL Breaking
XSS 101
XSS 102
XSS Embed/Evade
XSS Gecko
XSS HTML Breaking
XSS Image Tag

```
       =[ metasploit v4.4.0-dev [core:4.4 api:1
+ -- --=[ 861 exploits - 475 auxiliary - 144 po
+ -- --=[ 250 payloads - 27 encoders - 8 nops
       =[ svn r15358 updated today (2012.05.31)

>
```

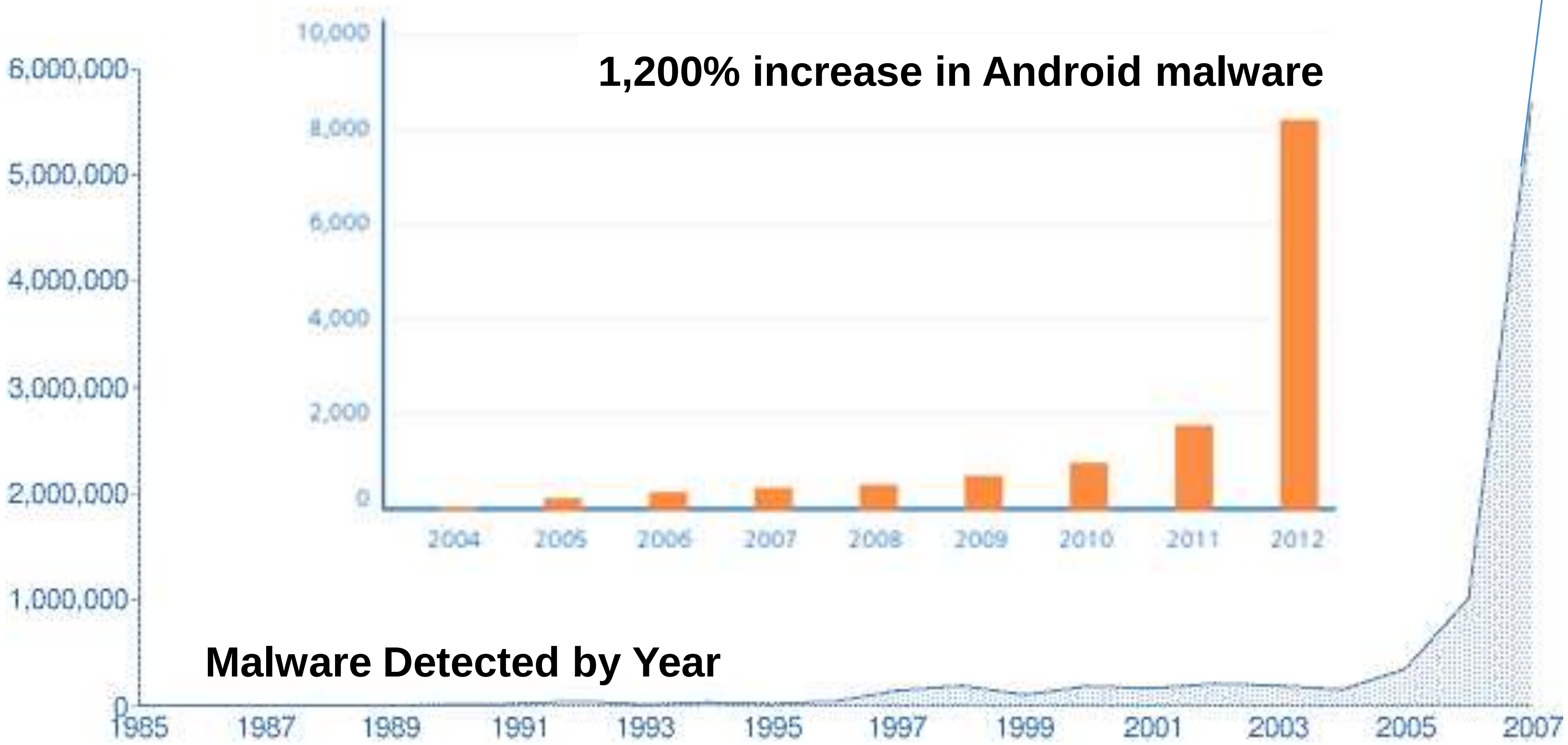
```
"\Device\MPS" <0xfffffa800242d27
IOCTL Code: 0x74008004,  Method:
    InBuff: 0x0000000000000000,
   OutBuff: 0x00000000003a93c0,

"C:\Windows\system32\svchost.exe
"\Device\MPS" <0xfffffa800242d27
IOCTL Code: 0x74008004,  Method:
    InBuff: 0x0000000000000000,
   OutBuff: 0x0000000000384130,

"C:\Windows\system32\svchost.exe" (PID: 972)
"\Device\NetBT_Tcpip_{7FF2847A-884E-4D31-A7C3-56A649747B23}" <0xfffffa800114d7b0
> [\SystemRoot\System32\DRIVERS\netbt.sys]
IOCTL Code: 0x00210096,  Method: METHOD_OUT_DIRECT
    InBuff: 0x000000000001aa16f8,  InSize: 0x00000018
   OutBuff: 0x000000000001aa1700,  OutSize: 0x00000400
```

Attack - Means

“Only 9 of the 22 tested products managed to block both variants of the exploit” (31 August 2012) *

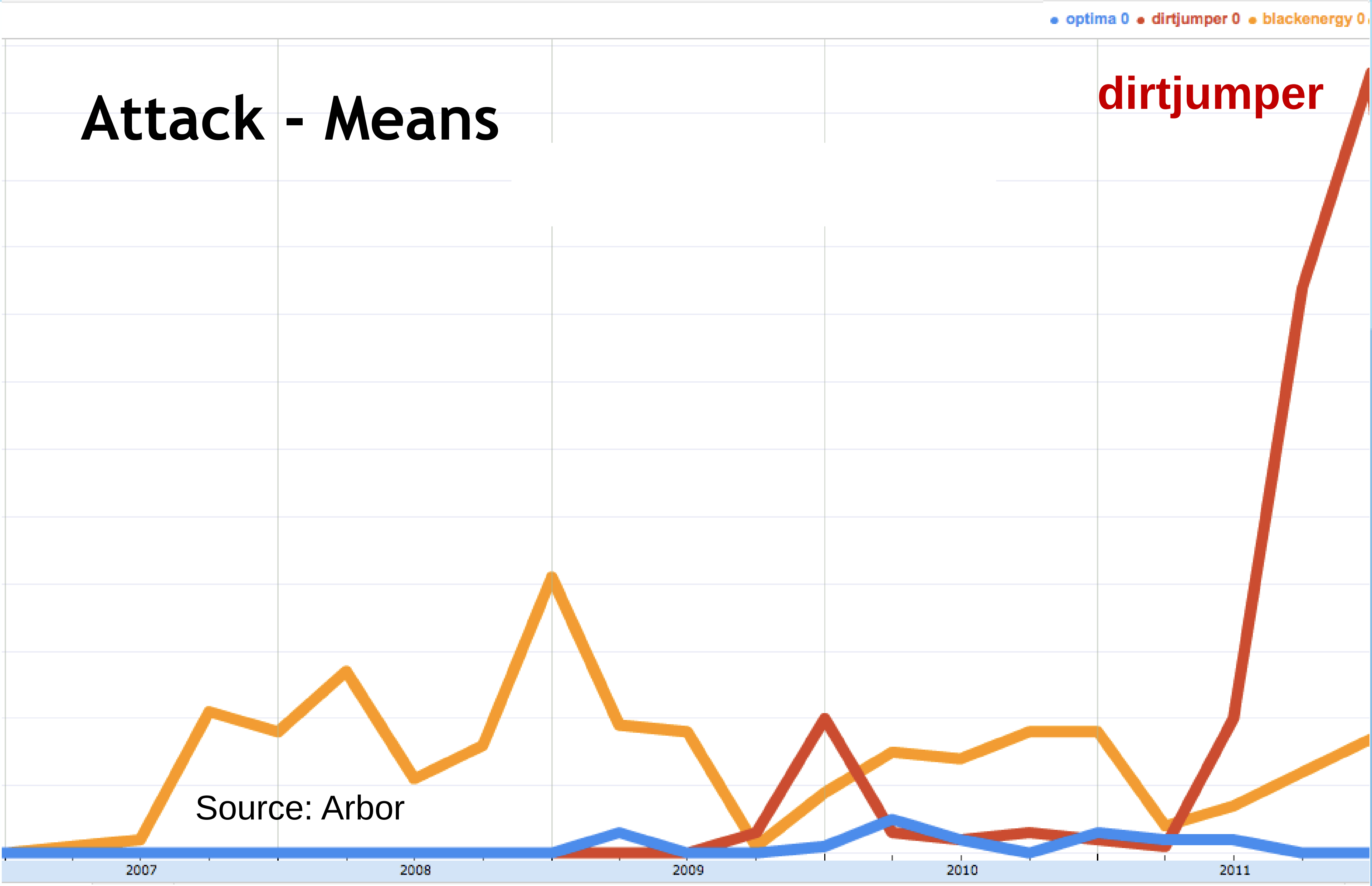


1,200% increase in Android malware

Malware Detected by Year

Sources: http://www.washingtonpost.com/wp-dyn/content/article/2008/03/19/AR2008031901439.html
* http://www.h-online.com/security/news/item/Only-9-of-22-virus-scanners-block-Java-exploit-1696462.html
http://www.scmagazine.com/report-finds-1200-percent-boom-in-android-malware/article/242542/

Attack - Means



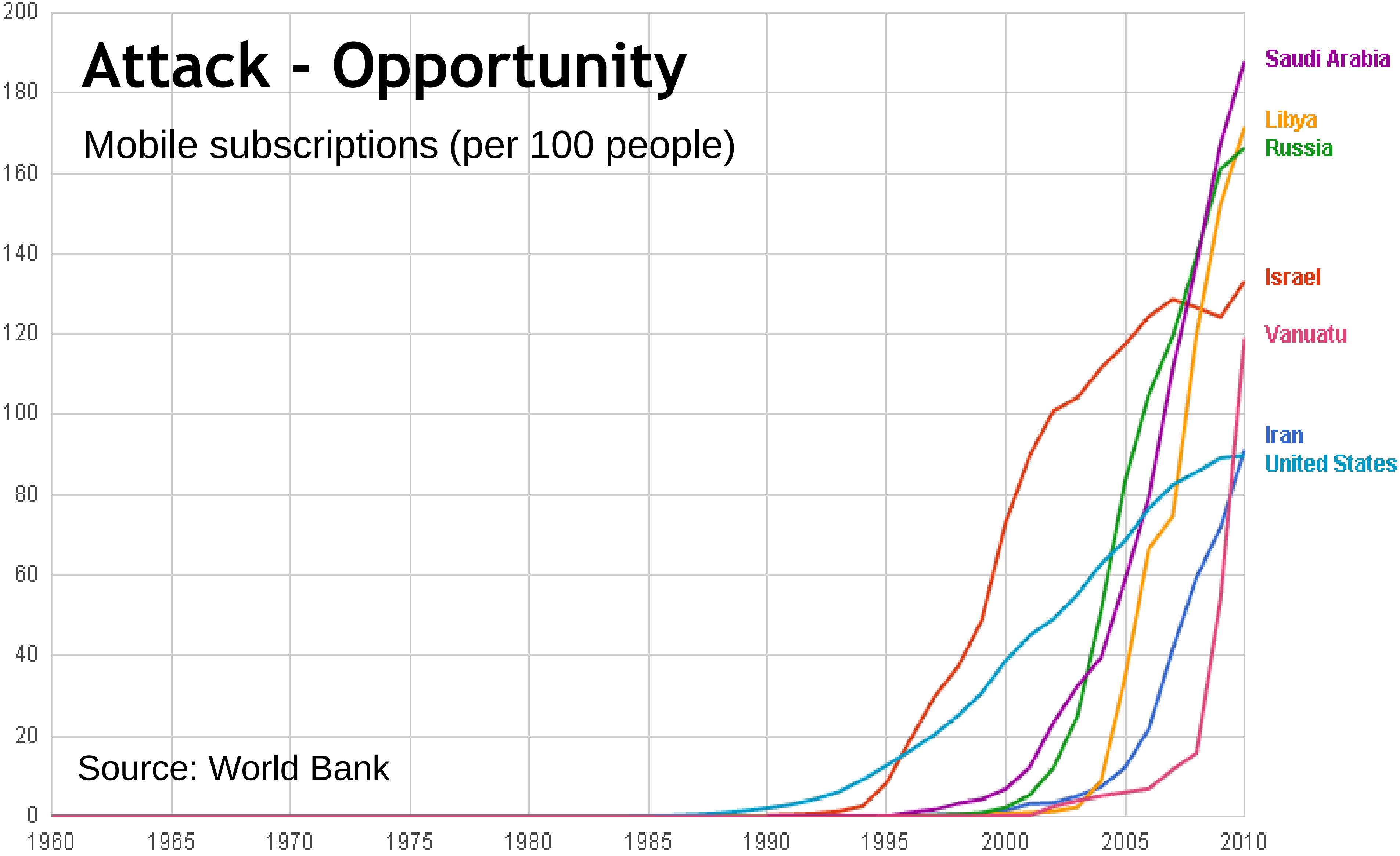
dirtjumper

Source: Arbor

http://ddos.arbornetworks.com/2012/05/dirt-jumper-ddos-bot-increasingly-popular/

Attack - Opportunity

Mobile subscriptions (per 100 people)

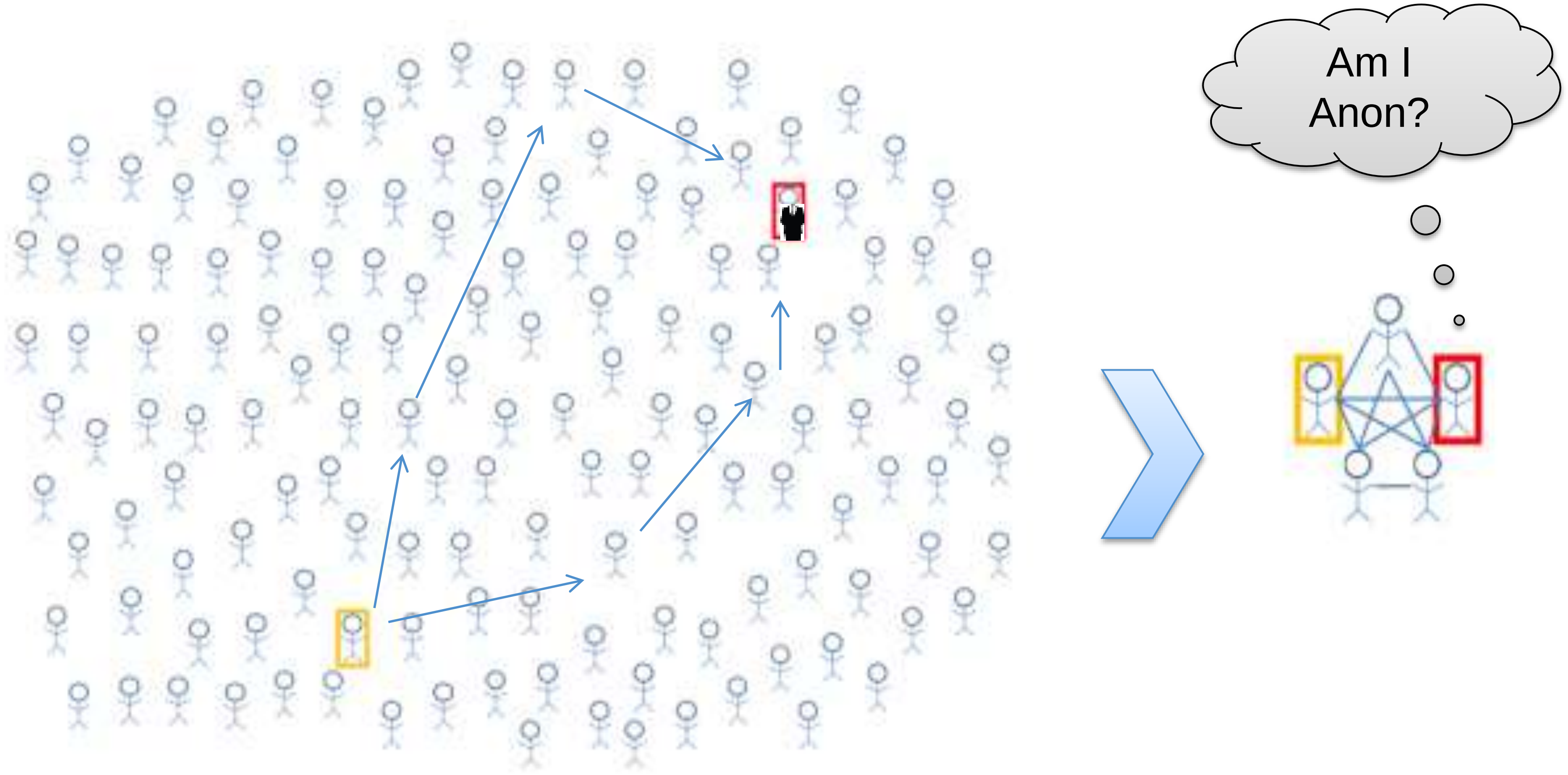


Source: World Bank

http://www.google.com/publicdata/explore

Davi Ottenheimer
David Willson

Attack - Opportunity

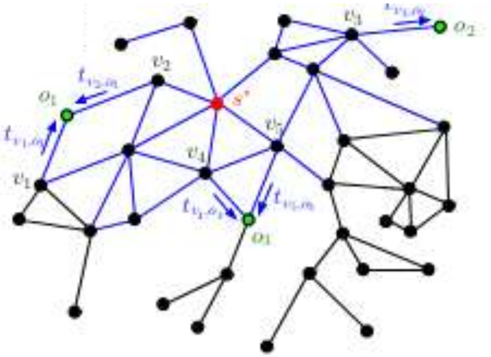


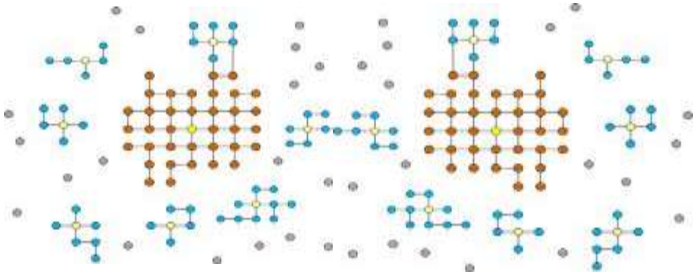
Am I Anon?

http://bhc3.com/2010/01/19/

Attacks

- Opportunity
  - More Connectivity
  - More Links / Social Networks
  - More Personal Data Available in More Places
  - Outsiders Become Insiders (e.g. Cloud)





http://www.flyingpenguin.com/?p=18259

Pop Quiz

- Stuxnet
- Gauss
- Flame
- Zeus

"I think what you're talking about is a moral crime."

– Marcus Ranum

"…a good tool to allow nation states to exert force without having to blow people up."

– Jeff Moss

"Ultimately the ethics of this don't really matter – the decision has been made and this kind of stuff is going to be unavoidable."

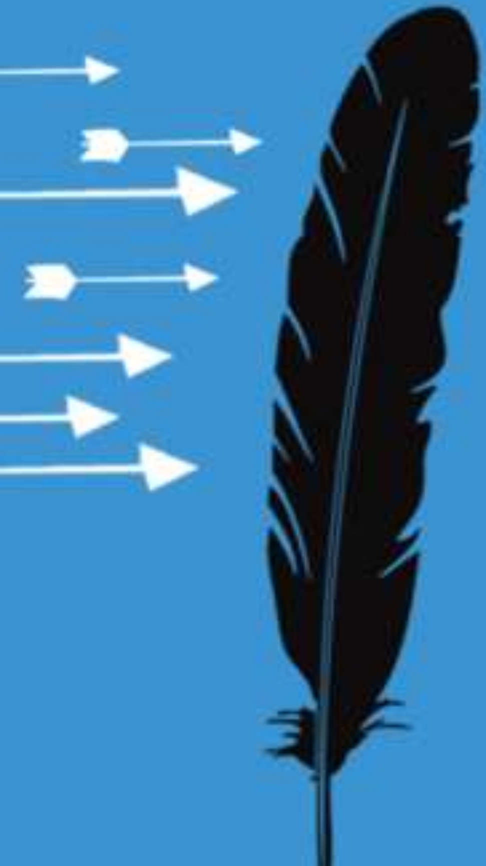
– Mikko Hypponen

http://www.theregister.co.uk/2012/07/26/stuxnet_moral_crime/

“The whole point of the doomsday machine is lost if you keep it a secret!”

“Why didn't you tell the world?”

http://www.flyingpenguin.com/?p=9621



Defense

Philosophy of Self-Defense

This makes him willing to quit a condition, which, however free, is full of fears and continual dangers: and it is not without reason, that he seeks out, and is willing to join in society with others, who are already united, or have a mind to unite, for the mutual preservation of their lives, liberties and estates, which I call by the general name, property.

-- John Locke, 1689, *Two Treatises of Government*

1. **Imminent Danger**
2. **Immediate Defense Believed Necessary to Prevent Danger**
3. **No More Action Than Necessary to Defend Against Danger**

http://books.google.com/books?id=3e_JisWPODoC&pg=PA109

Philosophy of Self-Defense

- Legal Hind-sight
  - **Beckford v R (1988) 1 AC 130**: A defendant is entitled to use reasonable force to protect himself, others for whom he is responsible and his property. It must be reasonable.
  - **R v Owino (1996) 2 Cr. App. R. 128 at 134**: A person may use such force as is [objectively] reasonable in the circumstances as he [subjectively] believes them to be.
- InfoSec Fore-sight
  - Threat Prediction
  - Vulnerability Assessment

Philosophy of Self-Defense

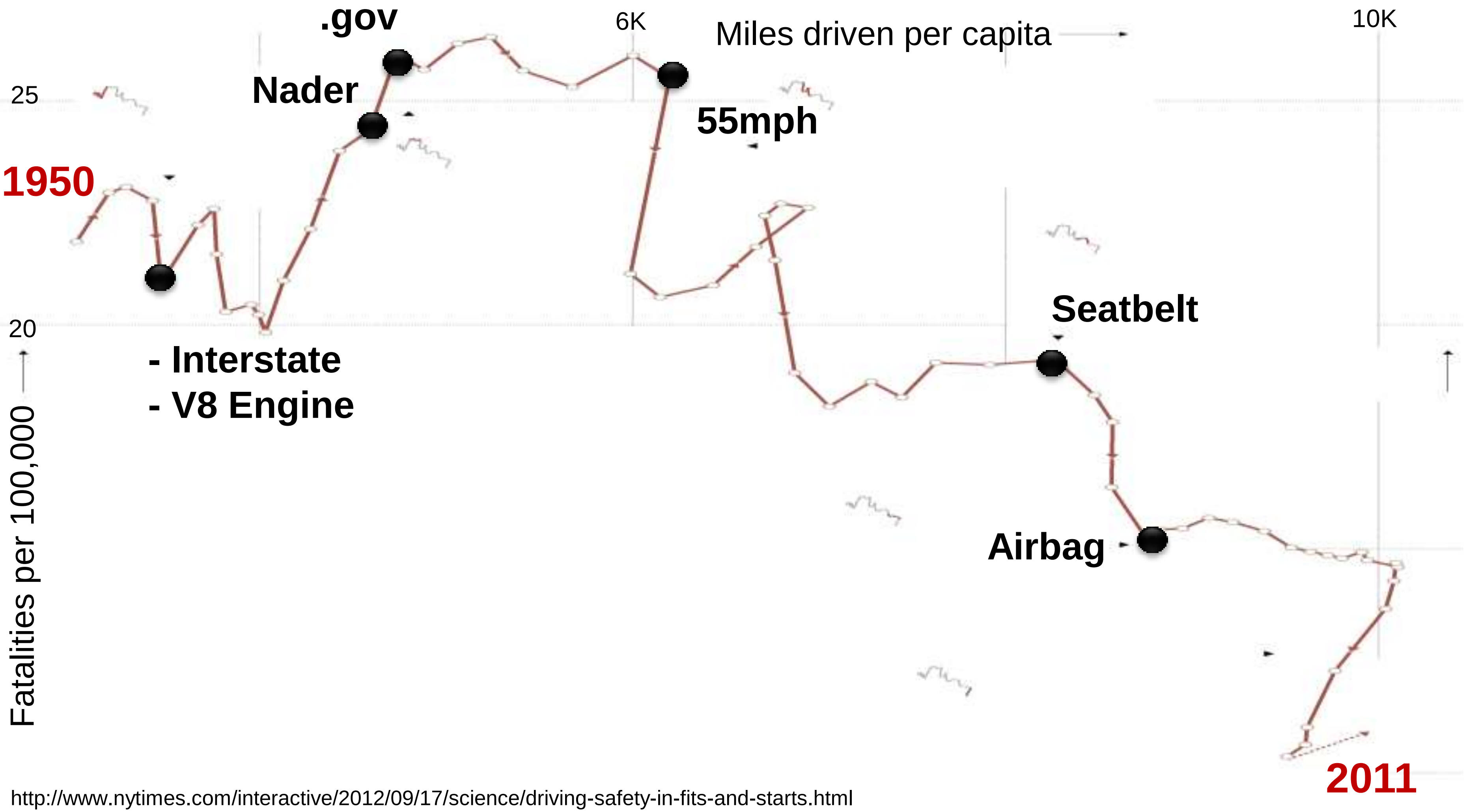
"…in line with their rules of engagement…"

"Turkey will never leave unanswered such kinds of provocation by the Syrian regime against our national security"

-- Turkish Prime Minister Tayyip Erdogan's office

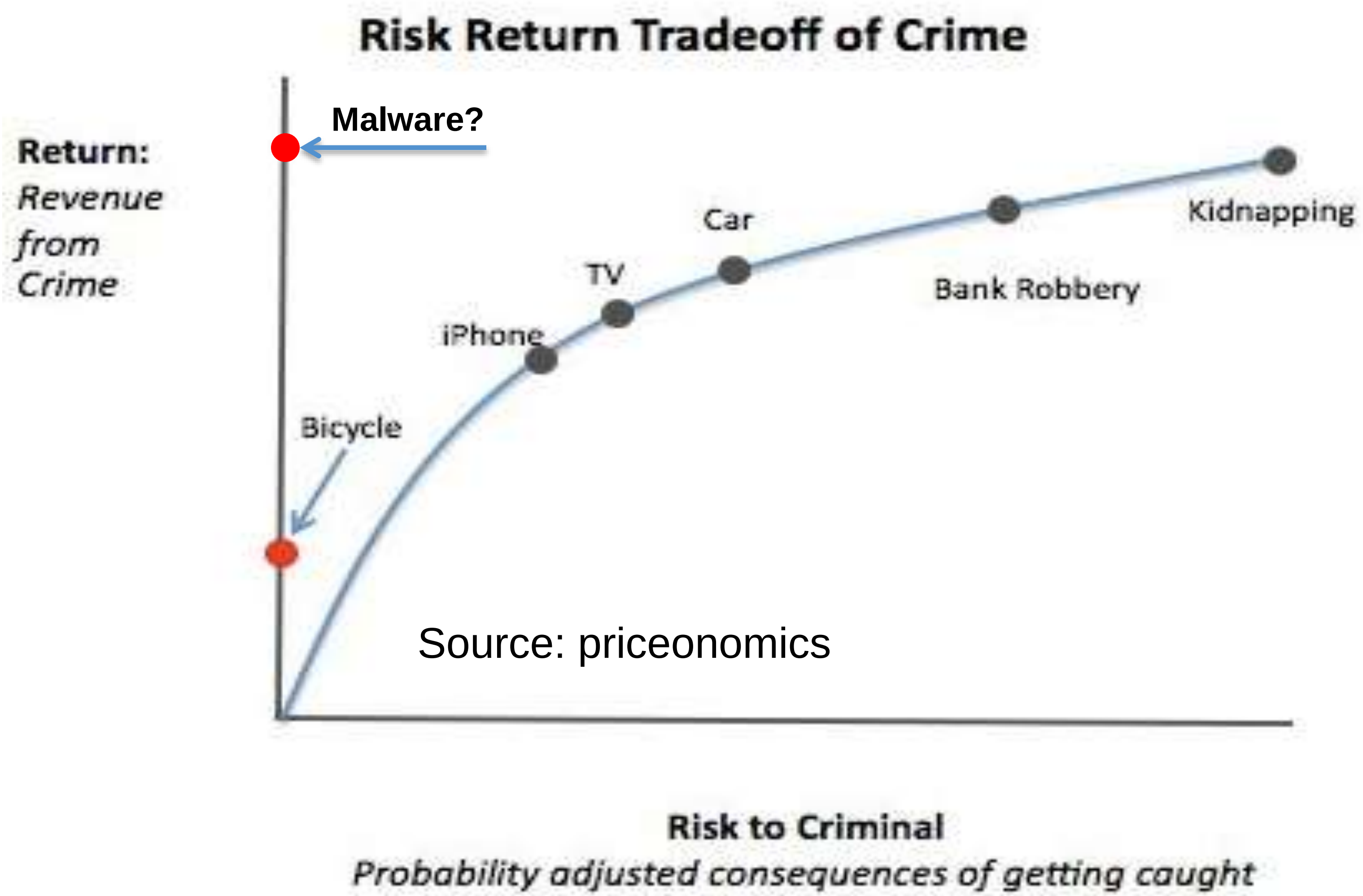
http://www.jpost.com/MiddleEast/Article.aspx?id=286516

Economics of Defense - Accidental Harm



http://www.nytimes.com/interactive/2012/09/17/science/driving-safety-in-fits-and-starts.html

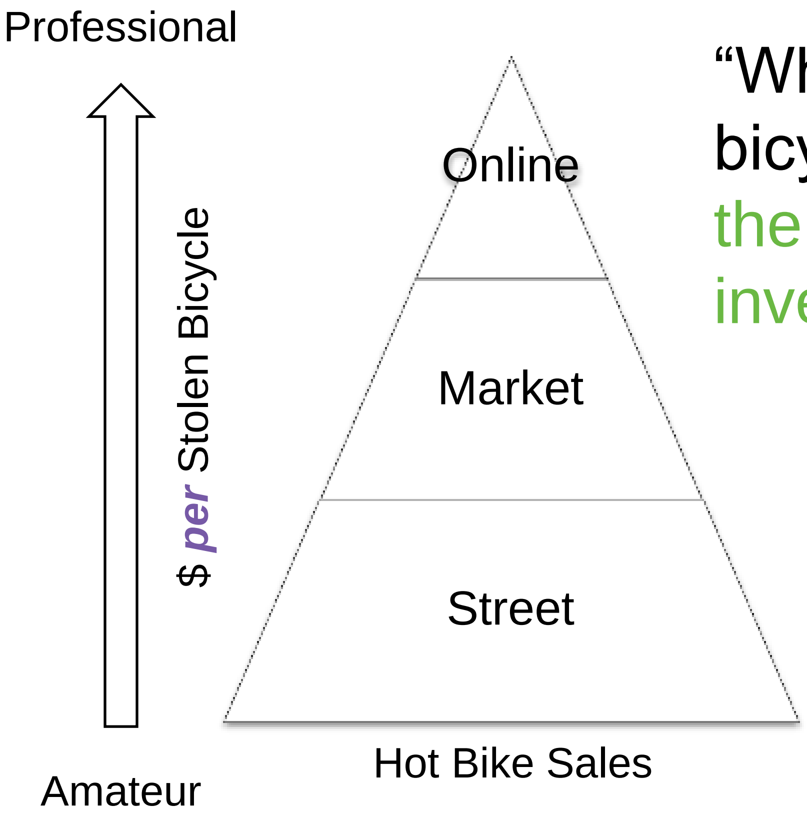
Economics of Defense - Intentional Harm



Source: priceonomics

http://blog.priceonomics.com/post/30393216796/what-happens-to-stolen-bicycles

Economics of Defense - Intentional Harm



"While the police may not penalize bicycle thieves, it's becoming easier for the person whose bike was stolen to investigate the bike theft themselves."

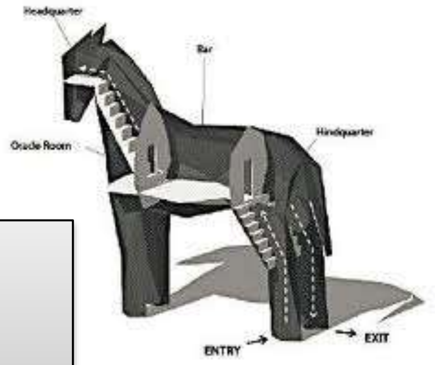
This is making it harder for the amateur thief to casually flip a stolen bike."

http://blog.priceonomics.com/post/30393216796/what-happens-to-stolen-bicycles

Economics of Defense - Malware

2009 Kaspersky on .br Banking Trojan Horses

- Motive: Low income population drawn into crime
- Means: Delphi (not taught in University)
- Opportunity: 1/3 of Brazil (70m) online. eBanking:
  - Banco do Brasil – 7.9mil
  - Bradesco – 6.9mil
  - Itau – 4.3mil



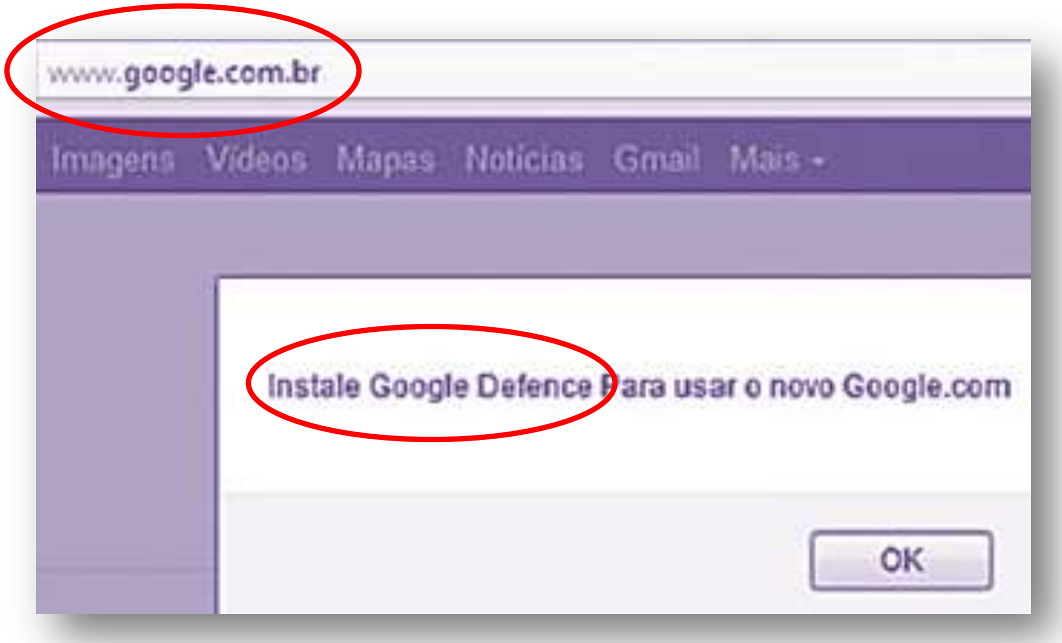
> “…banks wish to avoid public investigation of such thefts. In order to protect their reputation, banks prefer to compensate customers for losses incurred by infection with malicious code…”

http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans

Economics of Defense - Malware

2012 Kaspersky on .br **4.5mil** ADSL device CSRF

```
<form action=http://192.168.1.1/password.cgi; method="POST" name="form">
<input type="hidden" name="sysPassword" value="newpassword">
```



www.google.com.br

Instale Google Defence Para usar o novo Google.com

"…all of them in sunny, beautiful Brazil"

http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems

Economics of Defense - Malware

2012 Kaspersky on .br **4.5mil** ADSL CSRF

- Motive: Steal banking credentials
- Means: Public Disclosure 2011-03-04 - Comtrend ADSL Router CT-5367 C01_R12 Remote Root*
  - `dispara.sh:  if [ $ativos -le $simultaneos ];`
  - `roda.sh: curl $copts http://$ip_completo/password.cgi...dnscfg.cgi`

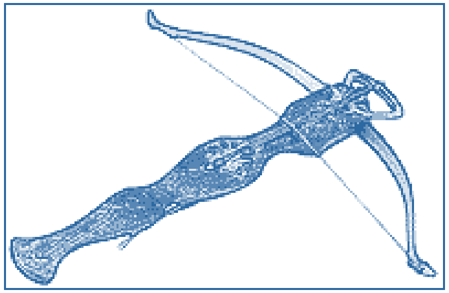
    ```
    echo $ip_completo >> modem-owned.log
    ```
- Opportunity: Scanned IP ranges on Internet (5 of 6 known vulnerable routers sold in Brazil and used by Brazil's National Telecommunications Agency)

ANATEL
Agência Nacional
de Telecomunicações

* http://www.exploit-db.com/exploits/16275/

Defense Law

- Who has the job of defense?
- Who defines what is reasonable?
- Can a higher authority defend you?
  - If No: are you responsible to defend yourself?
  - If Yes: what level and by which laws do you abide?



- 1097 Pope Urban II bans the crossbow
- 1139 Pope Innocent II bans the crossbow
- 2007 Chester MP: "…a Welsh person found within the city walls after sunset can be taken out with a crossbow"

http://www.bbc.co.uk/dna/place-nireland/A2866061
http://www.discoverchester.co.uk/BattleofChester616AD.html

Defense Law

- European and International Considerations
  - Computer Misuse Act
    - Section 1 – unauthorized access to computer material
    - Section 2 – unauthorized access with intent
    - Section 3 – unauthorized modification (add/del) with intent
  - Budapest Convention on Cyber Crime - CETS 185
  - UN Convention Against Transnational Organized Crime

Defense Law

- American Considerations
  - Computer Fraud and Abuse Act (CFAA)
  - State Computer Trespass Laws
  - Electronic Espionage Law
  - Stored Communications Act
  - Privacy Laws

I AM WATCHING YOU

Defense Law

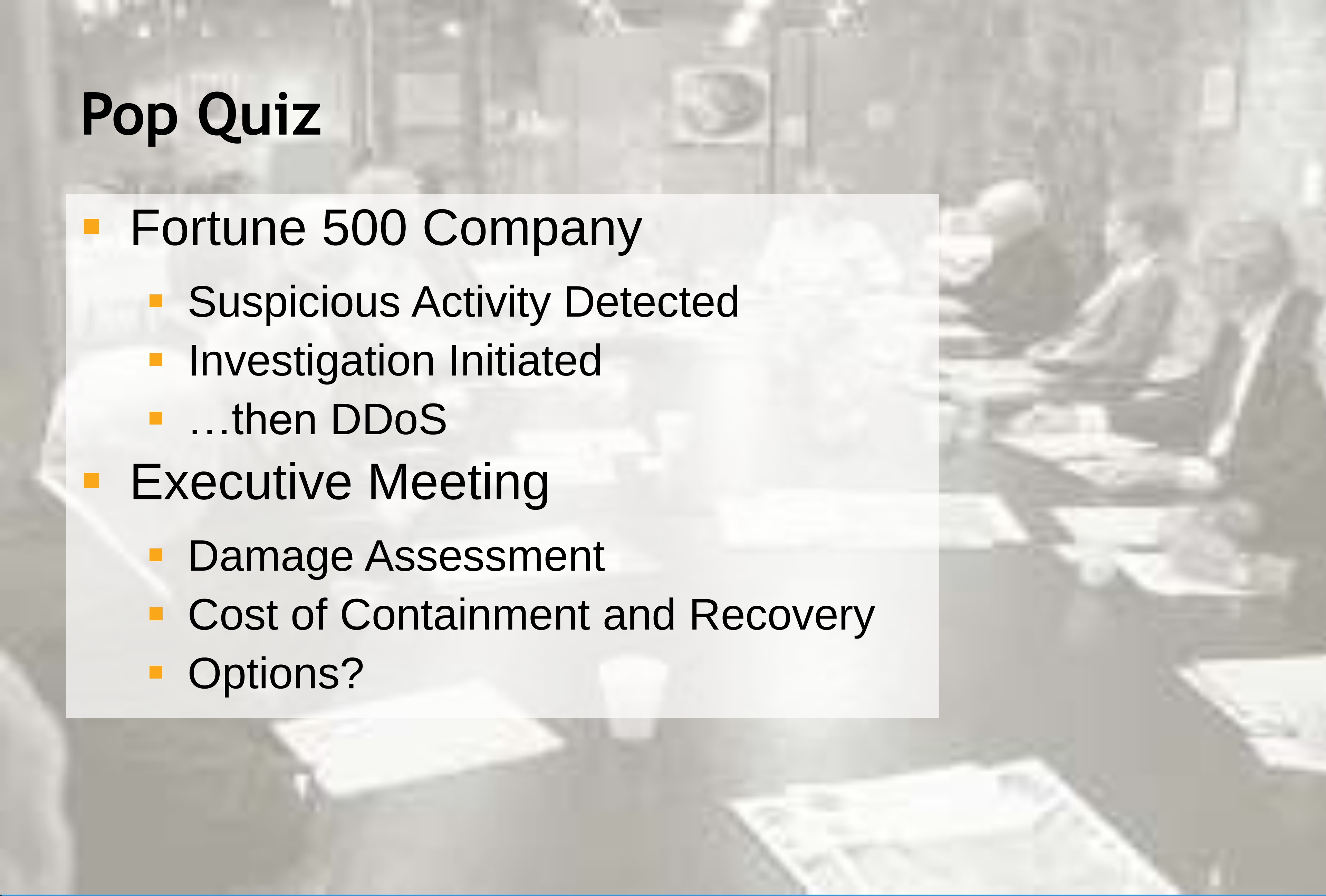
- What jurisdiction are you in?
- What jurisdiction(s) will you operate in?
- What tools do you plan to use?
- How do you plan to use them?
- What impact to you is anticipated?
- What impact to others is anticipated?
  - Retribution
  - Bystanders
  - Reputation

40 DNS Servers Used
Were Outside Brazil

Defense Law

- Potential liabilities of action *outside*
  - Expand harm to bystanders, mistaken target
  - Escalation or Conflagration
  - Reputational loss, weakened alliances
  - Law suit or regulatory violation
- Potential benefits of action *outside*
  - *Block or deny* attacks
  - Stop loss
  - Potential offset to defense costs
  - Strengthened partnership, alliances

Pop Quiz

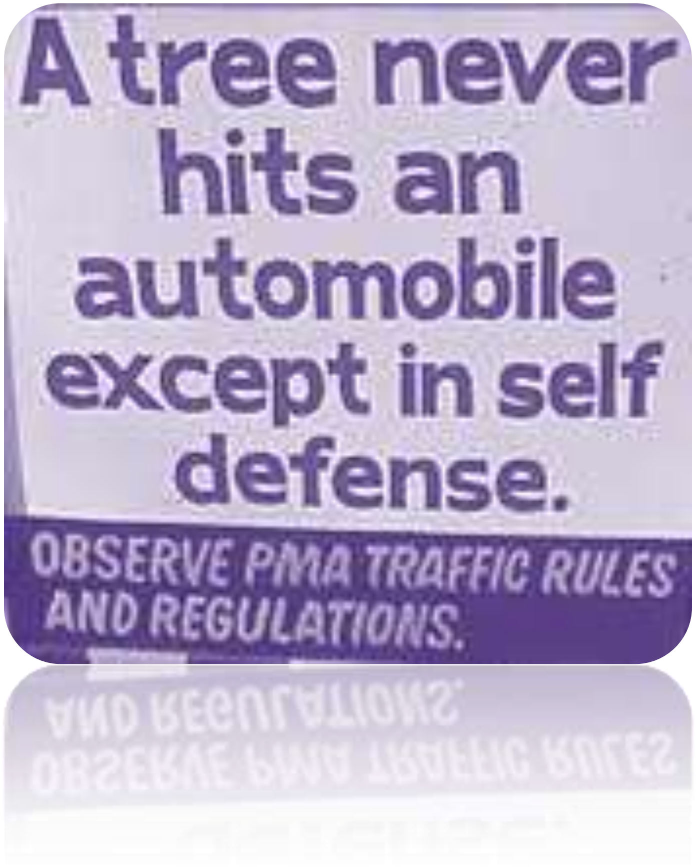


- Fortune 500 Company
  - Suspicious Activity Detected
  - Investigation Initiated
  - …then DDoS
- Executive Meeting
  - Damage Assessment
  - Cost of Containment and Recovery
  - Options?

Build an Active Defense

Three Steps

1. Assessment
   a) Internal
   b) External
2. Calculation
3. Action


A tree never hits an automobile except in self defense.
OBSERVE PMA TRAFFIC RULES AND REGULATIONS.

Step One - a) Internal Assessment

- Evidence of Imminence and Danger/Persistence
- State of Your Security

Step One - b) External Assessment

- Reconnaissance
  - Attack Tools
  - Attack Connections
  - Attack Links and Relationships
- Intelligence
  - Attacker Vulnerabilities
  - Attacker Assets

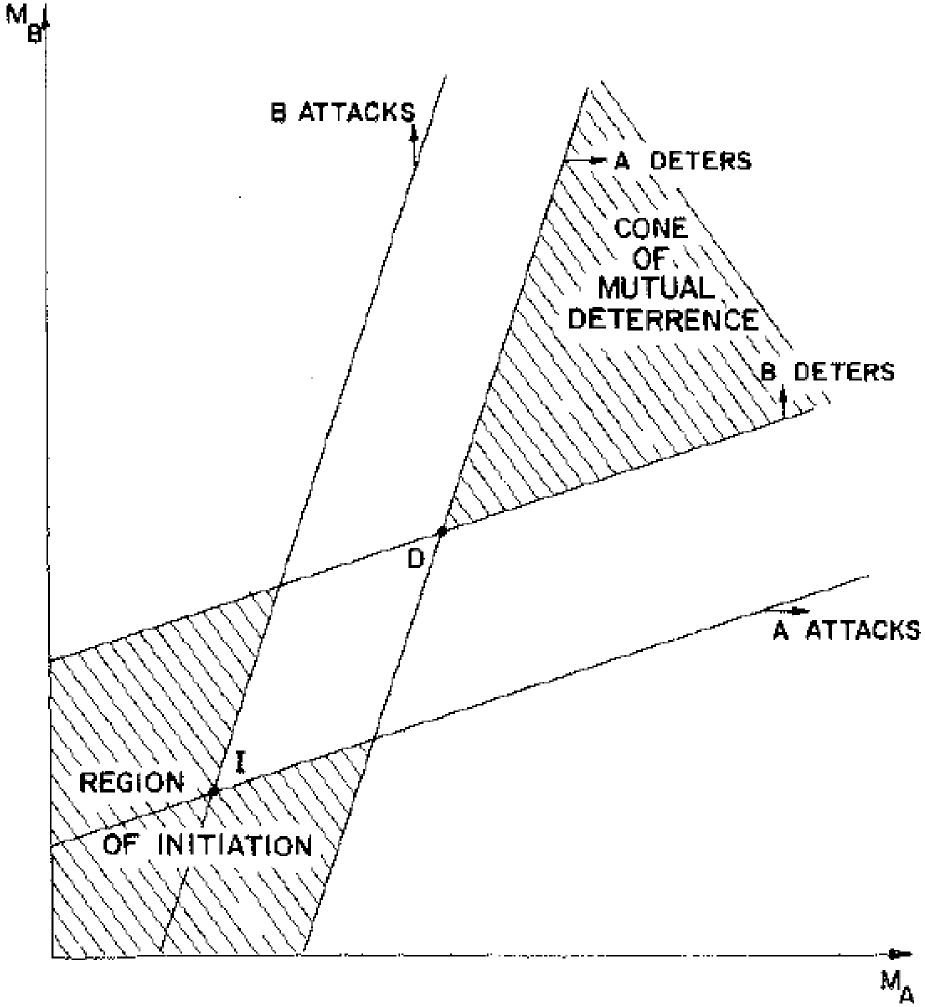
Step Two - Calculation

- Nature (Motive) of the Attack
- Threat: Imminence and Danger

	Commitment			Resources		
Level	Intensity	Stealth	Time	Power	Ability	Opportunity
3	H	H	Long	Organized	H	H
2	M	M	Varied	Grouped	M	M
1	L	L	Short	Isolated	L	L

- Terms: Jurisdiction and Restrictions
- Cost: Liabilities versus Benefits

Step Two - Calculation (Intriligator-Brito)



- Defensive Capabilities
  - Block Attackers
  - Damage Attacker
  - Speed of Defense
  - Time to Discovery
  - Time to Retaliation
- Thresholds
  - Minimum unacceptable damage, estimated by attacker
  - Maximum acceptable casualties of retaliation

http://www.cas.buffalo.edu/classes/psc/fczagare/PSC%20504/Intriligator.pdf

Step Three - Action

- Plan

	Commitment			Resources		
Level	Intensity	Stealth	Time	Power	Ability	Opportunity
3	H	H	Long	Organized	H	H
2	M	M	Varied	Grouped	M	M
1	L	L	Short	Isolated	L	L

- Tool and Procedure Development
  - Survey
  - Access
  - Dump
  - Defend

http://arstechnica.com/security/2012/08/ddos-take-down-manual/

Example #1 - DDoS Takedown Manual

1. Trace Attacks (Three Degrees from Bacon)
2. Map Services and Vulnerabilities (Dirt Jumper)
3. SQL injection to Dump Config (sqlmap)

```
./sqlmap.py --level=5 --risk=3 -u http://www.evilsite.com/dj5/
-p k --data="k=" --technique=t --dbms=mysql --
fileread=”/var/www/html/evilsite.com/djv5/config.php”
```

4. Command and Control

http://arstechnica.com/security/2012/08/ddos-take-down-manual/
http://www.prolexic.com/knowledge-center-ddos-threat-advisory-pandora-and-vulnerability-disclosure-dirt-jumper/banners.html

Example #2 - Project MARS

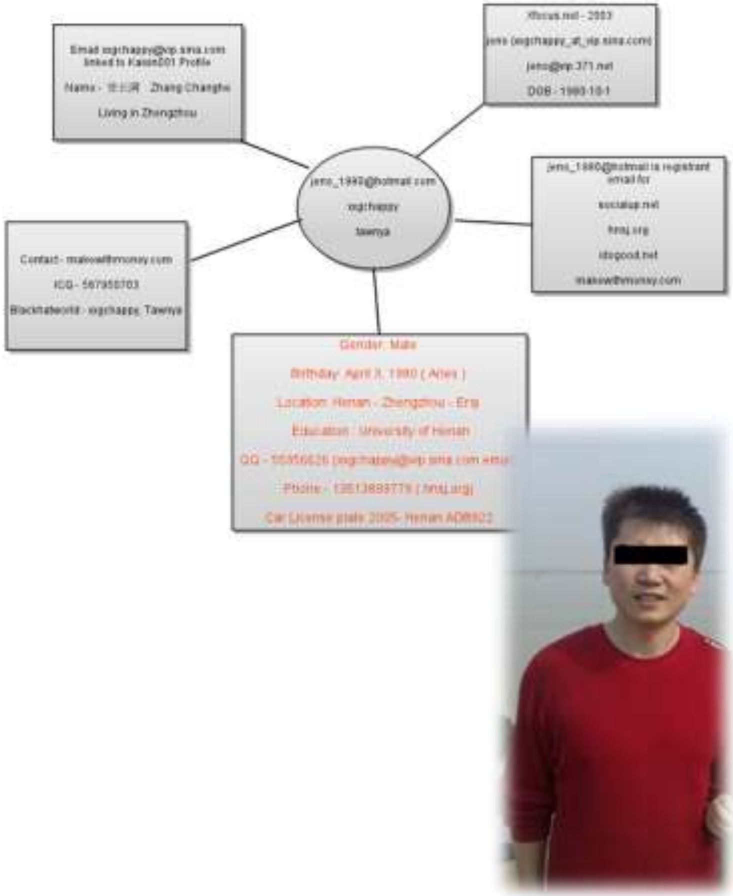
1. Trace Attacks (Elirks via Plurk, Nitol)
2. Sinkhole Communications
3. Reverse / Tag Infected Systems
4. Shutdown C&C

"In the 16 days since we began collecting data on the 70,000 malicious subdomains, we have been able to block more than 609 million connections from over 7,650,000 unique IP addresses to those malicious 3322.org subdomains. In addition to blocking connections to the malicious domains, we have continued to provide DNS services for the unblocked 3322.org subdomains. For example, on Sept 25, we successfully processed 34,954,795 DNS requests for 3322.org subdomains that were not on our block list."

http://www.secureworks.com/research/threats/chasing_apt/
http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-80-54/3755.Microsoft-Study-into-b70.pdf
http://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case.aspx

Example #3 - Wycores Investigation

1. Trace Attacks
2. Profile IDs
3. Dump (QQ#)
4. ??



Email xgchappy@vip.sina.com linked to Kaisin001 Profile

Name - 张昌河 Zhang Changhe

Living in Zhengzhou

Xfocus.net - 2003

jeno (xgchappy_at_vip.sina.com)

jeno@vip.371.net

DOB - 1980-10-1

jeno_1980@hotmail.com

xgchappy

tawnya

jeno_1980@hotmail is registrant email for

socialup.net

hnsj.org

idogood.net

makow@hmoney.com

Contact - makow@hmoney.com

ICQ - 567950703

Blackhatworld - xgchappy, Tawnya

Gender: Male

Birthday: April 3, 1980 (Aries)

Location: Henan - Zhengzhou - Erqi

Education : University of Henan

QQ - 15956626 (xgchappy@vip.sina.com also

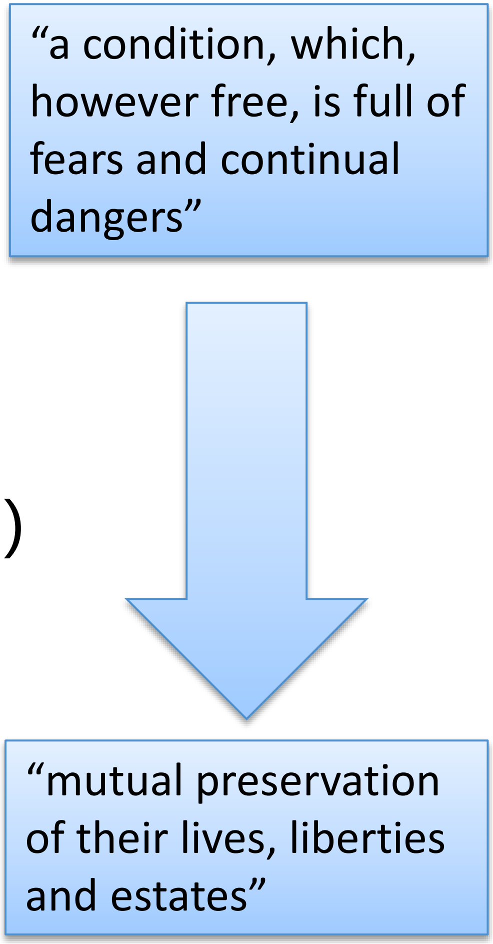
Phone - 13513893779 (hnsj.org)

Car License plate 2005- Henan AD8802

http://cyb3rsleuth.blogspot.com/2011/08/chinese-threat-actor-identified.html
http://cyb3rsleuth.blogspot.com/2012/03/chinese-threat-actor-part-3.html

Conclusion

1. Political and Economic Shift
   - Attacks High Profit Low Risk
   - Imminent Danger
2. A Right to Self-Defense
   - Risk and Cost Assessment
   - Terms of Authorization (Limited Action)
3. Reverse Shift
   a) Outlier
   b) Cooperative
   c) Group

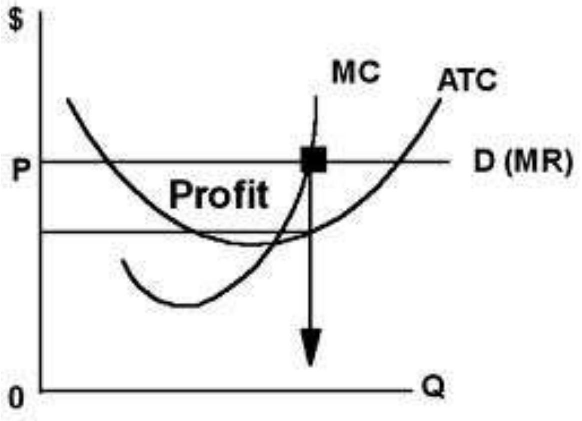


“a condition, which, however free, is full of fears and continual dangers”

“mutual preservation of their lives, liberties and estates”

Apply

1. Assess Rights and Options
   - Technical Capabilities
   - Legal Frameworks and Guidelines
2. Active Defense – Change the Equation



ACTIVE DEFENSE

DAVI OTTENHEIMER

DAVID WILLSON

Session ID: HT-302

Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012