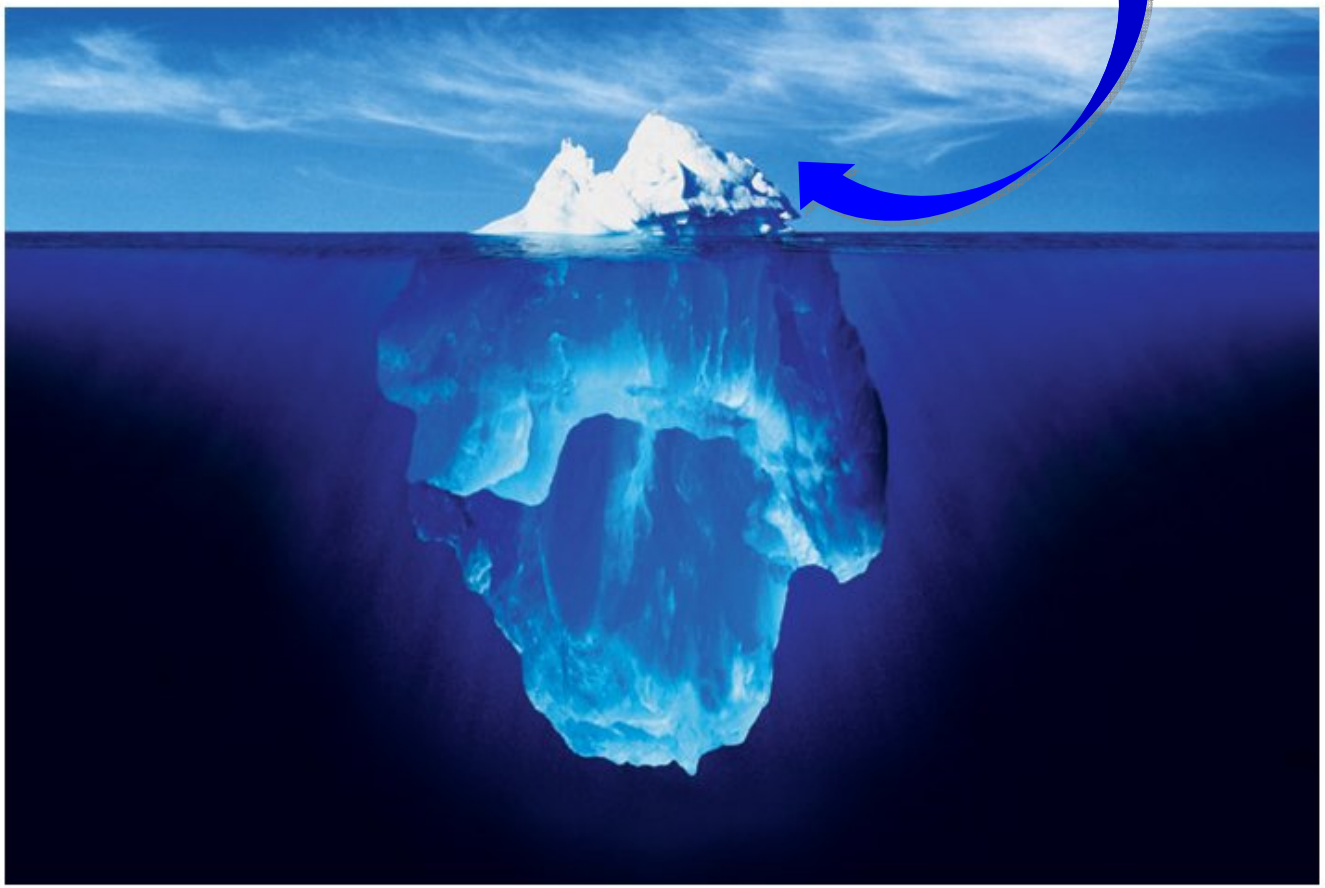
How Good Is Your Network Neighborhood Watch?

Jerry Dixon
Director, Analysis
jd@cymru.com
Team Cymru

Who is "Team Cymru"?

- **Hobby in 1998, Incorporated in 2004**
- **Network of** researchers **and dedicated to supporting the Internet community in maintaining security**
- **25+ full-time employees;** non-profit
- Global investigators **previously from Dutch NHTCC, UK Scotland Yard, Polish Police, USSS, US-CERT, Homeland Security**
- **Funded by multinational banks, CERTs/CSIRTS, security vendors..and you?**

Tired of hearing about botnets?



What is a botnet?

- **A collection of compromised computers**
- **Controlled by a third party**
  - IRC, HTTP, P2P, IM, UDP, etc.
- **Generally for nefarious purposes:**
  - Data exfiltration, Money, Spam, DDoS, Warez

What are they after?

- **They're after our money, our identity, and it's a dangerous place out there on the Net**
- **The targets**
  - Individuals
  - Companies
  - Government

The Current Environment

- **Users and systems facing increase in targeted, adapting attacks from skilled, motivated, and persistent adversaries**
- **The traditional opportunistic hacker has been replaced by a more dangerous adversary**
- **Preventive measures and technologies are continuing to be circumvented through social engineering and zero day attacks**
- **Definition of insider threat is dynamic due to network interconnectivity amongst organizations and globalization of the supply chain. It's a complicated cyber-world**

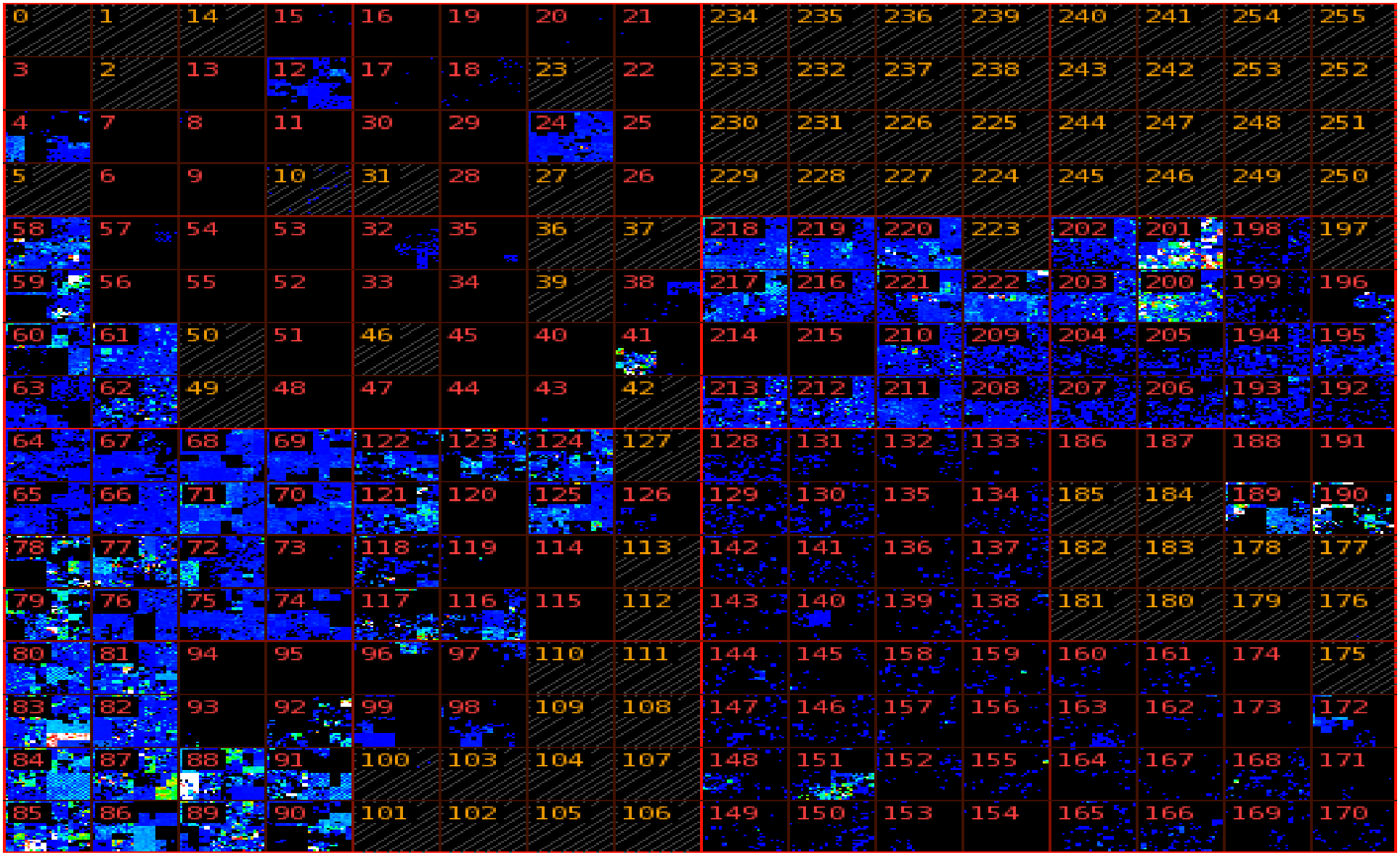
Motivations behind the attacks: *yesterday and today*

- **About five years ago, on-line miscreants had the following motivations:**
  - "fame" among the hacker underground
  - "fun"
  - to elevate control among IRC users
  - Web defacement
  - Denial of Service attacks against your IRC nemesis
  - scripted intrusions

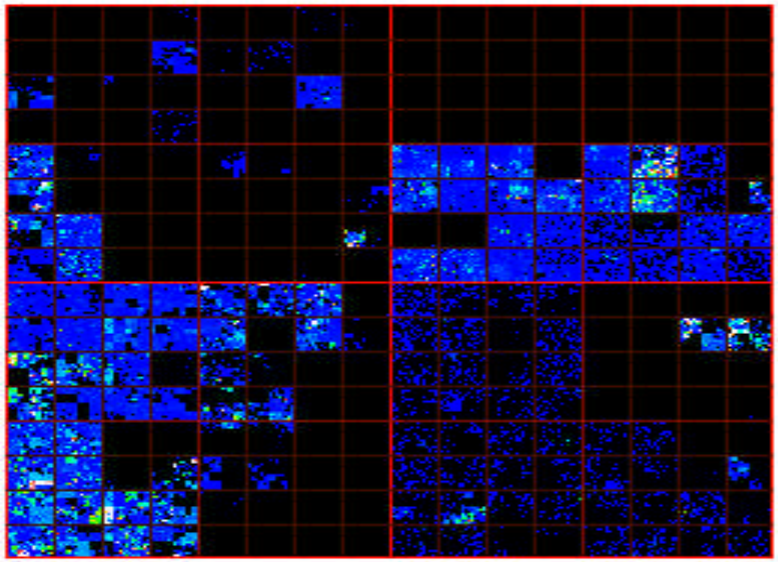
Motivations behind the attacks: *yesterday and today*

- **Well, the hacker underground has grown up**
- **Today, an online underground economy exists solely for the buying and selling of financial data (*your* bank account), identity data (*your* national ID information), and almost anything else you can imagine (passports, airline tickets, etc, etc)**
- **Today's miscreants are *criminals***

Malicious Activity Heat Map



Internet Malicious Activity Map



Learn more

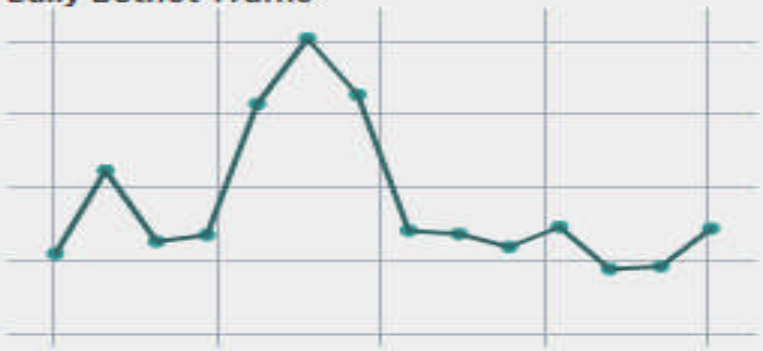
Welcome to the new Team Cymru Website!

Welcome to the new web home of Team Cymru! Take a look around to see examples of the insight and services we are able to provide. Team Cymru – making the Internet a safer place!

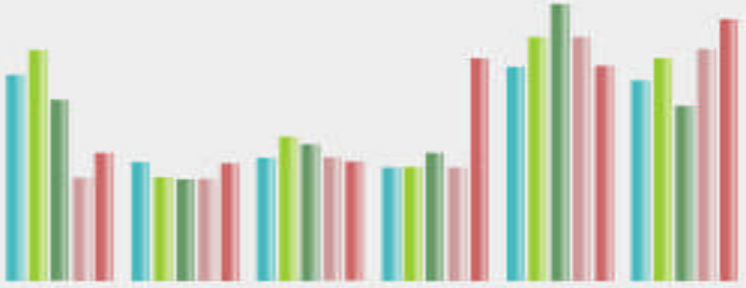
Team Cymru chosen as one of the most Influential in security today by eWEEK !

eWEEK recently recognized Team Cymru's contributions to making

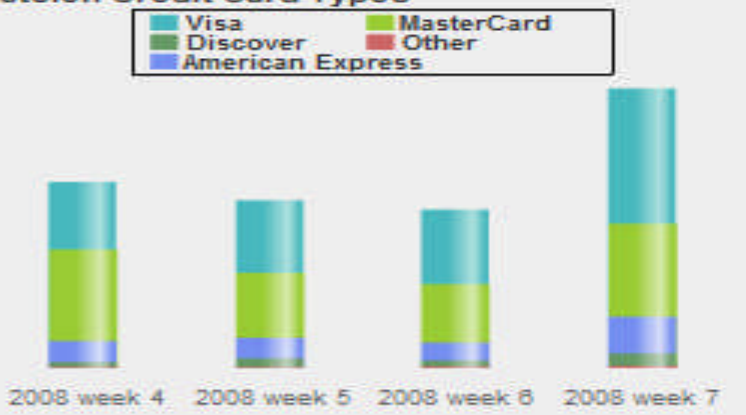
Daily Botnet Traffic



Underground Economy Transactions Per Day

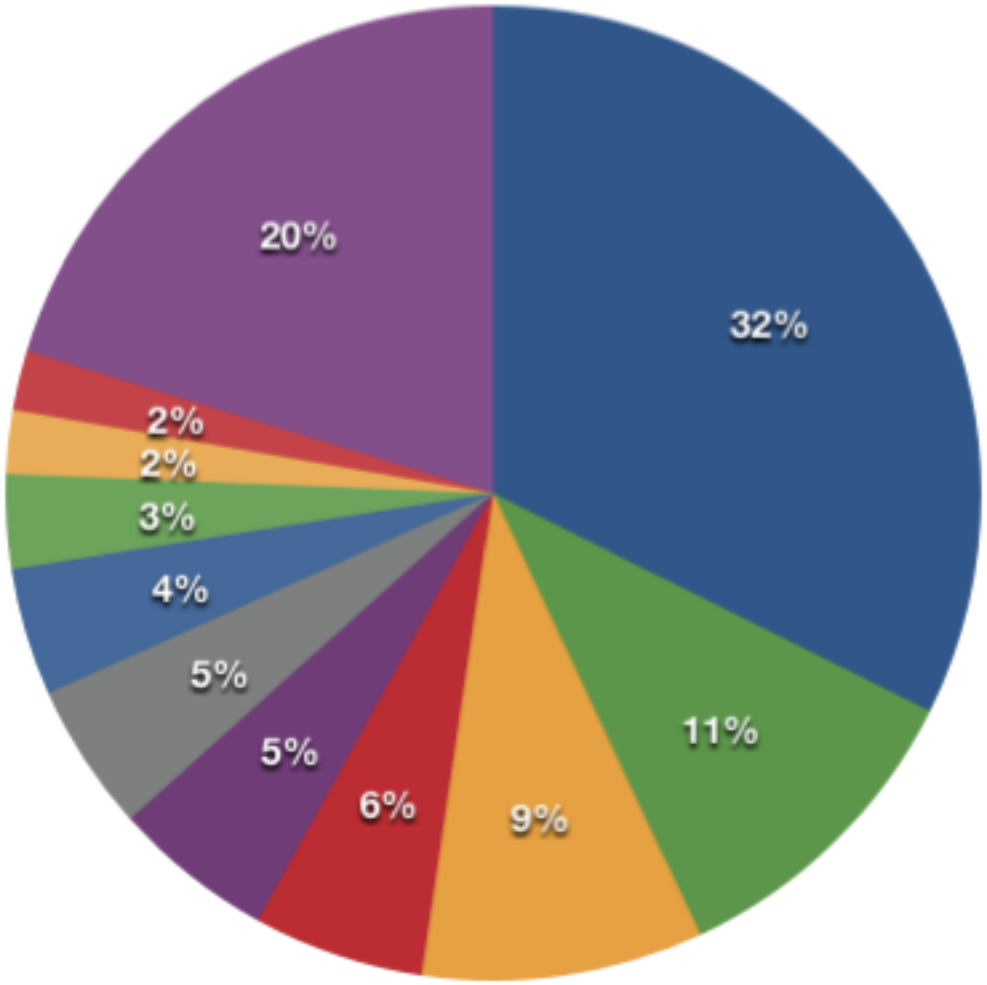


Stolen Credit Card Types



SearchFinancialSecur

IRC BOTNET DDOS ATTACKS BY COUNTRY

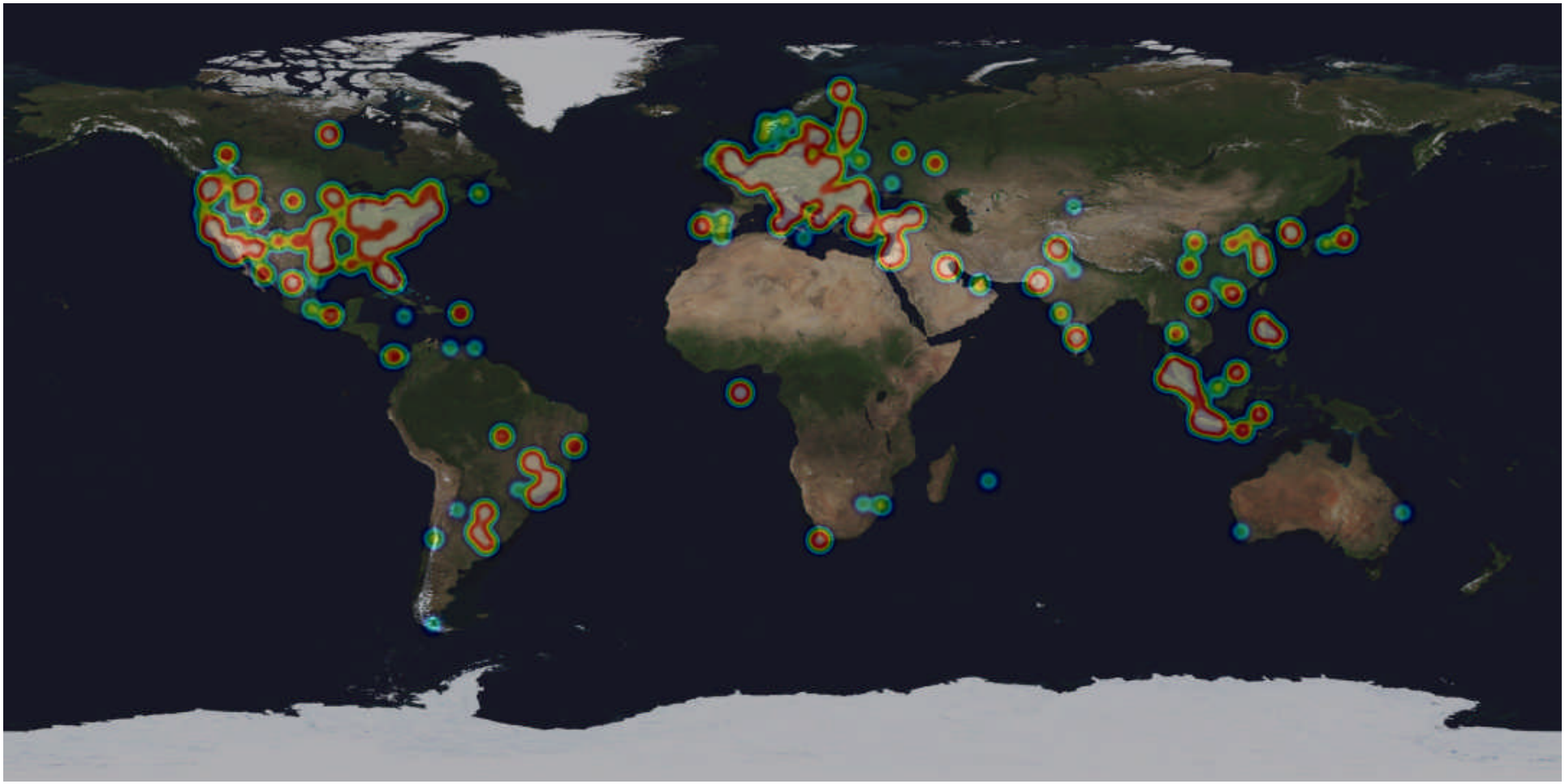


- United States 32%
- Germany 11%
- Indonesia 9%
- Poland 6%
- Turkey 5%
- Brazil 5%
- Malaysia 4%
- Netherlands 3%
- Kuwait 2%
- Slovenia 2%
- Other 20%

Motivations behind the attacks: *yesterday and today*

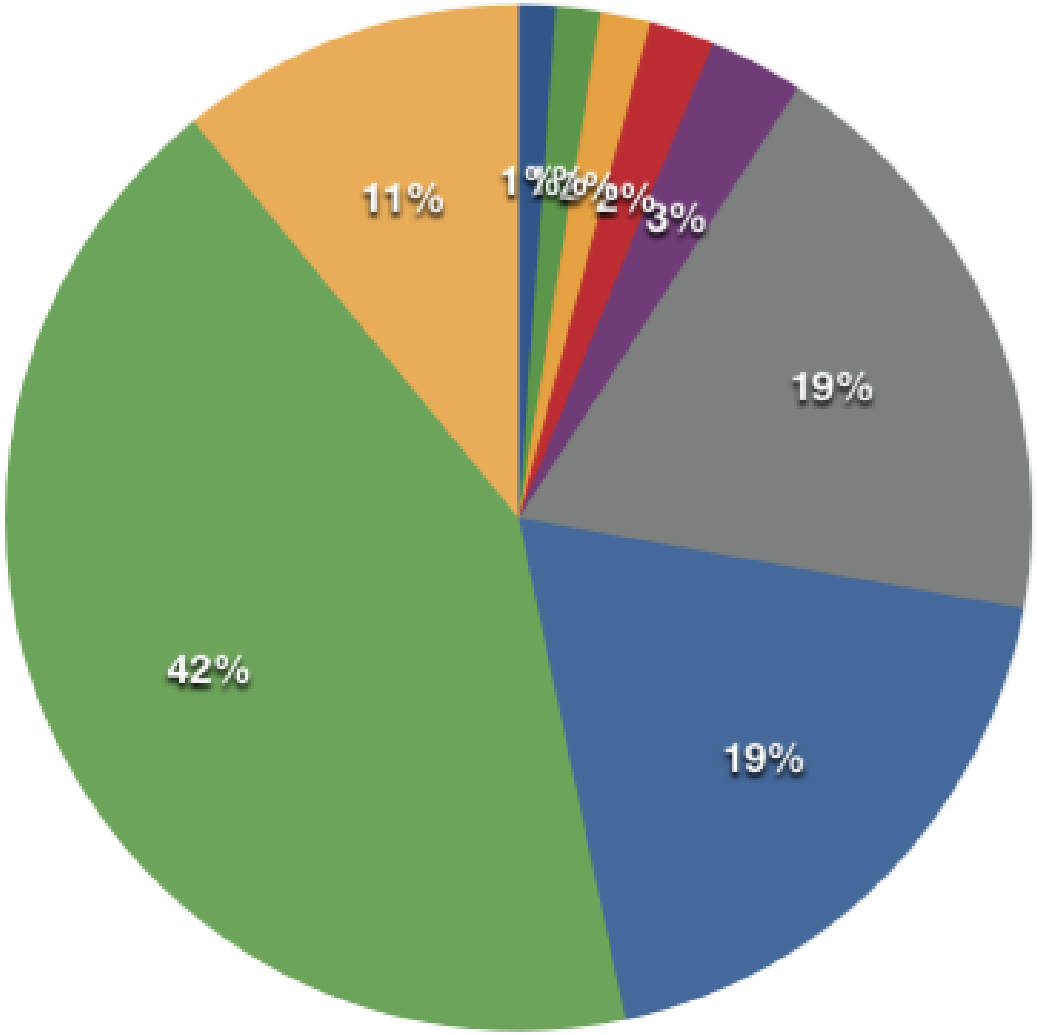
- **Well, the hacker underground has grown up**
- **Today, an online underground economy exists solely for the buying and selling of financial data (*your* bank account), identity data (*your* national ID information), and almost anything else you can imagine (passports, airline tickets, etc, etc)**
- **Today's miscreants are *criminals***

IRC botnet ddos targets



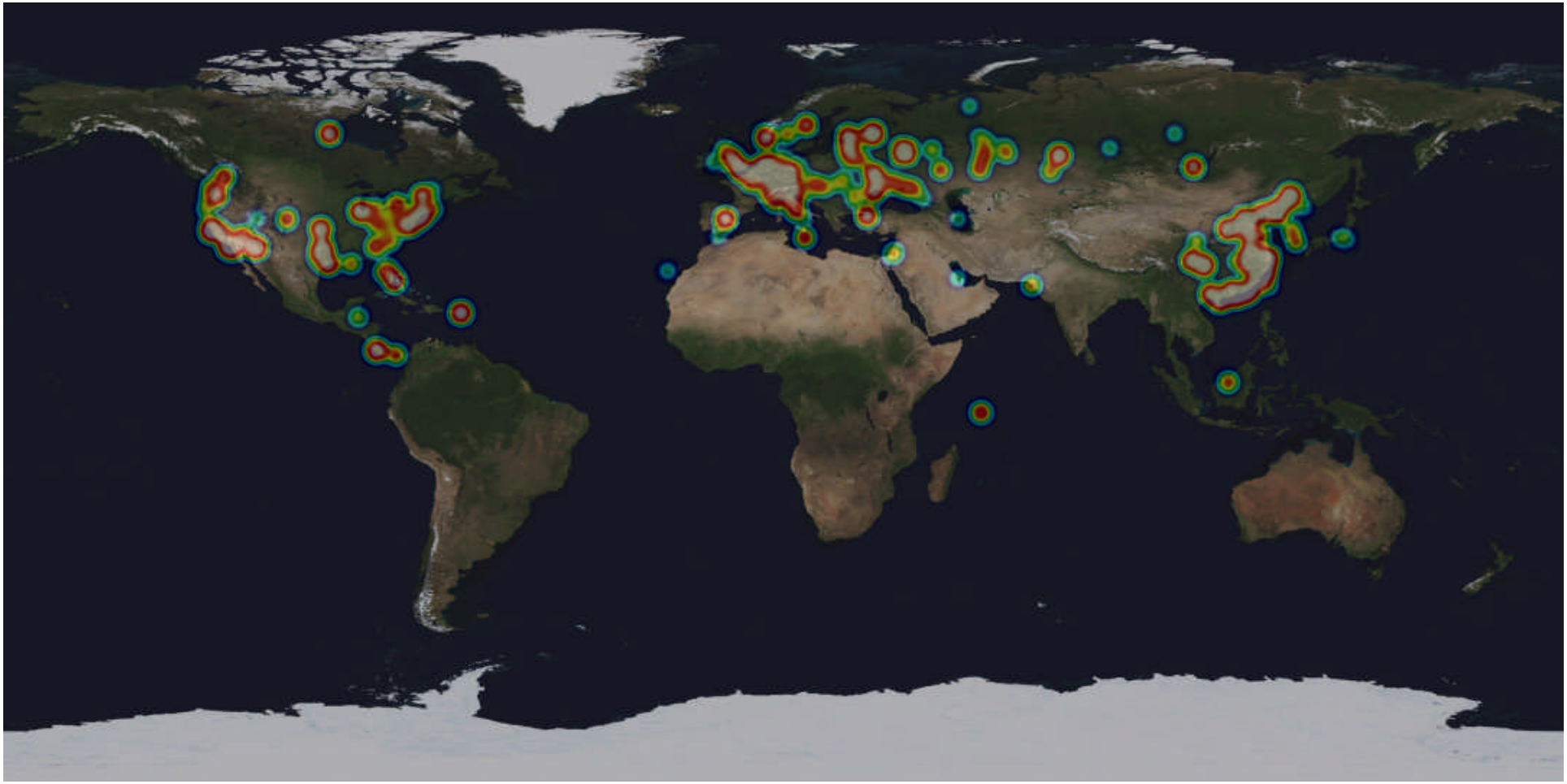
SearchFinancialSe

HTTP DDOS ATTACKS BY COUNTRY



- Canada 41
- United Kingdom 55
- Germany 105
- Russian Federation 662
- Other 384
- Ukraine 49
- Netherlands 72
- United States 656
- China 1491

HTTP botnet ddos targets



Malware Still on the Internet

Malware	IPs detected		
Beagle	349445		
Blaster	24857		
Bots	363683	380185	-4.34%
Bruteforce	170	152	11.84%
Dameware	470	584	-19.52%
Botnet C&C	560	583	-3.95%
Defacement	264	427	-38.17%
Dipnet	72	84	-14.29%
Mail Viruses	7803	8497	-8.17%
Malware URL	1839	1471	25.02%
Mydoom	63	63	0%
Nachi	18234	18066	0.93%
Phatbot	14318	14535	-1.49%
Phishing URLs	327	346	-5.49%
Proxy	34504	35051	-1.56%
Routers	447	461	-3.04%
Scanners	117328	127017	-7.63%
Sinit	86	73	17.81%
Slammer	13652	13335	2.38%
Spam	3197528	2814731	13.60%
Spybot	41177	44613	-7.70%
Toxbot	291928	316994	-7.91%
TOTALS	**4320203**	**3996672**	**8.10%**

Running 1066 samples through 32 AV packages yielded a 37% detection rate

What's it all about?

- **It isn't about malware; it's about people and** crime
- **Taking your hard earned money, information & identity**

Extracting your Ca$h

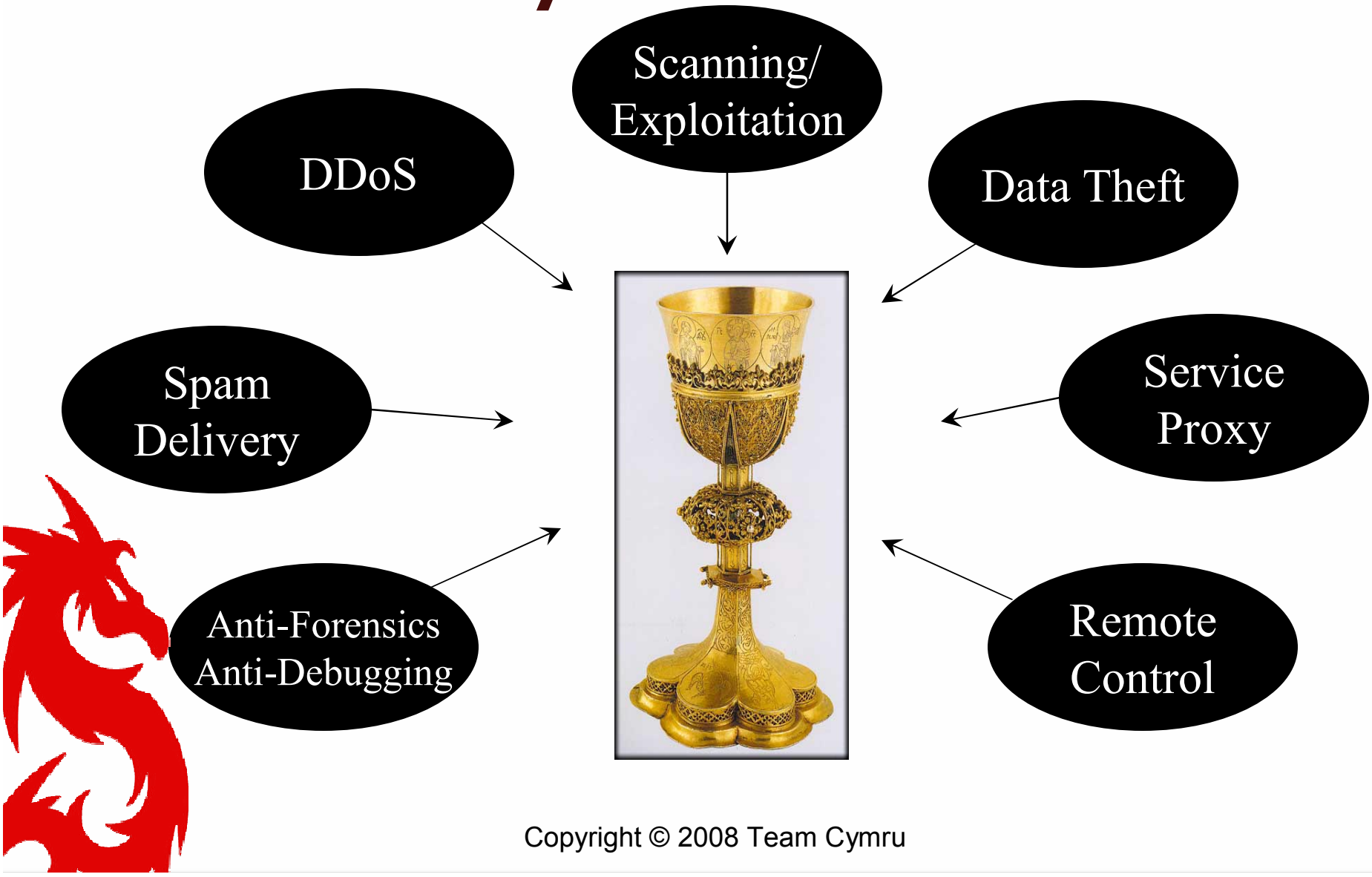
Miscreant perception of computers

underground cash registers

Attack Trends

- Movement toward high-power *NIX boxes with big pipes as bots
- Encrypted command & control communication for botnets
- P2P for botnet control
- DDoS extortion as a profit maker
- Better knowledge of "bad neighborhoods" of the internet – these are areas of the internet that are most vulnerable
- Better knowledge of countermeasures against hacking attempts – where the honeynets are, for instance
- Better packing & obfuscation of malware, making reverse engineering more difficult

What are they after?



The chase continues: new techniques needed

Old botnets:

- Central point of failure
- IRC based C&C
- Limited obfuscation
- Limited lifetime/size
- Modular exploits

New botnets:

- Distributed achitecture
- http + p2p based C&C
- Extensive encryption
- Immortal/unlimited size
- Social engineering
- Self protection
- Self healing
- Custom packing
- VM aware
- Local DNS poisoning
- Double fast fluxing

Extracting the Ca$h

- Proxy Sales, Bot Sales
- Malware Sales
- Spam, Phishing
- Compromised Routers, .mils, .govs, .edus, .com
- Full Infos (50/50)
- DDoS for Hire
- Spyware/adware/malware "affiliate programs"
- The obvious – charging to stolen credit cards, clearing out bank accounts
- Illustrative article (the story of Ancheta and Sobe): http://reviews.cnet.com/4520-3513_7-6427016-1.html

The Storm is a brewing

When good guys strike, guess who strikes back?

- Storm worm strikes back at security pros
- Researcher says those discovered trying to defeat worm suffer DDoS attacks
- **By Tim Greene, Network World, 10/24/07**

What are the enablers?

- Lack of a dedicated operational security team
- Lack of network cognizance
- Need for more trained cyber law enforcement personnel at the State & Local Level
- It's International! No matter what our laws are the Internet is Global
- Complex software

Challenges

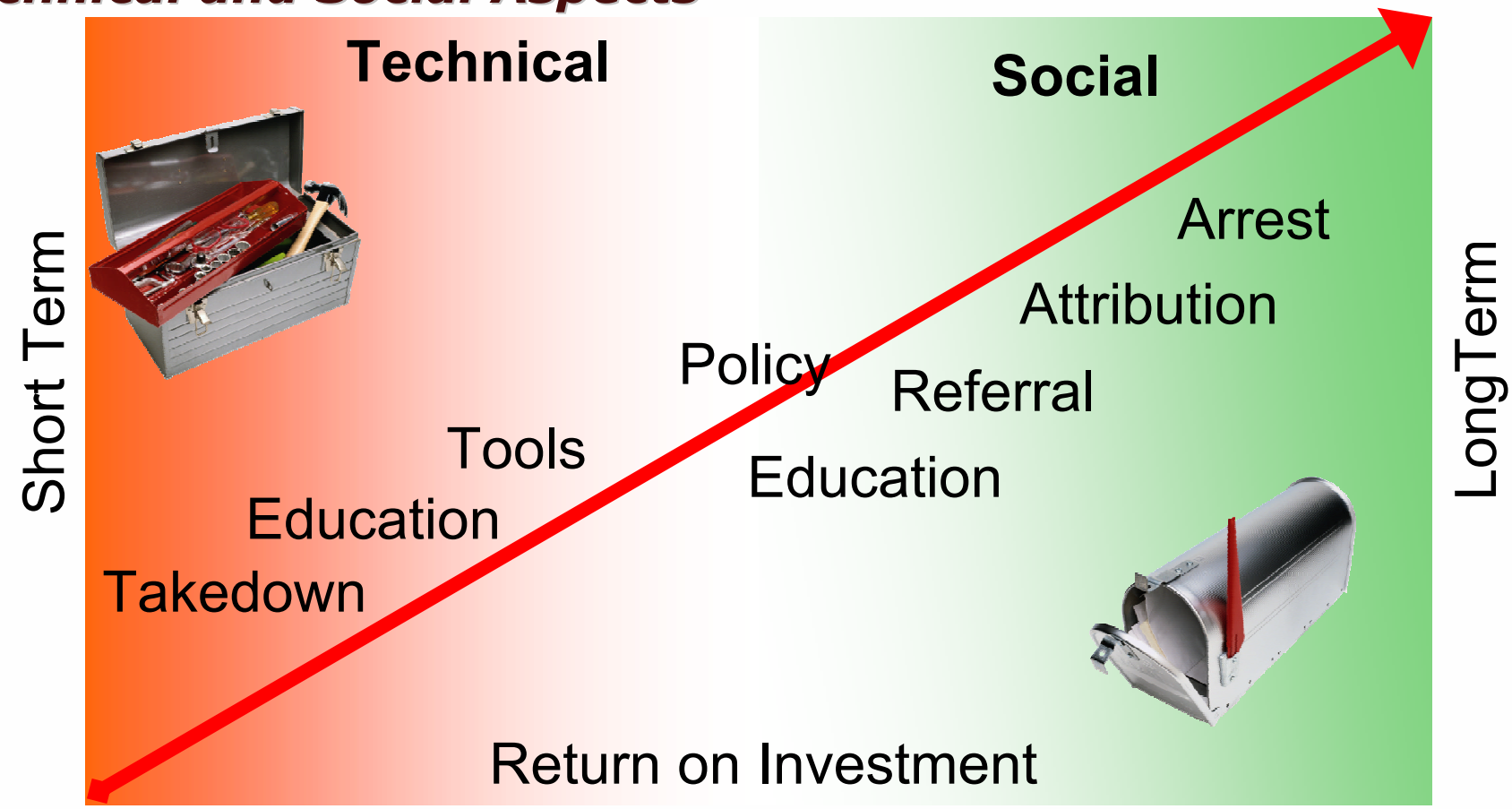
- Having the right contacts in place worldwide (ISPs, Registrars, LE)
- Not enough data sharing and collaboration
- Globalization
- Enforcement issues
- Corporate Involvement

Security Misconceptions

- "…but I use NAT."
- "I block everything inbound."
- "Our Antivirus keeps us safe."
- "We've got a good FISMA grade."
- "We have a DMZ."
- "I'm not a target."
- "I use encryption/IPSec."
- "I use IPv6."

Mitigation Continuum

Technical and Social Aspects



Efforts Underway to tackle these issues

- **Cyber Commission for the 44th President**
- **Infragard**
- **Homeland Security Efforts & Cyber Initiative**
- **SANS & ISC2 Training Efforts**
- **Technical Community Efforts**
- **Internet Law Center**

When Collaborating, EVERYONE benefits – not just YOU.

Thank you!

Jerry Dixon

Team Cymru

jd@cymru.com