How Economics and Information Security Affects Cyber Crime and What This Means in the Context of a Global Recession

Turbo Talk

BH 2009

Peter Guerra

Full Disclosure

- My opinions only – not of my University, Employer, Family, pets, etc.
- Why this topic
- What to get out of it
- What not to get out of it

Our Dilemma

"Accept the Security Breach or Clean A Litter Box.

Take Your Pick."

Non Sequitur, Wiley

Two Questions

- How do economics create perverse incentives that leads to cyber crime?
  - What is the economic context of information security issues?
- What are the economics of cyber crime during a global recession?
  - Will the global recession cause cyber crime to go up?

Relevant Points

- Fundamental shift in security industry recently – economics is shaping security more than it ever has
- Cyber crime is growing because of perverse economic incentives created by IT market, global economic trends, and the impact of laws
- Impact on governments, markets, individuals could be significant
- Must start addressing the perverse economic incentives

Economic Context

- Economic Principles
  - Cost-Benefit, Scarcity, Incentives
- Economic Theories
  - Tragedy of the Commons
  - Lemon Car Market theory
  - Information Security as a Trust Good
- Predicts three target areas:
  - IT market security failure
  - Global economy and cyber crime
  - Economic impact of laws

Economic Principles

- The Scarcity Principle – Having more of one good thing usually means having less of another.

- The Cost-Benefit Principle – Take no action unless its marginal benefit is at least as great as its marginal cost.

- The Incentive Principle – Cost-benefit comparisons are relevant not only for identifying the decisions that rational people should make but also for predicting the actual decisions they do make.

Economic Theory: Tragedy of the Commons

- Tendency for a resource that has no price to be used until its marginal benefit falls to zero.
- Internet can be considered the commons for cyber crime – has inherit value but the cost to secure it is shared with all nodes
- Cost for each node to secure themselves has marginal benefit to the other nodes, all benefit
- Cost savings for each node to not secure themselves has marginal benefit to own node, all suffer

Tragedy of the Commons

- How much would you spend to protect your computer and data from compromise?
- But how much more would you spend to prevent your systems from attacking someone else?

Economic Theory: Lemon Car Market

- Buyer unable to distinguish between good used car and a lemon, so is only willing to pay the amount for a lemon
- Supply side of information security market similar lemon car market
- Secure products are indistinguishable from insecure ones from buyer's perspective

Information Security as a Trust Good

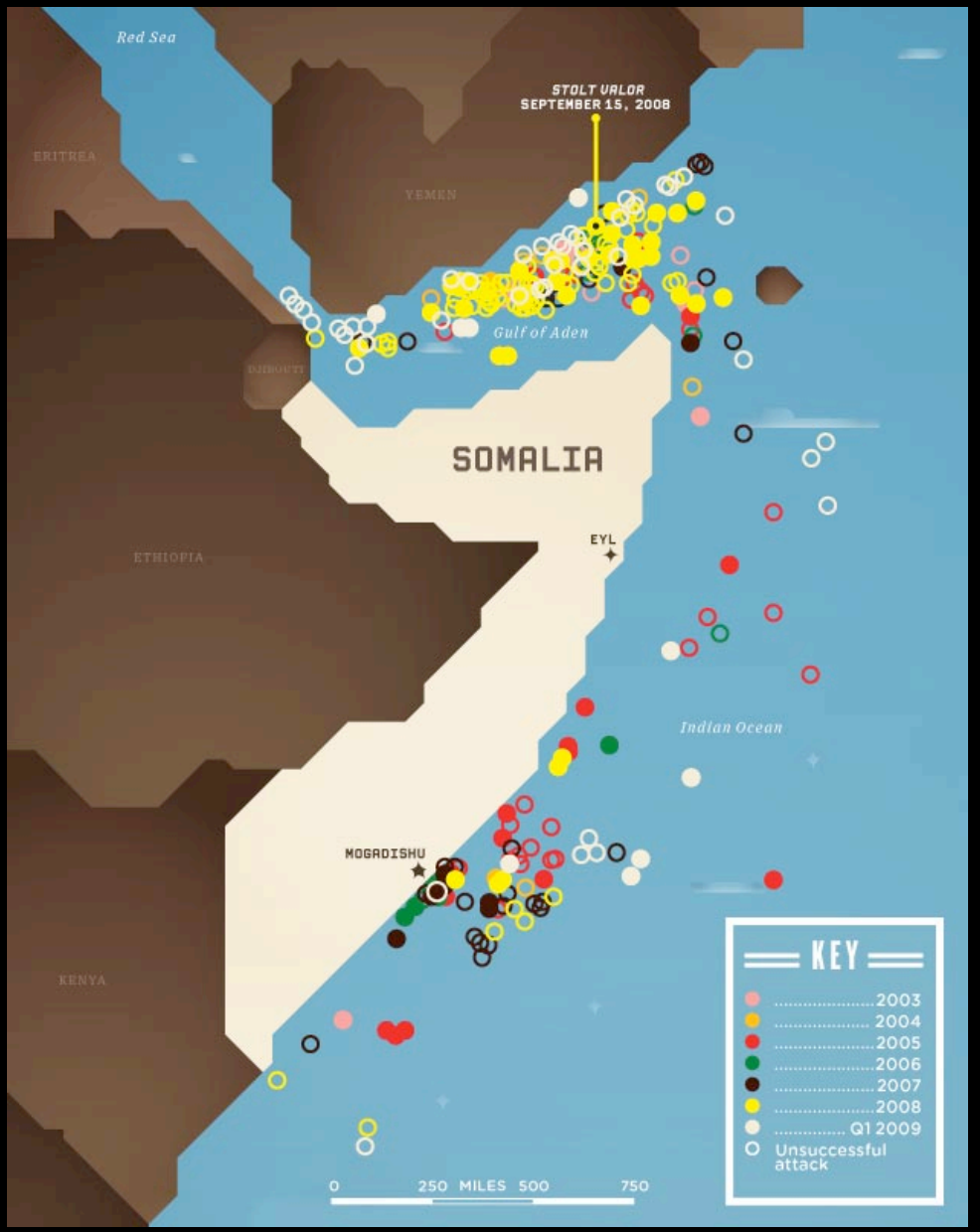
- Price drops to the level for insecure products
- Therefore, little incentive for IT companies to spend R&D dollars to ensure security
- Result == Low supply of information security in IT products (fix the code)
- Ross Anderson example -- Microsoft

Economic Incentives

- The IT market has little economic incentive to properly and thoroughly incorporate security in products == market failure
- Cyber crime can be extremely profitable, has low overhead, and has little risk of being prosecuted == market opportunity
- Criminals have a huge opportunity cost to NOT move into the cyber realm

Somalia Pirates

- Typical Somali earns about $600 a year fishing
- Even the lowliest pirate can make nearly 17 times that — $10,000 — in a single hijacking
- Can be high risk, but risk is relative (Mogadishu civil war has killed thousands)



Wired 17.07, An Economic Analysis of the Somali Pirate Business Model

Cyber Crime trends

- Difficult and impossible to get good data
- Indicators are at the margins – what is happening with the byproducts of cyber crime
  - How much things are bought and sold for
  - The sophistication of the tools (modern malware)
  - Size and number of botnets
  - Specialization of services
- All of these indicators are growing … so cyber crime must be growing?

What Constitutes Cyber Crime?

- Definitions are difficult
- Usually broken down by activities:
  - Phishing
  - Botnets
  - SPAM
  - Identity theft
  - Fake security software
  - Credit card fraud (Carding)
  - DDoS Extortion
  - Click fraud
  - Cyber squatting
  - Blackhat SEO
  - Pump-and-dump stock schemes

  - Copyright infringement

Cyber Crime Economy Difficult to Measure

Estimated loss	Methodology	Source
$100 billion	Research study estimated the global cost of spam to be $100 billion worldwide, including $35 billion in the United States.	Ferris Research (2007)
$67.2 billion	Survey projected annual loss to U.S. organizations because of computer crime in 2005.	2005 FBI Computer Crime Survey
$49.3 billion	Survey of 5,000 U.S. adults projected that 8.4 million consumers suffered losses due to identity theft in 2006.	Javelin Strategy & Research 2007
$56.6 billion	Survey of 5,000 U.S. adults projected that 8.9 million consumers suffered losses due to identity theft in 2005.	Javelin Strategy & Research 2006
$8.4 billion	Survey of 2,000 households with Internet access determined U.S. consumers' losses due to viruses, spyware, and phishing in 2004-2005.	Consumer Reports State of the Net 2006
$2.13 billion	Survey of 5,000 U.S. adult Internet users estimated phishing-related losses between April 2003 and May 2005.	Gartner Research
$183.12 million	Over 228,000 complaints were filed; 97,076 were referred to federal, state, and local law enforcement agencies for further consideration in 2005.	IC3 2005 Internet Crime Report
$68.14 million ($220 per complaint)	207,449 complaints were filed; 190,143 were referred to law enforcement agencies in 2004.	IC3 2004 Internet Crime Report
$125.6 million ($329 per complaint)	124,509 complaints were filed; 95,064 were referred to law enforcement agencies in 2003.	IC3 2003 Internet Crime Report

Economics of SPAM and Botnets

Revenue (Weekly)	Amount
SPAM sent	40 million
Click-through ratio	0.12%
Total click-throughs	48,000
Click-through to sales ratio	1/200
Total sales	240
Total sales revenue	$37,440.00
Spammer commission rate	50%
Total Spammer Income	$18,720.00

Cost (Weekly)	Amount
Bulletproof hosting	$230.00
4 days botnet access	**$6,800.00**
Email addresses	$4,000.00
Total Costs	$11,030

Profit (Weekly)	Amount
Spammer Net Profit	**$7,690.00**
Botnet Profit	**$11,900.00**

How Big versus Growth Rate

- "Cybercrime has significant economic impacts and threatens U.S. National Security interests, but its precise magnitude is unknown", *GAO report, 2007*

- Less important than how BIG is the market is how FAST has the market grown and why
  - Economic incentives the fuel on the fire?

Example Cyber Crime speed

- “[2004] was the first year that proceeds from cyber crime were greater than proceeds from the sale of illegal drugs […] *cyber crime is moving at such a high speed that law enforcement cannot catch up with it*”

— Valerie McNiven, US Treasury advisor on cyber crime, 2004

Cyber Crime margins

- Increasing specialization
  - Botnet rental
  - Carding templates and machines
  - SPAM campaign creation
  - Crimeware-as-a-service
  - Help desk when botnet taken down
- Swiftness of response to world events is increasing
  - 2008 Banks failing (days)
  - 2009 Michael Jackson death (hours)
  - 2009 Erin Andrews peep hole video (minutes)

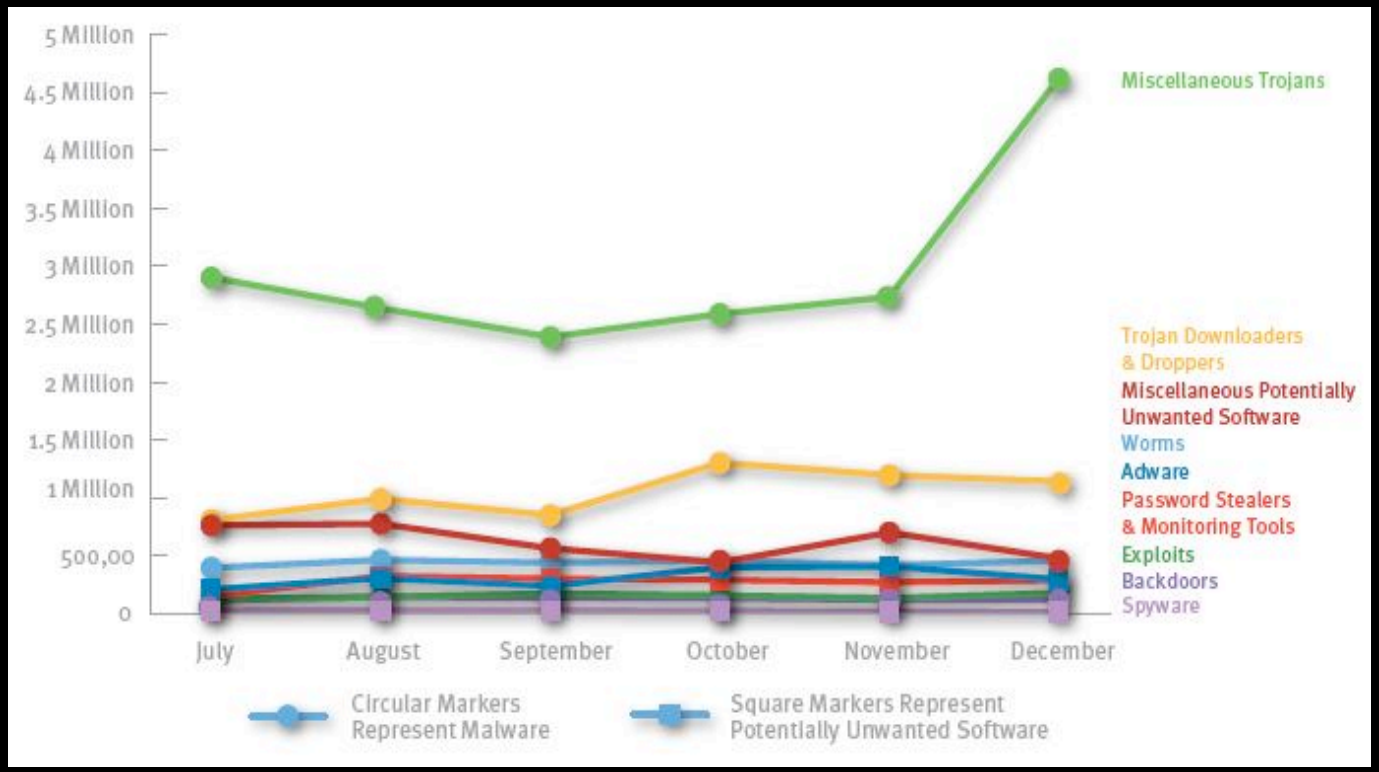
Crimeware costs

- Purchase crimeware kits like Zeus, Mpack (modular) for ~ $500
- Crimeware-as-a-service for $50 for 3 days access
- Botnet rentals of millions of nodes for around $1000 per day
- iframedollars.biz -- pays webmasters 6 cents for each infected machine
- Windows Vista zero day was available for $50K before Vista was even released

Crimeware Site FAQ

- *"[Q] What is XXXXXXXXX?*
- *[A] XXXXXX is a mix between the ZeuS Trojan and MalKit, A browser attack toolkit that will steal all information logged on the computer. After being redirected to the browser exploits, the zeus bot will be installed on the victims 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"*
  - *We also host normal ZeuS clients for $10/month.This includes a fully set up zeus panel/ configured binary"*

Example: Growth Rate in Attacks



Microsoft 2008 Breach Report

Wall Street Journal, 4/8/2009

Example: Growth Rate in Malware

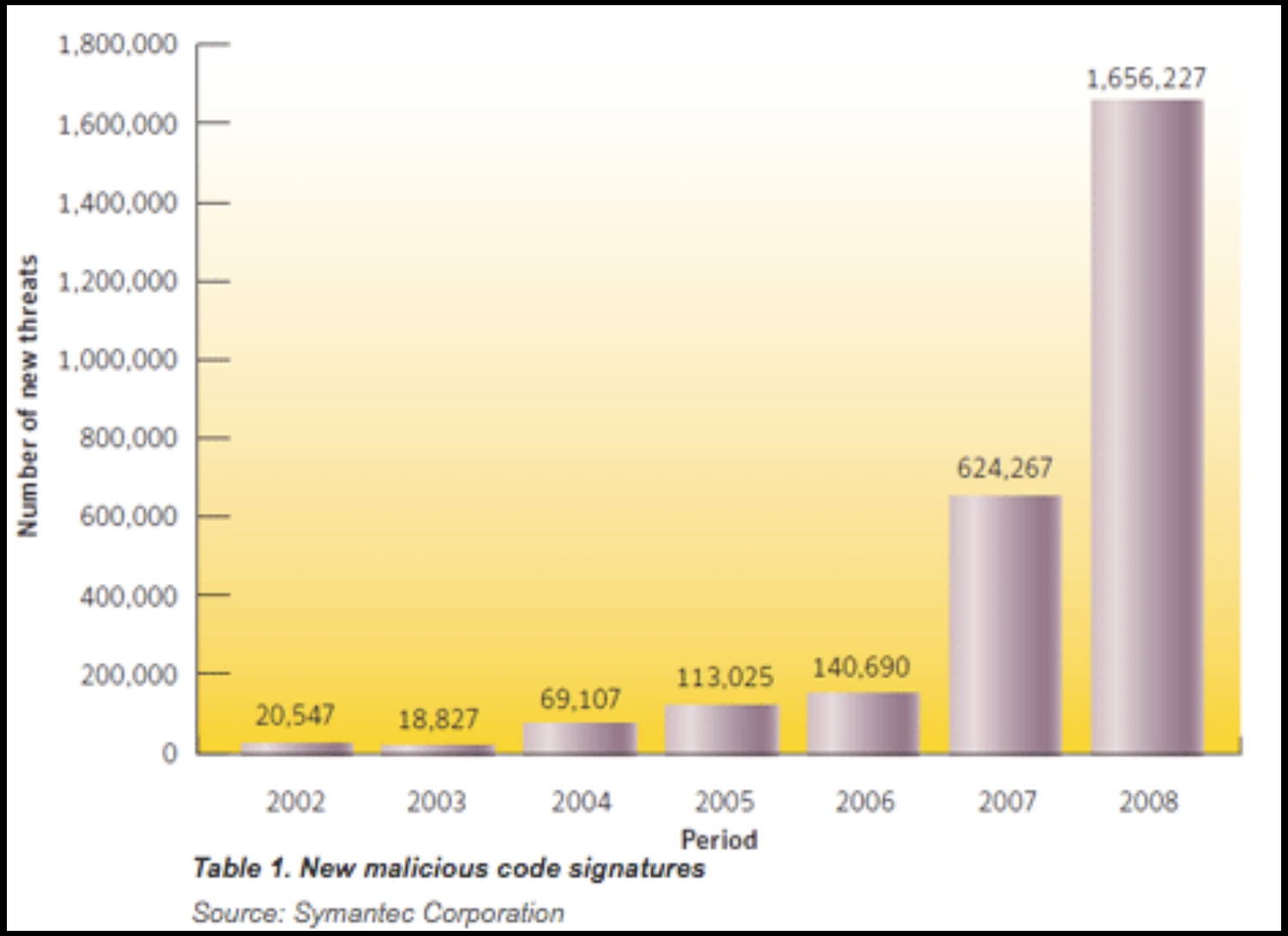


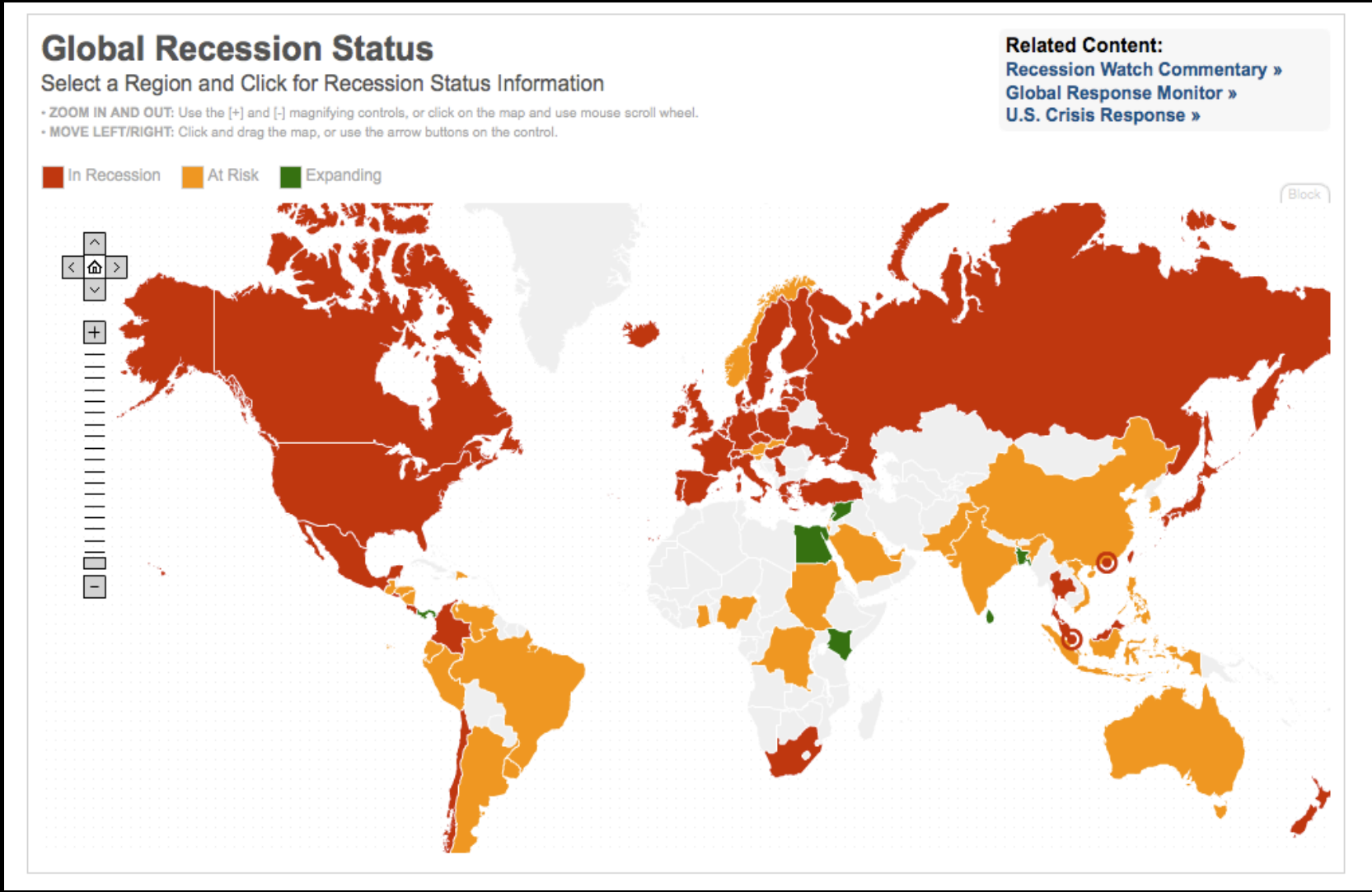
Table 1. New malicious code signatures

Source: Symantec Corporation

Economic Recession Impact

- Questions:
  - How has the global recession affected cyber crime – does it increase during recessionary periods like other crime?
  - How has Globalization helped to contribute?
    - Brazil, Russia, India, China (BRIC) countries?

Global Recession Map



Security in a Global Recession

- Job loss/disgruntled worker/insider threat increases – profit motive (cost-benefit)
- Rise in available computer talent with no job (incentives)
  - Hey cybercrime pays!
- Demand for counterfeit products grows (scarcity)
  - Cheap drugs!
- Ability to prosecute can be diminished (conflicting priorities)

Business Impacts of Recession on Cyber Crime

- Businesses, government and individuals have less money to spend on security, even as the threat grows
- Cost-benefit analysis means that less security means more cyber crime?
- On the other hand, what is there to protect if the business is in Chapter 7?

Recession Example: Fraud

- Level of fraud has significantly increased in the previous 12 months
- U.S. organizations lost 7 percent of their annual revenues from 2006-2008 due to fraud, a 2% increase from 2004-2006.
- Losses are ~$500 billion annually
- Increased financial pressure is biggest factor, over increased opportunity (27%) and increased rationalization (24%)
- Why – fraud is easier to commit now (cyber) and economic incentives

Globalization

- Thomas Friedman's *The World Is Flat*
- With Globalization and global networks brings global cyber crime
- Are emerging markets nations more vulnerable to cyber crime?
  - Brazil has invested many millions of dollars to build its Internet infrastructure
  - Russia has a well-organized criminal groups that has been actively recruiting computer specialists to commit cyber crime
  - India's technology revolution is the direct result of the massive outsourcing of IT and software development to the country
  - Chinese government has invested heavily in technology education and infrastructure and exports most goods

Malicious Activity by Country

2008 Rank	2007 Rank	Country	2008 Overall Percentage	2007 Overall Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	United States	23%	26%	1	3	1	2	1
2	2	China	9%	11%	2	4	6	1	2
3	3	Germany	6%	7%	12	2	2	4	4
4	4	United Kingdom	5%	4%	4	10	5	9	3
5	8	Brazil	4%	3%	16	1	16	5	9
6	6	Spain	4%	3%	10	8	13	3	6
7	7	Italy	3%	3%	11	6	14	6	8
8	5	France	3%	4%	8	14	9	10	5
9	15	Turkey	3%	2%	15	5	24	8	12
10	12	Poland	3%	2%	23	9	8	7	17

Table 2. Malicious activity by country
Source: Symantec

Perfect Storm?

- What is the impact on us as security professionals? Does this make our jobs harder? Do we keep our jobs?
- What is the impact on security innovation? The demand for security products may be there, but the global recession means less money to buy.
- What happens when the impact on organizations and governments is much higher than the costs to commit the crime (asymmetric)?
- What happens as more people are connected to the Internet, and more data and critical operations depend on it?
- What does the continuous rise in cyber crime affect future IT trends?
- What is the impact on:
  - Governments – cyber warfare just became *cheap*, maybe I shouldn't shut down that botnet
  - Businesses – cost to protect assets goes up at the exact time that it has less capital for costs like security
  - Consumers – price of goods goes up as increased business overhead is passed along (possible)
  - Security product market – increasing specialization to address market failures

- Without the data, we can only guess.

Conclusion

- Cyber crime is an economic issue and is growing because of perverse economic incentives created by IT market, global economic trends, and the impact of laws
- Fundamental shift in security industry – economics is shaping security more than it ever has
- What the impact on governments, organizations, markets, individuals, society?
- If we can address the economic incentives of cyber crime, maybe we can start to create a more secure Internet?
- More research is necessary, good data would be a great start