Emerging Economies:

The Vulnerability Market
Agenda

• Bio
• Evolution
• 60-second primer
• Key components defined
• Markets at a glance
• Economic Paradigm
• Wrap-up
• Questions
Emerging Economies: The Vulnerability Market

Terri Forslof
Manager of Security Response
TippingPoint Technologies
The Ghost of InfoSec Past

- Security Professional 10 years ago:
  - a nice although unfunded group you joined once no longer considered productive or relevant.

- Security Researcher 10 years ago:

InfoSec Today

- The New Face of Security
  - Hack for profit
Attacker Evolution

- **Evolution of tools for “hacking” and reverse engineering**
  - Barrier for entry into hacking has been removed
    - Widespread access to drag and drop tools for malware and exploits
    - No more script kiddies

- **Change in focus and goals**
  - defacements → worms → botnets → targeted attacks

- **Evolution of attacks**
  - Migration from widespread and noisy to targeted and malicious

- **A traditional economic structure has evolved**
  - As well as several parasitic micro economies
    - Malware market
    - ID theft rings
    - Organized crime

- **Criminal Organizations have matured**
  - Nearly unlimited money & resources
  - Longer term focus and multi year planning
  - Mature engineering practices
  - Focus on specifics…right down to the individual
  - “cyber espionage”
Information Security Evolution

• As attacks matured, security as a profession grew with demand for abilities to specialize.
  – MCSE certifications for security professionals
  – Academic offerings of Information Security degrees
  – Specialized certifications, such as CISSP

• New industries emerged.
  – Business dedicated to protecting the enterprise and consumer
  – Specialized companies protecting against ID theft and online fraud
  – Specialized hardware and tools for password protection, data protection
  – Organizations offering training to the enterprise on security practices
  – Insurance companies now offering “ID theft protection” policies

• Products and strategies were developed to disrupt some of the negative by-products.
  – Antivirus, IDS/IPS, Vulnerability Scanners
    • Zero Day Initiative
• **Defined:**
  – An economy is the realized system of human activities related to the production, distribution, exchange, and consumption of goods and services of a country or other area.

• **Six necessary components of an economy**
  – Product
  – Supply
  – Demand
  – Currency
  – Participants
  – Marketplace
In the mid-20th century two economists noted that a sign of a maturing economy was a transformation from industrial and production jobs to service jobs.

Three sectors of an economy:

- **Primary sector:**
  - Involves the extraction and production of raw materials, such as corn, coal, wood and iron.
  - In our Vulnerability Economy, the raw material is the flaw or “Vulnerability” itself

- **Secondary sector:**
  - Involves the transformation of raw or intermediate materials into goods e.g. manufacturing steel into cars, or textiles into clothing.
  - During this stage, the Vulnerability is transformed into exploit code, malware, viruses and the products which protect, defend against and scan for them.

- **Tertiary sector:**
  - Involves the provision of services to consumers and businesses
  - Enter the services organizations. Business has boomed in this sector, with entire companies popping up to provide a variety of “information security services” – Penetration Testing, training, etc.

Increased demand for services is a direct result of economic maturation!
Product and Supply: Vulnerabilities

- **Product**
- **Supply**
- **Demand**
- **Currency**
- **Participants**
- **Marketplace**

- 100,000+ Software Products
- 10,000+ Vulnerabilities
- >5000 Researchers

**Vulnerabilities in MITRE’s CVE**

- 1999
- 2000
- 2001
- 2002
- 2003
- 2004
- 2005
- 2006
- 2007
Demand

- Product
- Supply
- **Demand**
- Currency
- Participants
- Marketplace

- Vendors
- Solution/Protection providers
- Consultants, Pen Testers, Analysis firms
- Independent Researchers
- Government
- Malware markets
- Organized Crime
- The list could go on…
Currency

• Product
• Supply
• Demand
• Currency
• Participants
• Marketplace

• Trade for information, intelligence
• Trade for online useful wares, such as stolen CC numbers, compromised gear, botnets
• Trade for exploit code, tools, help with other research
• Trade for free software from vendor, trips to events
• Trade for favors, or future favors (Party Admission)
• Yes, money.
Participants

- **Product**
- **Supply**
- **Demand**
- **Currency**
- **Participants**
- **Marketplace**

- **The Software Vendors**
  - Most use a modified currency system of praise for positive behavior, contracting gigs, etc.

- **Protections Providers**
  - Most have independent research teams to ferret out unknown vulns, some contract with third party companies for information

- **Services Providers**
  - Most try to discover some 0day themselves for credibility, some purchase from others or hire out research

- **Independent Researchers**
  - Generally looking to make a living doing what it is they do well and enjoy. Often this means seeking resume building for employment and often selling directly to third parties.
Marketplace

- Product
- Supply
- Demand
- Currency
- Participants
- Marketplace

- Zero Day Initiative
- iDefense
- Wabasabi Labs
- Digital Armaments
- ImmunitySec
- Netragard/SONOSoft
- Government, Nation States
- Black market, organized crime
Key Vulnerability Markets at a Glance

**Vendor Partners**
- Vulnerabilities Purchased for AV/IDS/IPS protections
- Vulnerabilities reported to affected vendor
- Motivated to protect customers

**Brokers**
- Vulnerabilities are commoditized—bought and sold like an MP3
- Knowledge based on a subscription/membership or purchase of product and services
- Not motivated to protect users

**Underground**
- $$$ and information exchanged based on trust relationships
- Organized crime, individuals and .mil
- Not motivated to protect users
Economic Paradigm: Pharmaceuticals

The market for narcotics and medicine include:

- **Legitimate market** –
  - everything from over the counter pain relief, to prescription narcotics

- **Illegitimate market** –
  - Heroin, methamphetamine, marijuana, cocaine, etc

The market for vulnerabilities include:

- **Legitimate market** -
  - Legitimate vulnerability discovery and research
  - Useful tools to aid in research and development of secure products

- **Illegitimate market** -
  - Malware, exploit code, viruses etc.
The security economy has evolved during the age of information, and is now a global economic structure— with many interconnected and collaborative micro economies.

Economic Structure in place for years— created by consumer demand for secure products.

Demand and participants evolving— economy moving through “phases”.

The industry may never compare in size to the pharmaceutical industry but it can have just as much impact on society— chiefly through broad failures in information security.
Where do we go from here?

• The negative by-products of the InfoSec economy are not going away - we need to increase the ROI for legitimate markets.
  – Legitimate marketplaces for vulnerabilities can help keep that knowledge in the hands of defenders.
  – There is still little incentive for existing markets to handle the information properly.
  – Value of a vulnerability decreases once it’s reported to the affected vendor.

• As surely as security advances are discovered, so will new security attacks. Defenders must adapt and keep pace.
  – More positive cooperation with vendors
  – Increased collaboration between protections organizations
  – Building of stronger alliance and partnership within the security research community

• We must continue to invest in disruption of the illegitimate sector.
  – Increase the cost of doing illegal activities
    • Training, tools, and technical assistance for law enforcement
    • Encouraging appropriate penalties for malicious behavior
  – Provide security researchers access to programs, tools and opportunities that give them a legitimate outlet for their skills.

No organization can be secure alone - it will take a team of rivals working together to understand and combat the asymmetry between attack and defense.
Questions?

Terri Forslof
Manager of Security Response
tforslof@tippingpoint.com

www.tippingpoint.com
+1 888 TRUE IPS (+1 888 878 3477)