

# Undermining the Underground Economy: A Call to Arms

Giovanni Vigna

UCSB

[vigna@cs.ucsb.edu](mailto:vigna@cs.ucsb.edu)

FORWARD Workshop

Goteborg, Sweden, April 17-18, 2008

# The Underground Economy

- From “Hack For Fun” to “Hack For Profit”
- “Traditional” (Organized) Crime +  
Internet-scale Hacking = Large profit
- Complex composition of buyers, sellers, traders, service providers, etc
- Ever-changing, ever-expanding system

# A Motley Crew

- Computers with IP addresses registered to Telecom Italia accounted for the largest percentage of malicious activity in the world, with six percent of the total
- The United States was the top country of attack origin in the second half of 2007
- Madrid was the city with the most bot-infected computers, accounting for 3% of the worldwide total
- 43% of worms originated in the Europe, Middle East, and Africa (EMEA) region
- Government was the top sector for identities exposed

Source: Symantec Global internet Security Threat Report, 2Q 2007

# Varying Prices

Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	\$10-\$1000
2	1	Credit cards	13%	22%	\$0.40-\$20
3	7	Full identities	9%	6%	\$1-\$15
4	N/A	eBay accounts	7%	N/A	\$1-\$8
5	8	Scams	7%	6%	\$2.50/week-\$50/week for hosting, \$25 for design
6	4	Mailers	6%	8%	\$1-\$10
7	5	Email addresses	5%	6%	\$0.83/MB-\$10/MB
8	3	Email passwords	5%	8%	\$4-\$30
9	N/A	Drop (request or offer)	5%	N/A	10%-50% of total drop amount
10	6	Proxies	5%	6%	\$1.50-\$30

Source: Symantec Global internet Security Threat Report, 2Q 2007

# Analyzing the Underground Economy

- Identify the actors who participate in the underground economy and their different roles
- Analyze the structure of transactions and the information flow between actors
- Study the infrastructure used to support the criminal process
- Track relationships between events in different locations (e.g., eBay auctions vs. IRC chatter)

# Example: Clique Matching

- Some channels, such as IRC provide some form of anonymity (change of nickname)
- Some information stays fixed (e.g., ICQs)
- Generate graphs of social networks and then use “fixed-points” to identify cliques appearing in different environments

# Example: Active Information Tracking

- Create unique (email addresses, personal info, CC) and inject them in the (web, IRC)
- Track the information across domains and environments
  - Advertised shoe auction is bot sale on eBay
  - Email address scraped from host in Redwood, CA, three days later receives spam from host in China

# Example: Identify Shared Infrastructure

- “Bullet-proof” hosting provides fundamental infrastructure support for miscreants
- Need to develop automated tool to identify bullet proof hosts that are shared among scams
  - To maximize impact on infrastructure
  - To identify collaborations among groups

# Disrupting the Underground Economy

- Identify the human-intensive, human-involved steps of the process
- Devise techniques to make it harder to carry out certain steps of the process
  - Confusion
  - Inflation
- Hit the infrastructure nodes

# Conclusions

- Need for information sources
- Need for techniques to process large amounts of data and track information
  - Identify cliques and recurring “migratory” patterns
  - Automatically track information flows
- Need for tools to infiltrate the economy
  - Use the advantage of anonymity that so far has been mostly leveraged by criminals