Underground Economy or How to make some easy bucks

Eurosec 2009

Forward Project
Main Motivation

- Moving from “Hack for Fun” to “Hack for Profit”
- Targeted areas change with the objectives.
- How and where can obtained data/information be sold to interested parties?
- Traditional fraud mechanisms combined with technological knowledge led to a well-established underground economy.
Now, the goal is:
Klikparty, 2007
Post-Fraud action: What now?

- An example: Compromised Data includes
  - Credit Card + Information (CVC, Balance, etc.)
  - Bank account, Address, etc.
  - Infected Machine.
- In earlier days (1980 ~ 2000)
  - Success was just bragged with
    - Machine brought down/formatted
- Now
  - Log to CC - IRC Channel, announce the information
  - “Rent” a money drop, that takes 50% but empties the CC and bank account for you.
  - Launder the money and go to Hawaii
Trends in the Underground

- **New propagation vectors**
  - From mail to social networks
  - Spam-advertising fraudulent offers
- **New communication domains**
  - IRC, Web pages
  - IM (ICQ, MSN, etc.)
  - E-Mail (Nigerian Scam)
- **Advanced Bot nets**
  - Strong cryptography
  - Hidden channel communication
  - Very low interaction → Stealthy
Solution Approaches

- Surveillance of underground Channels
  - IRC, Web Forums, etc..

- Understanding the internal structure
  - Who buys what?
  - Payment?
  - Critical Systems?

- Disrupting possible weak links
  - From a Web Page to the advertising Spam Mail
  - Spam the scammers (involves human interaction)