An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants

J. Franklin, V. Paxson, A. Perrig, S. Savage

Proceedings of the 14th ACM conference on Computer and communications security (CCS '07), pp. 375-388, October 2007.

Presented by Chris Pilcher

Quick Summary

This paper presents research into the trading of illegal information (stolen credit card numbers, compromised hosts, online credentials etc) and services (DoS attacks, sending of phishing emails etc) on public Internet Relay Chat (IRC) networks.

Offers Valuable New Information

Paper gives a good insight into underground markets which are generally hard to analyse

- **Value**:
  - Shows detailed information on how these underground markets generally operate
  - Gives a good indication of the level and type of information and services being traded in these markets
- **New**:
  - Highly original work

Questionable Assumptions

Market visibility is low which means big assumptions have to be made in order to give estimates on the wealth of internet miscreants. These assumptions are likely to lead to very inaccurate estimates.

Questionable Assumptions - Examples

- To estimate the wealth generated from credit card data in this market the authors assume that all of the valid credit card numbers seen will lose $427.50 USD
- Authors make the assumption that the assertions made by sellers is the same as the sellers intentions for certain information

Question

The paper ends by briefly discussing two countermeasures for disrupting these underground markets:

- Sybil attack
  - Establish multiple identities -> achieve verified status -> make deceptive sales
- Slander attack
  - Remove verified status of buyers and sellers through defamation

Do you think these are efficient countermeasures?