Problem: Underground Economy

Cybercriminals are networking extensively online and a competitive underground economy has emerged, allowing them to trade goods and services for profit gain. This in turn provides them with the incentive to innovate and it is this relentless innovation which has turned cybercrime into the persistent problem we are seeing today.

Methodology

In collaboration with the Serious Organised Crime Agency (SOCA), this project has access to the database of several online stolen data markets. Given both qualitative and quantitative data, an interdisciplinary approach is taken:

- Theories from Criminology and Social Psychology are used to reason and model cybercriminal behaviour
- Methodologies and latest theories from network science and graph theory are used to capture social dynamics and exploratory analysis of network properties

Methodology

Understanding Cybercriminals: Their Attitudes, Behaviour and Facilitating Environments

Michael Yip, Nigel Shadbolt, Thanassis Tiropanis and Craig Webber
Cyber Security Centre
University of Southampton

Criminal Behaviour

Some insights into the mind of the cybercriminals so far:

Why they entered the crime?
- Previous record
- "Get rich or die trying"
- Desperate

Do they have any regrets?
- Too late for regrets, keep going
- Regret not entering the crime earlier
- Regret of previous wrong doing but too late for regrets, keep going
- Tired of the way of life e.g. loneliness, pressure from law enforcement
- Too much to lose e.g. made enough already and too much to risk
- Addictive way of life e.g. competition with peers

Scam college kids?
- Only scam large institutions because they can afford the loss
- Sure, morals can't pay bills
- People who can scam college kids are also those who can scam their peers – not trustworthy
- Scamming students may jeopardise their education

Social Dynamics

In order to disrupt cybercriminal networks, it is useful to capture the social dynamics so that behavioural patterns can be better understood and vulnerable regions can be identified:

- Preferential attachment – vendors with high reputation are preferred
- Random interaction – networking amongst cybercriminals leads to some interaction patterns that do not obey the rule of preferential attachment
- The integration of the two leads to a resilient social structure that is hard to disrupt

Carding Forum

Carding forums are online forums operating as online stolen data markets. They facilitate cybercrime in two ways:

- Mitigate transaction costs caused by the uncertainties surrounding online criminal trading and collaboration
- Provide a ready-made hybrid structure that offers power delegation and control – allowing administrators to enforce honest trading and create a network boundary from the rest of the web

Aim

To produce actionable intelligence for law enforcement to better understand and tackle cybercrime. Also, to enable other stakeholders to better anticipate risks to their assets. In order to achieve this, this project seeks to develop a thorough understanding of the cybercriminals: their attitudes, behaviour and social dynamics, both situational and general.

Questions to address include:
- Why do cybercriminals engage in the crime?
- How do they feel about their actions?
- When do they exit from the crime? Do they stay away?
- How can we capture their social dynamics?
- How to better disrupt their social networks?
- How do the cybercriminals behave differently when they encounter law enforcement on their social networks?