Organised Cybercrime

Matthew Edwards

Focus: Cybercriminology

November 8, 2020

Changes in Cybercrime

While some elements remain constant, there have been some significant changes in cybercrime over the past couple of decades.

In particular, we see a rise in:

1. Sophistication
2. Commercialisation
3. Organisation

Increasing complexity of cybercrime

2000s

- Botnets dial a central command location.
- Broad-spectrum scams hit inboxes everywhere.
- Ad-hoc spies probe unsecured university systems.

Modern

- Botnets self-organise communications in a peer-to-peer fashion.
- Highly-targeted, personalised spear-phishing emails.
- TBs of trade secrets and sensitive data exfiltrated.

Commercialisation of cybercrime

Many early offenders were not interested in money, but reputation.

There are nowadays many more “hackers for hire”, botnets, exploit kits & much more available for purchase or leasing.

Vulnerabilities are becoming extremely valuable, some selling for 100s of thousands of dollars – to many different buyers.

Organisation

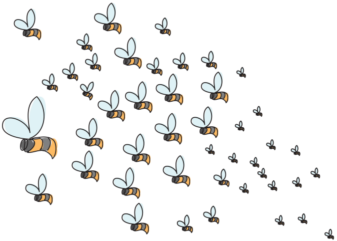
There are, to be sure, some cybercriminals who mostly work alone. They are more likely to be ‘hobby’ cybercriminals who don’t depend on cybercrime for a living, and at most exchange tips with peers.

Much of cybercrime, however, is the work of formal or informal organisations.

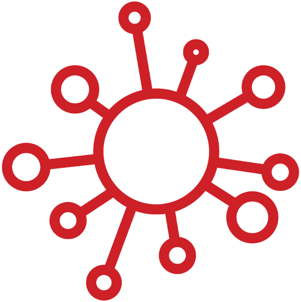
Increased organisation of criminal activity helps drive complexity & commercialisation.

Online structures

Swarm

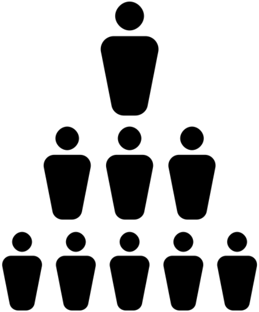


Hub



'Hybrid' structures

Offline and online offending can be combined by traditional organised crime groups, which have their own, often *hierarchical* structures.



Interests: Organised Crime

Traditionally, pre-existing offline social ties were a requirement for involvement. This is now changing as organised crime moves online, and merges with online crime's norms around anonymous online social ties.

Benefits from overlap in capabilities, e.g., online criminals providing exploits, offline criminals providing money mules to move and launder funds.

Specialisation & roles

Most sophisticated cybercrime relies on *specialisation* – like any other industry.

By creating an *economy*[1] where these specialisations can interact and individuals get paid for their work, better work can be achieved.

A major fraud operation might involve the work of various coders, technicians, vendors, fraudsters, hosts, cashiers and money mules, not to mention the individuals finding and selecting targets.

[1] Foreshadowing – more on cybercriminal economies later.

Interests: State Actors

Governments commit cybercrime[2].

A range of levels of involvement:

- State monopoly on cybercrime (e.g., North Korea);
- Formal collaboration between state and non-state cybercriminals (e.g., NSA data capture);
- Loose cooperation with cybercriminals (some Chinese espionage);
- Sponsorship of cybercriminals (e.g., Russian disinfo);
- Tacit encouragement of non-state cybercrime (e.g., Russia);
- Selective ignorance of certain cybercrime;
- State incapable of stopping cybercrime;

[2] Gasp.