THREAT ACTORS IN THE CYBER BLACK ECONOMY

Andrew Smith, Research Assistant
Centre for Risk Studies
Economic Loss Caused by Threat Actor Categories

Percentage of Economic Loss per Threat Actor Category

- Organised Criminal Hub
- Nation State and State-Sponsored
- Organised Cyber Criminal: Hub and Hierarchical
- Mercenary Hackers
- Hacktivist
- Other: Script Kiddies, Cyber Terrorist

Estimated $1.5 Trillion of economic loss caused by threat actors
Sample of Known Threat Actor Groups

- Nation State
  - NSA
  - GCHQ
  - Comment Panda

- State-Sponsored
  - Sofacy (Fancy Bear)
  - Lazarus Group
  - Equation Group

- Mercenary
  - Hidden Lynx

- Organised Crime
  - Carbanak
  - Wolf Spider
  - Butterfly
  - Carberp
  - Cobalt
  - DarkHotel

- Vigilante Hackers
  - Lulsec
  - Lizard Squad

- Hacktivists
  - Anonymous
  - Syrian Electronic Army
  - TeaMp0ison

- Cyber Terrorism
  - Hezbollah Cyber Group
  - Tunisian Fallaga Team
  - United Cyber Caliphate

Energetic Bear

Lulsec

Syrian Electronic Army
Threat Actor Annual Activity

Threat Actor Activity 10/2016-12/2017

APT 28 (Sofacy)
APT 29 (Cozy Bear)
Lazarus
Turla Group
Annuak
Emissary Panda
Cobalt
Ener... Bear
APT 30

11 Events To Scale

- Russian State-Sponsored
- Organised Cyber Criminal
- North Korean State-Sponsored
- Chinese State-Sponsored
Organised Cyber Criminals Groups: Hub and Hierarchical

- Organised cyber criminal groups are motivated by financial gain
  - Maximise profits
- Two distinct business models of cyber criminal organisations
- Hierarchical groups are similar to traditional organised crime groups
  - Clear management structure
  - Division of labour
  - Often operate in physical premises
- Hub groups operate solely as a ‘black e-commerce’ organisation or as a ‘hybrid’
  - Core group of threat actors
  - Solicitate the help of associates in their network

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Skill Level</th>
<th>Labour</th>
<th>Resources</th>
<th>Visibility</th>
<th>Targeting</th>
<th>Motivations</th>
<th>Geo Target</th>
<th>Threat Rank</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub</td>
<td>Medium</td>
<td>8*</td>
<td>$0.1m</td>
<td>Covert</td>
<td>Opportunistic</td>
<td>Monetary</td>
<td>No</td>
<td>4</td>
<td>6400</td>
</tr>
<tr>
<td>Hierarchical</td>
<td>Medium</td>
<td>27</td>
<td>$1-3m</td>
<td>Covert</td>
<td>Opportunistic</td>
<td>Monetary</td>
<td>No</td>
<td>3</td>
<td>4500</td>
</tr>
</tbody>
</table>
Hackonomics: Behaviour of Cyber Criminals

- Hacknomics perspective: business model of threat actors
- Cyber threat actors have scarce resources
  - Opportunity cost
- Targeting decisions based on a cost-benefit framework
  - Logistical burden vs expected benefits
- Regime changes in the cyber risk landscape alter the equilibrium of the cyber black economy
Regime Shift: Cyber Black Markets

- The development of black markets has changed the business model of cyber criminals
- Estimated 18 active markets in the cyber black economy
- Emergence of new business model: Crime-as-a-service
- Marketplace products
  - Stolen records
  - Zero-day exploits/exploit kits
  - Malware
  - Mercenary hackers
Decreasing Price of Commodity Malware

- Cyber criminal business models are not following internal economies of scale
  - Outsourcing
- Commodity malware decreases the skill level and resource cost per attack
  - Lowers logistical burden
  - Reduces barriers to entry
- More cyber criminals in the black economy
- Likely increase in the frequency of attacks

![Graph showing Decreasing Price of Ransomware Sold on Black Markets](graph.png)
Internal Production vs Outsourcing Example

Locky Ransomware: Internal Production

- Skills: Highly Experienced Coder
- Team size
- Resource Cost
- Time
- Total Logistical Burden: 260

Petya Ransomware: Outsourcing

- Skills: Coder
- Team size
- Resource Cost
- Time
- Total Logistical Burden: 180
Mitigating Threat Actor Activity

- **What does hackonomics teach us about reducing cyber risk?**
- **Targeting behaviour**
  - Map companies characteristics to motivations and capabilities of threat actors
  - Target substitution: path of least resistance for threat actors
- **Combat crime as-a-service model**
  - Patch maintenance
  - Incentivise ‘white/grey’ hat actors
  - Increases logistical burden
- **Understand how future trends alter the fragile equilibrium between cyber attackers and defenders**