Cambridge Centre for Risk Studies

Advisory Board Research Showcase – 23 January 2018

Hackonomics:
Regime Shifts in the Black Economy

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Andrew Smith
Research Assistant
Cambridge Centre for Risk Studies

Hackonomics and the Cyber Black Economy

- The cyber black economy
  - Part of the cyber landscape which is unrecorded/untaxed
  - Illegal activity: Interaction between hackers and companies/organisations
  - Black markets
- Cyber threat actors operating in the black economy
- Hackonomics: Understanding threat actor behaviour
  - Business model perspective
- Regime changes can alter the black economy

Sample of Known Threat Actors in the Black Economy

- Nation State
  - NSA
  - GCHQ
  - Comment Panda
- State-Sponsored
  - Sofacy (Fancy Bear)
  - Lazarus Group
  - Equation Group
- Elite Mercenary
  - Hidden Lynx
- Organised Crime (APT)
  - Carbanak
  - Wolf Spider
  - Butterfly
- Organised Crime (Other)
  - 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

Sample of Known State Sponsored/ Nation State Groups

China
- APT 1(Comment Panda)
- APT 3 (Gothic Panda)
- APT12 (Numbered Panda)
- APT 16
- APT 17(Deputy Dog)
- APT 18(Dynamite Panda)
- Putter Panda
- APT30 (Naikon)

North Korea
- Bureau 121
- DarkSeoul Gang
- Lazarus Group

Russian
- APT 28 (Fancy Bear)
- APT 29 (Cozy Bear)
- Energetic Bear (Crouching Yeti)
- Turla (Venomous Bear/Snake)

US
- Equation Group
- NSA
- Tailored Access Operations
- Animal Farm

Iran
- Tarh Andishan
- Ajax Security Team/ 'Flying Kitten'
- ITSecTeam

Israel
- Unit 8200
- Duqu Group

Palestine
- AridViper

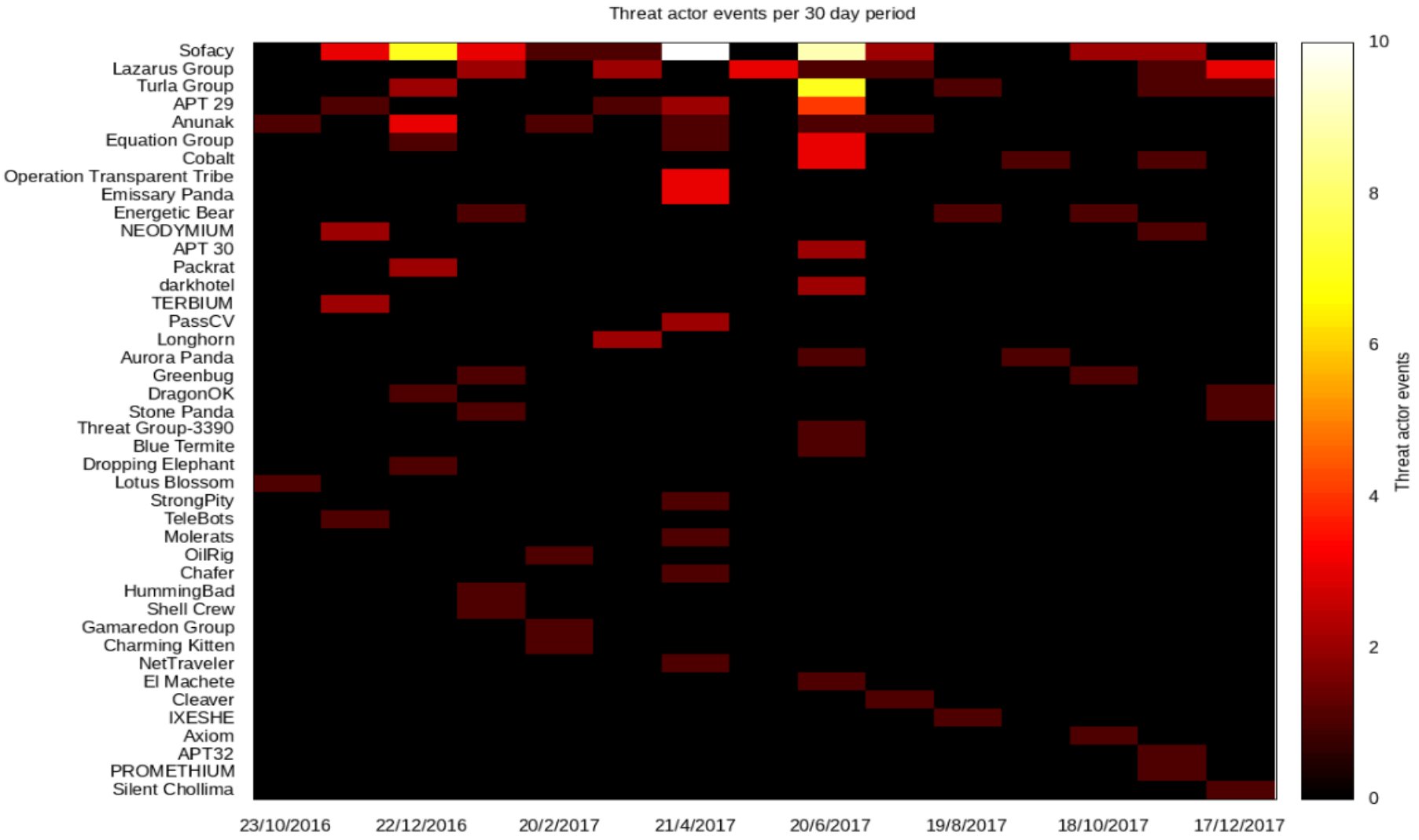
Lebanon
- Volatile Cedar

Syria
- Syrian Electronic Army

Vietnam
- APT32

Estimated total state-sponsored/nation state groups: **91**

Threat Actor Annual Activity



Source: MISP Database

Hackonomics: Behaviour of Threat Actors

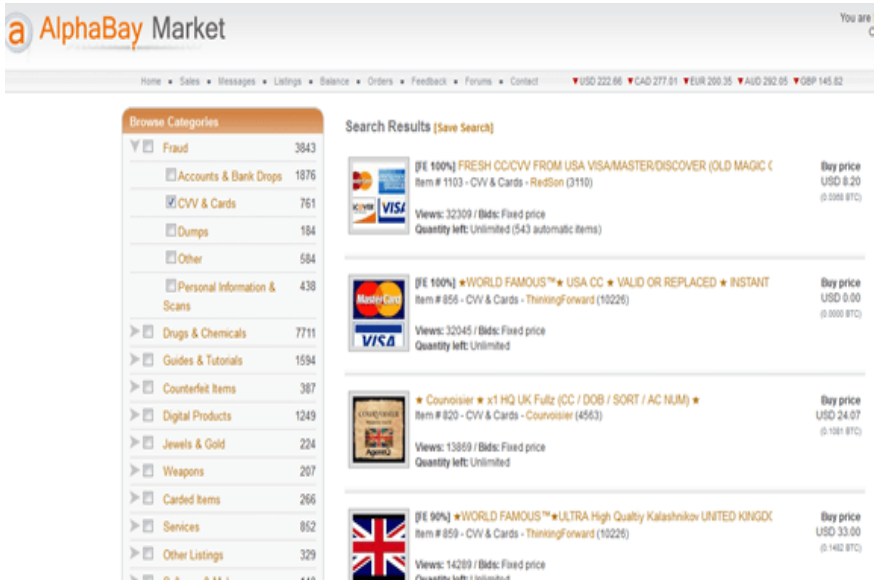
- Business model of threat actors
- Cyber threat actors have scarce resources
  - Opportunity cost
- Targeting decisions based on cost-benefit framework
  - Logistical burden vs expected benefits
- Regime changes in the cyber risk landscape can alter the economics of hacking (hackonomics)

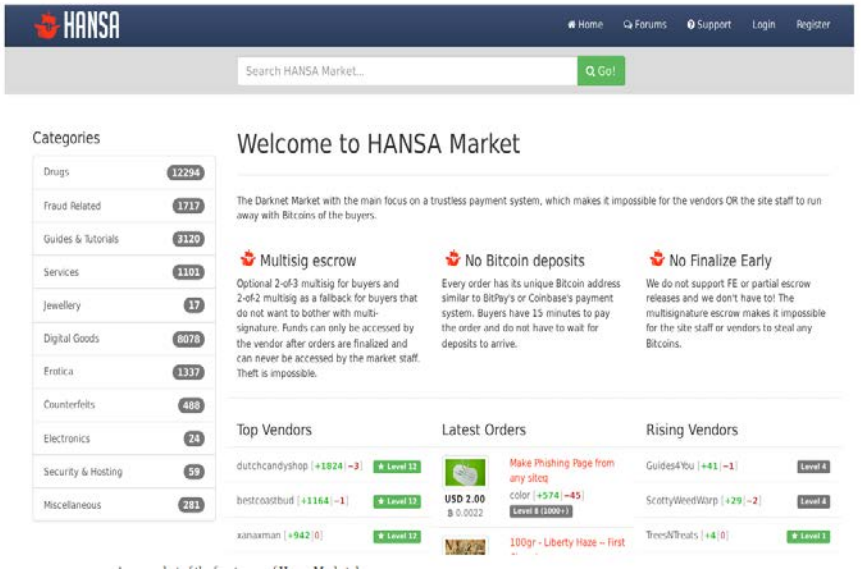
Regime Shift: Cyber Black Markets

- The development of black markets has changed the business model of threat actors
- Estimated 18 active markets in the black economy
- Emergence of new business model: Crime-as-a-service
  - Malware-as-a-service
  - Ransomware-as-a-service
- Marketplace products:
  - Stolen records
  - Zero-day exploits
  - Exploit kits
  - Malware
  - Mercenary hackers

Examples of Cyber Black Markets

- Two of the largest black markets were AlphaBay and Hansa Market.
- AlphaBay had an estimated 300,000 listing:
  - Hansa 14,544 listings
- AlphaBay facilitated an estimated $292 million worth of sales
  - Hansa $3.2 millions
- Both markets were taken down by the U.S. and Dutch law enforcement





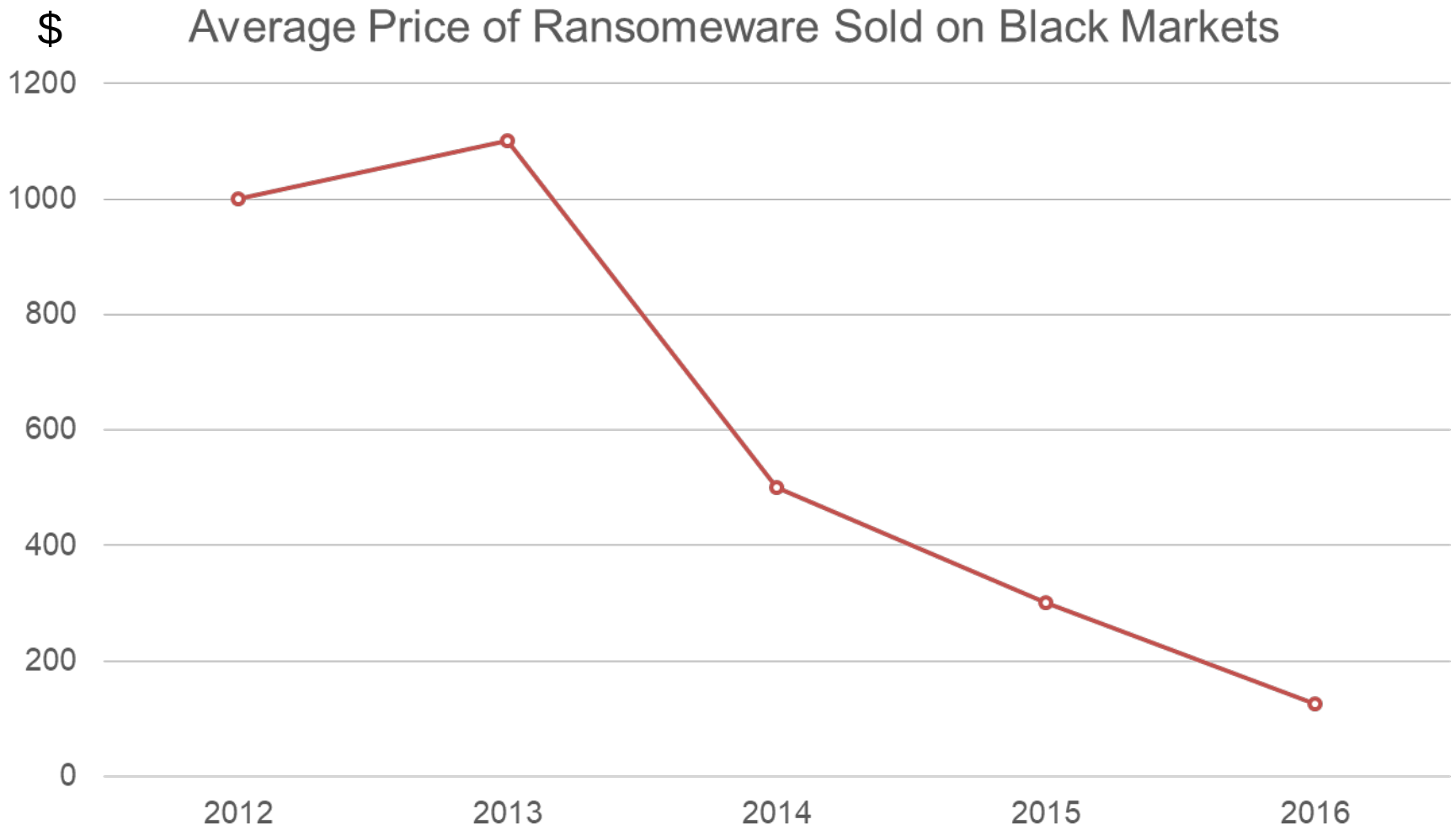
Sample Price List of Black Market Products

Internal Cost of Production of Zero-Day's: up to $1 million; Cost of Commodity Zero-Day's: $5000-$100,000

Type	Malware Name	Price
Exploit Kits	Whitehole	$600 month
	Sweet Orange	$1800/month
	Eleonore	$1000
	Gpack	$1000
	Cool (+crypter+payload)	$10,000/per month
Zero-Day	Windows	$60,000
	Microsoft Office	$50,000
	Mac OSX	$20,000
	iOS	$100,000
	Chrome/Internet Explorer	$80,000
	Abode Reader	$5000

Source of Data: RAND, 2015

Average Price of Ransomware Declines



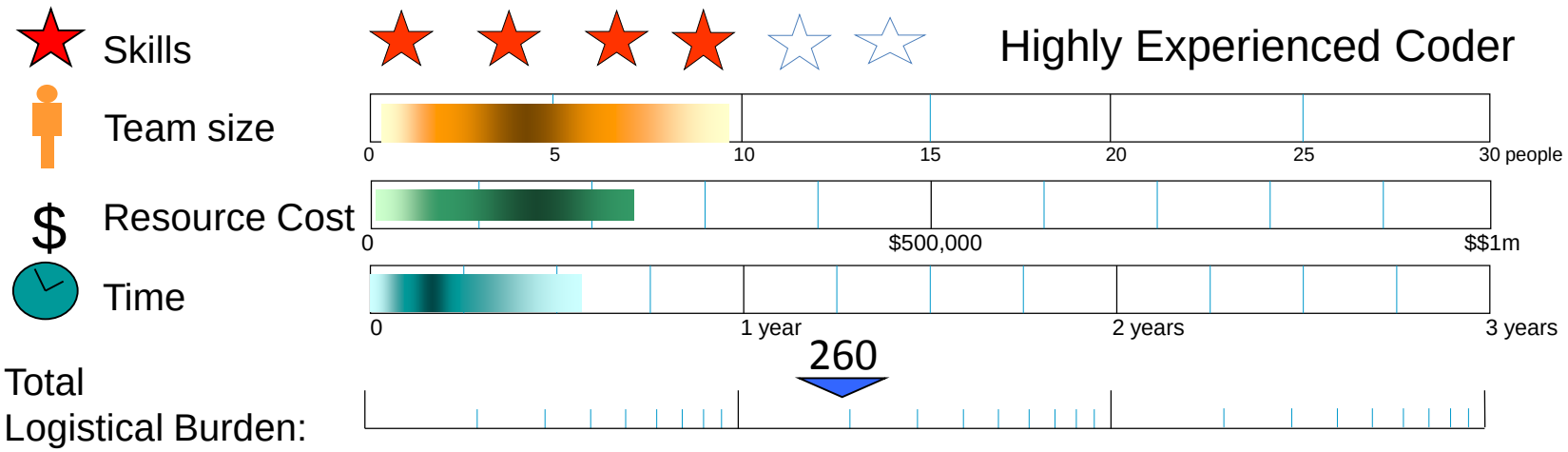
Sources: Trend Micro, 2016; Barkley Blog, 2015

Hackonomics of Commodity Malware

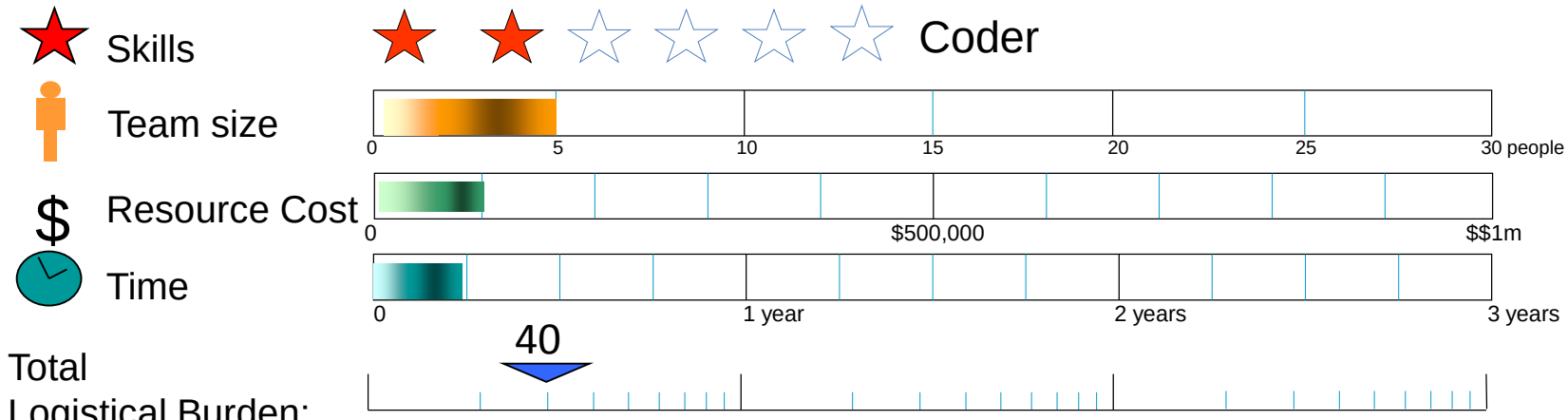
- Threat actors business model is not following internal economies of scale
  - Outsourcing
- Commodity malware decreases the skill level and resource cost per attack
  - Lowers logistical burden
  - Reduces barriers to entry
- More threat actors in the black economy
- Likely increase in the frequency of cyber attacks

Internal Production vs Outsourcing Example

NotPetya Attack: Internal Production



NotPetya Attack: Outsourcing



Hackonomics and Cybersecurity

- Hackonomics perspective of mitigating cyber attacks
  - Increase logistical burden
  - Reduce profits available to threat actors
- Combat crime-as-a-service model:
  - Patch maintenance
  - Incentivise ‘white hat’ hackers
- Understand how future trends alter the fragile equilibrium between cyber attackers and defenders
- Law enforcement losing the battle for resources

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Andrew Smith
a.smith@jbs.cam.ac.uk