Cambridge Centre for Risk Studies Advisory Board Research Showcase – 23 January 2018

#### **Hackonomics:**

#### **Regime Shifts in the Black Economy**

Centre for Risk Studies



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

- 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

1

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



- Palestine
  - AridViper
- Lebanon
  - Volatile Cedar
- Syria
  - Syrian Electronic Army
- Vietnam
  - APT32

Estimated total state-sponsored/nation state groups: 91



# **Threat Actor Annual Activity**

Threat actor events per 30 day period



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-aservice
  - 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

initia e para e managar e pa	ings • Bala	nce • Orders • Feedback • Forums • Contact VUSD 222.86 VCAD 277.01 VEUR 200.35 VAUD 292.05 V	G8P 145.82			5ea
Browse Categories		Search Results (Save Search)				
Y E Fraud	3843	WE MAN EDGEN COMMAN EDGE UPA MEANINGTED DISCOULED (ALD MARKS)	Province .	Categories		We
Accounts & Bank Drops	1876	Rem # 1103 - CW & Cards - RedSon (3110)	USD 8.20 (0.000 8TC)	Drugs (12294)		
CVV & Cards	761	VISI Views: 32309 / Bids: Fixed price		Fraud Related	1717	The D
Dumps	184	Geantity left: Unlimited (543 automatic tiems)		Guides & Tutorials	3120	away
Personal Information &	438	IFE 100% +WORLD FAMOUS*** USA CC * VAUD OR REPLACED * INSTANT	Buy price	Services	1101	*
Scans		Madel Curv Item # 856 - CVV & Cards - ThinkingForward (10226)	USD 0.00 (0.000 BTC)	lewellery	<b>67</b>	Optio 2-of-2
Drugs & Chemicals	7711	Viso Views: 32045 / Bids: Fixed price				de not signate
Guides & Tutorials	1594	Second Arts of the second seco		Digital Goods	8078	the v can n
> 🗈 Counterfeit Items	387	+ Consider + of HOLEV Fully (COLODRY SODT / AC MINA +	Bre price	Erotica	1337	Theft
E Digital Products	1249	construction # 820 - CV/ & Cards - Councilsier (4563)	USD 24.07 (0.1001 8TC)	Counterfeits	488	
>  ☐ Jeweis & Gold	224	Agent		Electronics	24	Top Ve
➤	207	- Annual Arc Commun		Security & Hosting	59	dutch
Carded Items	266	IFE 90%] +WORLD FAMOUS **+ULTRA High Quality Kalashnikov UNITED KINGDC	Buy price	Miscellaneous	(281)	besto
Services	852	Nem # 859 - CW & Cards - ThinkingForward (10226)	USD 33.00			

HANSA				# Home	🔾 Forums	• Support	Login Regist	
		Search HANSA Market		Q Go!	ļ.			
tegories		Welcome to HANS	A Mark	et				
rugs (	12294							
aud Related	1717	The Darknet Market with the main focus on a away with Bitcoins of the buyers.	a trustless payme	nt system, which makes it im	possible for t	he vendors OR th	ne site staff to run	
uides & Tutorials	3120							
rvices	1101	Multisig escrow	✤ No Bitcoin deposits Every order has its unique Bitcoin address similar to BiPysis or Cohases apament system. Buyers have 15 minutes to pay the order and do not have to wait for deposits to arrive.		🕹 N	✤ No Finalize Early We do not support FE or partial escrow releases and we don't have to! The multisignature escrow makes it impossible for the site staff or vendors to steal any Bitcoins.		
wellery	Ð	Optional 2-0F3 multisig for buyers and 2-oF2 multisig as a fallback for buyers that do not want to bother with multi-			release multisie			
gital Goods	8078	signature. Funds can only be accessed by the vendor after orders are finalized and			for the Bitcoin:			
otica	1337	can never be accessed by the market staff. Theft is impossible.						
unterfeits	488							
actronics	23	Top Vendors	Latest Orders		Risin	Rising Vendors		
curity & Hosting	69	dutchcandyshop [+1824  -3] * Level 12	65	Make Phishing Page from any sites	Guides	4You  +41 -1	Level	
scellaneous	281	bestcoastbud [+1164[-1] + Level 12	USD 2.00 8 0.0022	color [+574]-45]	Scotty	WeedWarp [+29]	-2 Level	
		xanaxman [+942]0] * Level 12	NEIGHT	100or - Liberty Haze Firs	TreesN	heats (+4(0)	+ Level	



# **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

Туре	Malware Name	Price	
	Whitehole	\$600 month	
	Sweet Orange	\$1800/month	
Exploit Kits	Eleonore	\$1000	
	Gpack	\$1000	
	Cool (+crypter+payload)	\$10,000/per month	
	Windows	\$60,000	
	Microsoft Office	\$50,000	
Zero-Day	Mac OSX	\$20,000	
Zei 0-Day	iOS	\$100,000	
	Chrome/Internet Explorer	\$80,000	
	Abode Reader	\$5000	

Source of Data: RAND, 2015



#### **Average Price of Ransomware Declines**



## **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**



# **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**



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