RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: MASH-F01

INTO THE WEB OF PROFIT: TRACKING THE PROCEEDS OF CYBERCRIME

Dr. Michael McGuire: University of Surrey

Backgrounds

- Web of Profit Project
- Brief: – to understood the outputs of cybercrime, not its inputs
- Not what cybercriminals ‘do’ - attack vectors, malware types, perpetrators, computer dependent v computer enabled crime variants, etc
- Why cybercriminals ‘do’ - Revenues, laundering, spending investments, etc.

Once upon a time…..

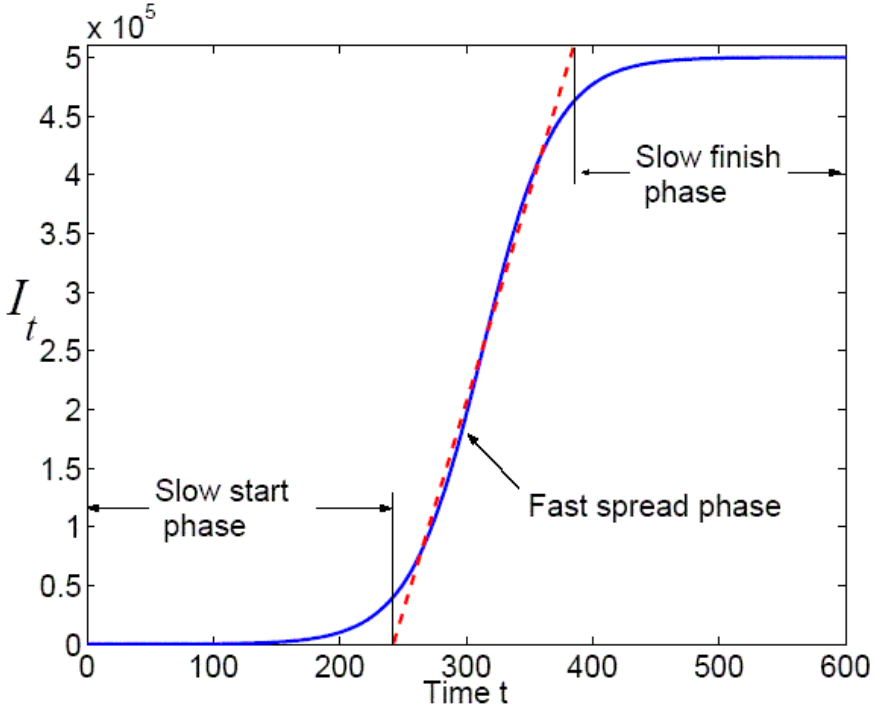
- We (thought) we knew what ‘the problem of cybercrime’ amounted to.
- It happened in a place called ‘cyberspace’

Once upon a time…..

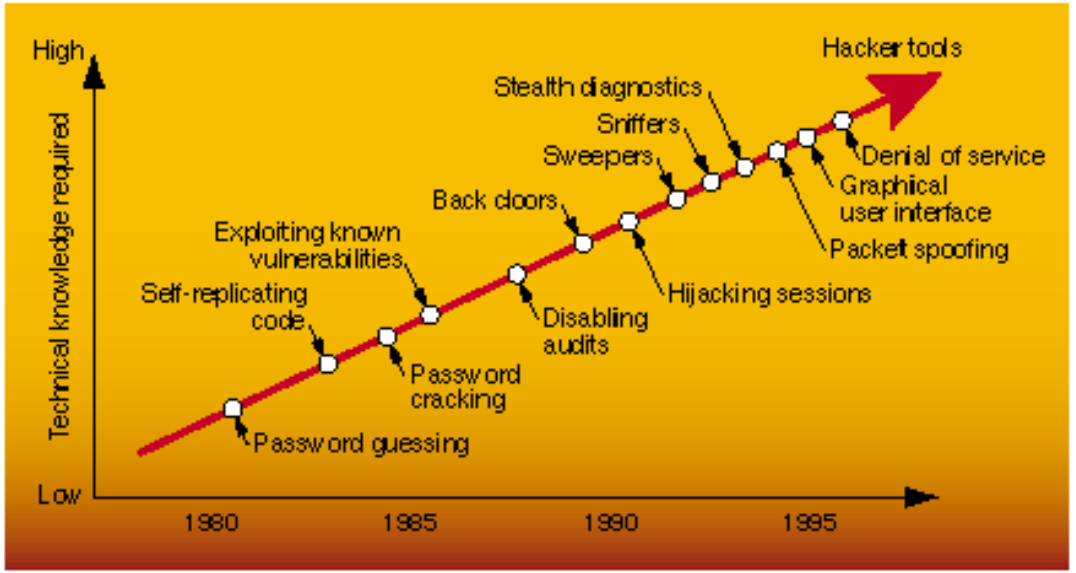
- It was something to do with ‘computer intrusions’

Once upon a time…..

- It involved ‘viruses’, ‘infection rates’, ‘firewalls’ and so on….



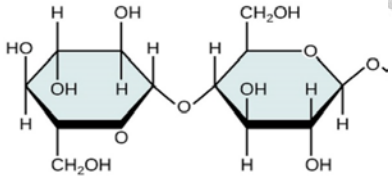
Once upon a time…..



- Tech savvy criminals acquiring ever more sophisticated technical skills
- An arms race, where law enforcement and governments “can’t keep up”

In 2018…

- A range of specialised economic agents, such as producers, suppliers, service providers and consumers
- The extraction and exchange of data as the key raw material and trading item
- Beyond the buying or selling data from stolen credit or debit cards
- Includes newer data forms with value:
  - hotel/airline loyalty points
  - Netflix log ins
  - ‘likes’ on Facebook
  - soft drink formulas
  - healthcare records



In 2018…

- Dedicated production zones and centres of income generation
- EG ‘Hackerville’ fraud villages in Romania
- Troll factories in Moscow

Râmnicu Vâlcea

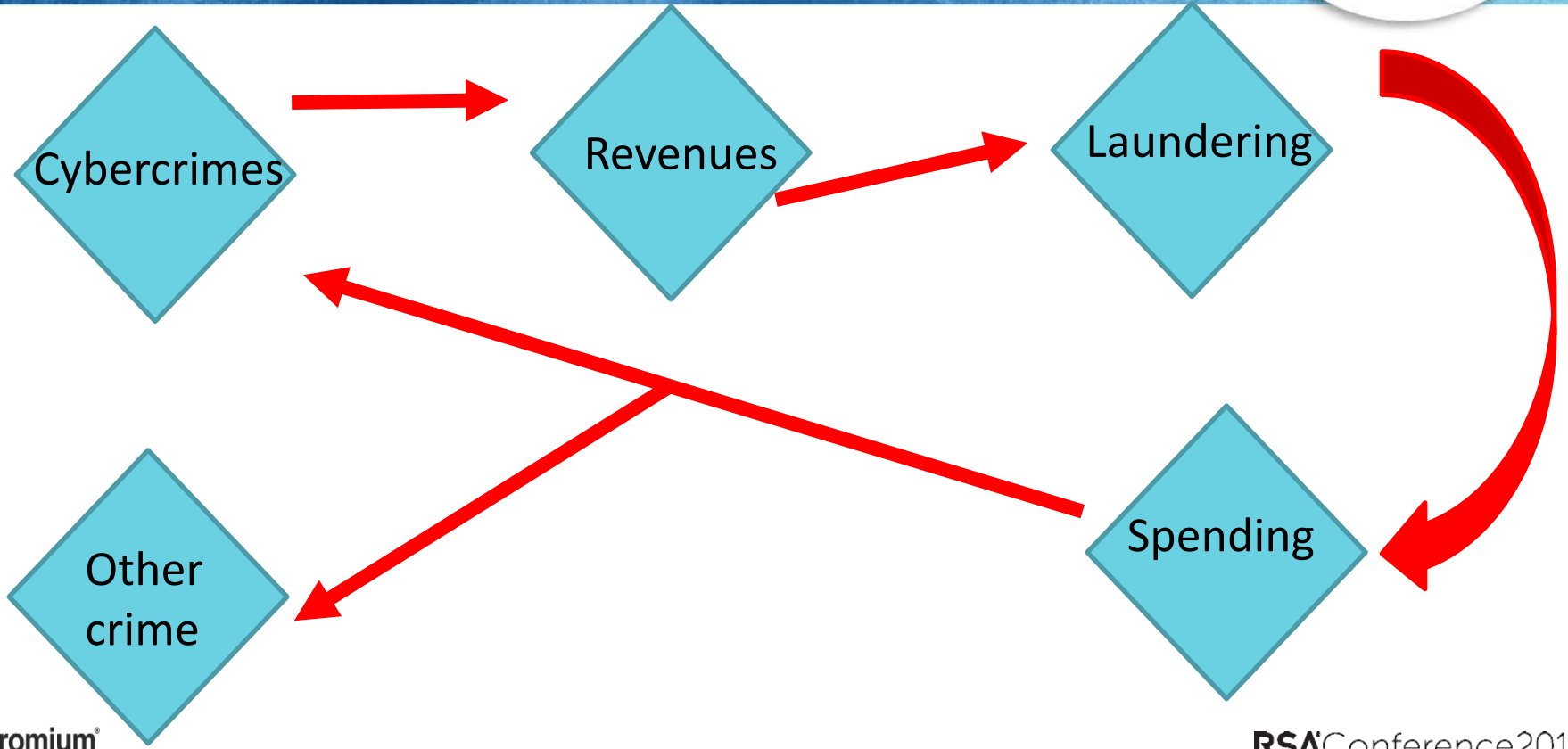
Internet Research Agency
Savushkina Street, St. Petersburg

In 2018…

- Romance fraud offices in Accra, Ghana

- Online counterfeiting centres in China/Vietnam/etc

A Cybercrime Economy



The Cybercrime Economy: Revenue Generation

$1.5 trillion dollars profits annually - AT MINIMUM

Illicit/illegal online markets	c**$860bn** *per annum*
Trade Secret/IP theft	c**$500bn** *per annum*
Data Trading	c**$160bn** *per annum*
Crimeware/CaaS	c**$1.6bn** *per annum*
Ransomware	c**$1bn** *per annum*

The Cybercrime Economy: Revenue Generation

- High earners make up to **$2m/£1.4m** – almost as much as a FTSE250 CEO
- Mid-level criminals make up to **$900,000/£639,000** – more than double the US presidential salary
- Entry level hackers make **$42,000/£30,000** – significantly more than the average UK graduate

The Cybercrime Economy: Laundering Revenues

- UN estimates that money being laundered equivalent to around 1.7 – 2% of Global economy
- Up to $2 tn
- Cybercrime revenues being laundered constitute anything between $80 – $200 bn

How is this done?

The Cybercrime Economy: Laundering Revenues

Three main methods:

(i) Digital Means

- 4% of global money laundered is by crypto currency (around $80bn)
- 10 - 20% of cybercriminals using PayPal or other DPS systems to launder money
- Use of e-commerce sites for ‘transaction laundering’
- Alternative ‘value-bearing’ digital means e.g gaming currencies - especially in Korea and Far East.

The Cybercrime Economy: Laundering Revenues

- Bitcoin ATMS, drugs and prostitution
- Israeli hacking services group VDos used Paypal to collect over $600,000 in revenues and to launder them
- Mueller investigation has revealed 13 Russians stealing US social security numbers to open PayPal accounts for fake IDs
- In 2016, 10 Dutch nationals were arrested after trying to launder up to 20m Euros from drug trafficking proceeds by selling these on the black market using bitcoins

(ii) Traditional Means

- Shell companies; money mules; casino laundering; wire transfers
- In 2017, Western Union ordered to pay $586m by DoJ
- Found to have enabled transfer of around $632 million up to 2015 in relation to online lottery scams, romance frauds, 419 scams and so on.

(iii) 'Mixed' Methods

- One operation tracked by researchers combined stolen cards used for online purchases with physical transport and subsequent resale.
- This brought in an annual revenue of $7.3 million and contributed to nearly $1.8bn in laundered revenue

The Cybercrime Economy: Spending Revenues

Not much changes?

- 15% of cybercriminals sampled spent the majority of their revenues on immediate needs – e,g. **paying their bills**
- 20% of cybercriminals sampled spent the majority of their revenues on hedonistic purchases – eg. **buying drugs** or **paying prostitutes**
- 15% of cybercriminals sampled spent the majority of their revenues on luxury items for status eg **expensive jewellery, sports cars etc**

The Cybercrime Economy: Spending Revenues

Everything changes?

- 30% of cybercriminals sampled spent the majority of their revenues on investments or assets – e.g **property** or **financial instruments**, and other items that hold value such as **art** or **wine**
- 20% of cybercriminals spend at least some of their revenues of reinvestments in further criminal activities – everything from **buying equipment** for additional **crimeware to terrorist funding….**
- Cybercrime could be recycling as much as **$300bn** into funding new or existing cybercrimes or for other, potentially more serious offending such as terrorism or trafficking

Conclusions: Platform Criminality: a revolution in crime?

- 'Platform capitalism'

- The cybercrime economy and 'Platform Criminality'?

Recommendations & Applications

For Law Enforcement

- Shift focus from crime control/prevention approaches
- Identify key disruptive nodes within the cybercrime economy
- Tailor traditional ‘market intervention’ strategies towards hyperconnected markets
- Develop more sophisticated tools & techniques such as network flow modelling; predictive software; automated/intelligent intervention
- Develop more specialised teams with cybereconomy specific skills
- Acquire methods for better kill chain analysis of revenue oriented malware
- Work more closely with platform providers to target misuse and reduce opportunity

Recommendations & Applications

For Cybersecurity professionals

- Move beyond simplistic ‘firefighting’ approaches
- Develop more holistic responses to the cybercrime economy
- Greater preparedness to work with financial agencies and the police
- Recognise that data and data protection is about more than privacy or security *simpliciter*
- Treat data more like traditional currencies
- Develop tools better able to isolate and uncover cybercriminal activity within the Web of Profit – eg virtualisation tools which generate ‘safe havens’ where illicit revenue generating activity can be diverted and neutralized
- Ensure that a key element in protecting data is the disruption of cybercrime supply chains