Cybercrime Inc.

Rui Miguel Feio

Security Lead

RSM Partners

Agenda

- Introduction
- Technical evolution
- The next-generation criminal organization – Cybercrime Inc.
- The organization
- Adapt to the new
- Examples
- The targets
- The hackers
- The mainframe
- Conclusion
- Questions

Introduction

- Rui Miguel Feio
  - Security lead at RSM Partners (UK)
  - I am a mainframe technician specialising in mainframe security
  - Experience in other platforms as well
  - I have been working with mainframes for the past 16 years
  - Happy to take questions as we go

Technical evolution

In the early years…

Technology

- Phones
- PC
- Bulletin Board Systems
- Internet

The ‘curious bunch’

- Phreakers
- Crackers
- Hackers

In nowadays…

Technology

- Phones
- PC
- Internet
- Smart phones
- Tablets
- Dark Web
- Internet of Things (IoT)
- Advent of Robotics

'Curious bunch' turned Pro

- Phreakers
- Crackers
- Hackers
- Carders
- Nation-states
- Foreign Intelligence Services
- Hacktivists
- Insiders
- Organized Crime Groups

Money, money, money

- Tech evolution + Internet = New Business Opportunities
  - Individuals started online businesses
  - New major companies have been founded:
    - Google, Facebook, Yahoo, etc.
  - Existing business sectors turned online to increase their earnings:
    - Retail, financial, insurance, etc.

Society has evolved…

- With the internet a new economic market has been created
- The new economic market has no borders
- A market with hundreds of millions of users
- An economic market worth… Trillions of Dollars!!
- Developed countries are now dependent on this new economic market

If there is money, there is crime!

- Criminal gangs and organizations moved into the new economic market:
  - Started recruiting Hackers
  - Started devising new “business ideas”
  - Developed a “business plan”
- Organized crime became professional in the new internet world.

The next-generation criminal organization CYBERCRIME INC.

Cybercrime Inc.

- Highly profitable (it's always about the money)
- Low risk (anonymity and geographical location)
- More efficient due to technology
- Globally dispersed, with special concentration in:
  - Ukraine
  - Russia
  - Romania
  - Bulgaria
  - China
  - Indonesia
  - Taiwan
  - India
  - Brazil
  - USA
  - Turkey

Cybercrime Inc.

- 80% of Hackers work with or as part of an organized crime group
- Highly organized
- Deeply sophisticated:
  - Business approach
  - Towards the ‘client’

Cybercrime Inc.

- Use typical corporate strategies:
  - Creative financing
  - Global logistics
  - Supply chain management
  - ‘Workforce’ management
  - ‘Client’ needs
  - Business and market analysis

Cybercrime Inc. - Business model

- Take advantage of ‘anonymous’ services to advertise and sell their ‘normal’ products and services online

- Some of the new ‘business’ opportunities:
    - Identity theft
    - Intellectual property theft
    - Trade secrets
    - Industrial espionage
    - Sensitive data theft
    - Online extortion
    - Financial crime
    - Data manipulation

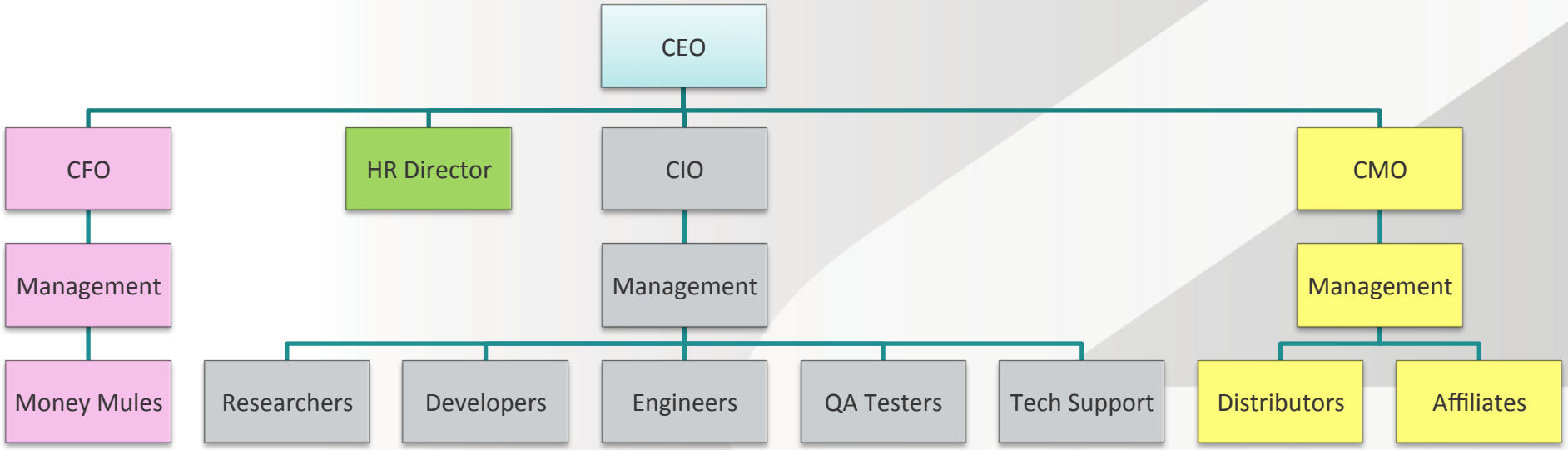
Cybercrime Inc. - Tactics used

- Some of the tactics and methods used by Cybercrime Inc:
  - Phishing and spear phishing
  - Man-in-the-middle
  - Vulnerabilities
  - Trojan horse software
  - Spam
  - Botnets
  - Scareware
  - Ransomware
  - Malware

The organization

Cybercrime Inc. – The organization

It looks similar to a traditional corporation:



Cybercrime Inc. – 'Business' roles (1)

- Chief Executive Officer (CEO)
  - Responsible for decision making and overseeing operations
- Chief Financial Officer (CFO)
  - Deals with every financial aspect of the cybercrime org.
- Chief Information Officer (CIO)
  - Responsible for the IT infrastructure of the organization
- Chief Marketing Officer (CMO)
  - Designs effective advertising methods for products and services

Cybercrime Inc. – 'Business' roles (2)

- Human Resources (HR) Director
  - Recruits the criminal workforce for the organization
- Management
  - Responsible for managing the 'criminal' workforce
- Researchers
  - Look for new exploits and 'business' opportunities
- Developers & Engineers
  - The techies, aka the brains!

Cybercrime Inc. – 'Business' roles (3)

- Quality Assurance (QA) Testers
  - Test all crimeware to ensure it bypasses any security measures of potential targets
- Technical Support
  - Tech support to clients, affiliates and members of the organization
- Affiliates
  - Drive potential clients to Cybercrime Inc.

Cybercrime Inc. – ‘Business’ roles (4)

- Distributors
  - Help distribute malware
- Money ‘Mule’
  - Helps with the money laundering

Adapt to the new

Cybercrime Inc. – Adapts to the New

- Constantly looking to innovate
- Overcome obstacles
- Meet market demands
- Explore new ‘business’ opportunities
- Use tools to help measure levels of success (e.g. Web analytics)

Old boys in a new age

- Traditional criminal organizations have ‘opened’ cybercrime divisions:
  - Cosa Nostra (Italian Mafia)
  - Japanese Yakuza
  - Chinese Triads
  - Russian Mafia
  - Nigerian mobs

Some examples

Cybercrime Inc. – Some examples (1)

- **Innovative Marketing Inc. (aka IMI)**
  - Founded by Sam Jain and Daniel Sundin (HQ in Ukraine)
  - Developed scareware rogue security programs:
    - WinFixer
    - WinAntiVirus
  - Offices in 4 continents with hundreds of employees
  - Support centres in Ohio, Argentina and India
  - Marketed products under more than 1,000 different brands and in 9 languages
  - From 2002 to 2008 IMI generated hundreds of millions of dollars in profit.

Cybercrime Inc. – Some examples (2)

- **Russian Business Network (aka RBN)**
  - Registered as an internet site in 2006
  - Based in St. Petersburg, Russia
  - Allegedly founded by the newphew of a powerful Russian politician
  - Specialises in:
    - Personal identity theft for resale
    - Provides web hosting and internet access to illegitimate activities
    - DoS attacks
    - Delivery of exploits via fake anti-spyware and anti-malware
    - Botnet

Cybercrime Inc. – Some examples (3)

- **The Carbanak Group**
  - Discovered in early 2015 by Kaspersky Lab
  - Used an APT-style campaign targeting financial institutions
  - Aim to steal money from banks
  - Estimated $1 Billion dollars have been stolen in an attack against 100 banks and private customers
  - Targeted primarily Russia, United States, Germany, China and Ukraine

The targets

Targeting - Mobility

- Cybercrime Inc. is focusing on mobile devices:
  - Used by individuals on a day-to-day basis:
    - Online banking
    - Online shopping
    - Socialising
    - Emails
    - Store personal data
    - GPS
  - Can be easy to compromise and hack (e.g. install “rootkit” to gain control to all features of the mobile device)

Targeting – The Cloud

- Cybercrime Inc. is focusing on The Cloud:
  - Network of computing resources available online
  - The Cloud can be used to store, manage and process information
  - Companies are outsourcing primary business functions using Cloud services
  - Critical and confidential data is now centralised in the Cloud
  - Instead of targeting several individual servers let's focus on the ones in the cloud shall we?

Targeting - Data

- Cybercrime Inc. is focusing on Data:
  - Personal data
  - Company's data
  - Government data
  - Military data
  - Data manipulation and disinformation:
    - Financial markets
    - What is displayed in our screens

Targeting - Internet of things (IoT)

- Cybercrime Inc. is focusing on IoT devices:
  - 2013 there were 13 billion online devices
  - Cisco Systems estimates 50 billion online devices by 2020
  - IoT is estimated to drive an additional $6.2 trillion to the global economy by 2025
  - IoT devices are developed without having security in mind

But Cybercrime Inc. can also target…

- SCADA devices
  - Supervisory Control And Data Acquisition (SCADA)
  - Specialised and often old computer systems
  - Being connected to the broader internet
  - These systems were not designed with security in mind
  - 2014 study revealed that 70% had suffered at least one security breach
- GPS Systems
- Tracking Systems
- Implanted medical devices (IMDs)
- And so many more!!...

The Hackers

Looking for a Hacker

- Hackers are not born they are trained
- Enormous amount of free educational material in the internet and in the underworld (dark web)
- PC games:
  - Uplink
  - Hacker Experience
  - Torn City
  - Hacknet

Who wants to be a Hacker?

- Anyone who feels attracted or enjoys:
  - Technology
  - Challenge
  - The thrill
  - Adventure
  - Danger
  - Money
  - Respect
  - Fame

The Mainframe

How about the mainframe?

- IBM is keeping the mainframe in sync with the new technologies:
  - Enterprise Cloud Computing
  - Enterprise Mobility
- The mainframe is securable but not secured by default:
  - Requires constant review of security settings
  - Security teams require resources and training
  - The mainframe is just another system
  - The mainframe is connected to other platforms
- People with no mainframe background are getting interested…
- If the mainframe is the core system of the major companies, what do you think Cybercrime Inc. will be targeting?

Can the mainframe be Hacked?

- YES!!! The mainframe can and has already been hacked!
  - IT firm Logica – more than 10,000 social security numbers (2012)
  - Swedish Nordea bank – personal data, money (2013)
  - Recent case in the UK:
    - Senior Applications developer
    - Detailed knowledge of the application
    - Exploited a known security control
    - Defrauded his employer of over £2 million!

Conclusion

Conclusion

- As always the bad guys are way ahead of the good guys
- Security must be taken seriously by everyone!
- People, Governments and companies need to be security conscious
- Technology reflects the evolution of human society but it can play against it
- Cybercrime Inc. is well organized. We must do the same!

Questions

Contact

Rui Miguel Feio, RSM Partners
ruif@rsmpartners.com
mobile: +44 (0) 7570 911459
www.rsmpartners.com