FRIEND AND FOE IN THE FIGHT AGAINST CYBERCRIME

Sir Rob Wainwright
Partner, Deloitte
Former Executive Director of Europol (2009-2018)
Big news, big impact

2 Canadian banks hacked, 90,000 customers’ data stolen
Two of Canada’s largest banks, Bank of Montreal and the Canadian Imperial Bank of Commerce’s Simplii Financial, confirmed hackers stole the personal and financial data of thousands of customers.

We are investigating the theft of customer data from our website and our mobile app, as a matter of urgency. For more information, please click the following link:

U.S. investigators point to China in Marriott hack affecting 500 million guests

British Airways

Cops Nab ATM Hacker Behind $1.2 Billion Swindle

Hacking Nation

Cops Nab ATM Hacker Behind $1.2 Billion Swindle

Hacking Nation
Smarter and stronger adversaries

Global networks expanding in scale

Better capability with bigger impact

Technology
Cops Nab ATM Hacker Behind $1.2 Billion Swindle
By Charlie Devereux
March 26, 2018, 11:18 PM GMT+8
- Gang leader behind Carbanak, Cobalt attacks arrested in Europe
- Attacks on over 100 financial institutions caused E0.16bn losses

The mastermind behind malware attacks that programmed ATMs to spit out cash on demand and caused more than $1 billion in losses ($1.2 billion) to banks, has been arrested in Italy.
Converging their crimes
Carbanak group operating across cyber, fraud, physical and money laundering domains

1 CYBER CRIME
Hacker develops malware and sends spear-phishing emails to bank employees to infect the system

2 FRAUD
Hacker transfers money into (foreign) BANK ACCOUNTS
ACCOUNT BALANCES are inflated and money is collected by money mules from ATMs
ATMs are infected and spit out cash, which is collected by money mules

3 MONEY LAUNDERING
STOLEN MONEY is laundered by being converted into CRYPTOCURRENCIES

From: “Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain”, Europol
Converging their crimes (cont.)
Skyscraper hack illustrates how a single actor steals data, creates fake accounts and enables money laundering

1. Personal information of hospital patients is stolen by a hacker.
2. Personal information is sold on the dark web.
3. Hacker launders proceeds of crime through accounts in various banks.
4. Syndicate buys stolen data and creates fake bank accounts.
5. Drug dealers physically deliver drug money to money mules.
6. Money mules deposit money into fake bank accounts.
7. Money is moved across banks.
8. Laundered money is collected by the drug syndicate.

1 - Based on the “Skyscraper” hack of U.S. hospitals and paediatricians.
Growth in malicious state actor activity
Military state hacking divisions targeting destructive attacks against government and commercial institutions

The threat group has attempted to steal more than $1.1 billion USD.

APT38 operates similarly to an espionage operation, carefully conducting reconnaissance while balancing financially motivated objectives.

On average, APT38 remains within a victim network approximately 155 days, with the longest time within a compromised system believed to be 678 days.

Organizations targeted for infrastructure use
Organizations targeted
Both organizations and infrastructures targeted
Major environmental hazards

PRO CYBER NEWS
One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs
Fedex says its expenses tied to malware attack was $400 million over past year, Merck put costs at $670 million in 2017

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Cyberattack cost Maersk up to $300M

Petya cyberattack cost Merck $135 million in revenue
Third-quarter revenue for the global pharma giant was drastically reduced in part by the temporary production shutdown, higher demand than planned and lost sales in certain markets due to the virus.

NotPetya: One year on – Have businesses learnt the lesson?
Today marks one year since the NotPetya attack hit a broad range of business - from law firms and ad agencies to supermarkets

'Clearly the impact of last year’s ransomware attacks has been far reaching. However, on a positive note, the publicity which these attacks garnered has made board members sit up and take notice of the potential impact to their organisation'
A new criminal economy

Mega-volume Darknet trade

Cyber infrastructure for hire
Data: the new currency of crime

Powering ransomware

Enabling fraud
Data powering the cops too
Bringing life to a powerful purpose

- Connecting more
- To see more
- To act better
An old concept for a new age

• Making them come
• Valuing knowledge
• Gaining insight to drive effect
The data network effect at Europol

Intelligence reports notified to Europol

Cross-border operations initiated or supported by Europol
Trust as the currency of Trade

- Hard won, easily lost
- Becoming a secure and reliable friend
- Valuing data privacy
Global privacy regulatory landscape
Becoming increasingly complex but an opportunity for change
Towards a more self-confident digital age

- Better aware of risk
- Smarter digital operation
Bringing major benefits

- To your business
- Customers
- And your reputation with regulators