Cyber-Crime, Cyber-Warfare, Cyber-Conflict

Part 1

John DiMarco
john.dimarco@utoronto.ca
http://www.cs.toronto.edu/~jdd

What is Cyber-crime? Cyber-warfare?

- "Cyber" – Computers and machines

- Cyber-crime – Crime using/exploiting computers
- Cyber-warfare – Warfare using/exploiting computers
- Cyber-Conflict – Other: e.g., political contests, hacktivism, social conflict, state/citizen conflict

Ever-growing Internet

- 2018: 23B+ machines, 4.2B users, 4.6B pages

Internet in your pocket, everywhere you go:

- Web browser use: 52% mobile worldwide as of May 2018.
  - Africa: 63%, Asia: 67%, and India: 80%

High Stakes

- "…computers aren't just tools of the bank. Increasingly, they *are* the bank." – Toronto Star, Monday July 19, 2004, p.D1

- "Why do I rob banks? Because that's where the money is." – attributed to Willie Sutton

Cyber-Crime

Learning from Examples

Phishing

- From: BMO Service
- Action: Changes made in your Internet Banking Profile
- Date: January 13, 2018.
- This is to inform that your profile data was changed by you or by someone logged in using your BMO DEBIT Card Number and password on 01/13/2018 from IP 91.59.84.61
- If you didn't change your profile data please visit and complete our BMO Online security measures
- 2017 BMO Support Center

Invoking Fear

- The motivation
  - …your profile data was changed... by someone … using your BMO DEBIT CARD…
- The hook
  - If you didn't change your profile data please visit and complete our BMO Online security measures

The Fraud

- Note BMO Online security measures link.
- Real URL (actual URL the link points to)

  http://accbm-on.is-found.org/bmoservice-support-alertinternet/
- URL: http://HOST/otherstuff
- HOST accbm-on.is-found.org is not BMO!
- Web page, set up by criminals, looks like BMO.
- Real BMO credentials captured, used.

419/411 Fraud

From: "mrs maria" mrs.maria.j3@msn.com Date: Mon, February 20, 2012 9:05 am

Compliments of the season, I am Mrs Maria The Head of file Department in Bank of Africa (BOA).I seek your assistance and I assured of your capability to champion this business opportunity to remit $15 million U.S.A dollars. In account belongs to a foreign customer who died along with his entire family in a plane crash. my private email ID :mrs.maria0@yahoo.cn I agree that 30% of this money will be for you as an aspect to the provision of a foreign account, 10% will be set aside for expenses incurred during the business and 60% would be for me. Thereafter, I will visit your country for disbursement according to the percentage indicated. This is the Website of the air crash. http://www.alaskajournal.com/stories/081301/foc_native_corps.shtml Reply me if interested. So that I can send you the details of the transaction Your urgent response will be highly anticipated and appreciated. please fill this information for me to know you morAs soon as I receive these dates, Best regards, Mrs Maria

Invoking Greed

- The motivation
  - …to remit $15 million U.S.A dollars… I agree that 30% of this money will be for you as an aspect to the provision of a foreign account…
- The hook
  - Reply me if interested…Your urgent response will be highly anticipated. please fill this information for me to know you mor[e]…

The Fraud

- 419 Scams operate as follows: the target receives an unsolicited fax, email, or letter often concerning Nigeria or another African nation…
- At some point, the victim is asked to pay up front an Advance Fee of some sort…. If the victim pays the Fee, there are often many "Complications" which require still more advance payments until the victim either quits, runs out of money, or both….
  - The 419 Coalition http://419coalition.org

Trojan Malware

- From: Voicemail noreply@utoronto.ca
- To: info@utoronto.ca
- Subject: New Voicemail Message

Voice redirected Message

Sent: Tuesday, 05 Jun 2018 09:18:13

ATTACHED: MSG006052018.zip (8 KB)

Invoking Curiosity

- Subject: New Voicemail Message

- Illusion of normalcy
  - From: Voicemail noreply@utoronto.ca
  - Sent: Tuesday, 05 Jun 2018 09:18:13 MSG006052018.zip (8 KB)

The Fraud

- MSG006052018.zip (8 KB)
- Attachment is a ZIP archive (bundle of other files)
- ZIP bundle contains a .EXE program
- Payload: RANSOMWARE
  - Encrypt entire hard drive
  - Extort BITCOIN payment to decrypt

Data Breach ("Hacking")

- Equifax: consumer credit reporting agency
- One of the three largest in USA

- Spring/Summer 2017 Data Breach
- Personal data of 140+M consumers stolen
- Hundreds of Thousands of Credit Card numbers stolen

Breach Details

- Equifax website/database
- Believed to be unpatched Apache Struts vulnerability
- Struts patch released in March 2017
- Equifax indicated exploit in May 2017

Abstracting Key Elements

Identification and Defence

Deception

- Human issue
  - Cyber = communications channel only
- Defence: **be savvy!**
  - Beware of messages invoking strong emotion
  - Confirm communication through other channels

Malware

- **Mal**ware – prefix "**mal**": "bad", "evil", "wrong"
  - **Mal**ice **Mal**evolence **Mal**feasance **Mal**ediction
- Mal**ware** – root "**ware**" same as:
  - Soft**ware** Hardware
- Defence: Control what runs on your computer
  - Windows Antivirus
  - Software updates
  - **Backups!**

Credentials

- Identify "friend" from "foe"
  - Gardening Warfare Herding Sports
- Password: ***knowledge of information***

- Ddefence: Guard your credentials
  - Good passwords
  - Guard password reset mechanisms too!
  - Two-factor

Vulnerabilities and Exploits

- Vulnerability: flaw allows unauthorized access
  - "Loose fence board"
- Exploit: use of a vulnerability to access
  - Break-in, theft, destruction
- Defence: Guard sensitive data
  - Data and Privilege Minimization
  - Patch Vulnerabilities ASAP

More Resources

- University of Toronto Security Matters
  - https://securitymatters.utoronto.ca
- Citizen Lab Security Planner
  - https://securityplanner.org
- CERT Security Tips
  - https://www.us-cert.gov/ncas/tips
- Public Safety Canada Cyber Security
  - https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt