Cyber-Crime, Cyber-Warfare, Cyber-Conflict

Part 2

John DiMarco

john.dimarco@utoronto.ca

http://www.cs.toronto.edu/~jdd
Cyber-Warfare

International and Civil Conflict
Stuxnet Worm+

- March 2010: Windows and Embedded
- Spreads via USB flash drives (virus)
- Exploits many different network vulnerabilities to propagate on a network (including three “0-day” vulnerabilities). (worm)
- Payload: targets certain Siemens Supervisory Control and Data Acquisition (SCADA) Controllers: modifies rotational frequency.
Jan 15, 2011: **New York Times** reported on “newest and strongest clues that the [Stuxnet] virus was designed as an American-Israeli project to sabotage the Iranian [Nuclear] program.”

Feb 15, 2011: “this malware contained important evidence indicating that its target was the IR-1 centrifuges at… [the Iranian nuclear enrichment facility at ] Natanz – **Institute for Science and International Security**, Dec 22, 2010 Report on Stuxnet Malware
Iran vs Dissidents

- The Iranian Government appears to be engaging in … deep packet inspection… to monitor [internet communications] to gather information about individuals… – Wall Street Journal, 22nd Jun 2009

- “Nearly 4000 people were arrested solely on the basis of monitoring of their private internet traffic” – Iranian journalist Ahmad Jalali Farahani 30th December 2011.

- SSL/HTTPS provides privacy?
Iran and DigiNotar

- July 2011 – Small Dutch SSL certification authority DigiNotar hacked, fraudulent certificates issued for google.com and others.
- August 2011 – Substantial surge in Iranian uses of DigiNotar certificates
- “…Iranian Internet users were exposed to a large-scale man-in-the-middle attack… to read all of the email messages an Iranian Internet user sent with his/her Gmail account.” – Trend Micro blog, 5th Sept 2011
Submarine Warfare Breach

- June 8, 2018: *Washington Post* reports that US Naval Undersea Warfare Center contractor hacked in Jan/Feb 2018, 614GB data stolen
- Included anti-ship missile plans for submarines
- Data not “classified” but “highly sensitive”
- Data was stored on an unclassified network.
- “Chinese government hackers” believed responsible
Key Element: Targeted Attack

- Target a company or government facility
  - Corporate or International Espionage, Sabotage
- Target an official
  - Blackmail, Public Embarrassment
- Target a dissident
  - Identification of Associates, Arrest
- Defence: Citizen Lab’s
  - [https://securityplanner.org](https://securityplanner.org)
Cyber-Conflict

Social and Political Struggle Online
“Anon Down”

- July 17, 2015: RCMP fatally shoots a protestor wearing a Guy Fawkes mask
- July 19, 2015: Hacker group “Anonymous” DDoSes RCMP, releases federal Cabinet secrets (Doxing)

- DDoS: distributed denial of service
- Dox: publish private information about, typically malicious intent
Legal Doxing

- **Feb 2009:** *NY Times*: Prop 8 Donor Map Web Site
  - “Proposition 8 changed the California state constitution to prohibit same-sex marriage. These are the people who donated in order to pass it.”
  - Mashup of public donor data and Google maps.

- **Dec 2012:** White Plains NY *The Journal News* publishes handgun owner interactive map.
  - Shortly after Sandy Hook Elementary School shooting.
  - Public records of handgun permit holders and a map showing where they live.
Jurisdiction in Law

- Feb 2012: Gambling site Bodog was shut down by the state of Maryland.
- Bodog.com is a registered Canadian company, whose domain is registered with a non-US registrar. Bodog’s activities were/are legal in Canada.
- “Maryland authorities … sent a court order to Verisign, the California-based operator of the .COM top level domain. Verisign complied, and edited the rootzone servers to reroute Bodog.com to a takedown page…” – itworld.com, 1st March 2012
This domain name has been seized by the U.S. Immigration and Customs Enforcement - Homeland Security Investigations, Office of the Special Agent in Charge, Baltimore, Md. in accordance with a warrant obtained with the assistance of the U.S. Attorney’s Office for the District of Maryland, and issued pursuant to 18 U.S.C. §§ 981 and 1955(d) by the U.S. District Court for the District of Maryland.

It is unlawful to conduct an illegal gambling business in violation of 18 U.S.C. § 1955 and any property used in violation of that section is subject to seizure and forfeiture pursuant to 18 U.S.C § 1955(d).
Facebook & Cambridge Analytica

- Facebook “This is my Digital Life” app
- 270k quiz-takers -> 87M friends of quiz-takers
- Aleksandr Kogan -> Cambridge Analytica
- Psychometric profiles created
- Psychometric profiles used to target political messages to Facebook users
What next?

- Prepare for Stormy weather: Cyber-Crime, Cyber-War, Cyber-Conflict are all increasing.

- Be aware, be willing to adapt, be prepared.
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