CSCI 1800 Cybersecurity and International Relations

Cyber Attacks

John E. Savage

Brown University

Outline

- 2012 Flame espionage software discovered
- 2012 Shamoon wiper attack on Saudi Aramco
- 2013 Mandiant Report on APT1
- 2013 US Defense Science Board Report
- 2013-2018 Carbanak – The Great Bank Robbery
- 2014 Regin surveillance toolkit discovered
- 2014-5 JP Morgan penetration
- 2015 Ukraine power grid
- 2016 DNC hack
- 2017 NotPetya
- 2017 Equifax breach
- 2018 New Vulnerabilities to Disinformation

Today's Readings

- Stuxnet and the Limits of Cyber Warfare by Jon R. Lindsay, *Security Studies*, August 2013
- Inside Project Raven
- USA Karma
- Web War I: The Cyberattack that Changed the World.

Optional Readings

- Significant Cyber Incidents, CSIS' large database of prominent cyber attacks since 2006.
- APT1: Exposing One of China's Cyber Espionage Units, Mandiant, 2013.
- Advanced Persistent Threats: A Symantec Perspective, Symantec
- Exploit Kits published by F-Secure.
- SON OF STUXNET: The Digital Hunt for Duqu, a Dangerous and Cunning U.S.-Israeli Spy Virus by Kim Zetter, The Intercept, November 12, 2014

Flame

- Goal: Espionage in Middle East, not damage
  - Found in 2012, started in ~2007, suicide command sent to it on 6/8/12 from its command & control site
  - Called the most complex malware ever found
  - Highly modular and at least 20 times size of Stuxnet
  - Records audio, screen shots, keyboard activity, Skype sessions and network traffic. Disguised as MSFT update!
  - Collected AutoCAD files (designs), PDFs, and text files
- Wash Post* said was developed by NSA and Israel. Leaked document said done by NSA and GCHQ.

* https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

Attacks on Oil Producers

- The Shamoon malware, found in 8/12, overwrote master boot record of computers (first track of disk) making them unusable.
- Shamoon wiped 30,000 Saudi Aramco machines!
  - Saudi Aramco is biggest OPEC oil producer!
  - Production not halted but valuable info lost.
  - Attacker took control of one computer, propagated malware to others, then disabled them together.
- Was it retaliation for Flame attack against Iran?

2013 Mandiant Report

- Mandiant* investigated APT† groups since 2004
- Concludes Chinese group (APT1) most prolific.
  - APT1 active since 2006
  - Reported on APT1 because of its scale and impact
- Mandiant examined ~150 attacks on victims.
- Discovered APT1's attack infrastructure, Command & Control, and modus operandi (TTP)
- Also identified APT1 personnas.

* http://cs.brown.edu/courses/csci1800/sources/2013_Mandiant_APT1_Report.pdf
† http://www.brookings.edu/research/articles/2012/05/21-cyber-threat-singer

The Telegraph

Meet the Chinese hackers accused of cyber-espionage

Listening to rock music, playing Angry Birds and obsessed with coding: a portrait of the five alleged Chinese army hackers wanted by the FBI

(Clockwise from top left) Sun Kailiang, Wen Xinyu, Wang Dong, Gu Chunhui and Huang Zhenyu Photo: Reuters

See https://www.telegraph.co.uk/news/worldnews/asia/china/10846301/Meet-the-Chinese-hackers-accused-of-cyber-espionage.html

Mandiant Report (cont.)

- Believes APT1 is likely government-sponsored and one of China's most persistent threat actors
- Tracked APT1 back to the People's Liberation Army (PLA) Unit 61398 in a Shanghai building.
- APT1 has stolen hundreds of terabytes of info from 141 organizations.
- Can steal simultaneously from dozens of orgs.
- Has about 1,000 C&C sites around the world.

APT Methodology

- Decide on target, e.g. F35 stealth jet designs
  - E.g. Lockheed Martin or Boeing
- Form a team of specialists with following roles:

1. Identify key personnel & system vulnerabilities
   - This reconnaissance can take months
2. Professional intrusion team breaches system
   - Requires clever campaign to reach potential victims
   - Perhaps enters via service company, e.g. HVAC
3. Reconnaissance team installs remote access tools (RATs)
4. Now the target is “pwned” (error in “owned”)

APT Methodology

- Exploitation team now does disciplined research
  - Plan for long stay
    - Insert new backdoors for reentry
    - Ensure RAT not visible, e.g. keep loads on processors small
  - Analyze folders for interesting file names
  - Capture data at network access points
  - Collect and encrypt data for surreptitious exfiltration
  - Possibly activate cameras & microphones
- Some files may be sabotaged, not just copied!

Persistence of APTs

- 2016 – FireEye says APTs persisted for 146 days on average world wide, 469 days in EMEA
- 2015 – Trustwave says 81% of APTs not detected by internal security procedures
  - Often discovered by news reports, law enforcement or external fraud monitoring

US Defense Science Board Report

- 2-year 2017 report* on cyber deterrence concludes
  - Russia, China, Iran & North Korea can put US critical infrastructure (CI) at risk via cyber
  - Can also thwart US responses – an untenable position
- US and the private sector must
  - Boost cyber resilience overall
  - Create a cyber deterrence strategy for each adversary
  - Protect select strike systems, cyber, nuclear, non-nuclear
  - Enhance cyber attribution, make joint forces & CI resilient

* https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

Carbanak – Great Bank Robbery

- 2013- ???? Gang stole $1Billion from 100 banks!
  - Example of commercial APT – still active!
  - Kaspersky thinks nation state behind it!
- Multi-national gang from Russian, Ukrainian, other EU, and China deploy Carbanak malware
  - http://fortune.com/2018/03/26/carbanak-europol-arrest-spain-malware-banks/
  - http://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf
  - https://www.scmagazineuk.com/carbanak-active-latest-cyber-bank-heist-took-months-carry/article/1586531

Regin*

- Malware toolkit for persistent mass surveillance revealed in 2014 by Symantec, Kaspersky, Intercept
- Said to have been developed by NSA and GCHQ
- Targeted primarily Russia, Saudi Arabia and many others to a much larger extent
- Like Flame, Regin uses a modular approach to load features that fit the target.
- Stealthy. Uses special virtual encrypted file system
- Unusual communication modalities with C&C server
- Spied on Belgacom, a Belgian telecom
- Found on USB owned by an Angela Merkel staffer

* https://en.wikipedia.org/wiki/Regin_(malware)

2014 JP Morgan Intrusion

- US Attorney: one of largest hacks ever discovered!
- 7 major financial insts., JP Morgan largest
  - Identified potential stock traders
  - Spammed them with positive info on penny stocks
  - Dumped the stocks when they ran up (pump & dump)
- Data stolen from 100 Million customers
- Hackers got $10s millions by pumping & dumping
- Two Israelis and one American accused of crime

* http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

† http://www.nytimes.com/2015/11/11/business/dealbook/prosecutors-announce-more-charges-in-jpmorgan-cyberattack.html

Ukraine Power Grid Compromise

- In December 2015 attacker compromised electricity control centers in Western Ukraine
- ≥ 230,000 residents lost power for up to 6 hours
- First cyber op to take down an energy grid
  - Power was restored by physically closing switches
- The electricity grid attacked again in 2016

2016 DNC Exploitation

- This was the work of a Russian team called by various names, such as APT28, Fancy Bear, names for a GRU hacking team.
- The GRU is Russian military intelligence.
- Investigated by special prosecutor Robert Mueller.

The NotPetya Worm
Most Devastating Cyberattack in History*

- On 6/27/17 Russia launched worm in update software for Ukraine's M.E.Doc accounting software
  - Estimated 10% of all computers in Ukraine corrupted!
- Effect spread quickly all over the world
  - Federal Express hit at a cost of $400 Million
  - Maersk, world's largest shipper, cost was $300 Million
  - Maersk crippled in 7 mins!
  - Merck lost $1.3B!
- White House estimated NotPetya cost at $10Billion!

* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

The NotPetya Worm
Most Devastating Cyberattack in History*

- NotPetya built using
  - NSA's EternalBlue, attacks SMB – ShadowBrokers
  - French tool, Mimikatz, scrapes RAM passwords
- Unpatched machines infected first. Then worm jumped to patched ones using stolen passwords!
- "[I]t was the equivalent of using a nuclear bomb to achieve a small tactical victory." – Bossert†
- Nation-state weapon loosed in borderless world!

* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

† Tom Bossert was the White House Homeland Security Advisor

Effect of NotPetya Worm

- Port Authority closed Maersk's NJ terminal
  - Just-in-Time supply chain was in serious trouble
  - Wait or opt for very expensive shipping alternative?
- Several days later staffers called to English office
- Essential domain controllers were wiped
  - Necessary to decide which users have which access
  - One controller found in Ghana – off before infection
  - Relay set up to carry gigabyte file to England
  - Ops restarted in two weeks, completed in 2 months

The NotPetya Worm

- Experts believe Russians were sending a message – don't do business in Ukraine.
- Experts agree this type of event can occur again.
- Some say it's the Sputnik event of cyberspace
- But it has not yet been recognized as such.

The 2017 Equifax Breach

- The breach due to bug in Apache Struts
- Bug revealed in 3/2017, not fixed by Equifax
  - Equifax CEO: One person was responsible to fix such bugs!
- Avivah Litan of Gartner Inc.: "On a scale of 1 to 10, [it] is a 10. It affects the whole credit reporting system in the United States because nobody can recover it, everyone uses the same data."
- Senator Mark Warner: "In today's information economy, data is an enormous asset. But if companies like Equifax can't properly safeguard [it] then they shouldn't be collecting it in the first place."

More on 2017 Equifax Breach

- From about 5/13 – 7/30/18 hackers had access to names, SSNs, driver's licenses, addresses, email addresses, credit card expiration dates, taxpayer ID numbers of 145.5 million Americans!
- A cybersecurity loss can be very expensive.
  - Such info widely used, even for disaster relief!
- Victims did not provide this information to Equifax but Equifax claims they own it.

The 2017 Equifax Breach

- Equifax waited about six weeks to report breach
- Execs sold $2 M stock 2 days before breach notice
- Board of Directors has fiduciary responsibility for co.
- Breach suggests failure by CEO & Equifax board
  - They should have ensured that security had priority
- 2/20/20 – Four PLA officers charged with breach.
  - They routed traffic through 34 servers in 20 countries
  - Encrypted communication
  - Deleted log files daily to remove evidence of hacking

New Vulnerability to Disinformation

- Nations that experience political divisions are vulnerable to disinformation campaigns
  - Many Western nations are in political turmoil
  - E.g. France, Germany, Poland, Hungary, US
- Social media amplify emotional attachment
  - Algorithms are designed to keep users on sites
  - Human interest issues attract attention
  - Provides a vehicle to weaponize information

Social Media Vulnerabilities

- Nations want to address these vulnerabilities
- The question is “How should they do that?”
  - Legislatively?
  - By regulation of social media companies?
  - Via the public?
- There is risk associated with premature action
- Scholarly study is needed
  - You can contribute!

Review

- 2012 Flame espionage software discovered
- 2012 Shamoon wiper attack on Saudi Aramco
- 2013 Mandiant Report on APT1
- 2013 US Defense Science Board Report
- 2013-2015 Carbanak – The Great Bank Robbery
- 2014 Regin surveillance toolkit discovered
- 2014-5 JP Morgan penetration
- 2015 Ukraine power grid
- 2016 DNC hack
- 2017 NotPetya
- 2017 Equifax breach
- 2018 New Vulnerabilities to Disinformation