Attack on Sony 2014

Sammy Lui

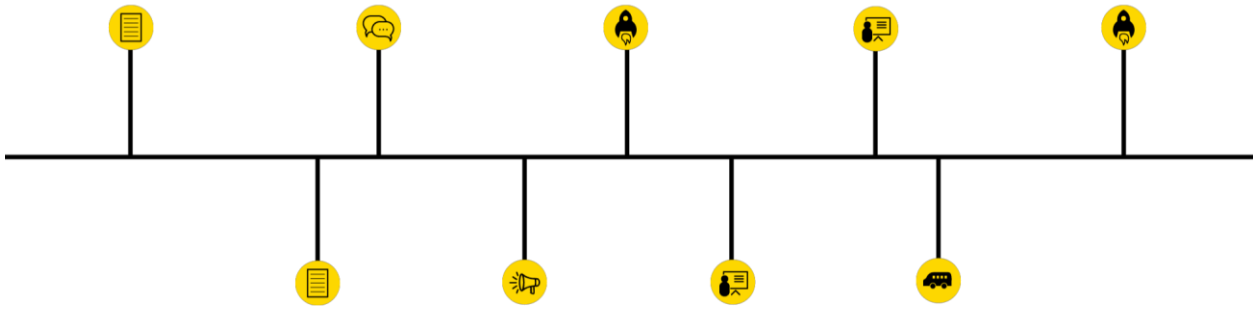
Index

Overview

- Attack lead by the Guardians of Peace hacker group
- Stole huge amounts of data from Sony's network and leaked it online on Wikileaks
- Data leaks spanned over a few weeks
- Threatening Sony to not release *The Interview* with a terrorist attack

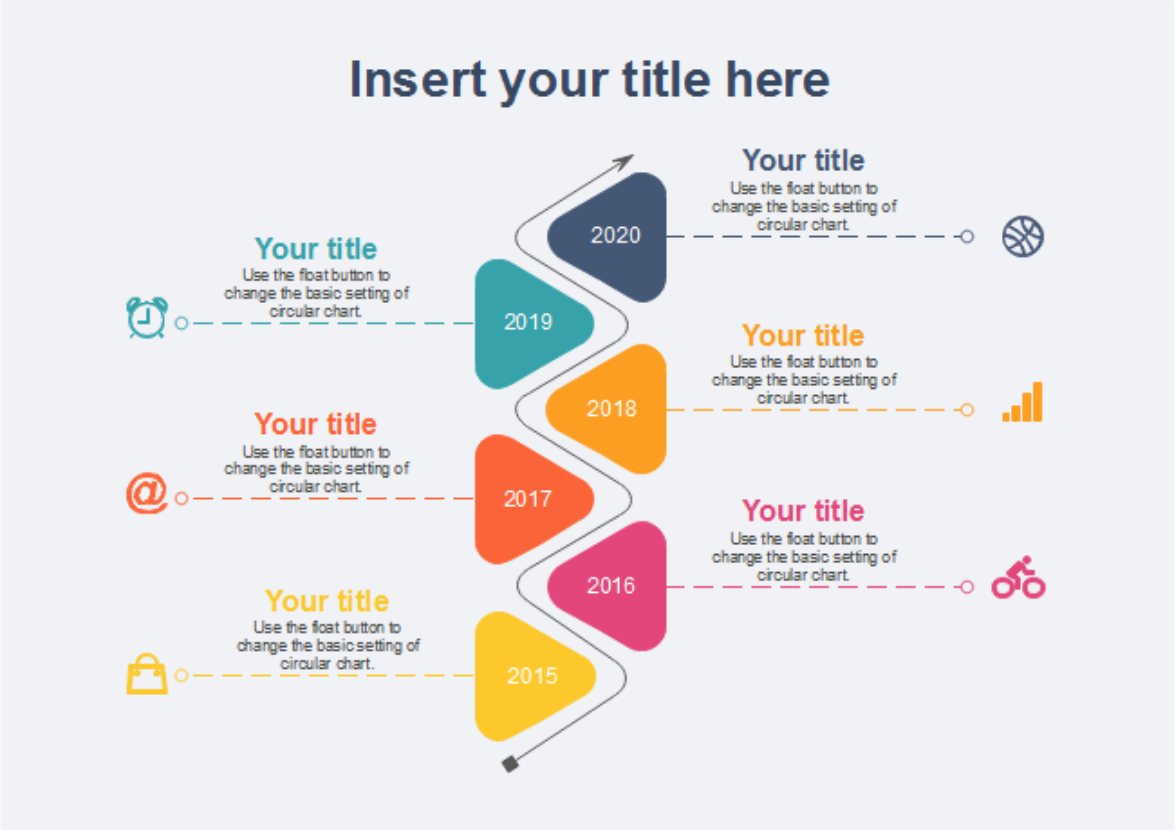
Timeline

- 11/24/14 - Employees find Terabytes of data stolen from computers and threat messages
- 11/26/14 - Hackers post 5 Sony movies to file sharing networks
- 12/1/14 - Hackers leak emails and password protected files
- 12/3/14 – Hackers leak files with plaintext credentials and internal and external account credentials
- 12/5/14 – Hackers release invitation along with financial data from Sony



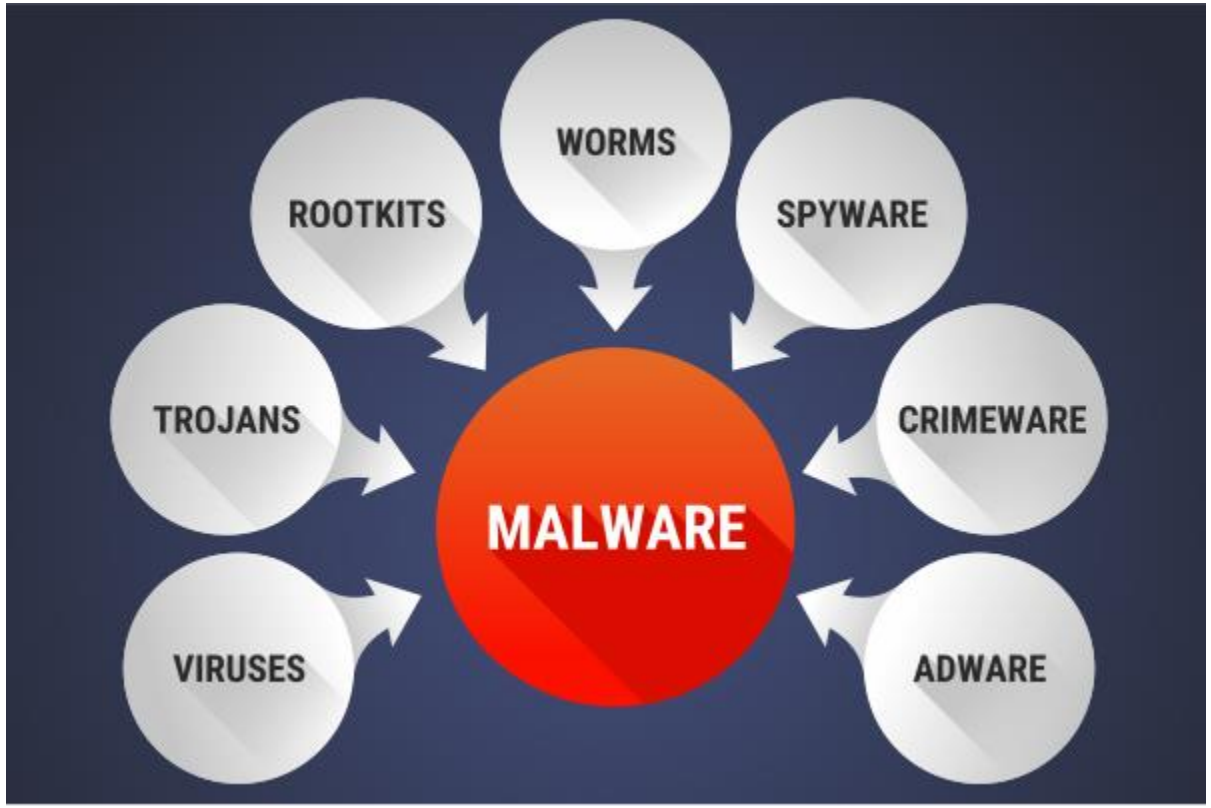
Timeline

- 12/07/14 – Hackers threaten several employees to sign statement disassociating themselves with Sony
- 12/08/14 - Hackers threaten Sony to not release *The Interview*
- 12/16/14 – Hackers leaks personal emails from employees. Last day of data leaks.
- 12/25/14 - Sony releases *The Interview* to select movie theaters and online
- 12/26/14 –No further messages from the hackers



Tools

- Targeted attack
- Inside attack
- Wikileaks to leak data
- The hackers used a Wiper malware to infiltrate and steal data from Sony employee computers
- Malware
  - Any malicious software that is harmful to a computer user
  - Include Worms, Spyware, Crimeware, Adware, Trojans and Viruses



Wiper Malware

- Collects and destroys data
- Used Microsoft Windows management & network file-sharing to spread, shut down networks and reboot computers
- Used to cause financial and reputational damage to companies
- Targets files, boot section of OS and backups of system and data

Wiper Continued

- Can overwrite files that are small enough by destroying headers
- Erase sectors of physical disc quickly
- Destroys files randomly
- Can evade detection by using a boot loader to bypass OS protections
- Can replicate to other systems
- Rarely used for financial motivation

Wiper Continued

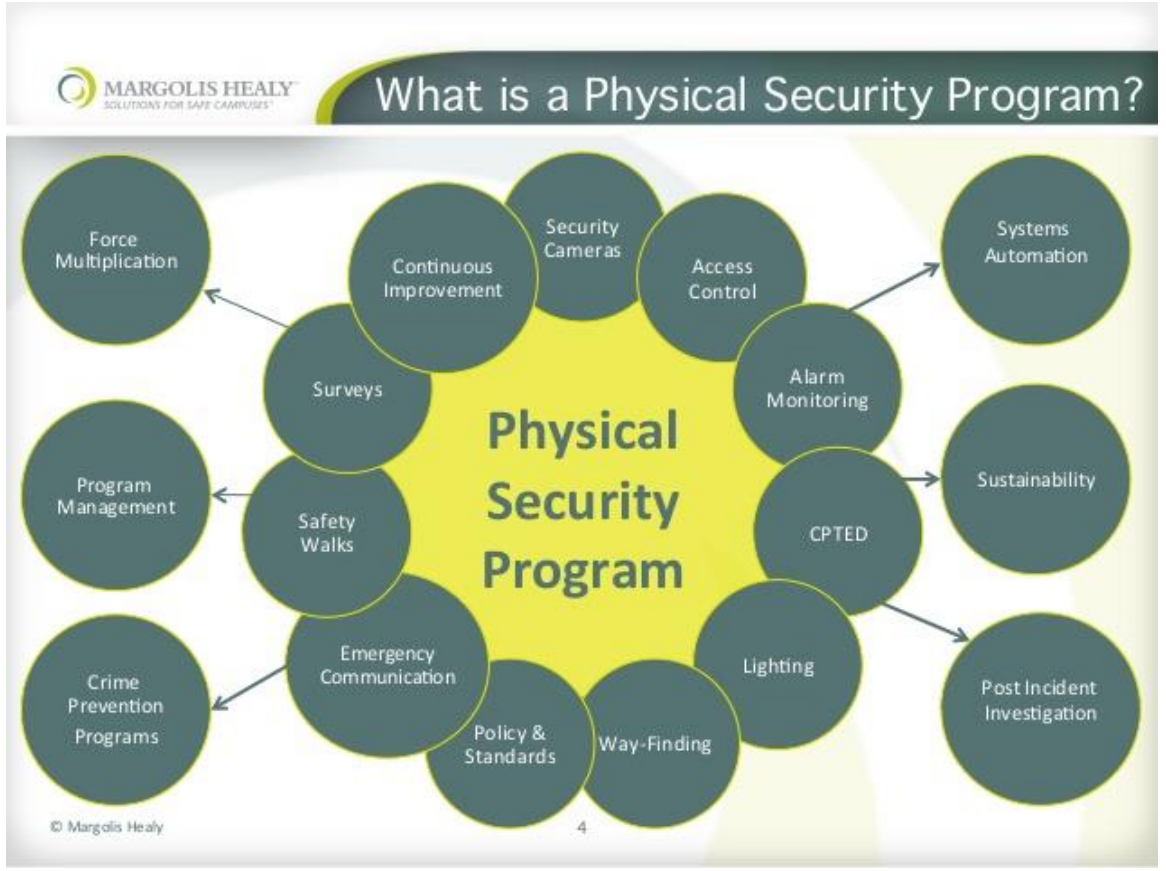
- Delivered through compromised computers in Thailand, Italy and Poland
- Exploits WMI to infect machines in network and then wipe harddrives
- Used EidoS RawDisk to directly access Windows drives

Implications

- The FBI and NSA have found info confirming North Korea made the malware
  - Hackers' interest in *The Interview*
  - Hackers' threats can be translated from Russian or Korean
  - No official information can be released
- Weak physical security allegedly allowed GoP member to enter Sony building
- Sympathetic employees allegedly aided GoP member
- Cyberterrorism
  - Politically motivated use of computers and IT to cause disruption and fear

Need For Physical Security

- Physical security – protection of personnel, hardware, software, and networks from physical actions
- The best way to get through cybersecurity is physical access
- Sony neglected to spend money on securing email servers and password files
- Examples
  - Heat detectors
  - Biometrics
  - Mantraps



Employees – Accomplices?

- Employees can be easily swayed if untrained
  - Individuals can play on their sympathy
- Employees may be insiders
- Employees may be willing accomplices
- Employees should check individuals for
  - Passwords, IDs
  - Background
  - Specific questions
- Still unknown whether employees who helped the hackers were inside men or unwitting accomplices

Dangers of Cyberterrorism & Cyberwarfare

- Cheaper to launch
- Threatens infrastructure
- Grid attacks
- Information systems being predominantly digital
- “Cyber attacks should be treated like acts of war if their consequences are great enough” – Dave Aitel

Damages & Repercussions

- Several thousand computers at Sony needed to be repaired
- Sony shut down its internal computer network to prevent further data wiping
- Employees had to work on whiteboards for weeks
- Damage = $15 million
- Wiper Malware made advanced recovery tools useless, making recovery even more tedious
- Countless lawsuits against Sony from information found in leaks

Dangers of Malware

- Disguised as a harmless file
- Self replicable
- Damage computer and make it less functional
- Breakdown of corporate networks
- Malware can be modified to easily avoid detection by antivirus software

Defense

- Cybersecurity incident response plan
- Risk-based patch management program
- Cybersecurity-aware business continuity plan
- Network and user segmentation
- Software security stack

Reparations & Ramifications

- Sony brought back systems that focus on generating revenue first
- Japanese government will increase cybersecurity to protect against foreign attacks
- The FBI has found that the IP addresses used by the GoP were from North Korea because they didn’t use proxy servers
- Analysts are able to link different hacks to the same hacker group

Aftermath

- 1/05/15 – hacker group Anonymous announces attack on Sony for lying about North Korea hacks
- 12/06/16 – Adam Schiff attributes rigged 2016 election to lack of responding to Sony Attack
- 9/06/18 – Department of Justice files charged against North Korean spy for role in Sony Attack and creation of Wannacry 2.0 malware
- 2018 – Senior VP of Norse identifies 6 individuals involved with the attack but cites that they are not connected to North Korea

Similar Attacks – Sony Attack 2011

- 04/19/2011
- DDoS attack on Sony's PlayStation Network by hacker group Anonymous
- Compromised data of 1000s of users
- Result of poor cybersecurity
- Required shutdown of services and weeks of repair

Similar Attacks – Target Attack

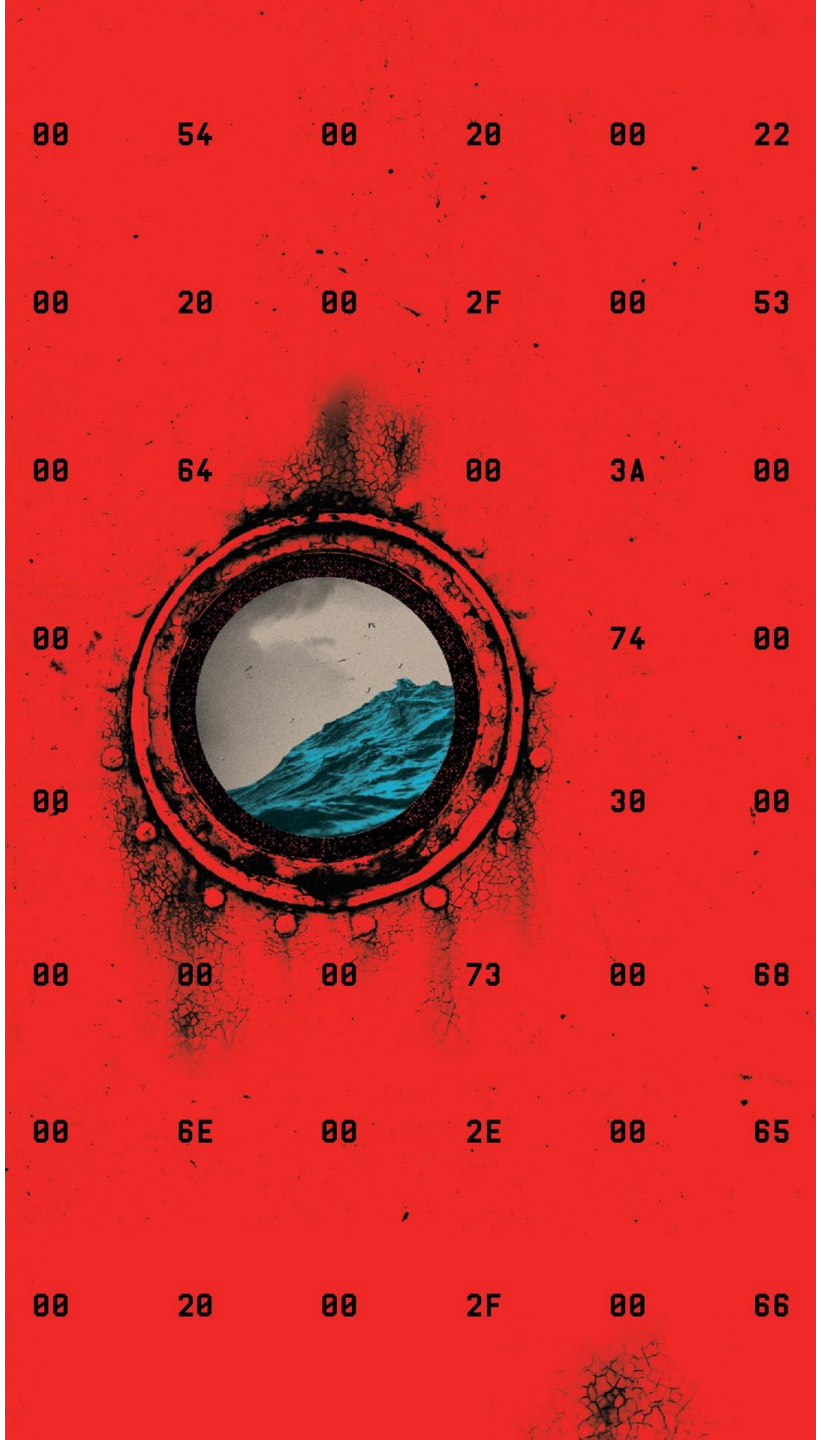
- 11/27/2013
- Hackers steal 40 million credit and debit card information from customers
- 11 Gigabytes of data stolen
- Customers in danger of having their cards exploited
- Hacked the database through compromised third party vendor
- Hackers used POSRAM Trojan to infect Target's POS system

Similar Attacks - NotPetya

- 06/27/17
- Hacker group Sandworm infects Maersk company with NotPetya wiper malware
- 1000s of computers connected to the Maersk company's network shut down
- Several demanding $300 worth of bitcoin ransom to unlock encrypted important files

NotPetya

- Propelled by two hacker exploits, EternalBlue & Mimikatz
  - EternalBlue to remotely run code on an unpatched machine
  - Mimikatz to pull passwords and uses them to hack into other machines
- Like with the Wiper, bypasses security easily by being able to infect patched computers
- Paying ransom didn’t help because it irreversibly encrypted master boot records



Sources

- https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea
- https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.5f1bed012389
- https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/
- https://www.recode.net/2014/12/2/11633426/details-emerge-on-malware-used-in-sony-hacking-attack
- https://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12
- https://threatpost.com/secrets-of-the-wiper-inside-the-worlds-most-destructive-malware/131836/
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://www.reuters.com/article/us-sony-cybersecurity-investigation/sony-pictures-struggles-to-recover-eight-days-after-cyber-attack-idUSKCN0JG27B20141203
- https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219
- https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/
- https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today