Sony Hack:

The Most Puzzling Security Story of 2014

by N. Vlajic

Sony hack is unprecedented in nature due to undetectable malware and overall an unparalleled and well-planned crime.

[1] NetworkWorld.com

http://www.networkworld.com/article/2856258/microsoft-subnet/sony-hack-dubbed-unparalleled-crime-unprecedented-due-to-undetectable-malware.html

Hack Timeline ...

NOVEMBER 2014

November 21

Sony receives an e-mail from a group calling itself "God'sApstls" threatening "great damage" to Sony unless the hackers received "monetary compensation," Mashable reports.

November 27

A group claiming credit for the attack, called "Guardians of Peace," begins releasing data stolen from Sony, including high-quality digital copies of new movies that have yet to see their U.S. or global release, the Guardian reports.

November 24

Wiper malware that has infected an unknown number of Sony Pictures systems detonates, reportedly erasing PC and servers' hard drives, as well as the machines' Master Boot Record, thus "bricking" the devices. Sony Pictures appears to initially downplay the severity of the attack, telling The Hollywood Reporter it is "investigating an IT matter" following reports that the breach affected employees' computers and may have exposed sensitive data.

DECEMBER 2014

December 1

The FBI sends a confidential "flash" alert to numerous U.S. businesses, warning them that hackers have recently launched a destructive "wiper" malware attack, Reuters reports. The agency also confirms that it's assisting in the Sony breach investigation. G.O.P. continues to leak more information online, including a spreadsheet listing salaries for more than 6,000 Sony employees, its top bosses included, pop culture news site Fusion reports.

December 3

G.O.P. leaks, among other items, internal documents from Deloitte, including salary information for more than 30,000 employees, according to The New York Times. That same day, anti-virus vendor Trend Micro ties the Sony hack to the "Destover" malware.

December 4

The "wiper" malware attack against Sony Pictures has numerous commonalities with previous wiper attacks in Saudi Arabia and South Korea, says Kurt Baumgartner, a Kaspersky Lab principal researcher.

December 5

G.O.P. sends a new e-mail threatening the company and its employees, entertainment publication Variety reports.

December 7

After days of speculation over Pyongyang's potential involvement in the Sony attack, a spokesperson for North Korea's National Defense Commission denies that the country was involved, but does refer to it as a "righteous deed" that may have been launched by its "supporters and sympathizers."

December 8

Sony Pictures issues a **data breach notification letter** to current and former employees, confirming that various personal details, including medical information, may have been compromised.

Another batch of Sony data is released, which includes this message for Sony: "Stop immediately showing the movie of terrorism which can break the regional peace and cause the war!"

December 9 & 10

Sony Pictures co-chairman **Amy Pascal** has her e-mails leaked to file-sharing and BitTorrent sites, according to The Independent. Among the compromised details is a conversation with producer **Scott Rudin** in which they exchange racially charged comments about President Obama.

Amy Pascal

Scott Rudin

December 11

G.O.P. distributes links to a new batch of leaked data, which allegedly includes the Outlook mailbox for Sony's general counsel.

December 12

Executive Amy Pascal says in an interview with Bloomberg: "I don't think that anybody thinks that this was anyone's fault who works here, and I think continuity and support and going forward is what's important now."

December 13

Hackers release a fresh batch of stolen information, including an early version of the screenplay for the James Bond film Spectre.

December 14

David Boies, an attorney retained by Sony, sends a letter to multiple media outlets threatening to sue them if they reproduced the leaked information, and demanding that they delete all leaked e-mails, contracts and other information.

December 15

Sony Pictures is hit with its first class-action lawsuit by former and current employees who blame the company for failing to protect their private information. Additional lawsuits were filed over the days that followed.

December 16

G.O.P. publishes a "terror" threat against movie theaters and theatergoers in relation to the release of "The Interview." According to various press reports, the group also releases the Outlook mailbox for Sony Pictures CEO Michael Lynton, which includes 32,000 e-mails dating from 2013 to just days before the wiper malware attack.

December 17

DHS says "there is no credible intelligence to indicate an active plot against movie theaters." Sony Pictures says it will cancel the film's Dec. 25 release.

December 18

G.O.P. tells Sony it's now free to release "The Interview," as long as it removes the Kim Jong-un death scene.

Kim Jong-un

December 19

The FBI says its technical analysis of the hack ties it to North Korea.

President Obama says the U.S. "will respond proportionately," and says Sony made a "mistake" in choosing to not release the film.

Sony Pictures chief Lynton: "We would still like the public to see this movie, absolutely."

December 20

The Obama administration, Reuters reports, has asked for help from Australia, New Zealand and the United Kingdom to spearhead an international response to North Korean hacking, and is also consulting with China, Japan, Russia, and South Korea.

December 21

North Korea denies being involved in the Sony Pictures attack, and issues a statement warning of "grave consequences" for the U.S. unless the White House agrees to a joint investigation.

December 22

The foreign ministry of China - North Korea's only major ally - says that while it condemns "all forms of cyberattacks and cyber terrorism," China sees no evidence tying Pyongyang to the Sony hack.

December 23

Sony Pictures issues a statement announcing that "The Interview" will debut in some U.S. theaters on Christmas Day.

How It All Began …

- **how Sony network was infiltrated – still NOT known**
  - ➢ most likely intrusion scenario: **phishing**
  - ➢ GOP claim 'they were siphoning data from Sony for 1 year'
  - ➢ 2-fold damage:
    - → stolen data
    - → injected malware ⇒ wiped hard drives

Malware Details

- **Wiper** (aka **Destover**) - key feature: erases data from hard drives & deletes master boot records
  - victim machines can no longer boot
  - **forensics investigation no longer possible!**
- Sony hack = first use of Destover against '**corporate North America**'
  - two previous victims of similar attacks in South Korea and Saudi Arabia

SONY PICTURES™

Description:
Movie and television studio
When: Nov. 24, 2014
Malware labeled: Destover/Wipall
Systems wiped: Unknown
Credit claimed by: Guardians of Peace

Description:
South Korean banks/insurers Jeju, NongHyup and Shinhan; broadcasters KBS, MBC and YTN
When: March 20, 2013
Malware labeled: Dark Seoul
Systems wiped: 32,000 (estimated)
Credit claimed by: Whois, as well as New Romantic Cyber Army Team

ارامكو السعودية
Saudi Aramco

Description:
Saudi Arabia's state-owned - and the world's largest - oil, gas and petroleum producer
When: Aug. 15, 2012
Malware labeled: Shamoon
Systems wiped: 30,000 (estimated)
Credit claimed by: Cutting Sword of Justice

Malware Details (cont.)

- **Destover** components (US-CERT):

(1) **Worm Tool**

→ communicates to C&C servers in Italy, Poland, Thailand, US, Singapore, Cyprus, ...

(2) **Listening Implant**

(3) **Lightweight Backdoor**

(4) **Proxy Tool**

(5) **Destructive Hard Drive Tool**

(6) **Destructive Target Cleaning Tool**

(7) **Network Propagation Wiper**

Leaked Information

- **10-s of Terabytes of data** likely stolen
  - so far, only 30 Gbytes released:
    - → 4 movies prior to opening date (*Annie*, *Still Alice*, …) and *Fury* - all made available on **illegal torrent sites** (e.g. Pirate Bay)
    - → scripts for upcoming movies & shows, …
  - other stolen data:
    - → personal data of 3,800 employees (emails, medical records, …)
    - → performance reports & salary information

Leaked Information (cont.)

- other stolen data, including:
  - → files with SIN numbers of 47,000 celebrities, employees, freelancers
  - → PDF files with passport numbers of crew and cast for various Sony productions
  - → media files related to films not produced by Sony (possibly illegal copies ?!)

How Actually Did It?

- **Theory 1 (by FBI): North Korean Gov.**
  - ➢ obvious connection to movie 'Interview'
  - ➢ evidence: malware was complied by a a computer with Korean language text settings
    - → nation-state attacks generally do not …
      a) announce themselves with showy images
      b) use catchy aliases (GOP)
      c) post stolen data on hacker sites
    - → what if the malware was simply purchased on the black market?!

How Actually Did It? (cont.)

- **Theory 2: Russians**
  - done by Russian government or stand-alone Russian hacker(s)
  - retaliation for sanctions against Russia over military actions against Ukraine
  - evidence: linguistic analysis of GOP's online communications suggest it was conducted by a native Russian (not Korean or English) speaker

How Actually Did It? (cont.)

- **Theory 3: Sony Insider(s)**
  - evidence: attackers knew the internal network - malware contained hardcoded names of servers inside Sony network & user names & passwords for internal systems
    - → an outsider would need to perform lots of reconnaissance to obtain all that data
    - → lots of reconnaissance ⇒ attack(er) more likely to be spotted

Is It Legal to Use Stolen Data?

- **Sony hack was illegal & unethical**
  - **how about the publishing of leaked data ???**
- **US First Amandment:**
  - **news agencies can publish stolen data as long as they themselves obtained the data without breaking the law …**
  - **however, some data is 'off limit'**
    - → medical records
    - → copyrighted material
    - → trade secrets

References

[1] NentworkWorld.com

http://www.networkworld.com/article/2856258/microsoft-subnet/sony-hack-dubbed-unparalleled-crime-unprecedented-due-to-undetectable-malware.html

[2] DataBreachToday.com

http://www.databreachtoday.com/sony-pictures-cyber-attack-timeline-a-7710?webSyncID=e26a8273-a1a6-ae22-ac64-bbb4628e3e19&sessionGUID=8624735c-1738-39ae-19d3-e34ceb0c7902

[3] Wired.com

http://www.wired.com/2014/12/sony-hack-what-we-know/

[4] SecurityWeek.com

http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony

[5] ArsTechnica.com

http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/

[6] TorrentFreak.com

https://torrentfreak.com/sony-movies-leak-online-after-hack-attack-141129/

[7] BankInfoSecurity.com
http://www.bankinfosecurity.com/sony-hack-destover-malware-identified-a-7638/op-1

[8] TheHackerNews.com
http://thehackernews.com/2014/12/sony-pictures-scarier-hack-hackers-leak.html

[9] CounterPunch.com
http://www.counterpunch.org/2014/12/30/who-was-behind-the-cyberattack-on-sony/

[10] SecurityLedger.com
https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk/

[11] Reuters.com
http://blogs.reuters.com/alison-frankel/2014/12/15/sonys-big-bluff-cant-beat-first-amendment/

[12] Vox.com
http://www.vox.com/2014/12/14/7387945/sony-hack-explained

[13] TrendMicro.com
http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-the-destructive-malware-behind-fbi-warnings/

[14] ReCode.net
http://recode.net/2014/12/02/details-emerge-on-malware-used-in-sony-hacking-attack/

[15] CNBC.com

http://www.cnbc.com/id/102305848

Questions

1) What type of damages have been inflicted on Sony in Dec 2014 GOP's hack?

2) What is the name of the malware used in Dec 2014 Sony hack, and why is this malware particularly 'difficult to deal with'?

3) What are the 3 hypothesis concerning the actual executor of Dec 2014 Sony hack?