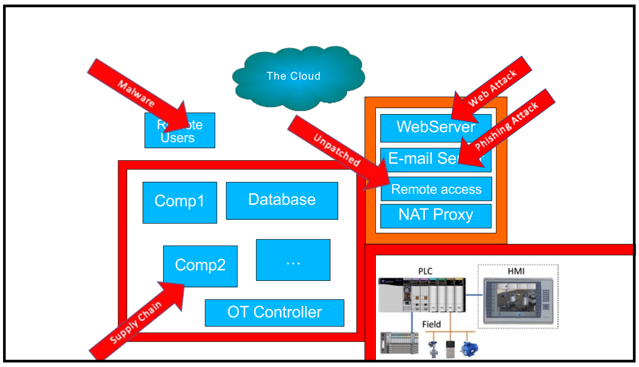
Attack Case Studies

A look at how attacks happen in practice.

Not on the exam, by will put some of what you have seen in context.

1



2

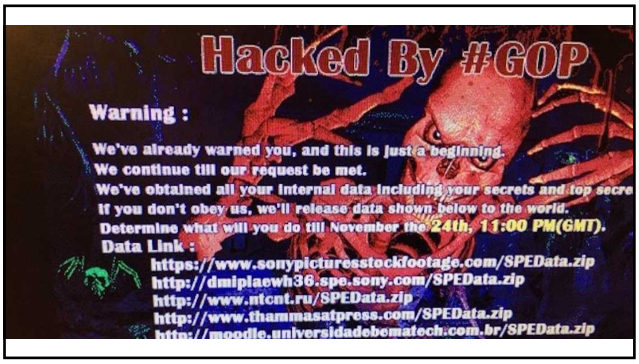
The Sony Hack

3

The Sony Hack: November 24th, 2014

- Employees arrive at work and their door passes don't work.
- All card payments on filming lots get refused.
- Computers don't connect to the network …

4

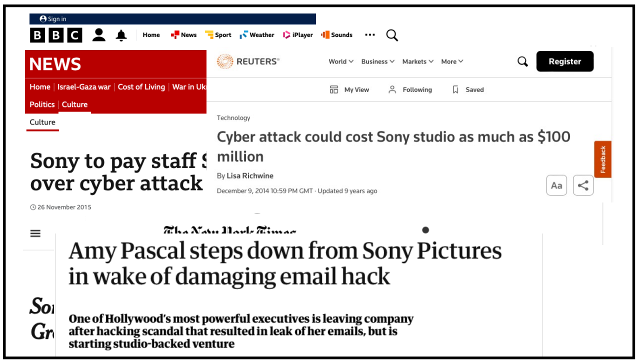


Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

5



Sony to pay staff $ over cyber attack

26 November 2015

Technology

Cyber attack could cost Sony studio as much as $100 million

By Lisa Richwine

December 9, 2014 10:59 PM GMT · Updated 9 years ago

Amy Pascal steps down from Sony Pictures in wake of damaging email hack

One of Hollywood's most powerful executives is leaving company after hacking scandal that resulted in leak of her emails, but is starting studio-backed venture

Soı Grı

6

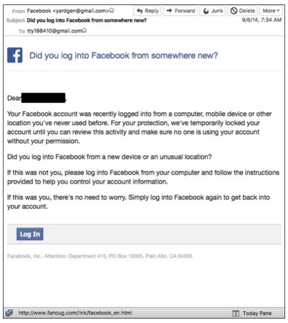
Mandiant/FireEye Investigation

- North Korean Hackers, angry about a film.
  - North Korea previously complained to the UN.
  - Seth Rogen: "People don't normally want to kill me for one of my films until after they have paid $12 to see it"
- A state sponsored group called APT38.
- Normally target companies making SWIFT money transfers.
- Aims to fund the North Korean economy and weapons programs.

7

Gaining Access

- Mass phishing campaign.
- Targeting 100s of Sony employees.
- E-mail, Facebook messages, LinkedIn in messages,…



From Facebook <yardgen@gmail.com>
Subject Did you log into Facebook from somewhere new?
9/6/14, 7:34 AM
To tty198410@gmail.com

Did you log into Facebook from somewhere new?

Dear [redacted],

Your Facebook account was recently logged into from a computer, mobile device or other location you've never used before. For your protection, we've temporarily locked your account until you can review this activity and make sure no one is using your account without your permission.

Did you log into Facebook from a new device or an unusual location?

If this was not you, please log into Facebook from your computer and follow the instructions provided to help you control your account information.

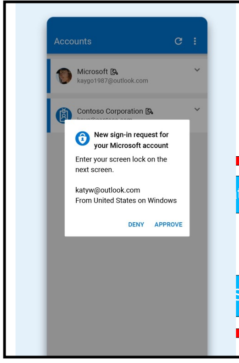
If this was you, there's no need to worry. Simply log into Facebook again to get back into your account.

Log In

Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

http://www.fancug.com/link/facebook_en.html

8

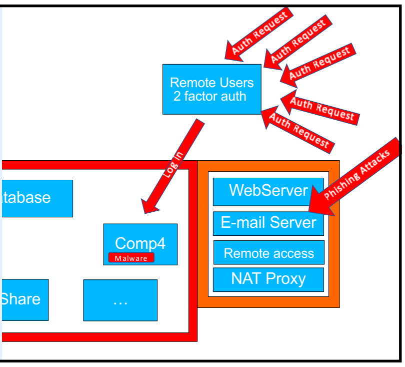


New sign-in request for your Microsoft account

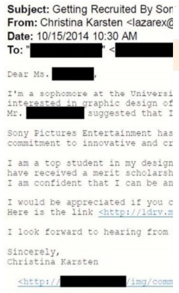
Enter your screen lock on the next screen.

katyw@outlook.com
From United States on Windows

DENY APPROVE

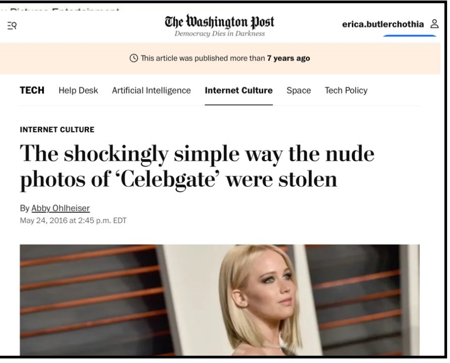


9



Subject: Getting Recruited By Son
From: Christina Karsten <lazarex@
Date: 10/15/2014 10:30 AM
To: "[redacted]" <[redacted]

```
Dear Ms. [redacted],

I'm a sophomore at the Universi
interested in graphic design of
Mr. [redacted] suggested that I

Sony Pictures Entertainment has
commitment to innovative and cr

I am a top student in my design
have received a merit scholarsh
I am confident that I can be an

I would be appreciated if you c
Here is the link <http://1drv.m

I look forward to hearing from

Sincerely,
Christina Karsten

  <http://[redacted]/img/comm
```



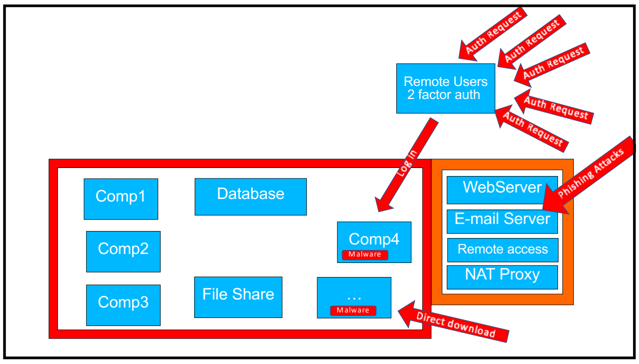
This article was published more than **7 years ago**

INTERNET CULTURE

The shockingly simple way the nude photos of 'Celebgate' were stolen

By Abby Ohlheiser
May 24, 2016 at 2:45 p.m. EDT

10

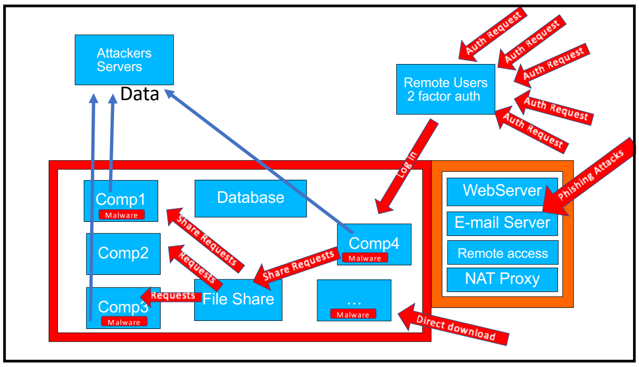


11

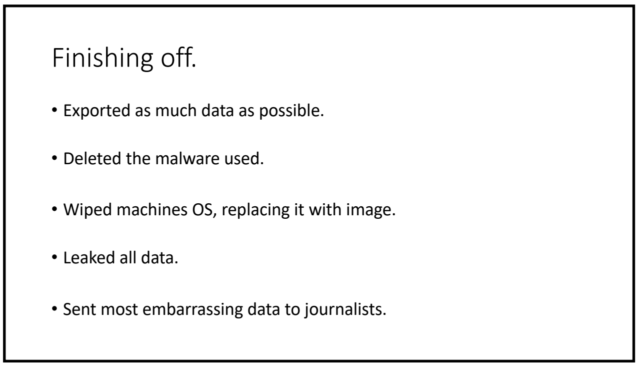
Traversing the network

- Once in the network the hackers installed custom built malware.
  - Sony's anti-virus system only looked for known malware.
- This malware abused vulnerabilities and brute force guessed passwords in the Server Message Block (SMB) file sharing systems.
  - Hackers used Sony's own infrastructure: "living of the land"
- Over 2 months, the malware copy itself from machine to machine, sending data to the hacker's servers.

12



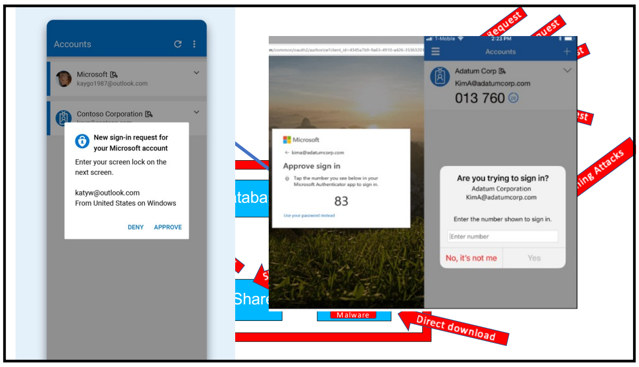
13



Finishing off.

- Exported as much data as possible.
- Deleted the malware used.
- Wiped machines OS, replacing it with image.
- Leaked all data.
- Sent most embarrassing data to journalists.

14



New sign-in request for your Microsoft account

Enter your screen lock on the next screen.

katyw@outlook.com
From United States on Windows

Approve sign in

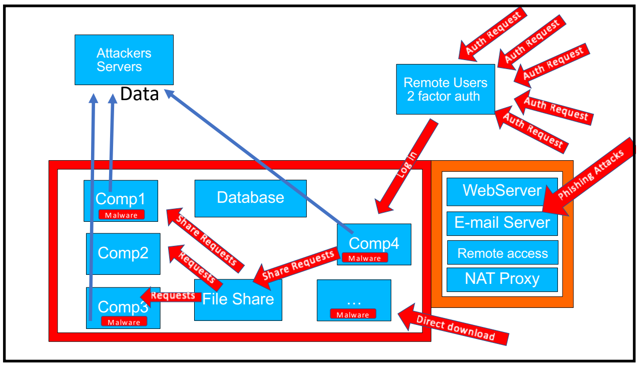
Tap the number you see below in your Microsoft Authenticator app to sign in.

83

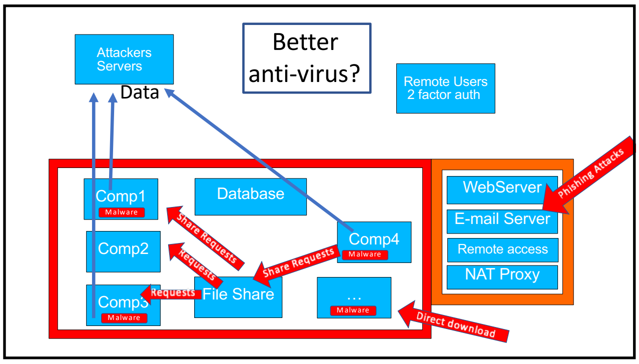
Are you trying to sign in?
Adatum Corporation
KimA@adatumcorp.com

Enter the number shown to sign in.

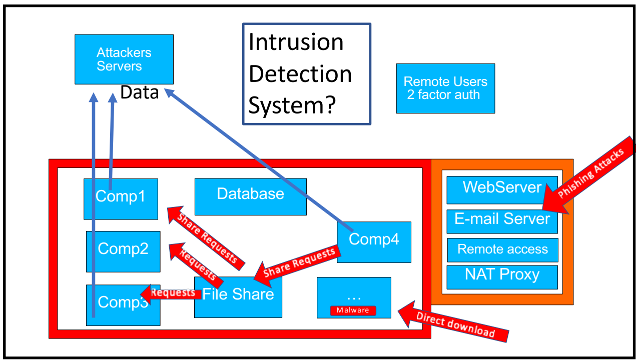
15



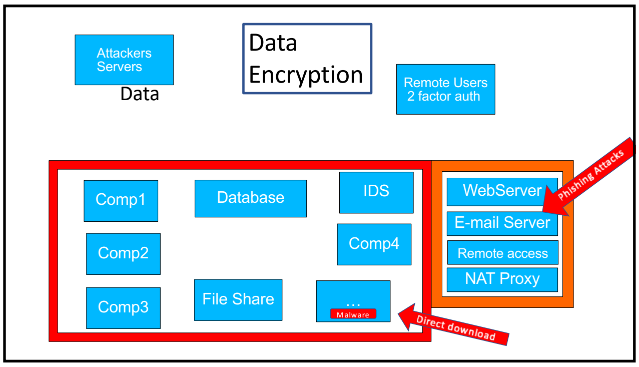
16



17



18



19

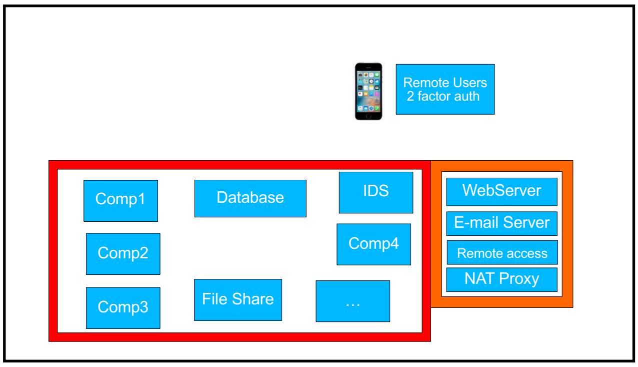
Sony Hack: Summing up

- Carefully crafted, targeted attacks. Highly capable attackers.
  - Access via phishing attacks
  - Then hand crafted malware
- Film cancelled, loss of all production, huge reputational damaged from leaked e-mails,
- Chairperson steps down,
- Sony sued by employees,
- North Korean internet goes down for 10 hours.

20

The Mandiant/FireEye Hack

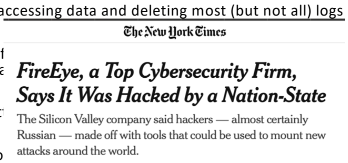
21



22

Mandiant/FireEye Hack

- Nov 10th 2020, Inspecting logs an analyst sees a 2-factor authentication phone, with no phone number… it was in a different state to the user!
- The account had been accessing data and deleting most (but not all) logs
- They had been looking f tools use to find vulnera
- No indication of how at
- Mandiant publicly anno

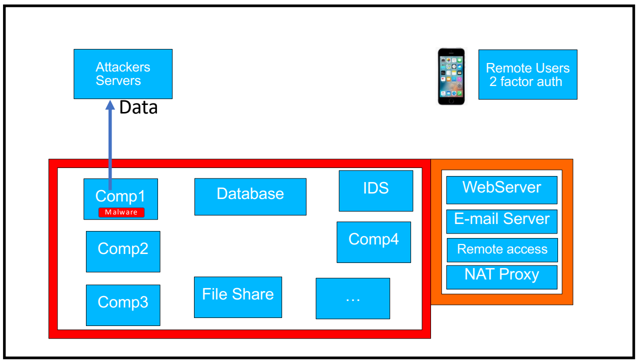


The New York Times

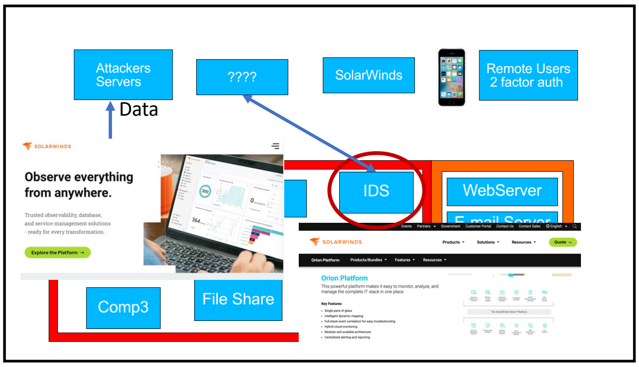
FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State

The Silicon Valley company said hackers — almost certainly Russian — made off with tools that could be used to mount new attacks around the world.

23



24



Observe everything from anywhere.

Trusted observability, database, and service management solutions - ready for every transformation.

Orion Platform

This powerful platform makes it easy to monitor, analyze, and manage the complete IT stack in one place.

Key Features

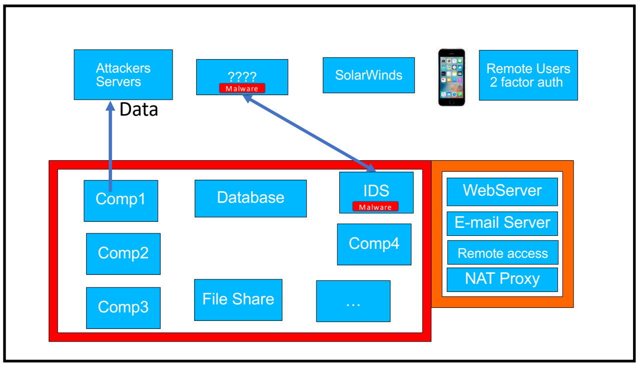
- Single pane of glass
- Intelligent dynamic mapping
- Full-stack event correlation for easy troubleshooting
- Hybrid cloud monitoring
- Modular and scalable architecture
- Centralized alerting and reporting

25

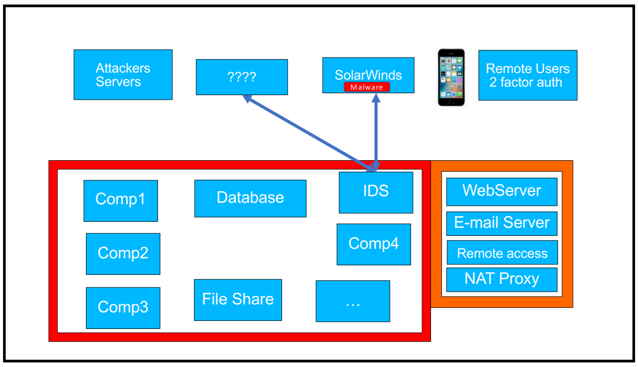
Investigation

- After months of investigation, they saw a computer communicate with an unknown server. The machine was running software from SolarWinds, part of their IDS system.
- It should have only connected to a SolarWinds server to check for updates. Instead, it was talking to an unknown IP address.
- Mandiant guessed this server had been hacked and examined all programs running on it.

26



27



28

Mandiant -> SolarWinds

- SolarWinds IDS was installing malware.
- New code from SolarWinds had the same bad code!
  - SolarWinds had been hacked.
- Mandiant informed SolarWinds, and gave them a deadline before going public.
- Also worked with the NSA and FBI.

29

SolarWinds

- Legal team put in charge of investigation. All information under attorney-client privilege.
- Attackers had been in their network for more than a year.
  - Monitoring all e-mail accounts! Investigators couldn't use their corporate e-mail.
- SolarWinds found that 18,000 customers were running the backdoored code.
- Added backdoor code copied the style of the original code. The hackers improved efficiency and fixed bugs.

30

The Malware

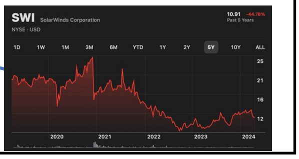
- Does nothing for 12 to 14 days. Then scans the system and reports back.
  - Detects and stops some security tools, removes data from system logs.
- It installs a different backdoor program on a different machine or deletes itself.
  - Targets included: US Department of Defense, Homeland Security, the Treasury Department, Intel, Cisco, and Palo Alto Networks, Microsoft, Mimecast, the antivirus firm Malwarebytes,…
- Attackers set up a server in same country as victim, with a name that matches a legitimate company hostname.
- Command and control masquerades as the legitimate SolarWinds Protocol
  - Hence evading anti-malware, IDS and firewalls.

31

Timeline

- January 30th 2019: hackers recorded downloading all source code.
- September 19th 2019: attackers return, insert dummy code and monitor all company e-mail accounts.
- February 19th 2020: The malware code is planted.
- June 4th 2020: All attacker connections stop.
- Nov 10th 2020: Mandiant start to investigate the attack
- Dec 12th 2020: Mandiant report attack to SolarWinds.
- Dec 14th 2020: Mandiant goes public.

In Spring 2020, FBI spotted bad traffic from SolarWinds software and e-mailed them. Then did nothing else.



32

Mandiant/FireEye Hack: Summing Up

- Largest intrusion into the federal government in the history of the US.
- Discovered by Mandiant analysts, by chance.
  - If they hadn't targeted Mandiant, they would probably not have been caught.
- Accessed Microsoft Windows source code.
- Many of the compromised companies also make security products.

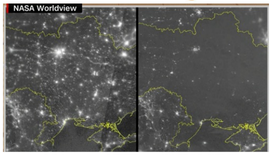
33

Ukrainian Power Grid: The Attack That Didn't Happen

34

Russia Targeting the Ukrainian Power Gird

- 2007 BlackEnergy1: Russian Hackers access Ukrainian power grid IT
- 2014 BlackEnergy2: Russian Malware found on OT power equipment.
  - Reconnaissance, data collection
- 2015 BlackEnergy 3: Software on OT power equipment wiped.
  - Blackout for 6 hours,
  - Year to get some elements working again
- 2016 Crashoverride/Industroyer:
  - 1 hour of blackout



35

24 February 2022: Russia Invades Ukrainian

- We know Russia is highly cyber capable and **will** target the power grid.
- Ukraine knows this is coming and has been preparing for years.
- Result:

36

24 February 2022: Russia Invades Ukrainian

- We know Russia is highly cyber capable and **will** target the power grid.
- Ukraine knows this is coming and has been preparing for years.
- Result: Nothing! Defenders win.
  - “Industroyer2” malware detect on system and stopped before it runs.
- A really good defense beats the best attackers.

37

Some links

- Sony hack
  - https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf
  - https://www.bbc.co.uk/programmes/w13xtvg9/episodes/
  - https://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony/
- SolarWinds supply chain
  - https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/
  - https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

38

Monday

- A table top cyber defense game.
- You will play in teams of ~5
- Try to defend a company against attack.

39