The PlayStation Network Breach and Outage (2011)

“..the biggest Internet security break-in ever“ – Reuters News Agency

JONATHAN FLUM
CSCI 301

Context that led up to the breach:

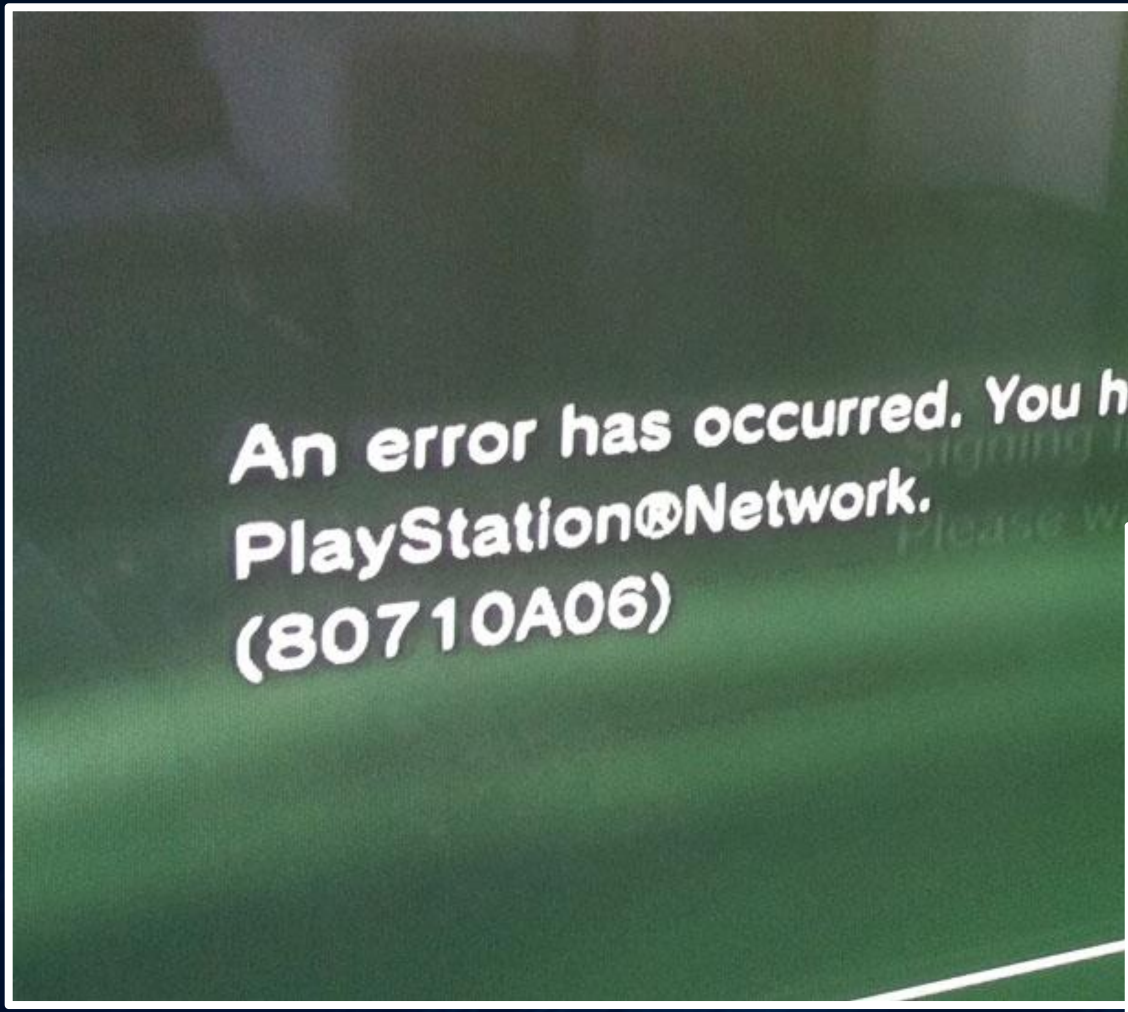
- ***January*** – Sony sues hacker “GeoHot” and his accomplices for circumventing the security system of the PlayStation 3 and making the jailbreak tools publicly available
- ***March*** – Courts authorize Sony’s request to obtain the IP addresses of every person that that accessed his website to download these tools
- ***April 3rd*** – The hacktivist group “Anonymous” launches various cyber attacks on Sony websites in retaliation for their legal pursuit.

A looming threat:

- ***April 11th*** – Sony settles lawsuit with "GeoHot," but "Anonymous" announces it will continue its protest…

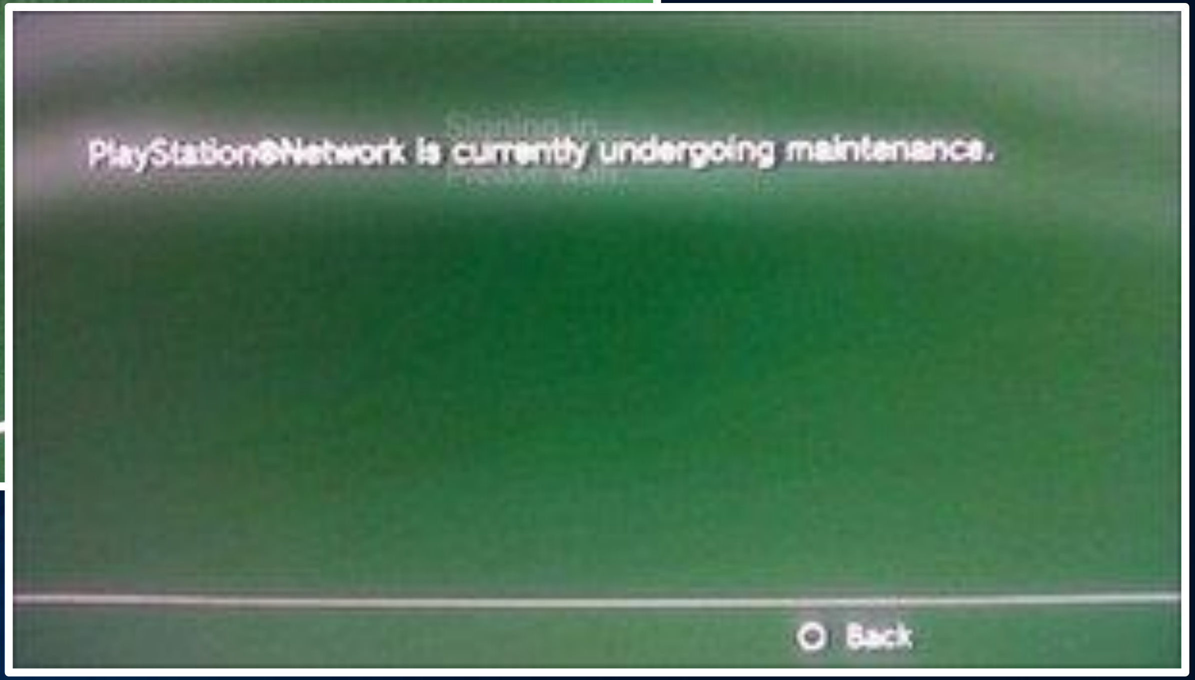
“Anonymous” keeps their word:

- ***April 19th*** – Sony’s network team detects unauthorized activity in the PlayStation Network system.
  - 4 servers are taken offline
- ***April 20th*** – Early investigation indicates that data of some kind was transferred off their servers.
  - 6 more servers are taken offline.
- Sony is unable to determine what information was stolen and shuts down the entire network that same day.
  - The remaining 120 servers are taken offline.



An error has occurred. You have been signed out of PlayStation®Network.
(80710A06)

Signing in...
Please wait.



PlayStation®Network is currently undergoing maintenance.

Signing in...
Please wait.

Users are confused…

Sony’s action and response:

- ***April 21st - 25th*** – A second forensic team and computer security firm is hired, investigations intensify
  - The scope of data loss is determined, effectively all PII for every user
- ***April 26th*** – Sony provides a public statement regarding the intrusion (note: 6 days after the breach)
  - Does not immediately confirm Credit Card data was stolen
- ***May 14th*** – Firmware update 3.61 is released as a security patch and the PlayStation Network began restoring in geographical phases.

The aftermath and verdict:

- $171 million dollars in losses (just for Sony)
- Sony's "Welcome Back" Program = 2 free games and a 30 day PS Plus subscription for your trouble.
  - Public out roar, consolation prize not even close to being commensurate with potential for personal damages
  - Thus, several lawsuits filed against Sony
  - Loss of public trust in safeguarding information
  - Rulings indicated that there is no such thing as a perfect, unbreachable system
  - Sony later offered credit monitoring & identity theft insurance to affected users.

The aftermath and verdict, cont.:

- 77 million accounts compromised:
  - Name, address, and other personal details
  - Email accounts/passwords and other credentials
  - Credit card, stored payment information
  - Majority of data was not encrypted on the network!

How did it happen?

- Exact vector of attack never made public, but understood to likely have been a software exploit.
- SQL Injection?
  - External to network
  - Security vulnerability found through previous DDoS attacks on Sony?
- Development unit / Rebug CFW exploit?
  - Internal to network
  - Trusted credentials that allow access to customer details database

How could it have been prevented?

- If we subscribe to the Rebug custom firmware (CFW) theory:
  - PSN recognized the hardware (falsely) as a Development Unit
  - “Trusted Access” permission was given to console, authorizing access to databases and other internal network data
- Sony’s network security software likely did not account for an attack of this type to take place from within it’s ‘trusted network.’
  - Therefore, no mechanism in place to prevent it

How can we do better in the future?

- All powerful “Trusted Access” credentials are a bad idea
- Store Personally Identifiable Data with encryption
- Consider all the possible vectors, both internal and external
- Implement redundant safeguards where possible
- Continually evaluate, improve, and deploy measures

Questions?