2014 Apple iCloud Hack(s)

A.K.A

Celebrity Photo Hack
Celebgate
Find my iPhone Hack

Other various names on the internet
Timeline of Relevant Events

- Find my iPhone vulnerability released to the public August 30th
- Confidential photos were released on August 31st
- Apple allegedly patched the vulnerability on September 1st
- A second collection of private photos were released September 20th, containing additional celebrities
- September 26th: even more photos released
Media Speculation

- “While it's highly unlikely to be a security issue with iCloud, the incident has served to remind us all of the issues around internet security in general” - TechCrunch

- “A wide scale 'hack' of Apple's iCloud is unlikely. Even the original poster is not claiming that” - Rik Ferguson, VP Security at Trend Micro

- “My suspicion is that this isn't an iCloud security flaw as such” - Graham Cluley, Security Expert
Apple's Response

- Apple: “A very targeted attack on user names, passwords and security questions, a practice that has become all too common on the internet”

- No mention of iCloud
- Very general
Theories from the Media

- Social Engineering - A person in charge of a celebrities' social media was responsible
- Directed phishing attack
- Chaining – one account was compromised, which led to other accounts being compromised
- public WiFi networks – unencrypted photos were intercepted while being backed up to iCloud
Find my iPhone Vulnerability

- The sign in page for the Find My iPhone program in apple devices did not employ brute-force protection.
- Hackers were able to flood the sign in page with thousands of possible passwords without being locked out.
- Once the password was discovered hackers used it to gain access to the Apple iCloud.
Apple was aware of FindMyIphone!

- Posts on Apple's support page detailing the vulnerability since MARCH 2014
Hack in Australia

- Australian hackers exploited findMyIphone
- Hacked Find my iPhone and locked the device
- Ransomed locked devices and unlocked them only when they received money
Hack in Netherlands

- iCloud was hacked in the Netherlands by a pair of hackers named “Duolci”
- Exploit was able to unlock stolen iPhones very easily
Taking the Vulnerability to the Public
iBrute

- Released one day before the first photo-release
- Python script allowing for brute-force of apple iCloud
- Exploited the Find my Iphone vulnerability
- Common Dictionary attack
- Supposedly patched September 1st, 2014
iDict

- Able to bypass Apple's brute-force detection AFTER the iBrute patch in September
- Standard dictionary attack
- Same vulnerability
- Targets email must be known
iDict

- From the README:
- Why? “This bug is painfully obvious and was only a matter of time before it was privately used for malicious or nefarious activities, I publicly disclosed it so apple will patch it”
- Released on January 1st
- Patched on January 2nd
Apple's Response

- Patch of the find my iphone vulnerability
- Push notifications when there is a login on an unrecognized device
- Push notifications for data restored to another device
- Set up “two-step verification”
  - Many users do not use two-step verification
  - Two-step verification takes a long time to set up
What can you do?

- Use two-step authentication
- Follow good password policy
  - Use a good password
  - Change them frequently
- DON'T take compromising pictures
- DON'T upload compromising pictures to iCloud
Are we ok?

- If another vulnerability comes out, Apple should be more diligent in fixing the situation.
- Might need another public disclosure and exploit to have them act accordingly.
Sources

- https://github.com/hackappcom/ibrute
- https://github.com/Pr0x13/iDict