CLOUDSEC
CONFERENCE 2014
HAVE A SAFE JOURNEY

해커가 바라보는 클라우드 취약점과 공격 시나리오

박 찬 암
팀장
라온시큐어 보안기술연구팀

Cloud Hacking Cases and Vulnerabilities

1. Wired.com reporter hack
2. F*** my iPhone?
3. Celebrity photo leaks
4. Cloud **ck up
5. Amazon Cloud Vulnerability
6. Vulnerability by user configuration

How to improve cloud security against the attack

1. Multi-factor authentication
2. Abnormal behavior detection/alert
3. Offensive security by user viewpoint

Cloud attack scenario forecast

1. Cloud application parsing problem

CLOUD HACKING CASES AND VULNERABILITIES

Wired.com reporter hack

The damage

- Google account hacked
  - Account deletion
- Twitter account hacked
  - Used as a platform to broadcast racist and homophobic messages
- Apple ID hacked
  - Hackers used it to remotely erase all of the data on the reporter's iPhone, iPad, and MacBook
    - Daughter's photos, documents, e-mails, …

Apple account hacking process - 1

- **Get billing address**
  - Whois search on his personal web domain

Social Engineering Part

- **Get the last four digits of the credit card number**

1. Call Amazon to add a credit card number to the targeted account
   - All you need to verify yourself are as follows
     - Name on the account, Associated e-mail address, Billing address

(Continue)

Apple account hacking process - 2

2. Call Amazon again and tell that you've lost access to your account
   - Amazon will allow you to add a new e-mail address to the account if you provide a name, billing address, and the credit card number

3. Conduct password reset to the targeted account

(Continue)

Apple account hacking process - 3

4. See the Payment Methods menu

Payment Methods

Credit Card	Name on Card	Expires On
ending in 1[redacted]	Chanam Park	1/[redacted]

- **Contact the Apple tech support and provide the information as follows to access the targeted account**
  - Associated e-mail address, last four digits of the credit card number, Billing address

Apple's F*** my device?

- **Find** my device or **Fuck** my device?

- The easiest way to destroy your whole digital life
  - Don't put all your digital eggs in the Apple basket!

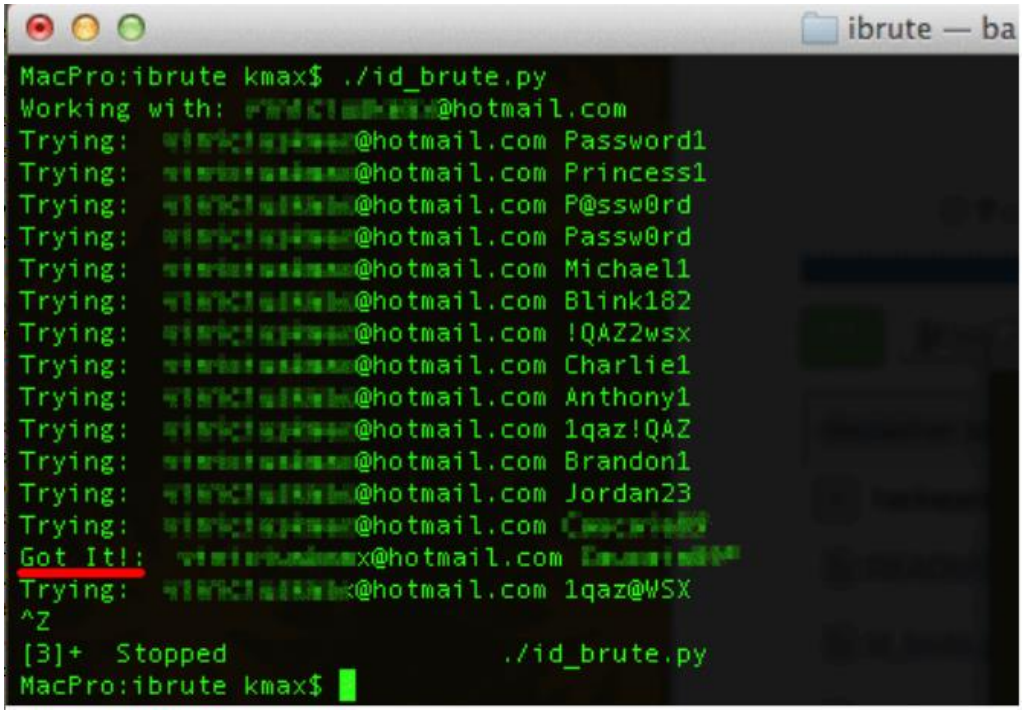
Apple's F*** my device?

- **Find** my device or **Fuck** my device?

- There have been some critical hacking accidents by the social engineering attack which is kind of cheating
  - Wired.com reporter hack
  - Celebrity photo leaks

Apple's F*** my device?

- Doesn't have brute force protection
  - It had allowed to try probable passwords with no limits



HOW TO IMPROVE CLOUD SECURITY AGAINST THE ATTACK

CLOUD ATTACK SCENARIO FORECAST

CLOUDSEC
CONFERENCE 2014
HAVE A SAFE JOURNEY

THANK YOU

박 찬 암

http://hkpco.kr

chanam.park@hkpco.kr

#CLOUDSEC2014