Monthly Research

Black Hat Asia 2016 Survey Report

FFRI,Inc.
http://www.ffri.jp

Ver 2.00.01

About Black Hat Asia

- Asian version of the famous security conference the Black Hat
  - Speakers have been selected from all over the world

- It has been held in the Singapore in every spring
  - Latest security research briefings and trainings are provided
    - New threat demo, exploit technique, defense technology
    - Slides and white paper have been published on the official site
  - Black Hat Asia 2016 was held on March 29 to April 1

- In this report, we pick up briefings of Black Hat Asia 2016

Our pick up research

- Mobile Security
  - Android Commercial Spyware Disease and Medication
    - Mustafa Saad
  - Su-a-Cyder: Home-Brewing iOS Malware Like a B0$$!
    - Chilik Tamir
- IoT Security
  - Lets See Whats Out There Mapping The Wireless IOT
    - Tobias Zillner
  - Hacking a Professional Drone
    - Nils Rodday
- Windows Security
  - DSCompromised:A Windows DSC Attack Framework
    - Ryan Kazanciyan & Matt Hastings

Android Commercial Spyware Disease and Medication

- About Commercial Spyware
  - These have been used to monitor children or employees
  - Price is about hundred dollars/year
  - Most spyware have web interface for monitoring
- Droid Smart Fuzzer is an anti-spyware solution
  - Get permissions in all installed apps
  - Check the permissions which are requested by spyware
    - RECEIVE_SMS
    - PROCESS_OUTGOING_CALLS
    - READ_PHONE_STATE
    - INTERNET
  - Perform tests that correspond to the permissions with the Internet connection
  - Consequently, detect spyware based on network traffic

Android Commercial Spyware Disease and Medication

- Droid Smart Fuzzer detected the top 15 of commercial spyware and the 4 free spyware

- **Comments of FFRI researcher**
  - Interesting to detect with spyware at like a heuristic
  - Their algorithm is simple and false positive rate is not discussed
  - The research is useful because the spyware might increase in the future

Su-a-Cyder: Home-Brewing iOS Malware Like a B0$$!

- iOS malware history, capabilities and worst scenario
- Demonstrated collecting data from the non jailbroken iPhone
- The attack to avoid enterprise MDM was successful
- Furthermore, attacks by icon-less stealth apps and Skype repackaging were also successful

- **Comments of FFRI researcher**
  - iOS malware is getting sophisticated every year
  - It is expected to increase in the future
  - You should not be off guard, even if you do not jailbreak

Lets See Whats Out There Mapping The Wireless IOT

- Wireless IoT devices are rapidly increasing
  - Samsung announced that their all IoT devices will support wireless by 2019
  - The US Director of National Intelligence, James Clapper mentioned about the possibility that IoT bring serious threats
- It is difficult to evaluate security of radio signal because tools are not enough
- The presenter has developed an integrated wireless security testing tool
  - In addition, he also showed ranking about risks of wireless IoT devices
    - He emphasized that wireless network have many threats

Lets See Whats Out There Mapping The Wireless IOT

- **Comments of FFRI researcher**
  - IoT device is rapidly spreading, but feels security is not enough
  - The integrated tools are useful for wireless IoT

Hacking a Professional Drone

- Demonstration of MITM attack on drone
  - The attacking targets are drone, remote controller and mobile app for control of drone
- Drone - Remote controller communication
  - XBee, encryption is not enabled
- Remote controller – Mobile app communication
  - Wi-Fi, encryption is WEP
- The presenter decompiled android app, decoded signal, analyzed payload
- He said the vendor can not fix vulnerability without OTA update
- He also said that the other drones have vulnerabilities.
- Proposing
  - Implement built-in encryption of XBee
  - Encrypt payload in application layer

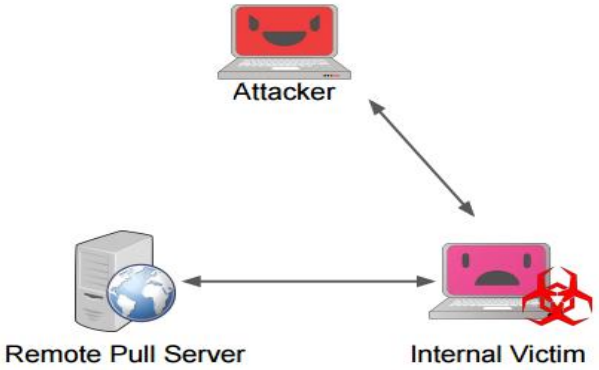
Hacking a Professional Drone

- **Comments of FFRI researcher**
  - The research was published in the RSA conference 2016 before Black Hat Asia 2016. It had attracted media attention
  - There are recall requests, but shipments will continue
  - There is a risk that cyber attacks make false accusation by the registration system of drone in the USA

DSCompromised:A Windows DSC Attack Framework

- About PowerShell DSC (Desired State Configuration)
  - Next generation configuration management platform for Windows
  - It is available Windows 8.1, Windows Server 2012 R2 or above

- The demo to infect persistent malware on using the DSC consistency check
  - Install the DSCompromised Framework to construct DSC pull server as C&C server
  - Put a malware in the DSC pull server, generate a MOF file
  - Intrude into victim network in any way
  - Modify victim's LCM to connect to the C&C
  - Malware will re-download by the DSC consistency check if malware is removed
  - It is also possible to create persistent user account in the same way



Attack image
DSCompromised: A Windows DSC Attack Framework: p22

DSCompromised:A Windows DSC Attack Framework

- **Comments of FFRI researcher**
  - This technique has not been confirmed yet in actual attack
  - However, it is necessary to caution the future attack for the following reasons
    - DSC is installed by default in the Windows 8.1 and Windows Server 2012 R2
    - PowerShell-based attack is increased
      This technique will accelerate it further

Conclusions

- Mobile security will be improved in the future
  - iOS security will become more important because malware is targeting non jailbroken iPhone
  - Android malware and research for its detection have been increased
- Practical security test methods and tools for IoT have been demanded
  - There are many research on test methods and useful tools
  - There are research to discover vulnerabilities through reverse engineering
- New attacks on the Windows system will be continued in the future

References

- Android Commercial Spyware Disease and Medication
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Saad-Android-Commercial-Spyware-Disease-And-Medication.pdf
  - For Their Eyes Only: The Commercialization of Digital Spying
    - https://citizenlab.org/2013/04/for-their-eyes-only-2/
- DSCOMPROMISED: A WINDOWS DSC ATTACK FRAMEWORK
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Kazanciyan-DSCompromised-A-Windows-DSC-Attack-Framework.pdf
- HACKING A PROFESSIONAL DRONE
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf
  - RSA Conference 2016
    - http://www.rsaconference.com/events/us16
- LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Zillner-Lets-See-Whats-Out-There-Mapping-The-Wireless-IOT.pdf
- Su-a-Cyder: Home-Brewing iOS Malware Like a B0$$!
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Tamir-Su-A-Cyder-Homebrewing-Malware-For-iOS-Like-A-B0SS.pdf

Contact Information

E-Mail ：research-feedback at ffri.jp
Twitter：@FFRI_Research