# Cyber@UC Meeting 60

Aircrack with Chris

# If You’re New!

- Join our Slack: ucyber.slack.com
- **SIGN IN!** *(Slackbot will post the link in #general)*
- Feel free to get involved with one of our committees:

  *Content* *Finance* *Public Affairs* *Outreach* *Recruitment*
- Ongoing Projects:
  - RAPIDS Lab!

# Announcements

- We cleaned up the lab :)
- **US Bank** visited us today!
- **CiNPA Security Meetup** tomorrow @6:30pm
    - Impact of Automation & Orchestration on IT and Security Operations

# Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** @CyberAtUC
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

# Weekly Content

# MDM Solution Used to Spy on iPhone Users

- Highly targeted mobile malware operating since August 2015 found to be spying on 13 selected iPhones in India
- Attackers are believed to be operating from India
- Abused mobile device management protocol, a type of security software used by large enterprises to enforce policies on devices used by employees
- Enrolling iOS device in MDM requires manual installation of enterprise development certificate, obtained via Apple Developer Enterprise Program
- Once installed, the company can remotely control the device

# MDM Exploitation (continued)

- Unclear how the attackers enrolled the devices, because enrollment requires user interaction
- Cisco’s Talos threat intelligence unit believe the attackers probably used social engineering, like a fake tech support call
- Used MDM to remotely install compromised versions of legitimate apps
- Attacker is unknown but suspected to be operating from India
- Found a “false flag” posing as Russians

https://thehackernews.com/2018/07/mobile-device-management-hacking.html

# A Deep Dive into Vermin RAT

- One of three RATs used by cybercriminals to exfiltrate data from and spy on Ukrainian government institutions
  - Quasar, Sobaken, and Vermin
  - https://www.welivesecurity.com/wp-content/uploads/2018/07/ESET_Quasar_Sobaken_Vermin.pdf
- Attackers have been tracked by ESET since mid-2017, first reported on in January 2018
- Have been using stealthy RATs to exfil sensitive data from victims
- All three RATs have been in use at the same time and exfil data to the same servers

# Vermin (continued)

- Quasar is open-source RAT available on GitHub, traced back to October 2015 using Quasar Rat binaries
- Sobaken is heavily modded Quasar RAT, slimmed down and added detection evasion and anti-sandboxing
- Vermin is custom-made full-featured backdoor, first appeared in mid 2016, slows detection by using commercial .NET code protection system .NET Reactor or the open-source ConfuserEx
- All three installed when a dropper drops a malicious payload into APPDATA folder, in a subfolder of a legitimate software, ex Adobe

# Vermin (continued)

- A scheduled task is then made to run every 10 min to ensure persistence
- Attempts to avoid sandboxing by only running if a Russian or Ukrainian keyboard layout is installed, the IP is located within one of the 2 countries, and is not registered to an antimalware vendor/cloud provider
- Also the malware doesn’t run if the username is typical of an automated malware analysis system

https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

# LuckyMouse

- Detected an ongoing campaign targeting national data centers in Central Asia in March 2018, believed to have been going since Autumn 2017
- Used for watering hole attacks, injecting malicious scripts into govt websites
- Used HyperBro Trojan as the final stage in-memory RAT
- Timestamps for the modules are from December 2017–January 2018
- Anti-detection launcher and decompressor use Metasploit tools
- Due to tools and tactics used, attributed to LuckyMouse, Chinese-speaking actor (also known as EmissaryPanda and APT27)
- HyperBro is popular for Chinese attackers and Metasploit has been used by LuckyMouse previously

# LuckyMouse (continued)

- How the data center was infected in unclear, potentially used another watering hole to infect data center employees
- Once inside the data center, three files were dropped, a DLL side loader, a DLL launcher, and a decompressor
- Compromised websites redirected visitors to malicious websites, a BEeF instance and a ScanBox instance
- The most worrying part were the attempts to disguise the campaign, which is unusual for chinese actors and could be a sign of a new approach that will be seen more in the future

https://securelist.com/luckymouse-hits-national-data-center/86083/

# Recommended Reading (legal)

- https://securelist.com/coinvault-the-court-case/86503/
- https://thehackernews.com/2018/07/google-android-antitrust-fine.html
- https://thehackernews.com/2018/07/alexander-vinnik-btc.html
- https://thehackernews.com/2018/07/selena-gomez-email-hacking.html
- https://thehackernews.com/2018/07/luminositylink-hacking-tool.html
- https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/
- https://www.welivesecurity.com/2018/07/16/irishman-extradited-us-silk-road/

# Recommended Reading

- https://thehackernews.com/2018/07/apple-china-icloud-data.html
- https://thehackernews.com/2018/07/microsoft-bug-bounty.html
- https://www.darkreading.com/threat-intelligence/one-third-of-businesses-lack-a-cybersecurity-expert/d/d-id/1332317
- https://www.darkreading.com/endpoint/scada-ics-dangers-and-cybersecurity-strategies/a/d-id/1332278
- https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/
- https://www.welivesecurity.com/2018/07/05/five-tips-pentesters-ios/

# Aircrack-ng!

# Part 11.1: Aircrack-ng suite

*I am a graphic designer*

# The Topics Today Go Something Exactly Like This

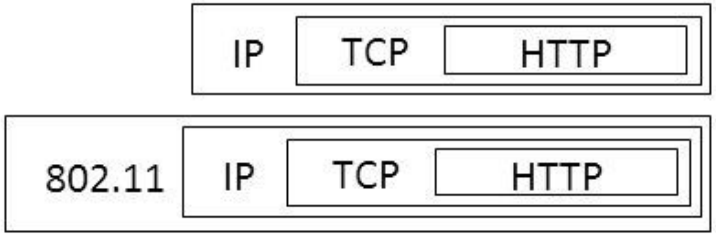
- Prereqs (monitor capable hardware)
- Getting to the aircrack website from uc
- Suite
  - Airmon-ng
  - Airbase
  - Aireplay
  - Others?
- Dodging techniques
  - Macchanger

# Wireless vs. Physical

| Wireless | Both | Wired |
|---|---|---|
| Proximity Based | IP Based (MAC, IP addr, DHCP) | Physical Connection |
| **Open Air (anyone can listen)** | | Limited by Cable Length |
| Device - AP Encryption in Standard | | |
| Limited by Radio Power | | |

# Adding a new layer

- When we move from wire to wireless, we need to add a new protocol to handle device connections to the router and encryption schemes.
- Most used protocol is 802.11 which originates from IEEE in 1997



# Wireless tools mentioned last time

## Software

- **aircrack-ng**, a collection of tools to play with wireless protocols.
  - **Requires certain chipsets and drivers to use**
- Scapy, python library for playing with wireless protocols
  - High capability but requires development from user
  - Also requires certain hardware for certain actions

## Hardware

- Raspberry Pi series
  - Powerful enough to use, cheap enough to use aggressively
  - Pumpkin Pi is a Pi based clone of the Wifi Pineapple
- AR150 Router series

# Our Chipset: RT5370

- Chipset != Model
- Really Cheap
- Very common chipset
- Typically in the lower end NIC's meant for embedded projects
- I have some with me if your built-in doesn't work

# Installing Aircrack-ng

- Kali
    - Built in
- Other *nix
    - Check package manager
    - Try building?
- Windows
    - Pre built binary at aircrack-ng.org (blocked by UC filter so you’ll need to proxy)
    - Drivers probably won’t work anyway but you should be able to do analysis on dumps from other machines
    - “You must write your own drivers” is never a good sign

# Enabling Monitor Mode

- What is monitor mode?
  - Lets us listen to all networks for meta data and management frames
  - Can see access points and client association
  - Can see pretty much everything required for 802.11
- How do
  - Find your interface with **iwconfig** or **ifconfig**
  - **airmon-ng start <interface>**
  - Make sure everything is working with another **iwconfig**

# Finding APs/Clients

- **airodump-ng <interface>**
- I had a final come up when I started writing these slides so we’ll just play around from here