Cyber@UC Meeting 57

SDR Fun!

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:
  - Malware Sandboxing Lab
  - Cyber Range
  - RAPIDS Cyber Op Center

Announcements

- **Cyber Operations** research opportunity
- Interview with **Bring Your Own Security Radio** Next Thursday 9pm
- **MITRE Network Security** position opportunity **SEND RESUMES**- Thanks Mike!
- **Gas Leak** in the lab :(
- **Stalking Threat Actors** meetup tomorrow **6:30pm**
- **Bylaws are looking good!**
- **Logo** in progress!

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

OpenBSD Disabling Hyperthreading

- What is OpenBSD? One of if not the most secure general OSs available
  - Described as Unix-like
- Made the decision to disable hyperthreading to prevent vulnerability to attacks like spectre and meltdown
- Hyperthreading was introduced in 2002 to allow an os to use a virtual core for each physical core present and improve performance
- OpenBSD has stated they do not believe this will negatively impact performance and suggested that leaving it enabled may actually slow performance when using more than two physical cores

https://thehackernews.com/2018/06/openbsd-hyper-threadin nl

MacOS Bug Shows Data on Encrypted Drives

- Quick Look feature creates a thumbnail for each file/folder so users have an easy way to evaluate the contents before opening it
- This information is stored in a known and unprotected location, even if the files/folders are from an encrypted container
- This vulnerability has existed and been known for at least 8 years but is not widely known by mac users
- This behavior even occurs to files/folders on password protected encrypted AFPS containers and USB drives
- The solution: not caching from encrypted containers, or clearing when the encrypted container is unmounted

https://thehackernews.com/2018/06/apple-macos-quickl

Mobile Providers Cut 3rd Party Location Deals

- Update from previous articles
- Mobile carriers are selling real time location data of their customers
- The parties that this data is being sold to have no obligations to protect it
- They allow the live location of any phone in the us to be tracked
- AT&T, Sprint, Verizon have made the decision to stop selling this data to 3rd parties

https://krebsonsecurity.com/2018/06/verizon-to-stop-sharing-customer-location-data-with-third-parties/

Alphabet Launches VirusTotal Monitor

- Like virustotal website, but files are uploaded to a private cloud
- Tests against all of the 70+ VirusTotal vendors
- Files are only shared if an alert is created and then only with the vendor(s) that create the alert
- The file that created the alert, its metadata (company behind the file, developer contact info, etc.)
- Allows vendors to prevent their software from creating false positives and the files are stored in a private cloud, so it will generate alerts in the future as well
- Great for AV vendors because they get context about a file

http://blog.virustotal.com/2018/06/vtmonitor-to-mitigate-fals[illegible]sitives.htm

https://www.darkreading.com/operations/alphabet-launches-virustotal-monitor-to

HeroRAT

- ESET discovered a family of Android RATs that abuse the Telegram protocol
- Source code for the RAT was made available on Telegram hacking channels
  - Spawned hundreds of variants of the malware
- One variant, HeroRat, is for sale at three different pricing models according to functionality and even comes with a support video channel
- Unclear if this was created from the source code, or it is the original source code that was leaked
- Attacker lures victim into downloading RAT through 3rd party app stores and social media/messaging
- Runs on all versions of android, but requires some special permissions, sometimes including giving the app administrator privs

HeroRat (continued)

- After HeroRat is installed and launched, a popup appears saying it can't be run on the device and will uninstall itself
- After uninstallation, app appears to be gone, but is controllable via Telegram's bot functionality
- Features include spying, file extraction, text message interception, sending texts, making calls, audio and screen recording, etc.

https://www.welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

Recommended Reading

https://www.darkreading.com/cloud/crowdstrike-secures-$200m-funding-round/d/d-id/1332088

https://www.crowdstrike.com/resources/news/crowdstrike-announces-200-million-series-e-financing-round/

https://www.crowdstrike.com/blog/crowdstrike-closes-200-million-series-e-financing-round-with-new-and-existing-investors/

https://krebsonsecurity.com/2018/06/bad-men-at-work-please-dont-click/

https://krebsonsecurity.com/2018/06/google-to-fix-location-d eak-in-goo ome-chromecast/

SDR Overview

Presentation Sponsor

- The Morrison Foundation

What is an SDR?

- Software where the hardware would be
- It’s not new
- Can work with lots of different signal protocols

Kamkar Car Key

- Cars with key fobs have rolling codes
- Car can be unlocked with a SDR

Control an RC Toy with a Replay

- Using GNU Radio to receive the controller signal
- Then transmit the signal back to move the RC thing

Super Cool Tips

Learn the rules by pursuing an amature radio license

ISM (2.4GHz) is unlicensed all over

Be mindful of your bandwidth and power

Try testing in a faraday cage or with a coax connection

RTL-SDR and HackRf One are great