

Cyber@UC Meeting 69

Enigma Machine

If You're New!

- Join our Slack: cyberatuc.slack.com (URL changed!)
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
 - Research lab!



Announcements

- **US Bank visit**
 - *Friday Sept 28th 2pm*
- **Rockwell Security Seminar**
 - September 20th 9am-3pm
 - Nippert Stadium
- **Chipotle Fundraiser**
 - Saturday Nov 3rd 4:00pm-8:00pm
- **Northrop Grumman**
 - Tonight @ Mick+Macks 6:30-8:30pm
- **CiNPA Security Sig Meetup**
 - Thursday Sept 20 @ 6:30



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](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: cyberatuc.org



Weekly Content

Cold Boot Attack

- Cold Boot Attack: A form of side channel attack, steals the information that remains in RAM after shutdown
 - Modern computers come with a safeguard that overwrites RAM when powering on, but the cyber-sec firm F-secure has found a workaround
 - Developed a tool to rewrite the non-volatile memory chip containing overwrite settings and disable it
 - Believed to be effective against almost all modern computers
 - Difficult to prevent this type of attack, but recommend using shutdown or hibernate instead of sleep as encryption keys are not stored in memory when using these methods
- 

Kodi Malware

- Kodi is a media player platform, does not carry its own content but uses add-ons to extend functionality
- A repository hosting one of these add-ons was shut down for copyright infringement and was then found to have a cryptominer hidden in it since late 2017
- Mines the Monero cryptocurrency, a version has not been seen which affects Android or macOS
- Top 5 aff



Kodi Malware (continued)

- Names itself after a popular add-on used by many other add-ons, ex “script.module.simplejson” but uses a different version number
- This add-on then pulls down another, more maliciously modified add-on
- This second add-on downloads and executes a binary file, which is actually a downloader
- This donwloader brings in the final payload, the cryptominer
- If this was sucessful, the python then removes itself



Recommended Reading

- <https://thehackernews.com/2018/09/iphone-crash-exploit.html>
- <https://www.welivesecurity.com/2018/09/17/bristol-airport-apparent-ransomware-attack/>
- <https://thehackernews.com/2018/09/cyberattack-bristol-airport.html>
- <https://www.welivesecurity.com/2018/09/17/uk-orgs-hit-cryptojacking-survey/>
- <https://thehackernews.com/2018/09/bitcoin-extradition-alexander-vinnik.html>
- <https://thehackernews.com/2018/09/kelihos-botnet-Peter-Severa.html>
- <https://krebsonsecurity.com/2018/09/govpaynow-com-leaks-14m-records/>

NSA Visit