Cyber@UC Meeting 61

Running a Linux box securely

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

- US Bank **Risk Analyst Position** open for application
- **All servers** are now moved into our server room ERC 513
- **US Bank visit** planned for some time in September
-

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

Calisto Trojan for macOS

- Origionally uploaded to VirusTotal in 2016 and not seen since, until recently
- Pretends to be Intego security solution for Mac, looks very similar
- Asks for username and password during installation
- Claims install fail and tells user to go to intego website for new version
- Calisto continues to work in the background

https://securelist.com/calisto-trojan-for-macos/86543/

Return of Fantomas, Decyphering Cryakl

- First occurred in spring 2014
- Spread through malicious emails containing attachments
  - Office doc with macro, js script, pdf with link to an executable
- One version of the ransomware changed the desktop wallpaper to a picture of the villain Fantomas from a French film
- Initially used basic and simple encryption but changed over many versions of iterations, eventually moving to asymmetric RSA encryption

https://securelist.com/the-return-of-fantomas-or-how-we-deciphered-cryakl/86511/

Recommended Reading

https://www.welivesecurity.com/2018/07/24/bluetooth-bug-expose-devices/

https://thehackernews.com/2018/07/bluetooth-hack-vulnerability.html

Failure to validate public encryption key received when pairing

https://www.welivesecurity.com/2018/07/20/canada-tackles-malicious-online-advertising/

https://www.welivesecurity.com/2018/07/19/british-airways-cancelled-flights-heathrow-system-issue/

Recommended Reading (continued)

https://thehackernews.com/2018/07/google-chrome-not-secure.html

https://thehackernews.com/2018/07/google-data-transfer-project.html

https://thehackernews.com/2018/07/wikileaks-julian-assange-ecuador-asylum.html

https://www.darkreading.com/endpoint/72--of-ceos-steal-corporate-ip-from-former-employers/d/d-id/1332376

https://krebsonsecurity.com/2018/07/human-resources-firm-co[illegible]olyright-br[illegible]che
d/

Recommended Reading (continued)

https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/

https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/

Running a Linux box securely