Cyber@UC Meeting 58

Cool GitHub Projects!

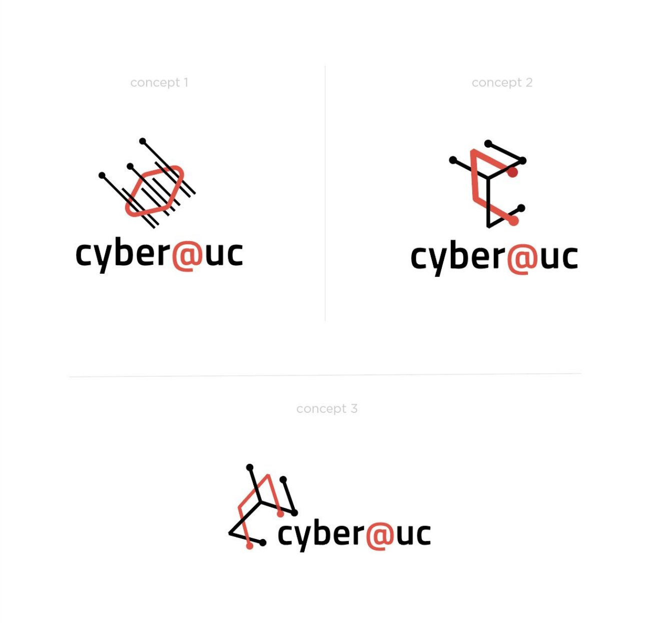
If You’re New!

- 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

- **Northrop Grumman** is donating us **~10K**
- Interview with **Bring Your Own Security Radio** tomorrow!
- **All server rails are in!**
- **CiNPA** meetup went great, **thanks for coming**!
- **Logo concepts are in!**
- **Welcom Dave!**



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

FIFA on cybersecurity

- SecureList compiled a comparison of the 11 host cities in the world cup and evaluated the level of safety/security in their public wifi access points
    - Saransk was best, st. petersburg was worst
- English Football Association gathered players and educated them on securing their devices and gave a crash course on avoiding being hacked
- Many previous global sporting events have suffered cybersecurity problems in the past few years
    - FIFA 2014, Summer Olympics 2016, UEFA’s Euro 2016, Winter Olympics 2018

PBot

- PythonBot or PBot is a python based adware that has been detected in several different variants in the wild
- First discovered over a year ago, but has evolved to try different money making schemes
- Originally designed to perform man-in-the-browser attacks
- Newer versions have been installing malicious extensions and miners
- Usually distribued through pop-up ads linking to PBot download page
- Malware is downloaded as an update.hta which downloads the origional PBot installer if opened
- A Python3 interpreter is added with some python scripts and a browser extension

PBot (continued)

- Newer versions of PBot obfuscate their scripts using Pyminifier
- If a browser is detected, a DLL is generated and injected into the browser to add the malicious extension

WPA3

- Wi-Fi Alliance launched WPA3
- Wi-Fi Alliance is a nonprofit group that certifies Wi-Fi networking standards
- WPA is short for Wi-Fi Protected Access
- New Features/Improvements
    - Protection from password guessing and dictionary attacks through a Simultaneous Authentication of Equals
        - meant to be a secure alternative to certificates
        - P2P protocol, no asymmetry, supports simultaneous initiation, can trade between speed and key strength
    - Supports forward secrecy
        - A compromised password will not allow an attacker to decrypt Wi-Fi traffic prior to intrusion

WPA3 continued

  - Enterprise WPA3 offers “the equivalent of 192-bit cryptographic strength”
  - Wi-Fi Easy Connect: intended to securely get IoT devices, those with limited to no display, onto a network by scanning QR codes with a smartphone
  - Wi-Fi CERTIFIED Enhanced Open: supports individualized data encryption to counter Man-in-the-middle attacks and allow for more secure use of public Wi-Fi
- WPA2 was launched back in 2004
- WPA3 expected to take a while to become commonplace

Recommended Reading

https://www.darkreading.com/endpoint/have-i-been-pwned-now-built-into-firefox-1password/d/d-id/1332152

https://www.darkreading.com/application-security/ieee-calls-for-strong-encryption/d/d-id/1332159

https://krebsonsecurity.com/2018/06/supreme-court-police-need-warrant-for-mobile-location-data/

https://thehackernews.com/2018/06/free-ransomware-decryption-tools.html

https://thehackernews.com/2018/06/wordpress-hacking.html

GitHub Star Night!

Not a Star but a Cool Site

https://car.mitre.org/caret/#/

- Based on MITRE’s ATT&CK Matrix
- Outlines various APT groups
- Shows techniques known to be used by each group
- Notes the analytical data to detect on each technique
- Includes sensors used to grab specified data

WiFi Pumpkin!

https://github.com/P0cL4bs/WiFi-Pumpkin

- Software that can be used to make your own “wifi pineapple”
- Claims to support partial HSTS bypass
- Phishing manager
- MITM capabilities
- Planning on using this for my HackPack project :)

Mobile Security Framework

https://github.com/MobSF/Mobile-Security-Framework-MobSF

- Supports dynamic analysis of Android iOS Windows apps
- Would be awesome to setup in our lab
- They have a docker image :)
- Looks like a Cuckoo type of project but focused on mobile

Iodine! DNS Tunneling

https://github.com/yarrick/iodine

- Very popular way to exfiltrate data from isolated environments
- Worth while for us to learn how to use for red v blue missions
- Allows you to tunnel IPv4 data through DNS Server
- DNS queries are typically allowed

Cuckoo! Malware Sandbox

https://github.com/cuckoosandbox/cuckoo

- I plan to set this up in our lab
- Most sandboxing services are modified Cuckoo instances
- Highly configurable
    - Integrates with Suricata, Moloch, MISP, VT, and more!
- We already have some experience in setting this up.

WinPwnage

https://github.com/rootm0s/WinPwnage

- Full of:
  - Payload scripts
  - Scanning scripts for flying undetected
  - Helpful links
  - Commented code :)

Chris Morrison’s Stars Page

- (Red) https://github.com/dafthack/DomainPasswordSpray
- (Red) https://github.com/deepzec/Bad-Pdf
- (Radio) https://github.com/ChristopheJacquet/PiFmRds
- (Blue) https://github.com/EgeBalci/The-Eye
- (Red) https://github.com/securestate/king-phisher
- (Misc) https://github.com/KnightOS/KnightOS
- (Red) https://github.com/0x90/wifi-arsenal
- (Red) https://github.com/offensive-security/exploit-database
- (Red) https://github.com/mattifestation/PowerShellArsenal
- (Blue) https://github.com/jpr5/ngrep
- (Radio) https://github.com/jopohl/urh