

Cyber@UC Meeting 59

Actually Doing Star Night!

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

- **Hope you all enjoyed the 4th of July!**
- **US Bank** VIP visiting next Wednesday at **2pm!**
- We need to **nail down what we want in a logo**
- Working out our **budget!**



Public Affairs

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

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

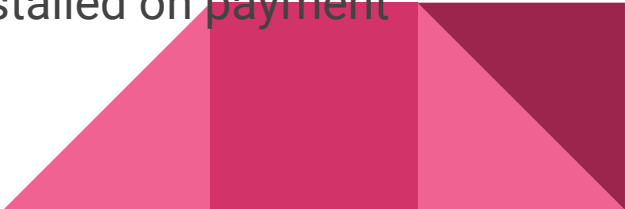
- **Twitter:** [@CyberAtUC](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: cyberatuc.org



Weekly Content

Trustwave sued over failure to detect malware

- Heartland was subject to a major breach in 2009
 - Details for >100 million payment cards from >650 customers were stolen
 - Heartland paid >\$148 million in settlement fees
 - Two insurance firms paid Heartland 20 and 10 million respectively
 - Civil suit filed in late June claims Trustwave failed to honor the service contract
 - Claim Trustwave failed to detect an attacker used a SQL Injection attack to breach Heartland in 2007
 - Trustwave also allegedly failed to detect malware installed on payment processor servers in 2008
- 

Trustwave (Continued)

- Lawsuit points out that Trustwave did not detect any suspicious activity during its security audits provided to Heartland for almost two years which included PCI DSS compliance and attestation
- Visa's review of Heartland's servers found that Trustwave incorrectly certified Heartland as PCI DSS compliant
- Lawsuit claims Visa discovered Trustwave ignored that Heartland didn't run a firewall, used vendor-supplied passwords, didn't have sufficient protection for the storage system used for card data, didn't have unique identification for each user, didn't monitor servers and data at regular intervals-comp rules
- Trustwave states they did not manage Heartland InfoSec

IOS USB restricted mode bypass

- IOS 11.4.1 added usb restricted mode feature, designed to make it harder to break into an iphone/ipad through the data port
- Disables data connection capabilities of the lightning port if the device has been locked for ≥ 1 hour, still allows charging
- Attaching a USB device within 1 hour of locking will reset the timer
- Pressing the power button five times will apparently immediately enter the device into USB restricted mode

<https://thehackernews.com/2018/07/bypass-ios-usb-restricted-mode.html>



Hybridized malware, is your computer worth it?

- New variant of Rakhni ransomware judges your computer and decides on the most profitable malware scheme
- If your computer is deemed worthy of infecting it will choose between a ransomware and a cryptominer
 - Ransomware: Bitcoin folder in AppData section
 - Cryptominer: no Bitcoin folder in AppData and ≥ 2 logical processors
 - Worm: neither of the above, worms onto other computers in local network
- Initially infects through a malicious word file sent through phishing email

<https://thehackernews.com/2018/07/cryptocurrency-mining-ransomware.html>

Recommended Reading

<https://www.welivesecurity.com/2018/07/11/polar-flow-app-exposes-geolocation-data-soldiers-secret-agents/>

<https://www.welivesecurity.com/2018/07/02/principle-least-privilege-strategy/>

<https://thehackernews.com/2018/07/facebook-cambridge-analytica.html>

<https://thehackernews.com/2018/07/intel-spectre-vulnerability.html>

<https://thehackernews.com/2018/07/arch-linux-aur-malware.html>

<https://thehackernews.com/2018/07/gaza-palestin-hacker.htm>

Recommended Reading (continued)

<https://krebsonsecurity.com/2018/07/exxonmobil-bungles-rewards-card-debut/>

<https://krebsonsecurity.com/2018/07/notorious-hijack-factory-shunned-from-web/>

<https://krebsonsecurity.com/2018/06/plant-your-flag-mark-your-territory/>





GitHub Star Night!

Rickify

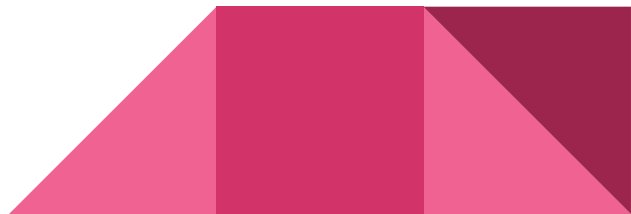
<https://github.com/kjempelodott/rickify>

- Spotify for Android streams over insecure HTTP for a few secs when it starts.
- This Python script MITMs the app to replace the audio with "Never Gonna Give You Up".



More stars from Hayden

- Scripts that make PHP segfault: github.com/hannob/php-crashers
- Encryption/encoding/etc Swiss army knife: github.com/gchq/CyberChef
- Just visit it and find out... superlogout.github.io



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>
- 

Invoke-WMILM

<https://github.com/Cybereason/Invoke-WMILM>

- Neat post-exploitation script for launching processes on locally networked windows machines (pivoting)

*Also nice for remote installs if you don't have any remote management tools installed



Just For Fun

<https://github.com/g0tmilk/VulnInjector>

<https://github.com/chrislgarry/Apollo-11>

<https://github.com/NiklasFauth/hoverboard-firmware-hack>

<https://github.com/google/gif-for-cli>

