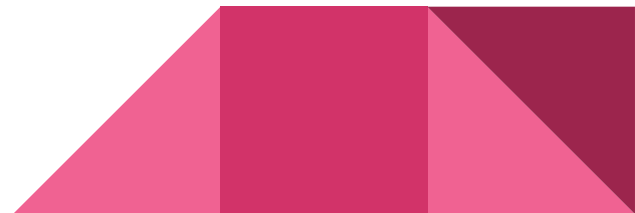


Cyber@UC Meeting 54

Router Login Bypass

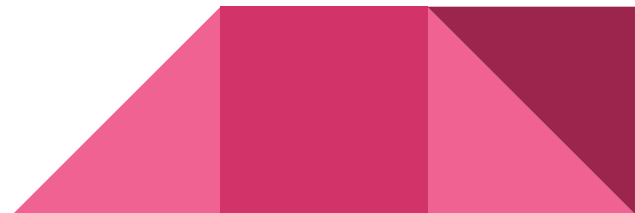
If You're New!

- 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

- We got a new **server rack** in!
- **UC Open House** went great, met **US Cyber Command Director!**



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


Scan4You administrator facing up to 35 years

- Scan4You, like virustotal, but didn't share its uploads with security vendors
- Ruslan Bondars, 37, arrested in Latvia last year
 - Convicted on one count of conspiracy to violate the Computer Fraud and Abuse Act
 - One count of conspiracy to commit wire fraud
 - One count of computer intrusion with intent to cause damage
- Scan4You is a counter anti-virus (CAV) site, it checks an uploaded file and sees if it gets caught by any anti virus solutions and lists back which ones
- Example of Scan4You user was the developer of Citadel malware which stole 40 million credit cards from Target
 - "Today's verdict should serve as a warning to those who aid and abet criminal hackers: the Criminal Division and our law enforcement partners consider you to be just as culpable as the hackers whose crimes you enable—and we will work tirelessly to identify you, prosecute you, and seek stiff sentences that reflect the seriousness of your crimes."

RCE Flaw in EOS Blockchain Platform

- What is blockchain: <https://www.youtube.com/watch?v=r43LhSUUGTQ>
 - EOS is an open source smart contract platform, used in products like ethereum
 - Buffer out-of-bounds write error in cod for parsing contracts allows for remote code execution
 - An attacker only needs to craft a malicious WASM file (smart contract) and upload it to the server
 - Once the parser reads this, takeover of the supernode can occur
 - Supernode is a server that creates blocks
 - From there an attacker can traverse between blocks/nodes
- 

BackSwap Malware

- Banking malware has been a dying breed of malware due to anti-malware softwares and built in browser protections making banking trojan attacks complicated and difficult
 - Instead of using process injection to monitor browsing activity, a new family of banker malware is hooking key window message loop events to inspect values of the window for banking activity, then injecting malicious JavaScript
 - This malware started in cryptocurrency by replacing wallet addresses in clipboard
 - Distributed through phishing emails
 - Installs event hooks through Windows GUI to monitor URL
- 

Other Recommended Reading

<https://krebsonsecurity.com/2018/05/why-is-your-location-data-no-longer-private/>

<https://www.welivesecurity.com/2018/05/23/amazon-rekognition-threat-civil-rights/>

<https://krebsonsecurity.com/2018/05/fbi-kindly-reboot-your-router-now-please/>

<https://thehackernews.com/2018/05/free-vpn-pornhub.html>

<https://www.welivesecurity.com/2018/05/25/amazon-alexa-acc/>

Managed Routers

- Once configured, normally are accessed via ssh
- Multiple authentication levels
 - Connection authentication
 - User mode authentication (User mode is mostly view only, minimal config changes)
 - Privilege Exec mode (Can make config changes)



Password Recovery

- Cisco has a built in method for bypassing authentication for local access
- Great for password recovery/resets, terrible if someone gets into your networking cabinet

